الجـــــــــــــــــــمهـوريـــــة الجـــــــــــــزائـريـة الديمـــــــقـراطيـة الـشـــــــــعبيـة

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التـــــــــــــــــــــــــعليـم العـــــــالي و البـــــــــحث العـــلـمـــي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جـــــــــــــامعة أبي بكـــر بـلـقـايد – تـلمســـــــــــــان –

Université Aboubakr Belkaïd– Tlemcen –

Faculté de TECHNOLOGIE

MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

En : Télécommunications

Spécialité : Réseaux et Télécommunications

Par : **ZAOUI Hassen**

Sujet

Développement d'une interface logicielle pour la supervision du réseau intranet

Soutenu publiquement, le 01 /07/2019, devant le jury composé de :

Mr F.T. BENDIMERAD	Professeur	Univ. Tlemcen	Président
Mr F. DERRAZ	MCB	Univ. Tlemcen	Examinateur
Mr D. MOUSSAOUI	MAA	Univ. Tlemcen	Examinateur
Mr G. ABDELLAOUI	MCB	ESSAT	Encadreur
Mr H. MEGNAFI	MCB	ESSAT	Co-encadreur

Année universitaire : 2018-2019

Remerciements

On remercie mon dieu le tout puissant de nous avoir donné la santé et la volonté d'entamer et de terminer ce mémoire.

*Tout d'abord, ce travail ne serait pas aussi riche et n'aurait pas pu avoir le jour sans l'aide et l'encadrement de (**Dr. GHOUTI ABDELLAOUI)**, on le remercie pour la qualité de son encadrement exceptionnel, pour sa patience, sa rigueur et sa disponibilité durant notre préparation de ce mémoire.*

*Je remercie vivement Monsieur **Megnafi Hicham** Docteur à l'école supérieurs en sciences appliquées de Tlemcen, qui me fait l'honneur de me Co-encadrer dans ce mémoire.*

*Mes remerciements vont également aux membres du jury**Mr le présidant BENDIMERAD Fethi Tarik** et **Mr DERRAZ Fouad** ainsi **Mr MOUSSAOUI Djilali** qui m'ont fait l'honneur de participer au jury pour l'intérêt qu'ils ont bien voulu porter à ce travail, en apportant sa valeureuse contribution en tant qu'experts et profond connaisseur du domaine (Réseau et Télécommunication).*

Mes remerciements par une immense reconnaissance envers toute notre famille. Il nous est impossible d'exprimer en quelques mots tout ce que nous devons, à ma mère, à mon père, et à toute la famille, pour leurs encouragements et leur appui moral qui m'ont permis de mener à bon terme ce travail.

Enfin, mes remerciements vont à tous ceux qui m'ont soutenu ou qui, d'une manière ou d'une autre, ont contribué à l'élaboration de ce travail.

Dédicaces

Je dédie ce modeste travail, fruit de 18 ans d'études, aux personnes les plus chères, mes parents, les prunelles de mes yeux qui ont fait preuve de dévouement et qui m'ont épaulé du début jusqu'à la fin avec leurs :
Prières, leurs sacrifices et leurs conseils durant tout mon parcours. Il s'agit de,

Mon père, pour le soin, la protection, la responsabilité et la confiance qu'il a toujours eus à mon égard.
Ma mère, pour toute l'attention, le réconfort et l'affection dont elle m'a entouré. Que Dieu les protège à Jamais.
Mon grand père et Ma grand-mère.
Mon frère Mohammed.
Mes sœurs, Rabia, Amina et Oum Elkheir.
Ma soeur fatima et son mari cheikh et ses enfants Mohammed Hassen et Islam abdelkader.
À ma tante Mama et son mari Mustapha et ses enfants : Djahida, Taher, Sid Ahmed et Yassine.
À mes oncles Ibrahim, Mohammed, Ahmed, Slimane et ses enfants.
À tous mes amis surtout (Ali, Boubaker, B. Mohammed, Sekouri, Serhane, Saleh, Belarbet et Houssem).
À toute la promotion : (Master 2 de Réseau et Télécommunication) 2018-2019.

SOMAIRE

Liste des Figures

Liste des Acronymes

AGL : Atelier de Génie Logiciel
AIR: Adobe Integrated Runtime
ASN: Abstract Syntax Notation
CAS: Central Authentication Service
CMS: Content Management System
CPU: Central Processing Unit
DARPA: Defense Advanced Research Projects Agency
EDI: Integrated Development Environment
ERP: Enterprise Resource Planning
HTTP: Hypertext Transfer Protocol
ICMP: Internet Control Message Protocol
ID: Identifier
IETF: Internet Engineering Task Force
IMAP: Internet Message Access Protocol
IP: Internet Protocol
ISO: International Organisation for Standardization
IT: Technologie d'informations
LAN: Local Area Network
LDAP: Lightweight Directory Access Protocol
MAN: Metropolitan Area Network
MIB: Management Information Base
NAS: Network Attached Storage
OID: Objet Identifier
OSI: Open Systems Interconnection
PDU: Protocol Data Unit
RAM: Random Access Memory
RCP : Plateforme Client Riche
RIA : Rich Internet application
RLE : Réseau Local d'entreprise
RTT : Round Trip Time
SAAS : Logiciel en tant que service
SAN: Storage Area Network
SMI: Structure of Management Information.
SMTP: Simple Mail Transfer Protocol
SNMP: Simple Network Management Protocol
SSH: Secure SHell
SSO: Single sign-on
TCP: Transmission Control Protocol
UDP: User Data Protocol
UML: Unified Modeling Langage
WAN: Wide Area Network
WLAN: Wireless Local Area Network
WMI : Windows Management Instrumentation

Introduction Générale

Introduction Générale

Les réseaux de transmission de données ne cessent de s'accroitre, les volumes de données échangés augmentent de plus en plus. Tout est désormais informatisé de nos jours, et que le domaine de la technologie d'informations (IT) devient prédominant. Les entreprises mettent en place des infrastructures réseau et des systèmes plus ou moins complexes pour garantir un service fiable et un accès à l'information quasi permanent et pour obtenir une bonne satisfaction de son infrastructure informatique. Toute entreprise doit pouvoir compter sur un réseau de haute performance [1]. Ainsi, pour atteindre ces objectifs, tout administrateur réseau doit mettre en place des outils nécessaires et suivre des procédures standard de gestion de réseau.

L'administrateur de réseau doit donc surveiller en permanence les nœuds réseau, une perte de connexion à un nœud engendre une perte de temps et un risque opérationnel et financier. Donc, sa principale tâche est d'assurer la surveillance au quotidien du comportement du réseau de l'entreprise par la supervision des équipements qui le constitue, le suivi des états des liens réseau, la consommation de bande passante, etc. Il doit aussi définir des procédures et des tableaux de bord de suivi, élaborer des rapports d'analyses réseau et de créer des sauvegardes de configurations relatives aux hôtes et équipements réseau. Et finalement, résoudre les éventuels incidents et pannes pouvant survenir.

1. Problématique

Malgré le déploiement des deux outils WATCH et Cisco Works, les objectifs souhaités n'ont pas été atteint. En effet l'outil WATCH se base sur des pings. Il s'agit d'un outil très basique qui se base sur des commandes ICMP. Alors que l'objectif des administrateurs réseau est disposé d'un outil complet qui supervise les liens, leur occupation de bande passante, les changements des états dans le routage dynamique.

Quant à l'outil Cisco Works, il est destiné aux équipements de marque Cisco et notamment dans l'archivage des fichiers de configurations et les images de systèmes d'exploitation des switches et des routeurs. L'affichage des alertes et des évènements ne permet pas une lecture aisée. En plus ce n'est pas en mesure de donner des informations sur l'utilisation de la bande passante (Bandwith IN/OUT).

2. Solution proposée

Dans ce projet de fin d'études, nous proposons de développer un outil simple consistant et fiable permettant la gestion et la supervision des serveurs, routeurs, et autres équipements constituant le réseau.

Cet outil devra assurer en premier lieu la surveillance des équipements et des ressources du réseau (bande passante), et en second lieu, il permettra de détecter de façon rapide les pannes pouvant affecter ces équipements. Tout évènement déclenché par un nœud quelconque du réseau devra être remonté à l'application.

3. Organisation du mémoire

Dans ce qui suit, nous allons étudier dans le premier chapitre les réseaux informatique d'une manière générale, puis nous allons détailler les réseaux INTRANET dans le chapitre 2. Par la suite, et dans le chapitre 3, nous allons détailler la supervision réseau ainsi que les différents protocoles qui interviennent dans cette dernière, et nous allons finir par le développement de l'application et le test de son bon fonctionnement dans le chapitre 4.

A la fin nous allons conclure notre mémoire par une conclusion générale et quelques perspectives pour ce projet de fin d'études.

En résumé, dans ce mémoire nous allons répondre aux différents points suivants :

- L'étude, la critique de l'existant et la solution proposée.
- Spécification de besoins et étude théorique.
- La réalisation et test de fonctionnement.

Chapitre1 : Architecture des réseaux informatiques

Architecture des réseaux informatiques

1. Introduction

Les réseaux informatiques sont partout à l'heure actuelle. Ils sont devenus indispensables au bon fonctionnement général de nombreuses entreprises et administrations. Tout problème ou panne peut avoir de lourdes conséquences aussi bien financières qu'organisationnelles. Par conséquent, la supervision des réseaux informatiques est nécessaire et indispensable. Elle permet d'avoir une vue globale du fonctionnement et de tous les problèmes pouvant survenir sur un réseau, mais aussi d'avoir des indicateurs sur la performance de son architecture. De nombreux logiciels qu'ils soient libres ou propriétaires existent sur le marché. La plupart s'appuie sur le protocole SNMP (Simple Network Management Protocol).

2. Définition d'un réseau

Un réseau est un ensemble d'objets ou de équipements connectés où maintenus en liaison, par extension, l'ensemble des liaisons établies, vient du latin rete qui signifie filet, les objets reliés sont appelés nœuds du réseau [2].

3. Réseau informatique

C'est un système permettant à plusieurs appareils d'échanger des informations. Bien sûr, les appareils en question sont souvent des ordinateurs. Cependant il peut s'agir d'autres machines telles qu'automates d'une usine communiquant entre eux [2].

Un réseau informatique peut être classé en fonction de son utilisation et des services qu'il offre. Ce découpage recoupe également la notion d'échelle. Ainsi, pour les réseaux utilisant les technologies Internet (famille des protocoles TCP/IP), la nomenclature est la suivante :

- Intranet : le réseau interne d'une entité organisationnelle.
- Extranet : le réseau externe d'une entité organisationnelle.
- Internet : le réseau des réseaux interconnectés à l'échelle de la planète.

3.1 Différent type de réseau

Les réseaux informatiques sont classés en différents types selon trois critères principaux (les distances, les débits et les types de câbles utilisés), dans ce contexte nous pouvons trouvez les types de réseaux suivants :

- Réseau LAN (Local Area Network) : Ce sont de petits réseaux locaux restreints à une maison ou à une entreprise. Ce type de réseau est également appelé RLE (Réseau Local d'Entreprise) en France. Il permet de connecter des éléments (ordinateurs, périphériques, ...) distants de quelques mètres à quelques certaines de mètres. Nous pouvons donc recensé sous cette appellation la plupart des réseaux informatiques présents dans les entreprises. La notion de surface géographique limitée n'implique pas un nombre faible de poste de travail interconnectés. Un réseau local peut en effet compter jusqu'à plusieurs centaines de machine. La transmission de données est réalisée par un support simple auquel chaque ordinateur accède, selon des méthodes d'accès définies par des normes établies. Les débits proposés par les réseaux locaux

s'étalent de 1Mbit/s à plus de 1Gbit/s, en fonction des normes et de l'évolution matérielle. Les délais de transmission sur de tels réseaux sont très courts [3].

- Réseau MAN (Metropolitan Area Network) : Réseau réparti sur une surface moyenne généralement de la taille d'une ville ou d'un campus. Il sert généralement à interconnecter des réseaux locaux distants de quelques kilomètres. La fonction d'un MAN est similaire à celui des réseaux locaux. Dans ce cas encore, diverses normes ont été établies. Ce type de réseau utilise généralement des fibres optiques.

- Réseau WAN (Wide Area Network) : Il s'agit là des réseaux d'opérateur pouvant acheminer les informations sur plusieurs centaines de kilomètres et utilisant généralement la fibre optique. C'est un réseau longue distance. Il est en effet utilisé pour permettre des échanges entre des réseaux locaux, mais qui sont séparés ici par des distances plus importantes, de plusieurs centaines à plusieurs milliers de kilomètres. Un WAN est en fait une association de plusieurs LAN. Le terme de MAN tend d'ailleurs de plus en plus à être intégré dans la famille des réseaux langue distance et devrait disparaitre prochainement. Sa structure est, par contre, plus complexe. Les ordinateurs indépendants ou regroupés en LAN des différents réseaux locaux ou métropolitains, la transmission des données entre ces ordinateurs n'est plus laissée à la seule charge du support de transmission, mais d'un sous-réseau de communication. Ce sous-réseau possède les lignes physiques ainsi que des éléments actifs (commutateurs) qui vont aiguiller l'information de l'émetteur vers le destinateur à travers le maillage. La complexité ce maillage varie avec la taille géographique et le nombre de commutateurs présents sur le parcours des données. Nous parlons aussi dans ce cas de réseau maillé. Le mode transmission des données, est généralement point à point. Chaque commutateur est un nœud qui possède une capacité de réflexion : lorsqu'il reçoit de l'information sur l'un de ses ports de communication, il détermine sur quel port émettre cette information pour qu'elle parvienne au plus vite au destinataire. Le support de communication entre deux commutateurs peut être un satellite. Dans ce cas, la transmission de l'information se fait par diffusion. Le plus grande réseau longue distance est aujourd'hui Internet. D'un point de vue physique, le réseau mondial n'est autre que l'interconnexion d'un très grand nombre de réseau locaux. Notons enfin qu'un Intranet est un réseau local utilisant les technologies d'Internet et proposant les mêmes services aux utilisateurs [3].
- Réseau WLAN (Wireless Local Area Network) : Sont apparus en même temps que les terminaux Mobiles (PC portables, téléphone cellulaire, PALM, …) et répondent à trois besoins : mobilité, rapidité d'installation et réseaux temporaires. L'impératif est l'économie d'énergie. Le mot Wireless signifie "sans fil" (wire = câble, less = sans).

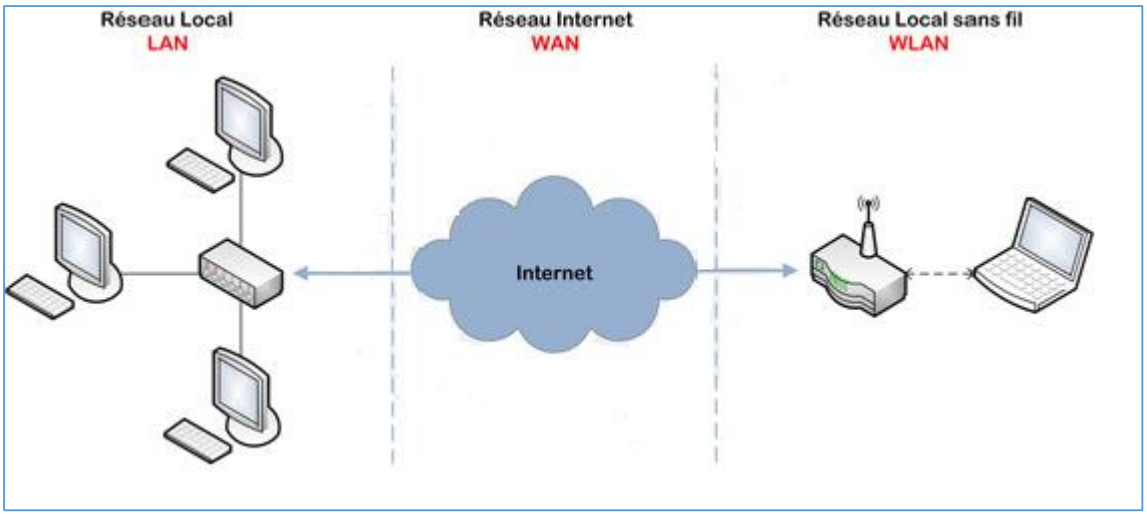

Figure 1 : Différent type de réseau

3.2 Caractéristiques du réseau local LAN

Parmi les différentes caractéristiques, il faut retenir :

- Le support physique: Outre le choix entre réseau filaire ou sans fil (Wireless), il faut déterminer le type de câble à utiliser, câble coaxial, fibre optique ou paire torsadée. Dans la plupart des cas, cette dernière solution sera retenue car c'est la solution la moins chère, la plus maniable et la plupart des équipements sont dédiés à ce type de câble.

- Le type de réseau : Ce choix est le plus déterminant car il va entraîner l'achat de matériels spécifiques au futur réseau. Le choix du type de réseau détermine bien souvent le niveau d'évolution du réseau et la méthode d'accès au réseau.

- La bande passante : Egalement appelée débit, c'est la quantité d'informations qui pourra circuler simultanément sur le réseau. Ce débit est donné en kilo bits par seconde (Kbps), en Méga bits par seconde (Mbps) ou même parfois en Giga bits par seconde (Gbps). Pour chaque type de réseau et en fonction du type de câblage utilisé, plusieurs débits différents sont disponibles.

- Les protocoles de communication : Ce sont les langages utilisés par les différentes machines afin d'échanger des informations. Plusieurs langages différents peuvent être employés en fonction des applications à exécuter, mais deux machines souhaitant échanger des informations doivent utiliser le même langage.

- Le système d'exploitation : Il déterminera la façon de configurer le réseau. De même, certains serveurs sont dédiés à un type de réseau spécifique ou une tâche précise (ex : Windows 2000 [4] pour le serveur d'application, Linux [5] pour le Serveur Proxy et Novell [6] pour le serveur administratif).

- Les éléments d'interconnexion : Plusieurs types de matériels existent afin de diriger l'information à l'intérieur du réseau ou vers l'extérieur comme Internet (Ex : Routeur). Ces éléments sont généralement dédiés à un type de réseau prédéterminé.

4. Topologies des réseaux locaux filaires

Il existe quatre architectures différentes pour les réseaux filaires. Ces architectures sont appelées topologies. Elles décrivent la façon dont les machines sont organisées géographiquement les unes par rapport aux autres dans le réseau et la façon dont elles sont interconnectées.

- Topologie en bus : Le bus s'étend sur toute la longueur du réseau, et les machines viennent s'y accrocher comme le montre la Figure 2. Lorsqu'une station émet des données, celles-ci circulent sur toute la longueur du bus et la station destinataire peut les récupérer. Une seule station peut émettre à la fois. Cette topologie a l'avantage de ne pas être perturbée par la panne d'une machine du bus. Par contre, en cas de rupture de bus le réseau devient inutilisable. Le signal n'étant jamais régénéré, la longueur de câbles est donc limitée (atténuation du signal). La topologie en bus est câblée essentiellement en câble coaxial. Nous utilisons pour cela des « bouchons » en bout de bus afin de supprimer définitivement les informations pour qu'une autre station puisse émettre.

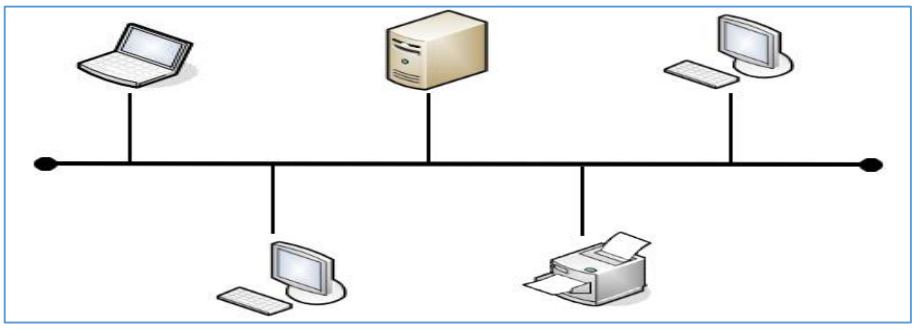

Figure 2: Topologie en bus

- Topologie en anneau : Un réseau en anneau est une forme de réseau informatique visant à raccorder l'ensemble des ordinateurs.
  Toutes les entités sont reliées entre elles dans une boucle fermée. Les données circulent dans une direction unique, d'une entité à la suivante. Une entité n'accepte une donnée en circulation sur l'anneau que si elle correspond bien à son adresse. Dans le cas contraire, l'entité en question fait passer la donnée à l'entité suivante.
  Un exemple d'implémentation du réseau en anneau est l'anneau à jeton. Cette implémentation utilise le protocole **Token Ring** pour réguler l'accès au réseau. Un « jeton » circule sur le réseau et seule la station qui possède le jeton a le droit d'émettre. NB : le protocole **Token Rin**g peut s'implémenter aussi bien sur un réseau physique (couche 1 du modèle OSI) qu'en étoile, puisqu'il s'agit d'un protocole géré en couche 2 (liaison de données), et donc indépendant de la topologie. La Figure 3 illustre le schéma d'un réseau d'ordinateurs interconnectés entre eux à l'aide de la topologie en anneau.

Avantages :

- La quantité de câble nécessaire est minimale.
- Le protocole est simple, il évite la gestion des collisions.

Inconvénients :

- Le retrait ou la panne d'une entité active paralyse le trafic du réseau.
- Il est également difficile d'insérer une nouvelle station.

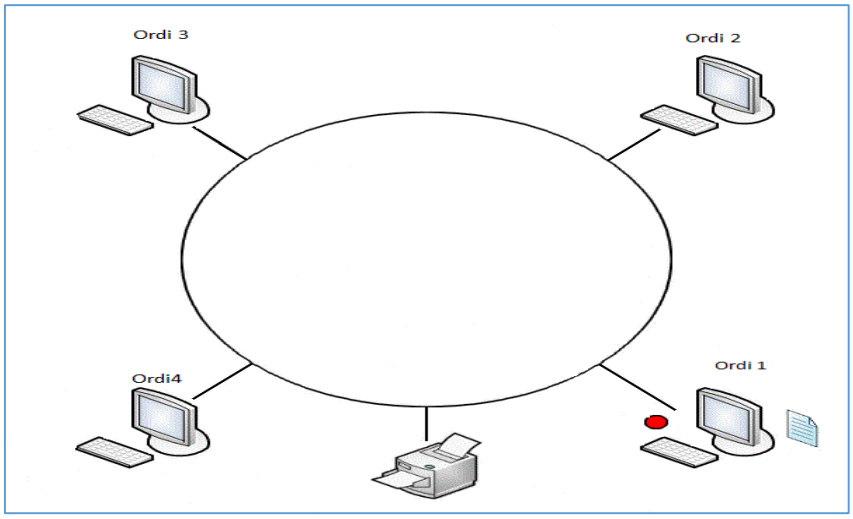

Figure 3: Topologie en anneau

➢ Topologie étoile :

C'est la topologie la plus courante. Toutes les stations sont reliées à un unique composant central : le concentrateur. Quand une station émet vers le concentrateur, celui-ci envoie les données à toutes les autres machines ou à celle qui en est le destinataire. Ce type de réseau est facile à mettre en place et à surveiller. La panne d'une station ne met pas en cause l'ensemble du réseau. Il faut plus de câbles que pour les autres topologies, et si le concentrateur tombe en panne, une grande partie du réseau est en « rideau ». De plus, le débit pratique est souvent moins bon que pour les autres architectures. Cette topologie est essentiellement utilisée par les réseaux Ethernet les plus courants. La Figure 4 illustre l'utilisation de cette topologie dans un réseau LAN.

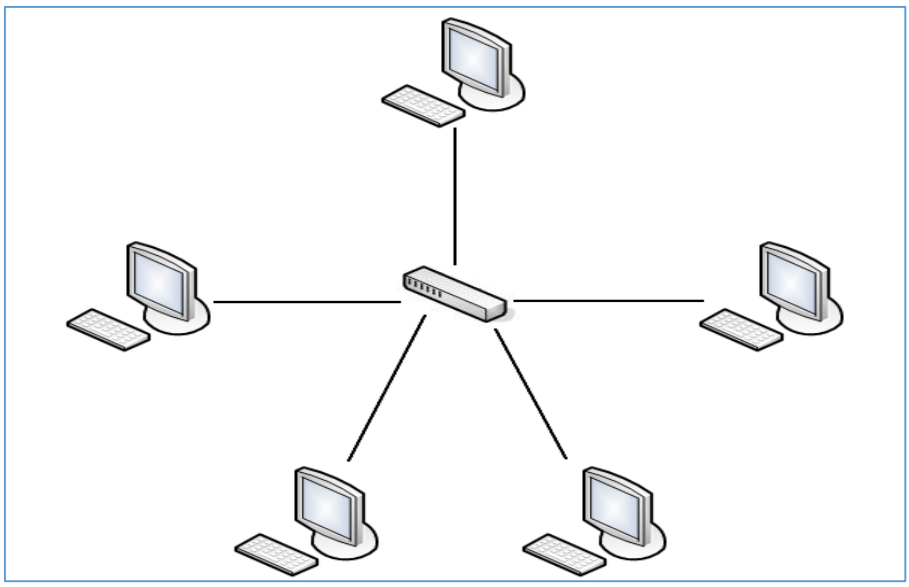

Figure 4: Topologie étoile

- Topologie Maillée :

La topologie maillée est une topologie réseau (architecture) hybride de type étoile mais avec différents chemins pour accéder d'un nœud à un autre (contrairement à un réseau Ethernet). C'est la méthode utilisée sur Internet : pour un transfert entre deux points, chaque nœud (un routeur intelligent, qu'on appelle switch dans le jargon technique) va sélectionner en temps réel la route la plus rapide pour le transfert.

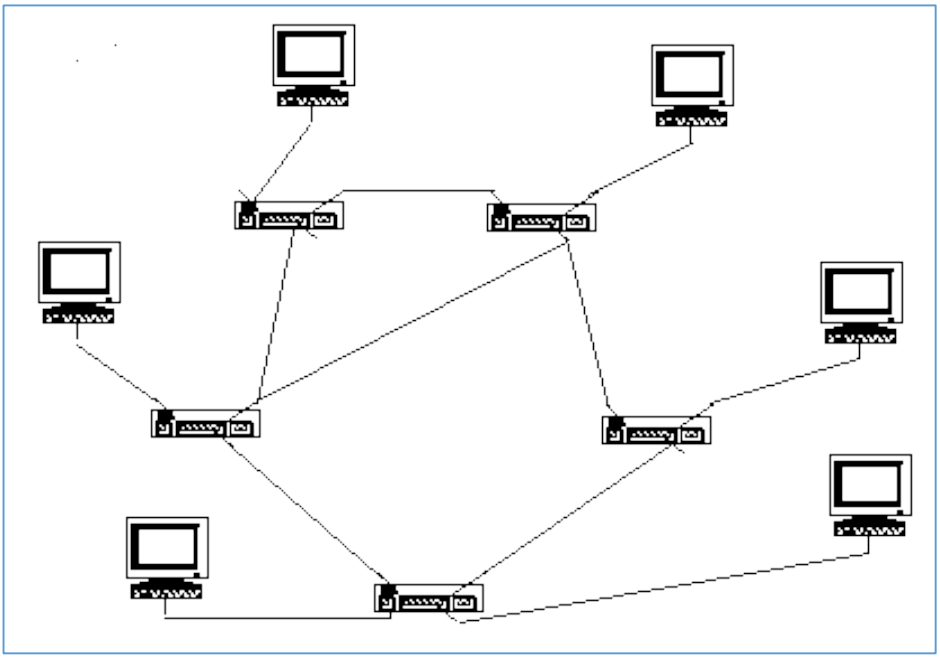

Figure 5: Topologie Maillée

Le principal avantage de ce type de topologie est l'adaptabilité : une ligne coupée ne perturbe pas les communications d'où son utilisation dans les réseaux sensibles. Le défaut est la difficulté technique liée aux concentrateurs dans chaque nœud.

5. Les différents types de Concentrateurs

Il existe trois types de concentrateur :

- Le HUB : Matériel permettant de relier plusieurs ordinateurs entre eux. Il ne fait aucune distinction du destinataire de l'information. Ce qui signifie que l'information envoyée par un poste est dirigée vers tous les postes. On considère ce matériel comme « très bavard ».

- Le SWITCH : A la différence du HUB, le SWITCH utilise l'adresse MAC du destinataire. Ainsi, l'information est directement envoyée à la machine concernée. Les autres machines ne reçoivent aucune information. Ce système est plus intelligent donc moins bavard. D'autre part, il élimine les collisions de paquets éventuelles (une collision apparaît lorsqu'une machine tente de communiquer avec une seconde alors qu'une autre est déjà en communication avec celle-ci..., la première ressaiera quelques temps plus tard).

- Le Router : C'est le concentrateur le plus intelligent puisqu'il permet, en plus d'identifier la machine destinataire de la donnée, d'identifier le réseau sur lequel le message doit être transmis. Le message est distribué par rapport à l'adresse IP (Internet Protocol) du matériel cible.

6. Conclusion

Dans ce chapitre nous avons étudié en détail le réseau informatique, qui nous permet, grâce à un équipement spécifique, de relier les ordinateurs entre eux et favoriser l'échange d'information à l'échelle planétaire et aider les entreprises de développer leur service et graniter la communication à haut niveau entre ces différents partenaires.

Actuellement, les réseaux locaux occupent le cœur des systèmes d'information dans les entreprises, les industries ou les institutions. Au-delà de l'accès aux ressources informatiques, les réseaux locaux offrent la possibilité d'utiliser une même infrastructure de transmission pour les communications téléphoniques, l'échange de données, et la vidéo.

Cette évolution n'a été possible que par l'augmentation des débits de transmission, qui dépassent maintenant 10 Gbit/s pour les réseaux Ethernet et 54 Mbit/s pour les réseaux locaux sans-fil.

L'étude réalisé dans ce chapitre, s'intègre dans ce mémoire dont l'objectif est de comprendre l'architecture d'un réseau informatique et tous les équipements possible qui peuvent figurés dans un tel réseau, afin de pouvoir réaliser une application qui permet la supervision et le suivit de tous ces équipements.

Chapitre2 : Les réseaux INTRANET

Les réseaux INTRANET

1. Introduction

INTRANET. En 1969, le DARPA, dépendant du pentagone, créait le réseau informatique Arpanet destiné à relier entre eux les services administratifs, les entreprises privées, les universités, les centres de recherches travaillant pour l'armée américaine. Ce réseau donna naissance en 1983 au réseau internet, communément appelé The Net ou encore The Web, un véritable réseau qui recours au même protocole de communication : TCP/IP. Géré par l'internet society, dont le siège est à Reston en Virginie, Internet relie l'utilisateur au monde et offre une multitude de services. Le plus connu de ceux-ci est la messagerie qui permet à des groupes de discussion (Usenets ou News groupes), qu'il s'agisse de chercheurs traitent un problème mathématique spécifie ou d'un groupe de sportifs d'un club de football, d'échanger des informations sur leurs centres d'intérêt [7].

L'INTRANET s'est développé en s'appuyant sur une technologie ouverte, simple et bon marché. Les outils qu'elle créa (le transfert de fichiers, le courrier électronique, les listes de diffusion, les forums, le World Wide Web) sont aujourd'hui de plus en plus employés au sein des entreprises qui les installent sur leurs réseaux locaux pour leurs besoins de communication. Cet Internet privé a reçu le nom d'Intranet.

L'INTRANET consiste un moyen simple de faire circuler l'information dans une entreprise, notamment lorsqu'elle est composée de groupes géographiquement dispersés et aux cultures informatiques très diverses, en leur permettant de disposer d'une interface identique. Il peut, moyennant certaines mesures liées à la sécurité, êtres ouvert vers l'Internet ; il devient alors un remarquable outil de communication avec les employés en déplacement, les télétravailleurs, les fournisseurs, les partenaires, les distributeurs et les clients, tout en constituant une vitrine de l'entreprise.

Parce que l'Intranet est une architecture moins couteuse et plus simple à déployer que le client-serveur traditionnel, il est vraisemblable que les entreprises vont multiplier l'installation de ces outils ; bientôt, pour un serveur Web installé dans une entreprise sur l'Internet, entre cinq et dix autres le seront sur l'Intranet. [7]

2. Définition

L'INTRANET est un réseau informatique privé utilisé par les employés d'une entreprise ou de toute autre entité organisationnelle et qui utilise les mêmes protocoles qu'Internet (TCP, IP, HTTP, SMTP, IMAP, etc.). Cette utilisation n'est pas nécessairement locale, un INTRANET pouvant s'étendre à travers le WAN.

Parfois, le terme se réfère uniquement au site web interne de l'organisation, mais c'est souvent une partie bien plus importante de l'infrastructure informatique d'une organisation.

Dans les grandes entreprises, l'INTRANET fait l'objet d'une gouvernance particulière en raison de sa pénétration dans l'ensemble des rouages des organisations, et de la sécurité nécessaire à sa circonscription à l'entreprise. Les grands chantiers de l'intranetisation des entreprises sont :

- La rapidité des échanges de données qui engendre une diminution des coûts de gestion.
- L'accessibilité des contenus et services.
- L'intégration des ressources.
- La rationalisation des infrastructures.

Le concept d'INTRANET rejoint de plus en plus les projets de Poste de travail. Pour répondre aux besoins des utilisateurs dans leurs situations de travail professionnelles, l'intranet doit être conçu selon trois principes fondamentaux :

- Toutes les ressources informatiques doivent être référencées et rendues accessibles aux ayants droit à partir d'un serveur Web ; chaque ressource doit être associée à un groupe d'utilisateurs habilités d'une part et à un profil d'intérêt d'autre part.
- Tout utilisateur doit être identifié et authentifié dans un seul référentiel (ou annuaire d'entreprise LDAP) pour l'accès à l'ensemble des ressources ; dès l'authentification assurée, l'intranet doit être en mesure de propager la session de l'utilisateur pendant toute son activité sans qu'il ait besoin de s'identifier à nouveau (Cf. CAS, SSO)
- Des mécanismes de mises en avant (profiling) et d'alertes doivent être mises en place pour pousser l'information pertinente vers l'utilisateur et rendre ainsi plus efficace l'utilisation des ressources.

Les projets intranet sont devenus au fil du temps de véritables projets de systèmes d'information et plus seulement des outils de communication interne.

3. Architecture

Généralement, un réseau intranet possède une architecture clients/serveur(s) *n* tiers qui repose sur tout ou partie des composants suivants :

- Serveur(s) de fichiers, NAS, SAN (pour le partage des données).
- Serveur(s) http de l'intranet (semblable(s) à un serveur web).
- Serveur(s) de bases de données (pour le stockage des informations).
- Serveur(s) de messagerie (pour l'échange de courriers électroniques ou la messagerie instantanée).
- Serveur(s) d'authentification (pour l'identification des utilisateurs et le stockage des annuaires)
- Serveur(s) et logiciel client de supervision réseau/systèmes (le protocole SNMP est généralement utilisé pour obtenir des informations sur le statut des différents composants du réseau).
- Serveur(s) de vidéoconférence
- Switches, routeurs, pare-feu (éléments de l'infrastructure)
- Serveur(s) d'application(s) qui prennent en charge tout ou partie de fonctions spécifiques de l'entreprise ou de l'organisation (gestion des congés, gestion des notes de frais…). Avec le développement du SAAS (Logiciel en tant que service), de très nombreuses applications et progiciels de gestion intégrés (ERP) sont déployés et accessibles par l'intranet de l'entreprise.

L'intranet d'une entreprise correspond souvent à la partie visible du système d'information d'une entreprise.

Il est généralement indépendant et hors « zone démilitarisée » (DMZ), et au cas où il est connecté au réseau mondial Internet cela doit être fait via une ou plusieurs passerelles et surtout un ou des pare-feu (firewall) qui l'isolent sur le plan de la sécurité.

Les fonctionnalités offertes aux utilisateurs d'un intranet ont tendance à être rassemblées via un portail web (qui s'affiche dans un navigateur web, comme Firefox, Internet Explorer, Opéra ou encore Google Chrome).

Le partage et stockage des fichiers sur un intranet s'effectue de façon privilégiée sur un CMS, un NAS (Network Attached Storage) ou SAN (Storage Area network) ou encore via WebDAV qui formera une partie dédiée du réseau interne.

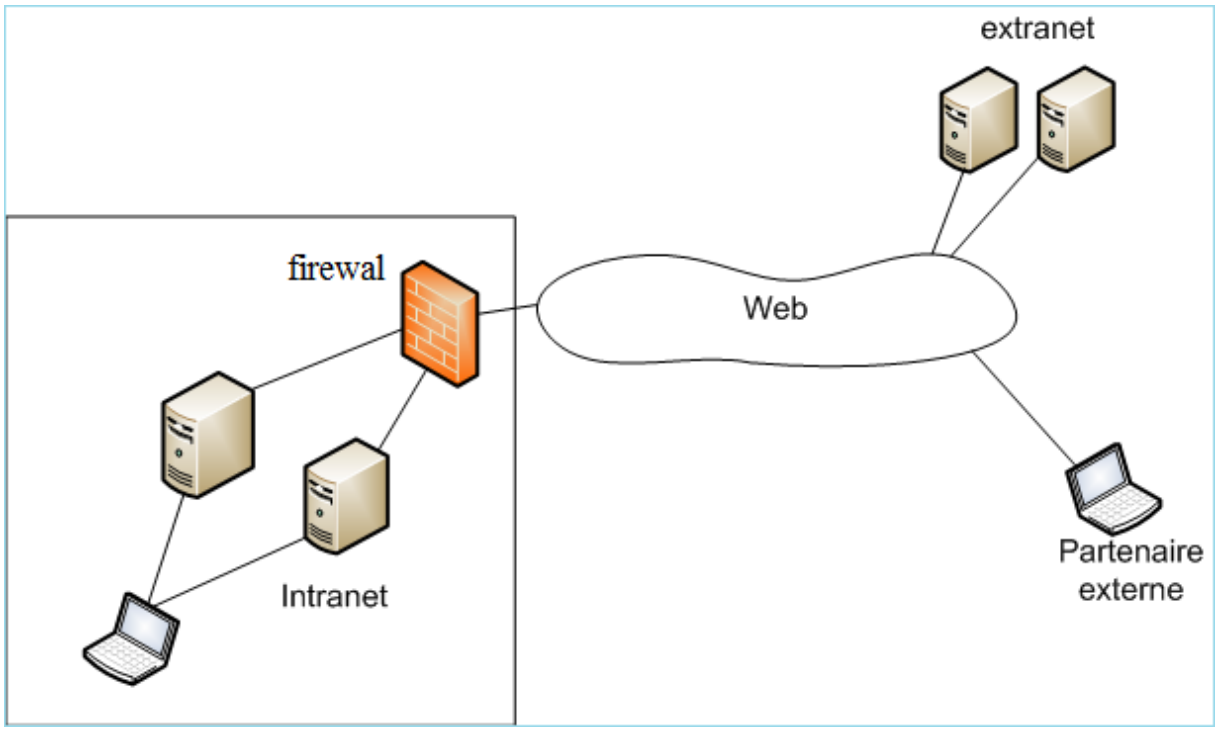

Figure 6:Intranet et extranet

4. Les avantages

- Travail des employés : L'intranet aide les employés à trouver et à visualiser rapidement des informations dans des documents électroniques et des applications pertinentes dans leurs domaines de compétences. Via une interface plus légère et plus intuitive (Navigateur web, Applet Java, AIR, RIA), les utilisateurs peuvent accéder aux données de n'importe quelle base de données qu'une organisation veut rendre disponible, n'importe quand, de n'importe où, augmentant par là même l'efficacité des employés dans leur travail.
- Communication : L'intranet est un puissant moyen de communication à l'intérieur d'une organisation, verticalement et horizontalement.

- Publipostage Web : l'utilisation d'intranet permet aux informations d'être publiées par des liens au-delà du simple hypertexte.
- Organisation et business : L'intranet est aussi utilisé comme une plateforme pour développer et déployer des applications de support aux transactions informatiques utilisées à des fins financières et décisionnelles.

5. Les inconvénients

Le premier inconvénient est que cette infrastructure coûte cher. Cela n'a l'air de rien mais, en ce moment, dans les entreprises, nous courons derrière les budgets. Entrer vraiment dans un projet intranet d'une certaine dimension, et surtout, qu'il soit accessible pour tous le mode, coûte cher. Donc, il faut arriver à surmonter ce premier inconvénient. Ainsi, de faire des choix d'investissement qui sont assez lourds au départ. Par la suite, une infrastructure est nécessaire, ainsi qu'une bonne administration du réseau intranet soit soutenu. Par conséquent l'interconnexion des ordinateurs n'est pas suffisante.

Le deuxième inconvénient est que les utilisateurs du réseau intranet peuvent y passer beaucoup de temps au départ, pour apprendre à utiliser les différents services du réseau, ce qui cause des fausses manipulations et une forte utilisation des ressources matériels du réseau. Cela peut donc être a priori négatif sur le fonctionnement de l'entreprise.

Cependant, nous pouvons dire que malgré ces inconvénients liés à un investissement, soit en termes de formation des utilisateurs, soit en termes techniques, à un moment ou à un autre, nous devons enrichir la qualité du service, afin d'améliorer l'image de l'entreprise.

Ainsi, nous pouvons ajouter aussi parmi ses inconvénients :

- La vulnérabilité du réseau, car nécessitant de disposer d'une connexion permanente à Internet.
- La panoplie d'outils incomplets

6. Place de l'intranet dans l'ingénierie des connaissances

Le métier qui consiste à organiser le partage des connaissances des employés et des dirigeants dans une entreprise s'appelle l'ingénierie des connaissances.

L'INTRANET constitue une partie de l'infrastructure technique d'un réseau qui permet de développer le travail collaboratif et les projets d'ingénierie des connaissances (knowledge management).

Un ou plusieurs intranets peuvent être employés pour structurer les communautés de pratique.

7. Conclusion

En fin, nous pouvons dire que l'INTRANET est un réseau local très utile pour l'entreprise, car il permet aux employés de celle-ci de disposer assez d'informations afin de faciliter la communication interne au sein de l'entreprise. Ainsi, il permet à l'entreprise d'avoir un certain nombre d'avantages facilitant la maîtrise de l'information, ce qui participe à l'homogénéisation, l'interactivité et la convivialité du système d'information au sein de l'entreprise. En tant qu'outil informatique l'INTRANET favorise également la sensibilisation des acteurs concernés.

Cependant, malgré l'existence de quelques inconvénients, l'INTRANET est aujourd'hui, parmi l'un des supports informatiques les plus utilisés en entreprise.

Chapitre 3 : La supervision réseau

La supervision réseau

1. Introduction

Il est aujourd'hui de plus en plus difficile d'administrer un réseau. En effet le nombre d'équipements à gérer est souvent de plus en plus important : stations, serveurs, imprimante, etc.

Le plus grand souci d'un administrateur est les pannes. En effet, il doit pouvoir réagir le plus rapidement possible pour effectuer les réparations nécessaires. Il faut pouvoir surveiller de manière continu l'état des systèmes d'information afin d'éviter un arrêt de production de trop longue durée. C'est là où la supervision intervient, elle doit permettre d'anticiper les problèmes et de faire remonter des informations sur l'état des équipements.

Plus le système est important et complexe, plus la supervision devient compliquée sans les outils indispensables.

2. La supervision des réseaux

2.1 Définition

La supervision réseau est un ensemble de protocoles, matériels et logiciels informatiques assurant plusieurs activités : 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. Nous supervisons 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.

2.2 Protocole de supervision

Il existe une panoplie de protocoles et d'outils de supervision de réseau aidant à collecter des informations sur les nœuds réseau et vérifier leur bon fonctionnement tels que SSH, ICMP, et SNMP. Mais en termes d'efficacité et consistance c'est le protocole SNMP qui se situe en premier rang.

2.3 Principe de la 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 la lumière sur d'éventuels problèmes.

La supervision peut résoudre les problèmes automatiquement ou dans le cas contraire prévenir via un système d'alerte (email ou SMS) 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. [8]

Un tel processus est réalisé à plusieurs niveaux d'un parc de machines : Au niveau interconnexions (Réseau), au niveau de la machine elle-même (Système) et au niveau des services offerts par cette machine (Applications). Que nous pouvons les résumés dans les trois points suivant :

- Supervision réseau **:** Par le terme réseau nous entendons ici l'aspect communication entre les machines. Le rôle est de s'assurer du bon fonctionnement des communications et de la performance des liens (débit, latence, taux d'erreurs). C'est dans ce cadre que l'on va vérifier par exemple si une adresse IP est toujours joignable, ou si tel port est ouvert sur telle machine, ou faire des statistiques sur la latence du lien réseau.
- Supervision système **:** La surveillance se cantonne dans ce cas à la machine elle-même et en particulier ses ressources. Si nous souhaitons par exemple de contrôler la mémoire utilisée ou la charge processeur sur le serveur voire analysé les fichiers de logs système.
- Supervision applicative **:** Cette technique est plus subtile, c'est elle qui va nous permettre de vérifier le fonctionnement d'une application lancée sur une machine. Cela peut être par exemple une tentative de connexion sur le port de l'application pour voir si elle retourne ou demande bien les bonnes informations, mais aussi de l'analyse de logs applicatifs. [8]

3. La norme ISO 7498/4

Le concept de supervision a été normalisé par l'ISO (International Organisation for Standardisation). Voici les différentes fonctions qui ont été défini par l'ISO :

3.1 Gestion des performances

Elle doit pouvoir évaluer les performances des ressources du système et leur efficacité. Elle comprend les procédures de collecte de données et de statistiques. Elle doit aboutir à l'établissement de tableaux de bord. Les informations recueillies doivent aussi permettre de planifier les évolutions du réseau. [9]

Les performances du réseau sont évaluées à partir de quatre paramètres :

- Le temps de réponse
- Le débit
- Le taux d'erreur par bit
- La disponibilité

3.2 Gestion des configurations (Management Configuration)

La gestion de configuration permet d'identifier, de paramétrer et de contrôler les différents objets du réseau. Les procédures requises pour gérer une configuration sont : [9]

- La collecte d'information
- Le contrôle d'état
- La sauvegarde historique de configurations de l'état du système.

3.3 Gestion de la comptabilité (Accounting Management)

Son rôle est de connaître les charges des objets gérés ainsi que leurs coûts de communication. 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. [9]

3.4 Gestion des anomalies (Fault Management)

La gestion des fautes permet la détection, la localisation et la correction d'anomalies passagères ou persistantes. Elle doit également permettre le rétablissement du service à une situation normale. [9]

3.5 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 à ce que les utilisateurs non autorisés ne puissent accéder à certaines ressources protégées.

Elle a également pour rôle de mettre en application les politiques de sécurité. [9]

4. Les protocoles TCP, IP, UDP et ICMP

Le réseau internet utilise au niveau transport trois protocoles principaux. Nous allons dans cette partie présenter successivement le protocole TCP, orienté connexion et complément direct du protocole IP, le protocole UDP, fonctionnant en mode non connecté et enfin ICMP, protocole de notification d'erreur.

4.1 Le protocole TCP

Le protocole TCP (Transmission Control Protocol) est le plus répondu au niveau transport. Il est dans la plupart des cas associe à IP pour améliorer la qualité de service offert par ce dernier, initialement restreinte. L'association de TCP et IP permet d'obtenir un service de transmission fiable orienté connexion, utilisable par un grande nombre d'application réseaux. Remarquons que le nom de protocole TCP/IP est souvent donné à cette association, la présentant comme un protocole unique [3].

Le protocole TCP propose des fonctions mettant en œuvre les divers rôles détaillés dans la première partie :

- Ouverture et fermeture de la connexion de niveau transport.
- Découpage des données reçues des couches supérieures en entités appropriées à la constitution de datagramme IP (au maximum 65536 octets) et réassemblage à l'arrivée si nécessaire.
- Contrôle de la qualité du service pour conserver un service fiable en mode connecté.
- Gestion des problèmes de transmission et reprise en cas d'interruption.

4.2 Adresses IP

Une machine (appelée aussi hôte ou host) est identifiée dans l'Internet par son adresse. L'adresse IP d'une machine correspond à un numéro qui est unique dans le monde. Il existe actuellement cinq classes d'adresses IP. Les trois premières permettent de gérer des réseaux de tailles diverses. La classe D permet de gérer une communication multipoint (un message est envoyé à plusieurs machines à la fois). La classe E est réservée et ne sera probablement

jamais utilisée puisqu'on devrait bientôt migrer vers la nouvelle version d'IP IPv6 qui stockera les adresses IP dans 16 octets [3].

Une adresse IP (avec IP pour Internet Protocol) est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque périphérique relié à un réseau informatique qui utilise l'Internet Protocol. L'adresse IP est à la base du système d'acheminement (le routage) des paquets de données sur Internet.

Il existe des adresses IP de version 4 sur 32 bits, et de version 6 sur 128 bits. La version 4 est actuellement la plus utilisée : elle est généralement représentée en notation décimale avec quatre nombres compris entre 0 et 255, séparés par des points, ce qui donne par exemple « 192.168.1.1 ».

4.3 Le protocole UDP

Le protocole UDP (User Data Protocol) son fonctionnement est très proche au protocole IP : son rôle est de reprendre la plupart des fonctions de ce dernier et leur octroyer plus de fiabilité au regard des couches de niveau supérieurs. En ce sens, UDP est similaire à TCP, mais en mode sans connexion [3].

Le segment UDP présente un format très simple. Les cinq champs nécessaires à la transmission en mode non connecté par UDP ne font pas appel à des mécanismes nouveaux ou complexes :

- L'interprétation du port source et port destination est la même que dans segment TCP. Notons que les ports (leurs valeurs) sont les mêmes dans les deux cas.
- Le champ contenant les données étant de longueur variable, sa longueur totale est précisée, de façon à pouvoir effectuer le contrôle d'erreur grâce au total de contrôle.

16 bits	16 bits	16 bits	16bitsnbits	
Port source	Port destination	Longueur totale	Total de contrôle	Données

Figure 7 : Format du segment UDP

Les utilisations du protocole UDP dans les systèmes d'informations sont beaucoup moins nombreuses que celle (multiples) de TCP. Il est cependant très fréquemment employé dans les architectures client-serveur, permettant d'échanger en mode non connecté entre deux extrémités et dans les deux sens de communication (requêtes émises par un processus client à une application serveur, réponses du serveur au client).

4.4 Le protocole ICMP

IP est un protocole non fiable. Ainsi, aucune garantie ne peut être obtenues quant au bon déroulement de livraison des donnés envoyer sur IP. Il est important, pour assurer un bon fonctionnement du réseau, de pouvoir disposer d'un protocole de notification d'erreur,

permettant d'informer l'expéditeur en cas de problème de remise de données. ICMP (Internet Control Message Protocol) assure cette fonction. Il s'agit d'un protocole de notification d'erreur permettant aussi la diffusion d'information d'administration sur internet. Les messages ICMP sont donc classés en deux catégories, les messages d'erreur et les message d'administration [3].

Le protocole ICMP est indispensable au bon fonctionnement des couches réseau et transport du modèle TCP/IP : il informe des cas d'erreurs survenant sur IP, TCP et UDP. Parmi ceux-ci, citons-les plus rencontrés :

- Destination inaccessible.
- Port inaccessible (fréquemment renvoyé par UDP).
- Corruption de message (problèmes physiques, mauvaises options).

La notification d'erreur est un point important pour assurer le bon fonctionnement d'un réseau. Ainsi, s'il est important de disposer de mécanismes permettant d'émettre de tels messages, il est tout aussi primordial de savoir quand ne pas utiliser ces mécanismes. Ainsi, un autre message ICMP de la catégorie erreur n'est jamais émis en réponse à un autre message ICMP de la catégorie erreur, un message contenant une adresse IP de diffusion, un fragment de message autre que le premier, ou un message dont l'origine n'est pas une vraie station (adresse de rebouclage, adresse nulle). Plus généralement, le message ICMP ne sera pas émis dans tous les cas où l'on risquerait de déclencher un phénomène d'avalanche

ICMP est aussi un protocole d'administrateur du réseau :

- Échange d'information concernant le routage.
- Annonce et gestion des masques d'adresses.
- Vérification de l'accessibilité (commande trace route, ping…).
- Gestion de l'heure.
- Aide au control de congestion (des algorithmes sont disponibles, mais ils ne sont généralement pas implémentés).

Le programme le plus connu utilisant le protocole ICMP est sans doute ping. Cet utilitaire permet de tester la présence (et l'accessibilité) d'une station distance. Il fonctionne par émission d'un paquet ICMP de type demande d'écho, destiné à solliciter l'émission d'un message de réponse a demandé d'écho par la machine destination : si le programme ping reçoit une réponse, la machine distante est joignable. En plus de la détermination de l'accessibilité, le programme ping effectue une mesure du temps d'acheminement de la réponse, permettant ainsi de connaitre le temps de propagation aller/retour (RTT : Round Trip Time).

5. Le protocole SNMP

5.1 Présentation

SNMP signifie Simple Network Management Protocol (protocole simple de gestion de réseau en Français). C'est un protocole qui permet comme son nom l'indique, de gérer les équipements réseaux ainsi que les machines informatiques. Ce protocole est donc utilisé par

les administrateurs réseaux pour détecter à distance les problèmes qui surviennent sur leur réseau.

Le protocole SNMP comme le montre la Figure 8 est un protocole de la couche 7 du modèle OSI (couche application). Il est utilisé sur tous les réseaux de type internet. Cette technologie se situe entre la couche 4(Transport) et la couche 7(application).

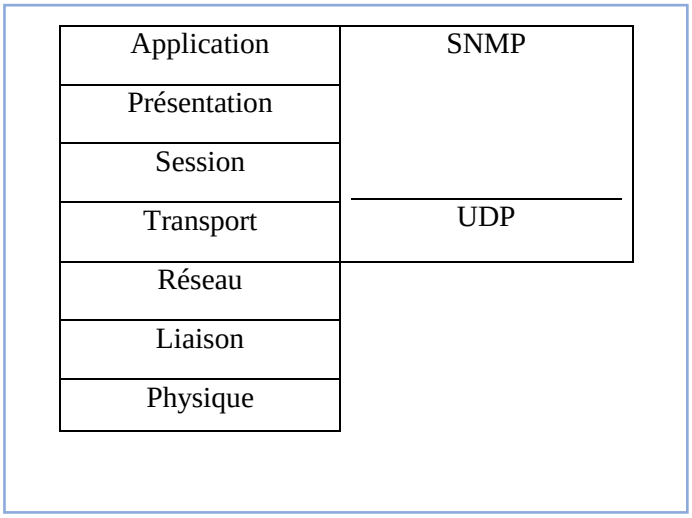

Figure 8: Position du SNMP dans le modèle OSI

Chaque machine, que ce soit sous Windows ou sous Linux possèdent de nombreuses informations capitales pour l'administrateur réseaux. Nous retrouvons des informations comme la quantité de RAM utilisé, l'utilisation du CPU, l'espace disque et encore bien d'autre Indicateurs.

SNMP va permettre de remonter ces informations à l'administrateur de façon centralisé pour pouvoir réagir au plus vite aux pannes éventuelles.

Les buts du protocole SNMP sont de :

- Connaître l'état global d'un équipement (actif, inactif, partiellement opérationnel...).
- Gérer les évènements exceptionnels (perte d'un lien réseau, arrêt brutal d'un équipement...).
- Analyser différentes métriques afin d'anticiper les problèmes futurs (engorgement réseau...).
- Agir sur certains éléments de la configuration des équipements.

5.2 Les différentes versions du SNMP

Depuis son premier développement au sein de l'IETF (Internet Engineering Task Force, voir RFC 1157 Annexe) au début des années 90, le protocole SNMP a connu plusieurs améliorations visant à optimiser son utilisation dans la supervision des réseaux en passant par plusieurs versions.

Ce protocole a connu des améliorations importantes. Cependant les précédentes versions (la V1 et la V2C) sont encore les versions les plus utilisées actuellement.

Un support de SNMP V3 a récemment été lancé car il est plus sécurisé si on le compare à ses prédécesseurs.

- SNMP V1 : C'est la première version du protocole. La console de supervision interroge l'agent SNMP par un datagramme UDP sur le port 161. Cet UDP contient :

la version de l'SNMP (0 pour SNMPv1), le nom de communauté déterminant les droits d'accès, la requête (get-request, get-next-request) et l'objet Identifier (OID, voir Annexe). La réponse de l'agent contient un datagramme contenant la requête get-response, avec pour et la valeur demandée correspondant à l'OID et un code d'erreur. L'agent peut également être configuré pour renvoyer des alertes à la même console par un datagramme sur le port 162 contenant la requête dite Trap, comme le montre **Error! Reference source not found.**. Cette version du protocole est définie dans les RFC 1155 et 1157. [10]

- SNMP V2C : C'est un protocole révisé, qui comprend les améliorations de SNMP V1 dans différents domaines tels que les types de paquets, les éléments de structure MIB et les requêtes protocolaires MIB. Cependant ce protocole utilise la structure d'administration de SNMP V1 (à savoir "communauté") d'où le terme SNMP V2C.
- SNMP V3 : Aussi connu sous le nom de version sécurisée de SNMP a été développée pour renforcer le volet sécurité des transactions. Ce volet comprend l'identification des parties communicantes et le cryptage de leur conversation. SNMP V3 facilite la configuration à distance des entités SNMP. [10]

Ces trois versions sont les principales, même si des versions intermédiaires ont vu le jour (SNMPSec, SNMP V2, SNMP V2U, SNMP V2P), celles-ci ne présentent que des mises à jour mineures plutôt que de véritables améliorations.

Actuellement les versions les plus utilisées (par ordre d'utilisation) sont : SNMP V1, SNMP V3 puis SNMP V2C.

Malgré tout, la version SNMP V1 persiste encore sur les périphériques, plusieurs facteurs expliquent ce phénomène :

- Les infrastructures déployées en V1 ne sont plus modifiées, tout simplement car cela fonctionnait suffisamment à l'époque, du coup aucune modification n'y est appliquée.
- Les autres versions de SNMP ont été implémentées tardivement par les différents constructeurs.
- SNMP V1 demande très peu de ressources sur des petits équipements tels qu'une imprimante ou un hub. [10]

La Figure 9 illustre le format des messages SNMP.

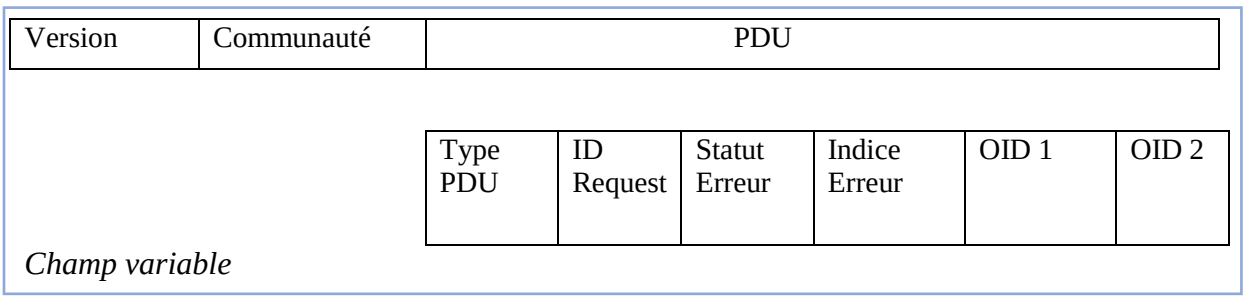

Figure 9: Format des messages SNMP

- Le champ version contient la version de SNMP utilisée.
- Communauté : le type de communauté.
- Type PDU : il s'agit du type de requête.
- ID request : permet d'associer les réponses aux requêtes.
- Statut erreur : Type d'erreur (0 si aucune).

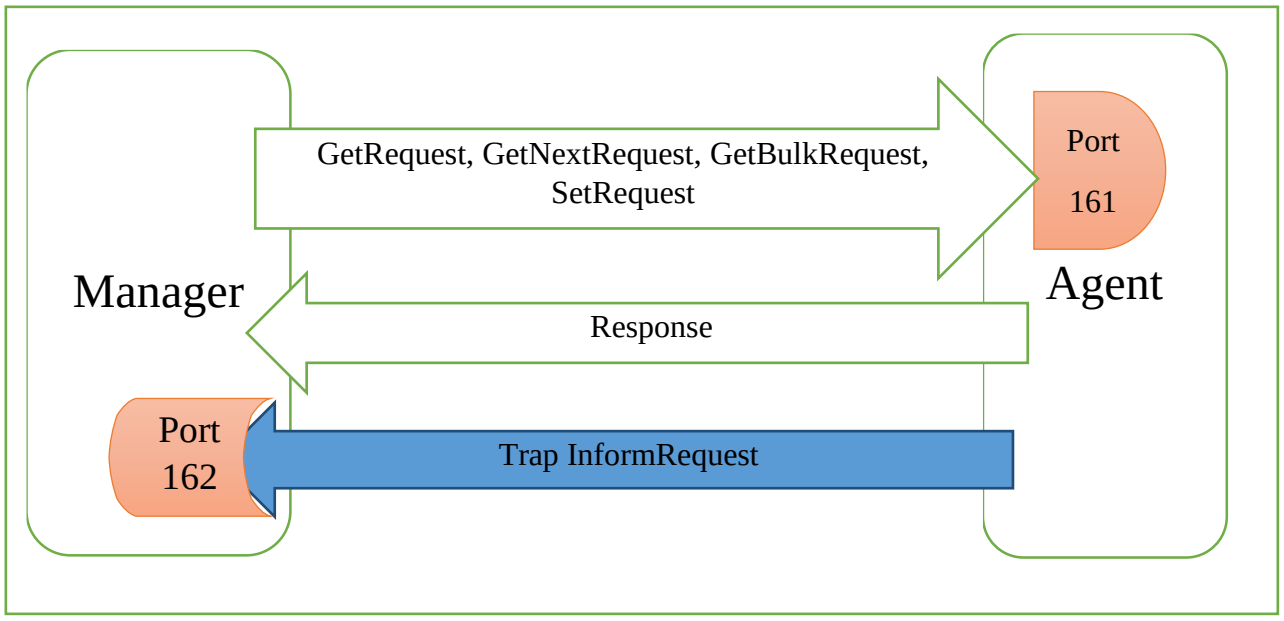

Figure 10: Les échanges entre le manager et l'agent SNMP

5.3 Communautés

SNMP fonctionne par des groupes d'agents ou communautés. Du côté de l'agent ont créé une communauté dite publique accessible pour tous mais en lecture seule et deuxième une communauté privée qu'on peut affecter un nom au choix et accessible en lecture/écriture et protégée par un mot de passe.

5.4 Architecture

Les différents éléments que l'on peut identifier avec le protocole SNMP sont synthétisés par le schéma ci-dessous.

- 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 : ce sont les informations dynamiques instanciées par les différents agents SNMP et remontées en temps réel au superviseur

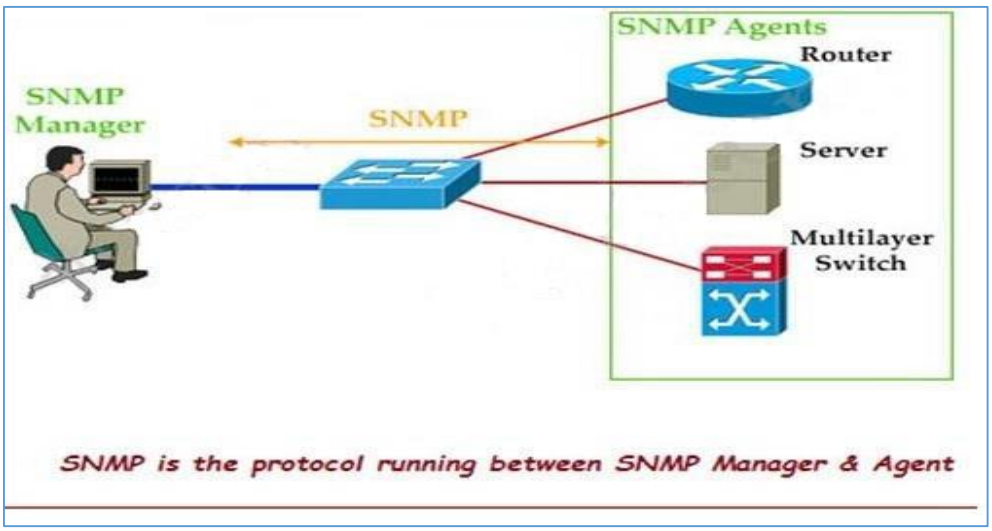

Figure 11: Architecture SNMP

5.5 Le manager

Rappelons que le Manager se trouvera sur une machine d'administration (un poste de travail en général). Il reste un client avant tout, étant donné que c'est lui qui envoie les différentes requêtes aux agents. Il devra disposer d'une fonction serveur, car il doit également rester à l'écoute des alertes que les différents équipements sont susceptibles d'émettre à tout moment.

Si l'on se base sur le schéma précédent, l'administrateur peut observer correctement le comportement de ses différents équipements en réseau.

Le Manager dispose d'un serveur qui reste à l'écoute sur le port UDP 162 ainsi que d'éventuels signaux d'alarme appelés des "traps". Le Manager peut tout autant être installé sur une machine.

5.6 L'agent SNMP

L'agent est un programme qui fait partie de l'élément actif du réseau. L'activation de cet agent permet de recueillir la base de données d'informations et la rend disponible aux interrogations.

Les principales fonctions d'un agent SNMP :

- Collecter des informations de gestion sur son environnement local.
- Récupérer des informations de gestion telle que déni dans la MIB propriétaire.
- Signaler un évènement au gestionnaire.

Par ailleurs même si la principale fonction de l'agent est de rester à l'écoute des éventuelles requêtes du Manager et y répondre s'il y est autorisé, il doit également être capable d'agir de sa propre initiative, s'il a été configuré.

Par exemple, il pourra émettre une alerte si le débit d'une interface réseau, atteint une valeur considérée par l'administrateur comme étant critique. Plusieurs niveaux d'alertes peuvent ainsi être définis, selon la complexité de l'agent (température du processeur, occupation disque dur, utilisation CPU...)

5.7 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 actifs 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 nœud 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. [10]

Une MIB est un arbre très dense, il peut y avoir des milliers d'OID dans la MIB.

Voici un exemple de structure MIB :

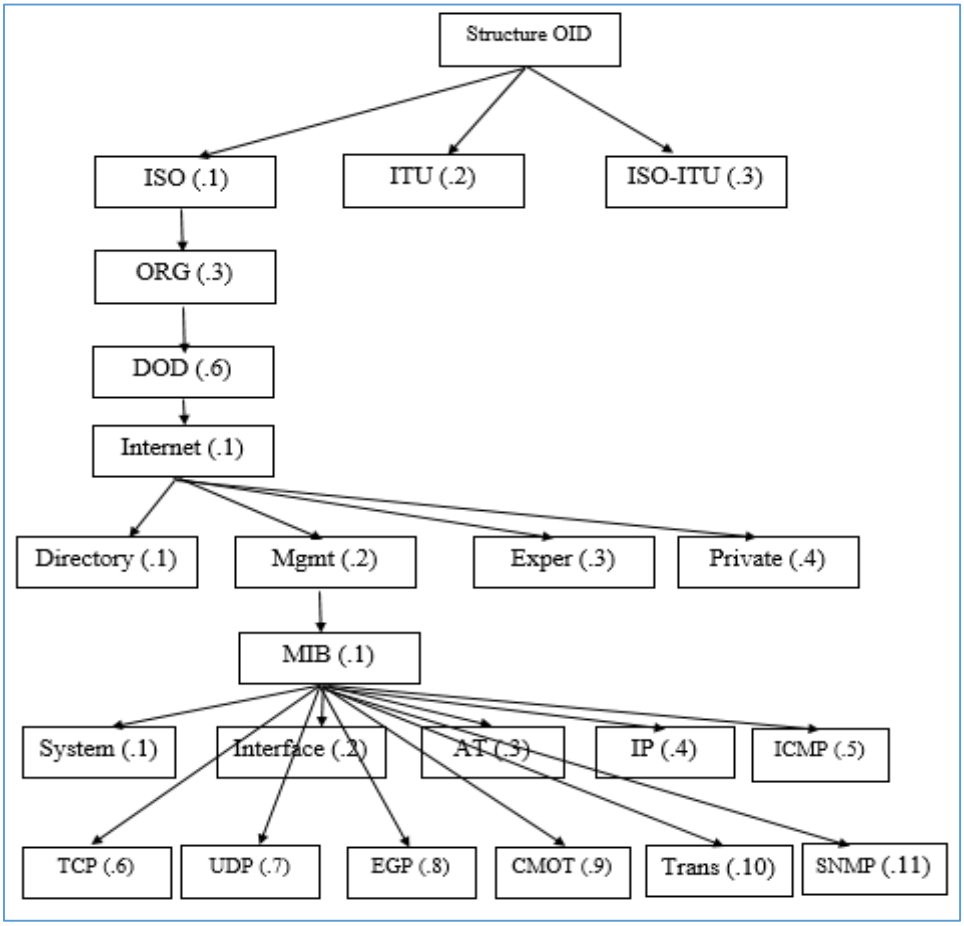

Figure 12: Structure OID

Ainsi, pour interroger les différentes variables d'activité sur un appareil, il faudra explorer son arborescence MIB. Celle-ci est généralement fournie par le constructeur mais il est aussi possible d'utiliser un explorateur de MIB tel que « Getif MIB Browser ».

Ensuite, pour accéder aux variables souhaitées, on utilisera l'OID (Object Identification) qui désigne l'emplacement de la variable à consulter dans la MIB. On aura par exemple sur un commutateur Nortel Passeport l'OID .1.3.6.1.4.1.2272.1.1.20 désignant le taux de charge du CPU.

5.8 Les requêtes SNMP

Le mécanisme de base du protocole SNMP est constitué d'échanges de type requête/réponse appelé PDU pour Protocol Data Unit. En fonction de la version du protocole SNMP utilisé, différentes commandes sont possibles. La structure des paquets utilisés par le protocole SNMP V1, est définie dans la RFC 1157. Les requêtes SNMP vont contenir une liste d'OID (Object identifier) à collecter sur l'agent SNMP.

Les types de requêtes du manager SNMP vers l'agent SNMP sont :

- Get Request : Le manager interroge un agent sur les valeurs d'un ou de plusieurs objets d'une MIB.
- Get Next Request : Le manager interroge un agent pour obtenir la valeur de l'objet suivant dans l'arbre des objets de l'agent. Cette interrogation permet de balayer des objets indexés de type tableau.
- Get Bulk Request : Introduite avec la version 2 du protocole SNMP, cette requête permet de mixer la commande GET et GETNEXT pour obtenir des blocs entiers de réponses de la part de l'agent.
- Set Request : Le manager positionne ou modifie la valeur d'un objet dans l'agent. [10]

Les réponses ou informations de l'agent vers le manager sont :

- Get Response: L'agent répond aux interrogations du manager.
- Trap : L'équipement génère un envoi vers son manager pour signaler un événement, un changement d'état ou un défaut. L'agent n'attend pas d'acquittement de la part du manager.
- Notification: Introduite avec la version 2 du protocole SNMP. L'équipement génère un envoi vers son manager pour signaler un événement, un changement d'état ou un défaut. L'agent n'attend pas d'acquittement de la part du manager.
- Inform: Introduite avec la version 2 du protocole SNMP. L'équipement génère un envoi vers son manager pour signaler un événement, un changement d'état ou un défaut. L'agent attend un d'acquittement de la part du manager et il y aura une retransmission en cas de non réponse. [10]

6. Conclusion

Dans ce chapitre nous avons effectué une étude théorique sur l'opération de supervision réseau ainsi que l'analyse des différents acteurs de cette dernière, notamment le protocole SNMP que nous avons étudié avec plus de détail, puisqu'il sera par la suite l'élément de base de notre solution et qui aura un impact très important dans la phase réalisation.

Chapitre 4 : Spécification des Besoins et Réalisation

Spécification des Besoins et Réalisation

1. Introduction

Dans ce chapitre, nous allons spécifier les besoins fonctionnels et non fonctionnels de l'application, ce qui nous amènera à identifier les possibilités du système et les besoins des utilisateurs que nous essayerons de les projeter dans des diagrammes de cas d'utilisations globales et détaillés. Par la suite nous allons développer une application JAVA, qui engendre ces besoins tout en respectant l'ensemble de diagrammes réalisés.

2. Spécification des besoins

La solution cible doit satisfaire les besoins fonctionnels qui seront exécutés par le système et les besoins non fonctionnels qui identifient la qualité logicielle du système. Ainsi les besoins architectural qui définies notre application.

2.1 Les besoins fonctionnels

Cette application doit couvrir principalement les besoins fonctionnels suivants :

- ✓ Authentification.
- ✓ Gestion des utilisateurs : ajout et suppression. Cette fonction est possible pour l'administrateur seulement et masqué pour les autres utilisateurs.
- ✓ Cartographie des nœuds réseaux et suivi en temps réel des équipements. Ce qui permettra aux différents acteurs et selon leur rôle de surveiller l'état des chacun des équipements (up/down, idle / faulty …).
- ✓ La gestion des logs et archivage des évènements dans une base de données pour d'éventuelles consultations.
- ✓ Suivi des charges sur les liens WAN (Occupation de bande passante).
- ✓ La possibilité d'avoir un accès à l'application à travers un agent Android.

Dans ce projet de fin d'études nous avons fait une étude complète sur la supervision d'une manière générale pour pouvoir modélisé un système général, mais à cause de la limite de temps nous avons réalisé que la cartographie des nœuds qui consiste à suivre l'état de chaque équipement (up/down, idle / faulty …). Par conséquent nous pouvons considérer ce projet comme une plate-forme pour d'autre projets connexe, afin d'améliorer et compléter les autres tâches de la supervision.

2.2 Les besoins non fonctionnels

Ce sont des exigences qui ne concernent pas spécifiquement le comportement du système mais plutôt identifient des contraintes internes et externes du système.
Les principaux besoins non fonctionnels de notre application se résument dans les points suivants :

- ✓ L'application doit être portable c'est-à-dire sa capacité à pouvoir être adapté plus ou moins facilement en vue de fonctionner dans différents environnements d'exécution.
- ✓ Le code doit être clair pour permettre des futures évolutions ou améliorations.
- ✓ L'ergonomie : l'application doit offrir une interface conviviale et facile à utiliser.

2.3 Les besoins architectural

L'application doit fonctionner dans un réseau. Certes l'accès doit donc être possible à partir de n'importe quel poste. L'importance d'avoir un système d'archivage de donnée (parmi le besoins fonctionnels) et de gestion.

Ainsi l'architecture à deux niveaux s'avère la mieux à adopter (aussi appelée architecture 2-tiers) caractérise les systèmes clients/serveurs dans lesquels le client demande une ressource et le serveur la lui fournit directement. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir le service.

Les avantages d'une architecture client-serveur c'est que tout d'abord les ressources sont centralisées sur le serveur. Il est donc plus simple de gérer les ressources communes aux utilisateurs comme la base de données par exemple.

Ensuite, cette architecture est plus sécurisée étant donné que le client dispose de moins de point d'entrée pour accéder aux données.

Comme l'indique la Figure 13, le client accèdent au serveur pour demander une ressource.

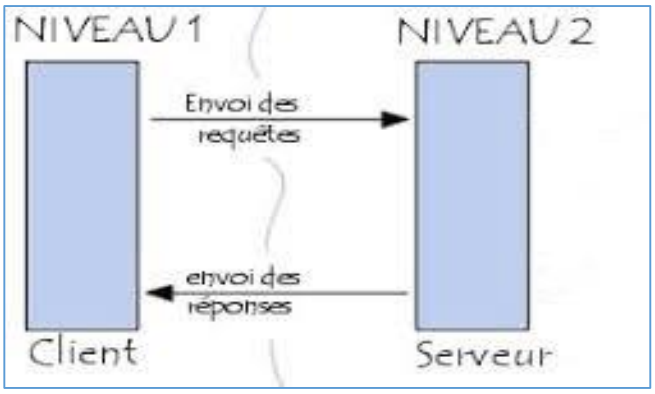

Figure 13: Architecture Client-serveur

3. Les outils de modulation

3.1 Modélisation des besoins

Nous avons choisi le langage de modélisation UML pour présenter les diagrammes des cas d'utilisation ainsi que les acteurs de notre application

3.2 Pourquoi UML ?

UML ou encore Unified Modeling Langage, est un langage de modélisation des données et des traitements, formel et normalisé qui offre un standard de modélisation. C'est alors un langage graphique qui entre dans l'optique de la programmation orientée objet et qui sponsorisé par les grands calibres du monde de l'informatique tel que HP, Microsoft et IBM. Il possède de multiples avantages : C'est un support de communication performant, il décrit une application en fonction des méthodes objet avec lesquelles elle a été construite. Il cadre l'analyse et facilite la compréhension de représentations abstraites complexes et il se caractérise par sa notation graphique simple qui permet d'exprimer visuellement une solution objet.

Dans UML chaque diagramme permet d'exprimer certains points d'un même problème. La combinaison de plusieurs digrammes permettra donc d'avoir une vue complète du système informatique. Ainsi en fonction du problème à résoudre, il convient de choisir les diagrammes adéquats à utiliser.

3.3 Les avantages de l'UML

UML est un langage formel et normalisé. Il permet ainsi : Un gain de précision, un gage de stabilité et l'utilisation d'outils. UML est un support de communication performant : Il cadre l'analyse et facilite la compréhension de représentations abstraites complexes. Son caractère polyvalent et sa souplesse lui font un langage universel en assurant les objectifs :

- Construire des modèles de systèmes.
- Organiser le travail.
- Gérer le cycle de vie d'A à Z.
- Gérer le risque.
- Obtenir de manière répétitive des produits de qualité constante.

En conclusion, nous avons choisi de travailler avec UML parce qu'il exprime mieux la vue statique et dynamique du système d'information et pour notre application, il est nécessaire de faire une analyse très approfondie pour pouvoir dégager les nécessités de développement ainsi que quelques scénarios d'exécution.

3.4 Digramme de classe

Un diagramme de classes est une collection de modélisations statiques, c'est un schéma utilisé en génie logiciel pour présenter les classes et les interfaces des systèmes ainsi que les différentes relations entre celles-ci. Ce diagramme fait partie de la partie statique d'UML car il fait abstraction des aspects temporels et dynamiques.

Une classe décrit les responsabilités, le comportement et le type d'un ensemble d'objets.

Les éléments de cet ensemble sont les instances de la classe. Les classes peuvent être liées entre elles grâce au mécanisme d'héritage qui permet de mettre en évidence des relations de parenté. D'autres relations sont possibles entre des classes, chacune de ces relations est représentée par un arc spécifique dans le diagramme de classes.

Elles sont finalement instanciées pour créer des objets (une classe est un moule à objet : elle décrit les caractéristiques des objets, les objets contiennent leurs valeurs propres pour chacune de ces caractéristiques lorsqu'ils sont instanciés).

Le diagramme de classes donne une vue statique du système logiciel puisqu'il décrit les types et leurs objets de ce dernier. Typiquement, il met en relation des classes mais aussi des interfaces, des types de données, des types énumérés. C'est donc est un réseau statique de classes et d'associations. En partant des classes et des associations trouvées précédemment, il faut construire un schéma sous forme de représentation graphique dans lequel les classes seront représentées par des rectangles et les associations par des traits pleins. Il faut ajouter à ce schéma des informations concernant les classes et leurs associations. Un exemple de diagramme de classes simplifié est donné dans la figure suivante (Figure 14). Une classe est représentée par un rectangle séparée en trois parties :

- La première partie contient le nom de la classe.
- La seconde contient les attributs de la classe.
- La dernière contient les méthodes de la classe.

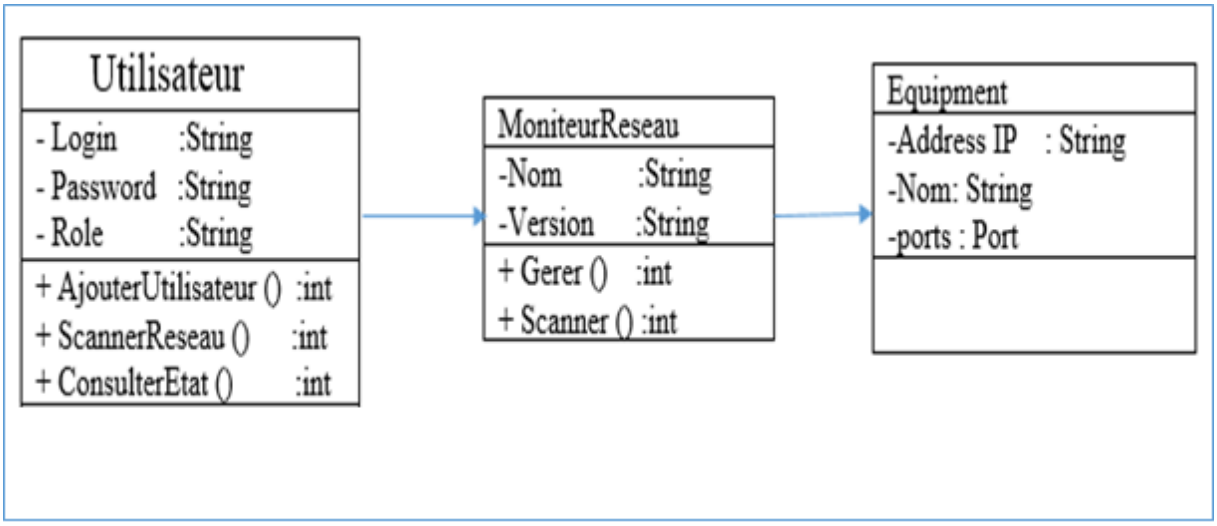

Figure 14: Exemple de digramme de classe

La Figure 14, illustre un fragment du diagramme de classe qui modélise les classes utilisateur, moniteur réseau et équipement. L'utilisateur peut consulter à temps réel l'état des équipements, des ports, des routeurs… en invoquant la méthode **ConsulterEtat()** à travers l'adresse du réseau propre qui est connu par chaque utilisateur autorisé à utiliser le programme et qui sont généralement des administrateurs réseau et systèmes.

La méthode **ConsulterEtat()** invoque la classe **MoniteurReseau** pour gérer et scanner tous les équipements réseau définit par la classe **Equipement**.

3.5 Le Diagramme de cas d'utilisation

Le digramme Uses Cases montre les interactions fonctionnelles entre les acteurs et le système à l'étude.

Acteur :

Rôle joué par un utilisateur humain ou un autre système qui interagit directement avec le système étudié. Un acteur participe à au moins un cas d'utilisation.

Cas d'utilisation (use case) :

Ensemble de séquences d'actions réalisées par le système produisant un résultat observable intéressant pour un acteur particulier. Collection de scénarios reliés par un objectif utilisateur commun.

Association :

Utilisée dans ce type de diagramme pour relier les acteurs et les cas d'utilisation par une relation qui signifie simplement « participe à ».

Inclusion :

Le cas d'utilisation de base en incorpore explicitement un autre, de façon obligatoire, à un endroit spécifié dans ses enchaînements.

Extension :

Le cas d'utilisation de base en incorpore implicitement un autre, de façon optionnelle, à un endroit spécifié indirectement dans celui qui procède à l'extension

Généralisation :

Les cas d'utilisation descendants héritent de la description de leur parent commun. Chacun d'entre eux peut néanmoins comprendre des relations spécifiques supplémentaires avec d'autres acteurs ou cas d'utilisation.

4. Conception

Dans cette section, nous allons utiliser les différents outils étudiés dans la section précédente pour modéliser les besoins fonctionnels de l'application.

4.1 Diagramme de cas d'utilisation

Afin de modéliser l'interaction du superviseur ou l'administrateur avec les différentes fonctionnalités du système de supervision nous allons proposer un diagramme de cas d'utilisation générale illustré par la Figure 15 qui engendre la totalité des fonctionnalités possible du système.

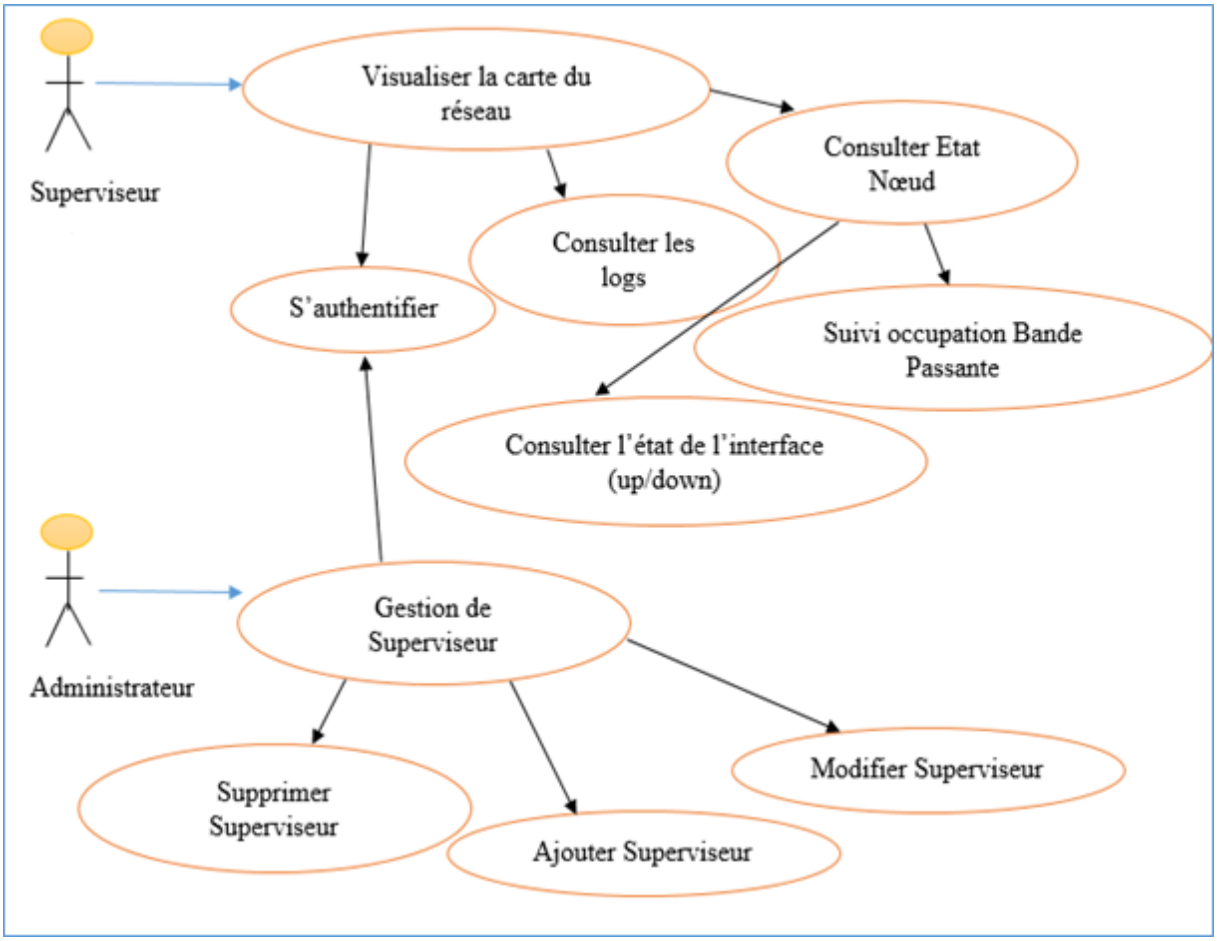

Figure 15: Cas d'utilisation Général

Description Textuelle de cas d'utilisation Général :

- Pour accéder au système il faut obligatoirement saisir un login et un mot de passe quel que soit l'utilisateur.

- L'acteur administrateur (super superviseur) a deux volets sur le système :
  - ✓ La gestion des utilisateurs qui permet d'ajouter, modifier ou bien supprimer utilisateur (Superviseur).

  - ✓ La gestion et la visualisation de la cartographie du réseau

- L'acteur superviseur a pour mission de consulter uniquement l'état du système sans avoir l'habilitation d'effectuer des modifications.

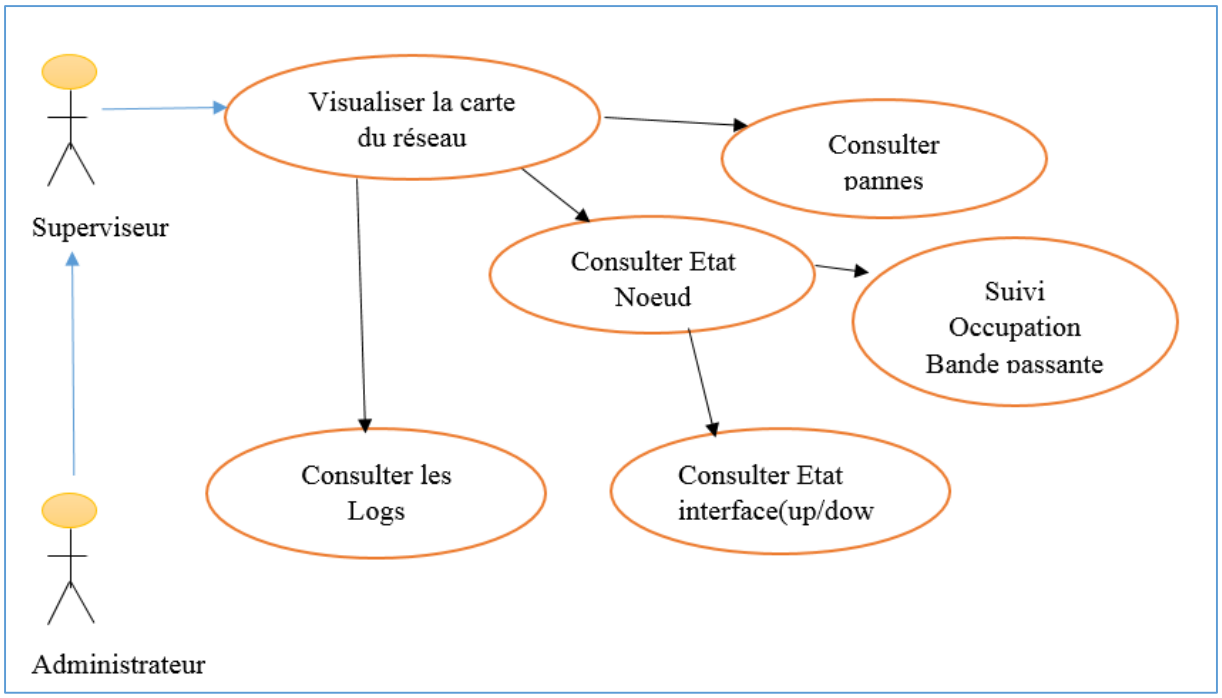

Figure 16: Cas d'utilisation « Visualisation de la carte du réseau »

Description textuelle de cas d'utilisation Visualisation de la carte du réseau :

La consultation d'état de système : consulter état serveur, consulter état routeur, consulter panne… est la même pour tous auteurs, elle est précédée par l'authentification.

Description textuelle de cas d'utilisation Gestions des comptes :

Seul l'administrateur réseau (superviseur) peut créer, modifier, ajouter, et supprimer un compte et un mot de passe. Les comptes et les mots passe valides sont initialisées et enregistrées par l'administrateur réseau (superviseur), elle est précédée par l'authentification.

4.2 Diagramme de class

La conception de notre application a fait l'objet un diagramme de classe, qui nous a permet de visualiser l'ensemble des classes de l'application ainsi que leur fonctionnalité. La Figure 17 illustre les classes suivantes :

La classe **SupervionReaseau**, représente l'interface graphique de notre application.

La classe **Network** contient les méthodes *getAddressList* et *setNetMask*. Cette classe donne la liste des adresses IP de tous les interfaces de la machine host ainsi que leurs Mask.

La classe **ScanNet,** est utilisé pour le scan les adresses de réseau, elle contient plusieurs méthodes tels que, *getNetAddress* pour obtenir l'adresse du réseau, *getTimeout* qui nous permet le paramétrage du scan ainsi la méthode isFixRange() qui permet de vérifier si l'utilisateur utilise un scan complet du réseau ou une plage d'adressage fixe.

La classe **SnmpWalk**, elle permet d'interroger a distante à l'aide des requêtes SNMP pour obtenir les informations sur l'état de cette dernière.

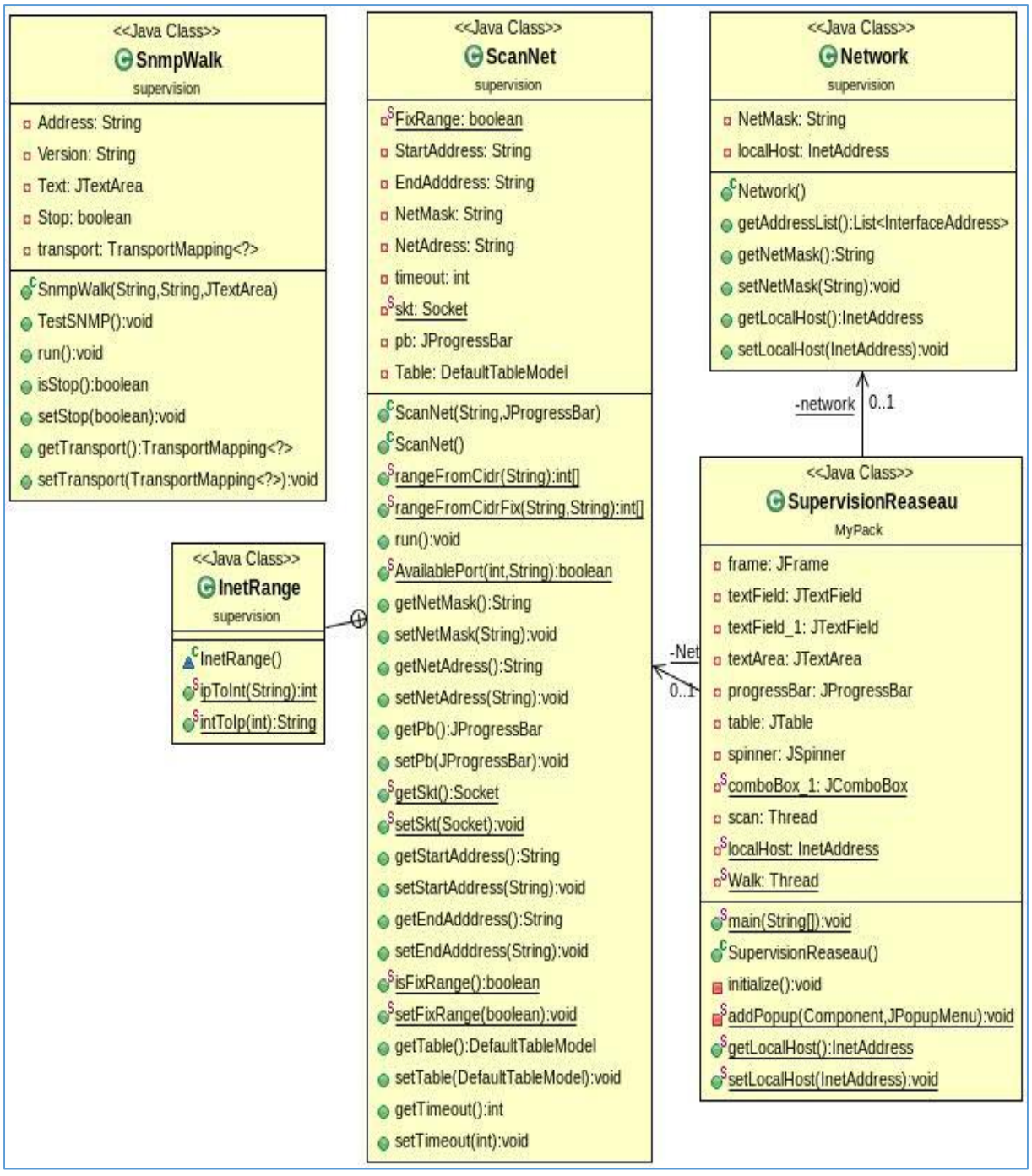

Figure 17: diagramme de classe supervision réseau INTRANET

5. Réalisation

Cette section est une description de la phase finale du projet. Il s'agit de présenter les différentes étapes de réalisation de l'application cible, l'environnement logiciel de développement, les configurations nécessaires du protocole SNMP et quelques tests de bon fonctionnement. Nous donnerons quelques captures d'écran des actions effectuées.

5.1 Architecture de l'application

L'architecture cible de notre solution peut être schématisée dans la Figure 18.

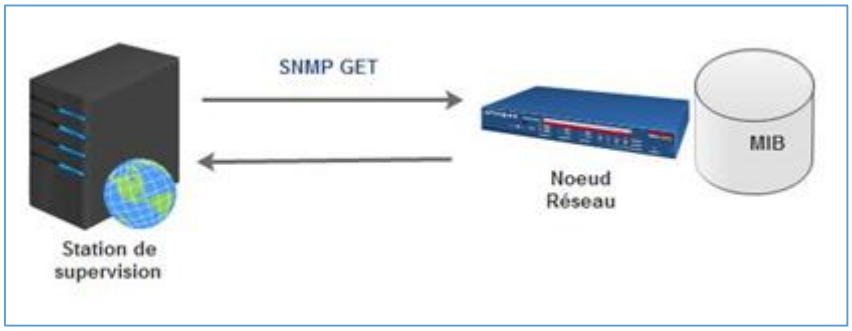

Figure 18: Schéma d'architecture cible

5.2 Environnement d'application

Tout le développement de l'application a été réalisé sur des machines dont le système d'exploitation Microsoft Windows 7 64 bits. L'environnement de développement utilisé pour la programmation des requêtes SNMP, se base sur le langage de programmation Java afin d'assurer la portabilité de la solution et nous avons utilisé le logiciel JAVA Eclipse avec la bibliothèque SNMP4J.

5.3 Langage de programmation JAVA

Java est un langage de programmation orienté objet créé par James Gosling et Patrick Naughton, employés de Sun Microsystems, avec le soutien de Bill Joy (cofondateur de Sun Microsystems en 1982), présenté officiellement le 23 mai 1995 au SunWorld.

La société Sun a été ensuite rachetée en 2009 par la société Oracle qui détient et maintient désormais Java.

La particularité et l'objectif central de Java est que les logiciels écrits dans ce langage doivent être très facilement portables sur plusieurs systèmes d'exploitation tels que Unix, Windows, Mac OS ou GNU/Linux, avec peu ou pas de modifications, mais qui ont l'inconvénient d'être plus lourd à l'exécution (en mémoire et en temps processeur) à cause de sa machine virtuelle. Pour cela, divers plateformes et Framework associés visent à guider, sinon garantir, cette portabilité des applications développées en Java.

5.4 Logiciel Java Eclipse

Eclipse est un projet, décliné et organisé en un ensemble de sous-projets de développements logiciels, de la fondation Eclipse visant à développer un environnement de production de logiciels libre qui soit extensible, universel et polyvalent, en s'appuyant principalement sur Java.

Son objectif est de produire et fournir des outils pour la réalisation de logiciels, englobant les activités de programmation (notamment environnement de développement intégré et Framework) mais aussi d'AGL recouvrant modélisation, conception, test, gestion de configuration, reporting… Son EDI, partie intégrante du projet, vise notamment à supporter tout langage de programmation à l'instar de Microsoft Visual Studio.

Bien qu'Eclipse soit d'abord été conçu uniquement pour produire des environnements de développement, les utilisateurs et les contributeurs se sont rapidement mis à réutiliser ses briques logicielles pour des applications clientes classiques. Cela a conduit à une extension du périmètre initial d'Eclipse à toute production de logiciel : c'est l'apparition du Framework Eclipse RCP en 2004.

Figurant parmi les grandes réussites de l'open source, Eclipse est devenu un standard du marché des logiciels de développement, intégré par de grands éditeurs logiciels et sociétés de services.

Les logiciels commerciaux *Lotus Notes 8*, *IBMLotus Symphony* ou *WebSphere Studio Application Developer* sont notamment basés sur Eclipse.

5.5 Activation du protocole SNMP

Pour collecter les données sur les évènements déclenchés sur les nœuds réseau (switch ou routeur) et pour installer l'agent Microsoft SNMP sur un Windows 7, nous devons l'activer en ouvrant le panneau de contrôle et cliquez sur programme puis dans le menu sélectionner Activer ou Désactiver des fonctionnalités Windows comme le montre la Figure 19.

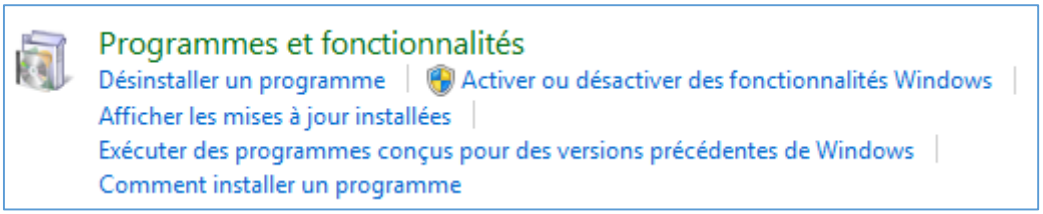

Figure 19: Programme et fonctionnalités

Dans la liste des fonctionnalités, cochés la case protocole SNMP (voir Figure 20)

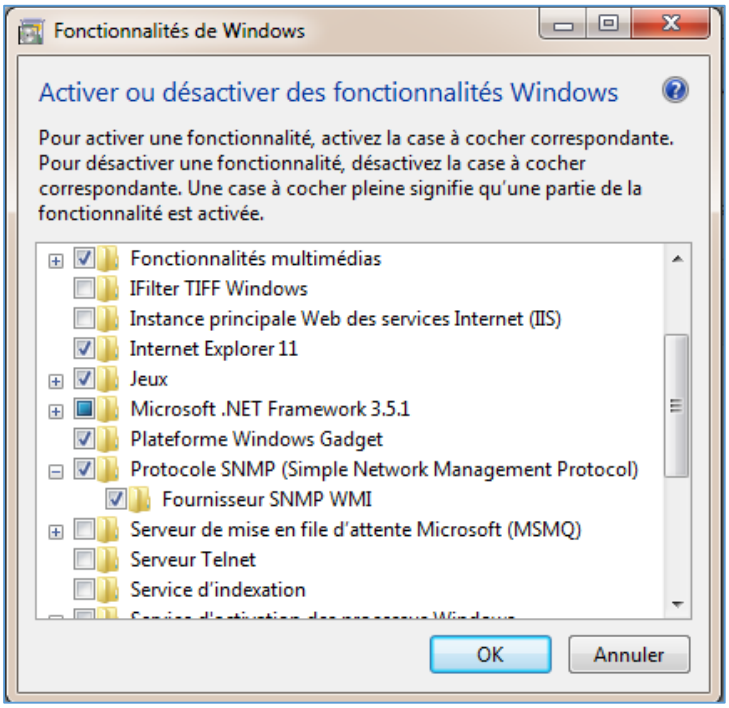

Figure 20: Fonctionnalités de Windows

Cocher le protocole SNMP simple Network Management Protocol. Ceci est nécessaire pour installer l'agent SNMP et d'autre service SNMP.

Il est normalement inutile d'avoir le fournisseur SNMP WMI. Le composant fournisseur de SNMP WMI permet aux applications WMI d'accéder aux informations SNMP (Simple Network Management) à travers WMI (Windows Management Instrumentation).

5.6 Configuration de l'agent

La configuration du service SNMP est effectuée par le biais de l'option de propriétés de service. Pour y accéder, ouvrez le panneau de configuration et sélectionner Outil d'administration (voir la Figure 21).

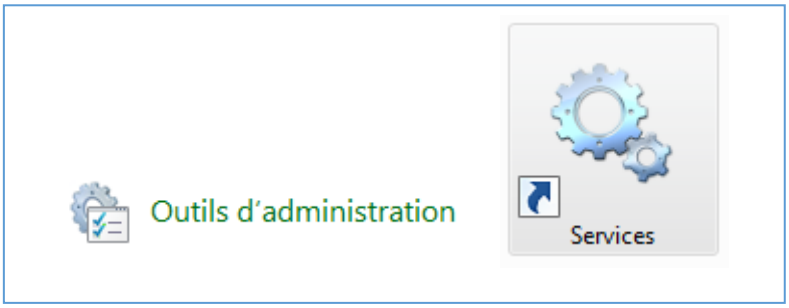

Figure 21: Outils d'administration et Service

Finalement sélectionner l'icône des Services puis la liste des services rechercher le service SNMP et double cliquer comme le montre la Figure 22.

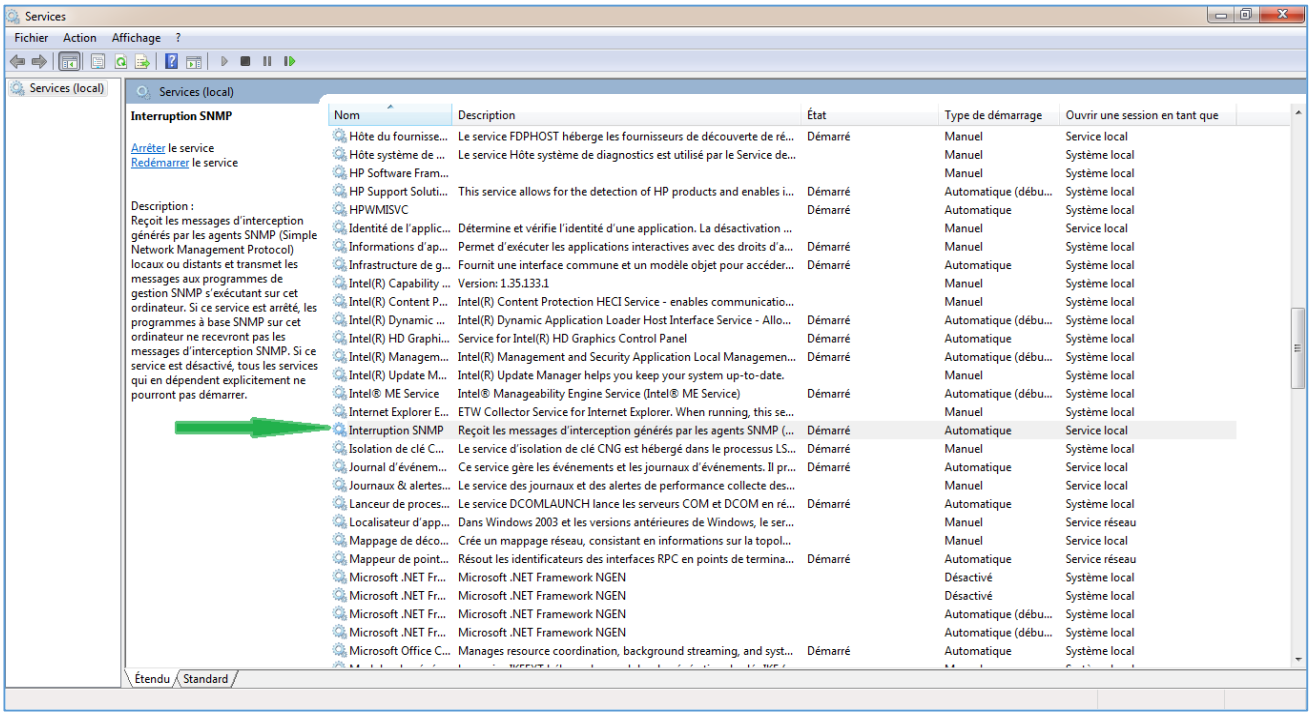

Figure 22: Service Interrogation SNMP

Le service Trap n'est pas utilisé pour envoyer des Traps SNMP mais seulement pour recevoir les Traps SNMP. S'il n'y a aucune application de réception du Traps sur ce système ne pas le démarrer.

En sélectionnant le service adéquat une fenêtre de propriétés de service SNMP est affichée comme le montre la Figure 23.

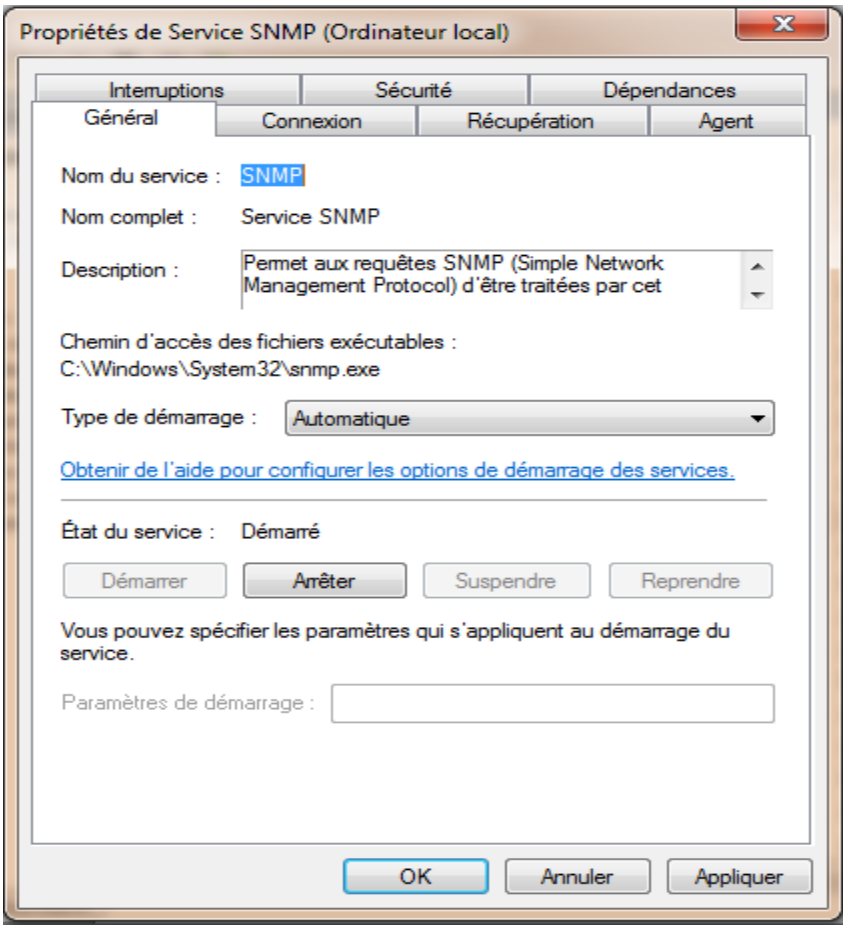

Figure 23: Propriétés de Service SNMP en Général

Vous pouvez aussi modifier le type de démarrage dans l'ongle **Récupération.**

Le processus SNMP s'exécute sous le compte système local ou un compte peut être spécifié, onglet **Connexion.**

Dans l'onglet Agent, les variables SNMP de la Mib2 system peuvent être définies (voir Figure 24).

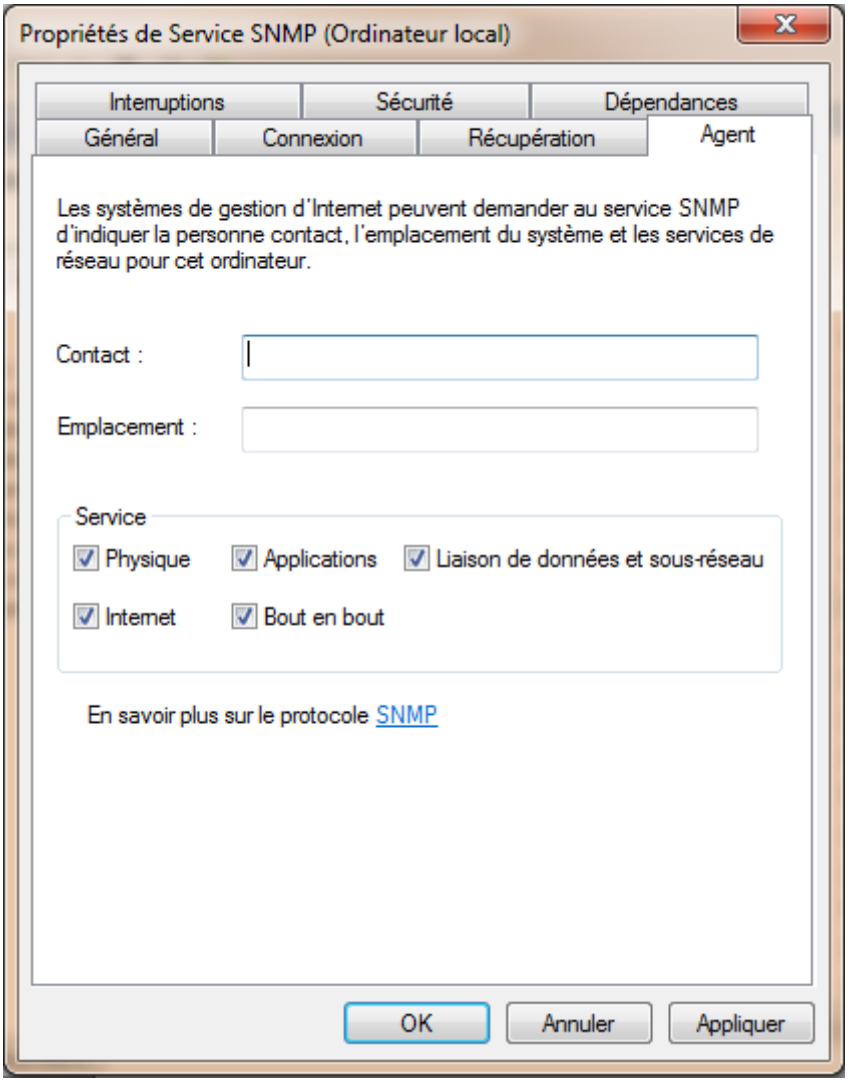

Figure 24: Propriétés de Service d'Agent SNMP

Spécification des propriétés de l'équipement. Vous pouvez définir ici la valeur standard mib2 ***syscontact*** et ***syslocation***. Le *sysname* est le nom de l'hôte et ne peut pas être modifiée ici (c'est le nom de la machine Windows).

Contact : Nom et les coordonnées de l'administrateur (objet *syscontact* de la mib2).

Emplacement : Emplacement du dispositif. Ici vous pouvez entrer l'adresse, le numéro de bâtiment, étage, salle, numéro de rack. (objet *syslocation*de la mib2)

Services : les propriétés avancées de l'agent indiquant les fonctions fournies par cet équipement : (objet *sysservices* de la mib2)

Physique : Cet équipement propose des services physiques au réseau, hub, répéteur Ethernet

Liaison de données et de sous-réseau : Cet équipement propose des services de liaison, par exemple, pont, (Couche 2 du modèle OSI).

Internet : Cet équipement propose des services de transport IP (Couche 3du modèle OSI)

End-to-end : Cet équipement propose des services de bout en bout (Protocole TCP). (Couche 4 du modèle OSI)

Applications : Cet équipement propose des services d'application, server d'application (couche 7 du modèle OSI)

Les modifications apportées ici modifient la valeur de l'objet SNMP **sysservices**
Iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1).sysServices(7)

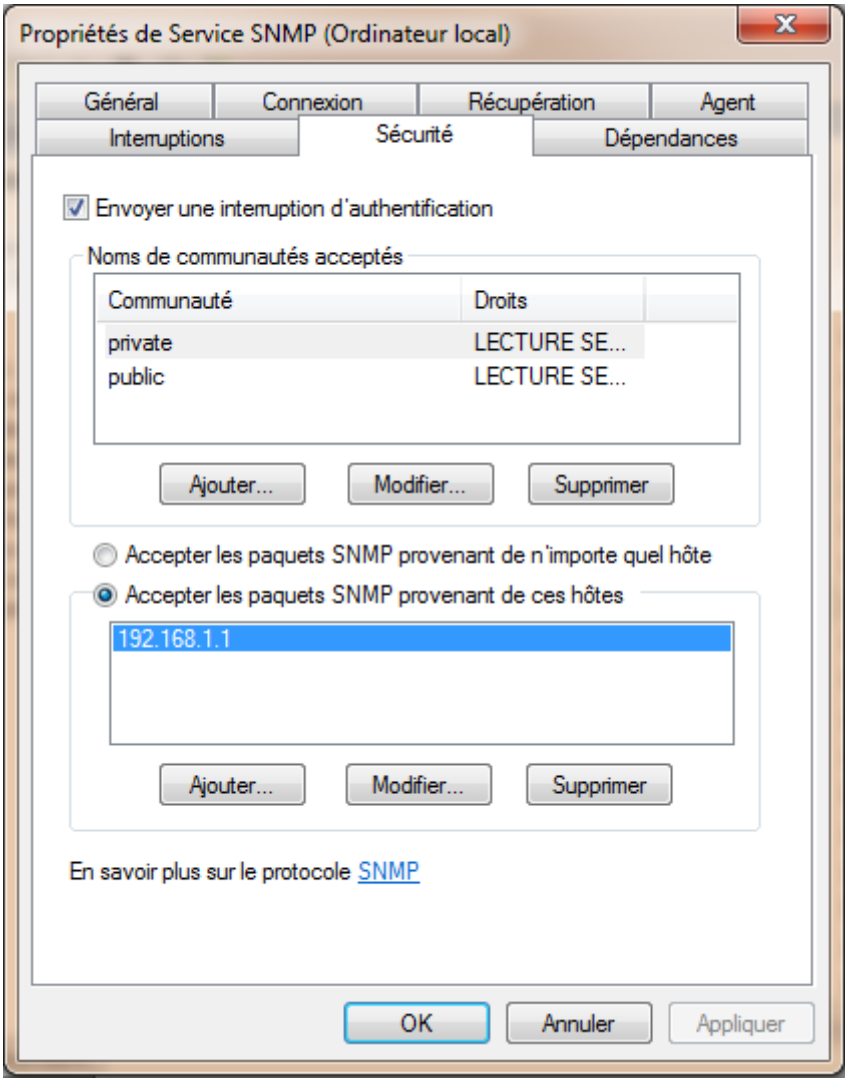

Figure 25: Propriétés de service Sécurité SNMP

Description de l'objet sysservices de la MIB2

Les options suivantes doivent être configurées pour activer la sécurité SNMP :

Nom de la communauté a accepté. Le services SNMP nécessite la configuration d'au moins un nom de communauté par défaut. Le nom **public** est généralement utilisé comme nom de la communauté parce que c'est le nom commun qui est universellement reconnu dans toutes les implémentations de SNMP. Vous pouvez supprimer ou modifier le nom de la communauté par défaut ou ajouter plusieurs noms de communauté. Si l'agent SNMP reçoit une demandé d'une communauté qui n'est pas sur cette liste, il peut générer un Trap d'authentification (option ci-après).Si aucun nom de la communauté n'est défini, l'agent SNMP refuse toutes les requetes entrantes SNMP en provenance des manager SNMP.

Autorisations. Vous pouvez sélectionner les niveaux d'autorisation qui déterminent la façon dont un agent traite les demandes SNMP de diverses communautés. Par exemple, vous pouvez configurer le niveau d'autorisation pour bloquer l'agent SNMP de traiter toute demande d'une communauté spécifique.

Accepter des paquets SNMP de n'importe quel hôte. Dans ce contexte, l'hôte de la source et la liste des hôtes acceptables consulter le système de gestion SNMP source et la liste des autres systèmes de gestion acceptable. Lorsque cette option est activée, aucuns les paquets SNMP ne sont rejetés, fondée sur le nom ou l'adresse de l'hôte source ou sur la base de la liste des hôtes acceptables. Cette option est activée par défaut.

Accepter uniquement les paquets SNMP provenant de ces hôtes. Cette option offre une sécurité limitée. Lorsque l'option est activée, seuls les paquets SNMP a reçu des hôtes sur une liste d'hôtes acceptables sont acceptés. L'agent SNMP rejette les messages des autres hôtes et envoie un piège d'authentification.

Envoyer des interruptions d'authentification. Lorsqu'un agent SNMP reçoit une demande qui ne contient pas un nom valide de communauté ou l'hôte qui envoie le message n'est pas sur la liste des hôtes accepter, l'agent peut envoyer un message Trap d'erreur d'authentification à un ou plusieurs destinations du Trap (manager SNMP).

5.7 Configuration d'un router

Activer le protocole SNMP il faut consulter l'adresse de router (l'adresse réseau par exemple 192.168.1.1) puis dans l'anglet management choisir SNMP dans le menu à gauche. Pour activer le SNMP, sélectionner énable (activé) puis activer Trap et entré Trap Manager IP.

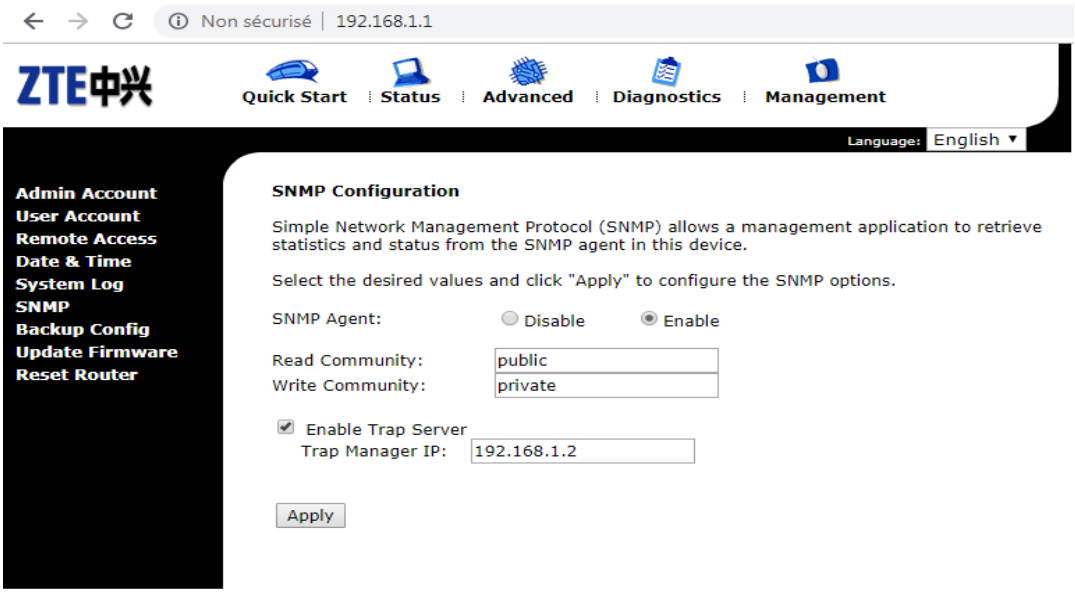

Figure 26: Exemple de configuration d'un modem Router

Remarquons que ces étapes sont liées au type de routeur utilisé car chaque routeur possède sa propre interface de configuration, nous pouvons aussi utiliser le mode SHELL pour activer le SNMP

6. Utilisation de l'application

Les points forts de notre application sont nombreux. Tout d'abord c'est un logiciel Libre. Il est aussi open source qui des objectifs de recherche scientifiques. L'application peut être recompilée dans la plateforme Windows ainsi que des versions RPM et Debian pour Linux. Elle supporte à la fois le protocole SNMP dans ses versions 1, 2c et 3. Elle permet d'envoyer des requêtes SNMP WALK.

L'application répartit les fonctionnalités principales en différents onglets. Le premier onglet **Tree** permet d'interroger un agent SNMP. La première partie correspond à l'agent qui sera interrogé. Ensuite, la deuxième partie **Discovery** sert à afficher le résultat du Scan de réseau.

La Figure 27 représente la première partie de l'application Discovery, qui permet de scanner les adresses IP des machines connectées dans le réseau, cette opération offre deux possibilités pour le scan :

- L'option Local subenet(s), permet de choisir un sous-réseau dans le quel l'une des interfaces de la machine locale est connecté, puis de scanner toutes les adresses IP des machines connectées dans ce dernier.
- L'option IP Network : nous permet de spécifier une plage d'adresses IP à scanner.

La barre de progression illustre le pourcentage du scan.

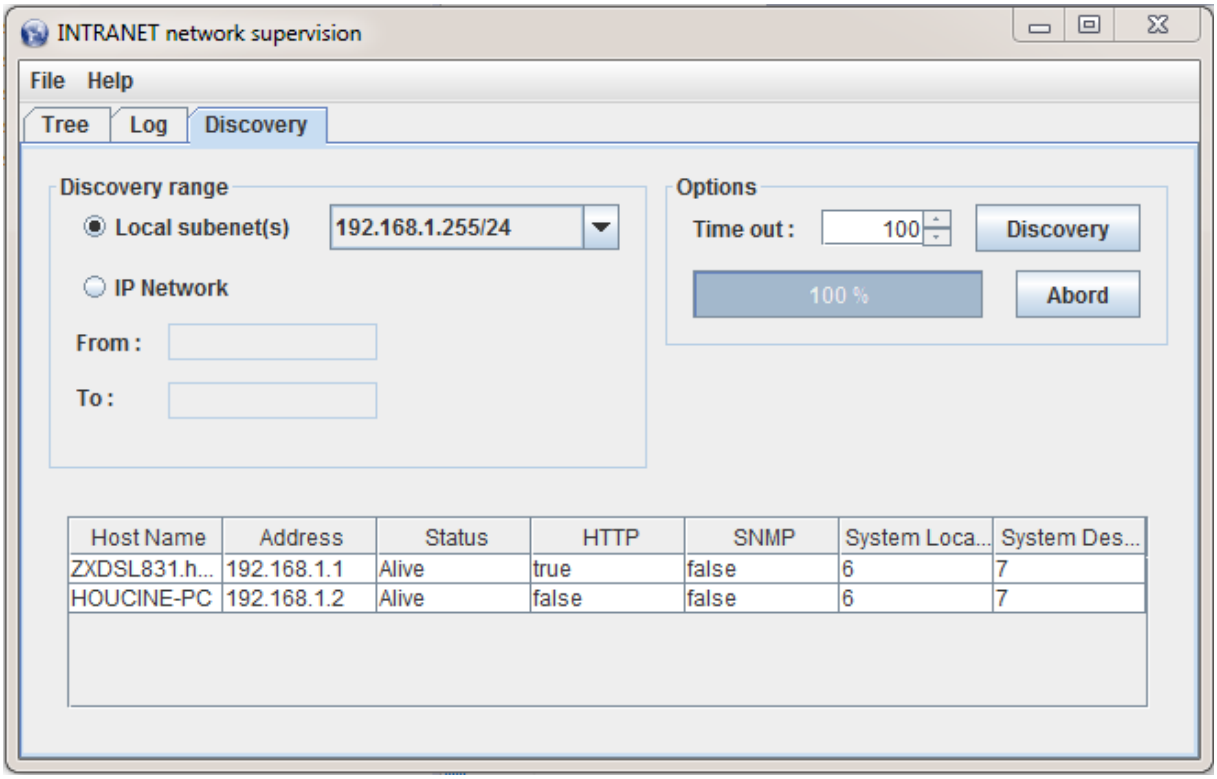

Figure 27: Scan des équipements du réseau

La Figure 28, Montre l'affichage obtenu dans le premier onglet. Afin de réaliser un walk SNMP, il faut tout d'abord choisir une adresse IP à partir de la liste (ComboBox), puis cliquer sur le bouton **Walk** pour lancer le scan, le bouton **abord** sert à annuler le scan SNMP. Le résultat de la requête est affiché dans le panel **Querry Result**.

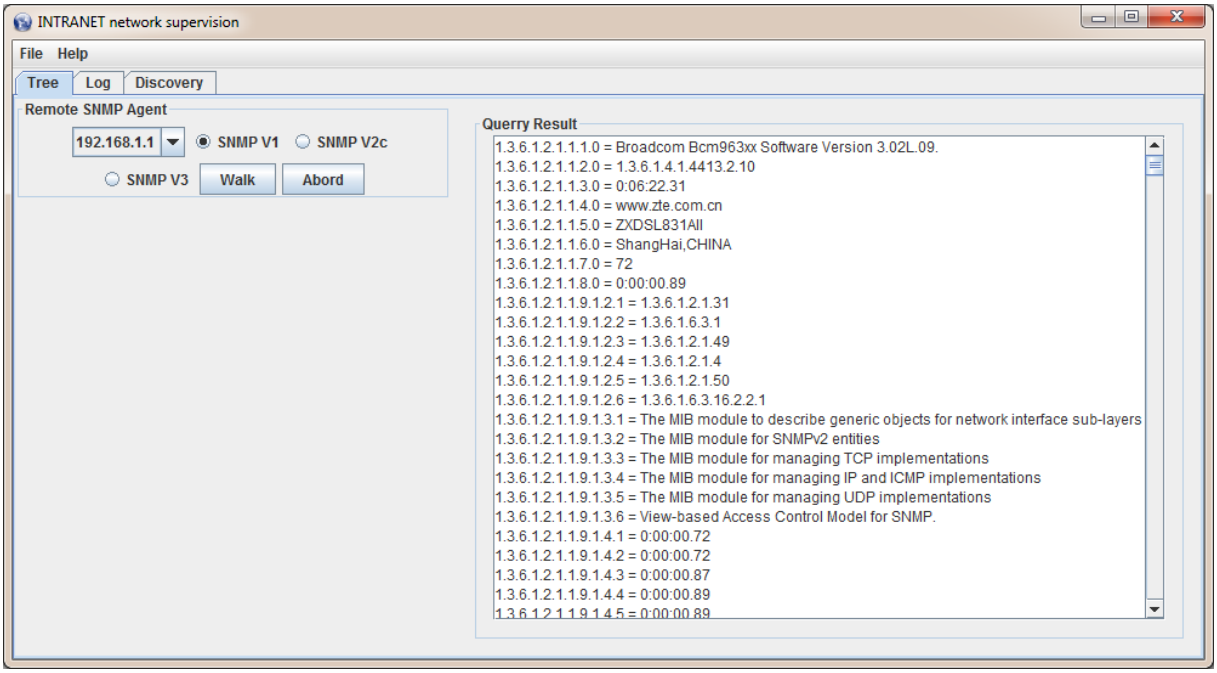

Figure 28: Interroger les équipements

7. Conclusion

Dans ce chapitre nous avons étudié les différents besoins fonctionnels d'une manière générale et qui peuvent être utiles dans une application de supervision, puis nous avons modélisé l'application grâce au langage UML pour avoir une présentation graphique et lisible de toutes les fonctionnalités possibles pour notre projet. Comme deuxième étape nous avons défini l'architecture de notre application pour pouvoir implémenter quelques fonctionnalités de base qui nous permet de scanner un réseau et interroger un de ces équipements afin d'obtenir l'ensemble d'informations nécessaire sur son état de fonctionnement.

A la fin, nous avons effectué quelques tests de validation et nous avons présenté quelques figures qui illustrent l'interface de notre application avec toutes les fonctionnalités possibles.

Conclusion Générale

Conclusion Générale

Ce projet de fin d'étude a été réalisé dans le but de réaliser une application fiable de supervision de différents équipements réseau intranet.

La réalisation de cette application a nécessité l'utilisation de toute une plateforme de développement et la maitrise des notions avancées de la configuration et la gestion des équipements réseau et a donné à son achèvement de bons résultat et a été conforme aux attentes.

Ce projet de fin d'étude, était sous forme d'une étude globale sur les besoins fonctionnels de la supervision, mais à cause de la limite de temps nous avons réalisé une tâche de tous les fonctionnalités possibles, que nous la voyons comme une tâche cruciale car elle nous permet de faire le suivi en temps réel des équipements réseau. Ce qui permettra aux différents utilisateurs et selon leur rôle de surveiller l'état de chacun des équipements (up/down, idle / faulty …), ce qui nous donne comme première perspective l'amélioration de l'application et la réalisation de tous les objectifs de la supervision.

Néanmoins, cette application restera ouverte à des améliorations et des optimisations tel que l'ajout d'une composante logicielle permettant l'accès à la cartographie réseau.

Bibliographie et Annexes

Bibliographie

[1] KAHLAOUI, Hatem. *Etude et Développement d'une Application de supervision du réseau de l'UBCI*. 2015. Thèse de doctorat. Université Virtuelle de Tunis.

[2] Devaloua Enoch, Mémoire : « Mise en place d'un réseau local avec connexion Internet », Abidjan, 2007

[3] PETIT, Bertrand. Architecture des réseaux. *Cours et exercices Corrigés*. Ellipses, 2006.

[4] SPALDING, George. *Windows 2000 administration*. McGraw-Hill, Inc., 2002...

[5] WELSH, Matt, DALHEIMER, Matthias Kalle, DAWSON, Terry, *et al. Le système Linux*. O'Reilly & Associates, Inc., 2003.

[6] VAN VUGT, Sander. *Pro Novell Open Enterprise Server*. Apress, 2006.

[7] PACHÉ, Gilles et PARAPONARIS, Claude. L'entreprise en réseau : approches inter et intra-organisationnelles. 2006.

[8] VU DUONG, Thang. *Découverte de chroniques à partir de journaux d'alarmes : application à la supervision de réseaux de télécommunications*. 2001. Thèse de doctorat. Toulouse, INPT.

[9] PRESUHN, Randy. *Transport Mappings for the Simple Network Management Protocol (SNMP)*. 2002.

[10] CHATZIMISIOS, Periklis. Security issues and vuluerabilities of the snmp protocol. In: *(ICEEE). 1st International Conference on Electrical and Electronics Engineering, 2004.* IEEE, 2004. p. 74-77.

Annexe

Document de normalisation SNMP par l'EITF

Network Working Group J. Case
Request for Comments: 1157 SNMP Research
Obsoletes: RFC 1098 M. Fedor
Performance Systems International
M. Schoffstall
Performance Systems International
J. Davin
MIT Laboratory for Computer Science
May 1990

A Simple Network Management Protocol (SNMP)

Table of Contents

1. Status of this Memo

This RFC is a re-release of RFC 1098, with a changed "Status of this Memo" section plus a few minor typographical corrections. This memo defines a simple protocol by which management information for a network element may be inspected or altered by logically remote users. In particular, together with its companion memos which describe the structure of management information along with the management information base, these documents provide a simple, workable architecture and system for managing TCP/IP-based internets and in particular the Internet.

The Internet Activities Board recommends that all IP and TCP implementations be network manageable. This implies implementation of the Internet MIB (RFC-1156) and at least one of the two recommended management protocols SNMP (RFC-1157) or CMOT (RFC-1095). It should be noted that, at this time, SNMP is a full Internet standard and CMOT is a draft standard. See also the Host and Gateway Requirements RFCs for more specific information on the applicability of this standard.

Please refer to the latest edition of the "IAB Official Protocol Standards" RFC for current information on the state and status of standard Internet protocols. Distribution of this memo is unlimited.

2. Introduction

As reported in RFC 1052, IAB Recommendations for the Development of Internet Network Management Standards [1], a two-prong strategy for network management of TCP/IP-based internets was undertaken. In the short-term, the Simple Network Management Protocol (SNMP) was to be used to manage nodes in the Internet community. In the long-term, the use of the OSI network management framework was to be examined. Two documents were produced to define the management information: RFC 1065, which defined the Structure of Management Information (SMI) [2], and RFC 1066, which defined the Management Information Base (MIB) [3]. Both of these documents were designed so as to be compatible with both the SNMP and the OSI network management framework.This strategy was quite successful in the short-term: Internet-based network management technology was fielded, by both the research and commercial communities, within a few months. As a result of this, portions of the Internet community became network manageable in a timely fashion. As reported in RFC 1109, Report of the Second Ad Hoc Network Management Review Group [4], the requirements of the SNMP and the OSI network

management frameworks were more different than anticipated. As such, the requirement for compatibility between the SMI/MIB and both frameworks was suspended. This action permitted the operational network management framework, the SNMP, to respond to new operational needs in the Internet community by producing documents defining new MIB items. The IAB has designated the SNMP, SMI, and the initial Internet MIB to be full "Standard Protocols" with "Recommended" status. By this action, the IAB recommends that all IP and TCP implementations be network manageable and that the implementations that are network manageable are expected to adopt and implement the SMI, MIB, and
SNMP. As such, the current network management framework for TCP/IP- based internets consists of: Structure and Identification of Management Information for TCP/IP-based Internets, which describes how managed objects contained in the MIB are defined as set forth in RFC 1155 [5]; Management Information Base for Network Management of TCP/IP- based Internets, which describes the managed objects contained in the MIB as set forth in RFC 1156 [6]; and, the Simple Network Management Protocol, which defines the protocol used to manage these objects, as set forth in this memo. As reported in RFC 1052, IAB Recommendations for the Development of Internet Network Management Standards [1], the Internet Activities Board has directed the Internet Engineering Task Force (IETF) to create two new working groups in the area of network management. One
group was charged with the further specification and definition of elements to be included in the Management Information Base (MIB).
The other was charged with defining the modifications to the Simple Network Management Protocol (SNMP) to accommodate the short-term needs of the network vendor and operations communities, and to align with the output of the MIB working group.
The MIB working group produced two memos, one which defines a Structure for Management Information (SMI) [2] for use by the managed objects contained in the MIB. A second memo [3] defines the list of managed objects.
The output of the SNMP Extensions working group is this memo, which incorporates changes to the initial SNMP definition [7] required to attain alignment with the output of the MIB working group. The changes should be minimal in order to be consistent with the IAB's directive that the working groups be "extremely sensitive to the need to keep the SNMP simple " Although considerable care and debate has gone into the changes to the SNMP which are reflected in this memo, the resulting protocol is not backwardly-compatible with its predecessor, the Simple Gateway Monitoring Protocol (SGMP) [8].
Although the syntax of the protocol has been altered, the original philosophy, design decisions, and architecture remain

intact. In order to avoid confusion, new UDP ports have been allocated for use by the protocol described in this memo.

3. The SNMP Architecture

Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management
stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements.

3.1. Goals of the Architecture

The SNMP explicitly minimizes the number and complexity of management functions realized by the management agent itself. This goal is attractive in at least four respects:

(1) The development cost for management agent software necessary to support the protocol is accordingly reduced.

(2) The degree of management function that is remotely supported is accordingly increased, thereby admitting fullest use of internet resources in the management task.

(3) The degree of management function that is remotely supported is accordingly increased, thereby imposing the fewest possible restrictions on the form and sophistication of management tools.

(4) Simplified sets of management functions are easily understood and used by developers of network management tools.

A second goal of the protocol is that the functional paradigm for monitoring and control be sufficiently extensible to accommodate additional, possibly unanticipated aspects of network operation and
management.

A third goal is that the architecture be, as much as possible, independent of the architecture and mechanisms of particular hosts or particular gateways.

3.2. Elements of the Architecture

The SNMP architecture articulates a solution to the network management problem in terms of:

(1) the scope of the management information communicated by the protocol,

(2) the representation of the management information communicated by the protocol,

(3) operations on management information supported by the protocol,

(4) the form and meaning of exchanges among management entities,

(5) the definition of administrative relationships among

management entities, and
(6) the form and meaning of references to management information.

3.2.1. Scope of Management Information

The scope of the management information communicated by operation of the SNMP is exactly that represented by instances of all non- aggregate object types either defined in Internet-standard MIB or defined elsewhere according to the conventions set forth in Internet-standard SMI [5].

Support for aggregate object types in the MIB is neither required for conformance with the SMI nor realized by the SNMP.

3.2.2. Representation of Management Information

Management information communicated by operation of the SNMP is represented according to the subset of the ASN.1 language [9] that is specified for the definition of non-aggregate types in the SMI.

The SGMP adopted the convention of using a well-defined subset of the ASN.1 language [9]. The SNMP continues and extends this tradition by utilizing a moderately more complex subset of ASN.1 for describing managed objects and for describing the protocol data units used for managing those objects. In addition, the desire to ease eventual transition to OSI-based network management protocols led to the definition in the ASN.1 language of an Internet-standard Structure of Management Information (SMI) [5] and Management Information Base (MIB) [6]. The use of the ASN.1 language, was, in part, encouraged by the successful use of ASN.1 in earlier efforts, in particular, the SGMP. The restrictions on the use of ASN.1 that are part of the SMI contribute to the simplicity espoused and validated by experience with the SGMP.

Also for the sake of simplicity, the SNMP uses only a subset of the basic encoding rules of ASN.1 [10]. Namely, all encodings use the definite-length form. Further, whenever permissible, non-constructor encodings are used rather than constructor encodings. This restriction applies to all aspects of ASN.1 encoding, both for the top-level protocol data units and the data objects they contain.

3.2.3. Operations Supported on Management Information

The SNMP models all management agent functions as alterations or

inspections of variables. Thus, a protocol entity on a logically
remote host (possibly the network element itself) interacts with the management agent resident on the network element in order to retrieve (get) or alter (set) variables. This strategy has at least two positive consequences:

(1) It has the effect of limiting the number of essential management functions realized by the management agent to two: one operation to assign a value to a specified configuration or other parameter and another to retrieve such a value.

(2) A second effect of this decision is to avoid introducing into the protocol definition support for imperative management commands: the number of such commands is in practice ever-increasing, and the semantics of such commands are in general arbitrarily complex.

The strategy implicit in the SNMP is that the monitoring of network state at any significant level of detail is accomplished primarily by polling for appropriate information on the part of the monitoring center(s). A limited number of unsolicited messages (traps) guide the timing and focus of the polling. Limiting the number of unsolicited messages is consistent with the goal of simplicity and minimizing the amount of traffic generated by the network management function.

The exclusion of imperative commands from the set of explicitly supported management functions is unlikely to preclude any desirable management agent operation. Currently, most commands are requests either to set the value of some parameter or to retrieve such a value, and the function of the few imperative commands currently supported is easily accommodated in an asynchronous mode by this management model. In this scheme, an imperative command might be realized as the setting of a parameter value that subsequently triggers the desired action. For example, rather than implementing a "reboot command," this action might be invoked by simply setting a parameter indicating the number of seconds until system reboot.

3.2.4. Form and Meaning of Protocol Exchanges

The communication of management information among management entities is realized in the SNMP through the exchange of protocol messages. The form and meaning of those messages is defined below in Section 4.

Consistent with the goal of minimizing complexity of the management agent, the exchange of SNMP messages requires only an unreliable datagram service, and every message is entirely and independently represented by a single transport datagram. While this document specifies the exchange of messages via the UDP protocol [11], the mechanisms of the SNMP are generally suitable for use with a wide variety of transport services.

3.2.5. Definition of Administrative Relationships

The SNMP architecture admits a variety of administrative relationships among entities that participate in the protocol. The entities residing at management stations and network elements which communicate with one another using the SNMP are termed SNMP application entities. The peer processes which implement the SNMP,and thus support the SNMP application entities, are termed protocol entities.

A pairing of an SNMP agent with some arbitrary set of SNMP application entities is called an SNMP community. Each SNMP community is named by a string of octets, that is called the community name for said community.

An SNMP message originated by an SNMP application entity that in fact belongs to the SNMP community named by the community component of said message is called an authentic SNMP message. The set of rules by which an SNMP message is identified as an authentic SNMP message for a particular SNMP community is called an authentication scheme. An implementation of a function that identifies authentic SNMP messages according to one or more authentication schemes is called an authentication service.

Clearly, effective management of administrative relationships among SNMP application entities requires authentication services that (by the use of encryption or other techniques) are able to identify authentic SNMP messages with a high degree of certainty. Some SNMP implementations may wish to support only a trivial authentication service that identifies all SNMP messages as authentic SNMP messages. For any network element, a subset of objects in the MIB that pertain to that element is called a SNMP MIB view. Note that the names of the object types represented in a SNMP MIB view need not belong to a single sub-tree of the object type name space.
An element of the set { READ-ONLY, READ-WRITE } is called an SNMP access mode.
A pairing of a SNMP access mode with a SNMP MIB view is called an SNMP community profile. A SNMP community profile represents specified access privileges to variables in a specified MIB view. For every variable in the MIB view in a given SNMP community profile, access to that variable is represented by the profile according to the following conventions:
(1) if said variable is defined in the MIB with "Access:" of "none," it is unavailable as an operand for any operator;
(2) if said variable is defined in the MIB with "Access:" of "read-write" or "write-only" and the access mode of the given profile is READ-WRITE, that variable is available as an operand for the get, set, and trap operations;
(3) otherwise, the variable is available as an operand for the get and trap operations.
(4) In those cases where a "write-only" variable is an operand used for the get or trap operations, the value given for the variable is implementation-specific.
A pairing of a SNMP community with a SNMP community profile is called a SNMP access policy. An access policy represents a specified community profile afforded by the SNMP agent of a specified SNMP community to other members of that community. All administrativerelationships among SNMP application entities are architecturally defined in terms of SNMP access policies.
For every SNMP access policy, if the network element on which the SNMP agent for the specified SNMP community resides is not that to which the MIB view for the specified profile pertains, then that policy is called a SNMP proxy access policy. The SNMP

agent associated with a proxy access policy is called a SNMP proxy agent.
While careless definition of proxy access policies can result in
management loops, prudent definition of proxy policies is useful in at least two ways:
(1) It permits the monitoring and control of network elements which are otherwise not addressable using the management protocol and the transport protocol. That is, a proxy agent may provide a protocol conversion function allowing a management station to apply a consistent management framework to all network elements, including devices such as modems, multiplexors, and other devices which support different management frameworks.
(2) It potentially shields network elements from elaborate access control policies. For example, a proxy agent may implement sophisticated access control whereby diverse subsets of variables within the MIB are made accessible to different management stations without increasing the complexity of the network element.
By way of example, Figure 1 illustrates the relationship between
management stations, proxy agents, and management agents. In this example, the proxy agent is envisioned to be a normal Internet Network Operations Center (INOC) of some administrative domain which has a standard managerial relationship with a set of management agents.

Domain: the administrative domain of the element
PCommunity: the name of a community utilizing a proxy agent
DCommunity: the name of a direct community

Figure 1
Example Network Management Configuration

Résumé

La supervision est une tâche cruciale dans le domaine de la sécurité réseau, elle nous permet d'avoir un contrôle sur l'ensemble des équipements et les activités qui se déroulent au sein du réseau, Pour cette raison nous avons réalisé une application qui nous permet d'aider les administrateurs réseau à contrôler poursuivre l'utilisation et l'état des équipements en temps réel et d'une manière permanente, ce qui est très utile pour eux pour garantir et assurer une bonne qualité de service.

Dans ce projet de fin d'études nous avons fait une étude complète sur la supervision d'une manière générale pour pouvoir modélise un système général de supervision et qui peut être une plate-forme pour d'autre projet connexes.

Abstract

Supervision is a crucial task in the field of network security, it allows us to have control over all equipment and activities that take place within the network, for this reason we have made an application that allows us to help network administrators to get a continued control of their equipment in real-time, which is very useful for them as a guarantees and ensure a good quality of service.

In this end-of-studies project we did a comprehensive study of supervision in general to be able to model a general supervision system and which can be a platform for other related projects.

ملخص

الإشراف هوخطوة مهمة وحاسمة في مجال أمن الشبكات ، فهو يتيح لنا التحكم في جميع المعدات والأنشطة التي تحدث داخل الشبكة ، ولهذا السبب قمنا بإنشاء تطبيق يتيح لنا لمساعدة مسؤولي الشبكة على التحكم في الاستخدام المستمر والإطلاع على حالة المعدات في الوقت الفعلي وبصفة مستمرة ، وهو أمر في غاية الأهمية لمسؤولي الشبكة لضمان جودة الخدمة.

في هذا المشروع النهائي للتخرج ، قمنا بإجراء دراسة شاملة للإشراف والمراقبة بشكل عام لنكون قادرين على تصميم نظام إشراف عام ويمكن أن يكون منصة للمشاريع الأخرى ذات الصلة.