MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du Diplôme de Master en Electronique
Option : Réseaux et Télécommunications

Thème :

Etude et conception d'une plateforme de réseau informatique couplant entre sécurité et supervision pour l'entreprise ENIEM

Proposé par :
M^r BOUTALEB Salim

Réalisé par :
M^elle BELHADJ Naïma

Dirigé par :
M^r LAHDIR Mourad

2012/2013

Remerciements

Je tiens à exprimer mes reconnaissances et gratitudes à M. LAHDIR Mourad, pour son encadrement. Je tiens aussi à remercier M.BOUTALEB Salim qui a accepté de diriger mes travaux tout au long de mon stage à l'ENIEM, et qui m'a toujours soutenu et fourni l'aide nécessaire afin de pouvoir réaliser mes objectifs dans les meilleures conditions.

Je souhaite par ailleurs souligner la contribution importante de l'équipe du département informatique, particulièrement Mme. SEDDIKI, Mme. DJELOUAH, et M. KHALDI le chef de service exploitation informatique, l'expertise de cette équipe a toujours été d'un précieux recours.

Je tiens à remercier également ma famille et mes amis qui m'ont soutenu, et particulièrement HAMOUNI. S, DOUANI. D, et ABTOUT. N, et tous ceux qui m'ont aidé de près ou de loin à réaliser ce modeste travail.

Merci.

DEDICACES

Je dédie ce modeste travail :

A Mes très chers parents et à ma grand-mère qui m'ont soutenu tout au long de mes études et qui ont contribué à ma réussite, que dieu les garde et leur donne une longue vie afin que je puisse leurs faire du bien à mon tour, et les rendre fières.

A Mes grands parents maternels, et à toutes ma petite famille.

A Mes frères : Noreddine, Djamel, Ghiles avec qui j'ai passé les meilleurs moments de mon existence ;

A tous mes amis : Dihya.M, Dihya, Katia.M, Katia.H, Rosa, Sihem.Z, Naima, Dalila, Nadjia, Nouara, Sihem, zahoua, Said.H, Hocine.M, Said.B, Lyes.B, DjamelA, Sofiane.H, Chabane.B, Djamel.H, Lotfi.H.

℘ Résumé ℜ

✍ L'objectif principale de notre mémoire consiste à étudier et concevoir une solution permettant de sécurisé et de supervisé le réseau informatique de l'entreprise national ENIEM

✍ Cette étude comporte deux grandes parties : une partie bibliographique et une autre réservée à la conception et les tests des solutions apportées à la maquette de réseau vulnérable (chapitre v).

- ✍ Dans le premier chapitre sont exposées le cadre et le contexte du projet: présentation de l'organisme d'accueil, l'architecture du réseau existant, le champ d'étude, …etc.
- ✍ Le deuxième chapitre est consacré pour les réseaux informatiques d'entreprises
- ✍ Le troisième chapitre traite la sécurité informatique : les risques, les menaces, la politique de sécurité, les mécanismes de sécurité...
- ✍ Le quatrième chapitre est réservé à la supervision des réseaux informatiques.
- ✍ Le cinquième chapitre est réservé pour la conception de la solution et les tests.
- ✍ Enfin, nous terminons notre travail par une conclusion générale et des perspectives sur le travail.

Listes des figures et des tableaux

Liste des figures :

Liste des tableaux :

Sommaire

Sommaire

Chapitre IV : La supervision des réseaux

Chapitre V: Conception et test de l'infrastructure de solution

Introduction générale

Introduction générale

Un système d'information (SI) est généralement l'ensemble des moyens nécessaires pour acquérir, stocker, exploiter, et faire circuler des informations. Le besoin de faire fonctionner ce genre de systèmes a abouti à la conception d'un moyen technique, plus connus sous « système informatique ». En effet, un SI représente un patrimoine essentiel de chaque entreprise ou organisation, qu'il convient de préserver et de protéger, et cela ne devient possible, qu'une fois que les insuffisances de sécurité du système informatique sont bien comblées. Le système informatique représente ainsi l'unité minimale d'un réseau informatique, La sécurité de celui-ci fait l'objet de préoccupation des administrateurs.

Les réseaux informatiques, considérés comme éléments essentiels des technologies actuelles pour raccorder les systèmes d'informations et assurer ainsi les transmissions des données entre sites informatiques. Les organisations et entreprises comptent beaucoup sur les services offerts par ces réseaux, ces services sont devenus très vite indispensables pour leurs fonctionnements, en effet ceux-là leur apportent un moyen efficace pour mettre en œuvre un travail coopératif, pour partager des données, mais aussi pour imprimer à distance, envoyer des messages, et accéder à des bases de données localisées ou délocalisées. Pour s'assurer que les services rendus par le réseau informatique d'entreprises soient convenables, il est nécessaire de le sécuriser et le surveiller et d'agir quand une erreur se produit. Pour ce faire, il faut obtenir les données de gestion des équipements des réseaux et, si nécessaire, contrôler ces équipements, d'où l'utilité de recourir aux outils de supervision des réseaux.

Cependant, un des principaux enjeux de la supervision de réseaux est ainsi de réussir à offrir une solution unique permettant de gérer son réseau. L'ampleur des réseaux pouvant varier grandement : que l'on parle d'un réseau d'un opérateur et fournisseur ou bien que l'on parle du réseau interne d'une petite entreprise, la supervision doit pouvoir apporter des outils performants, adaptables aussi bien à la taille des réseaux qu'à leur grande diversité technologique.

Un autre enjeu est l'automatisation du traitement de l'information. En effet, face à l'importance (taille et criticité) des réseaux dans tous les milieux professionnels, il reste difficile de prendre connaissance de toutes les informations et de réagir proactivement. Des lors, l'automatisation de l'analyse des informations remontées par la supervision permet la mise en place de statistiques et de procédures pour la résolution des problèmes.

Ce projet a été réalisé dans le cadre de la conception d'une infrastructure de gestion associée à une politique de sécurité adéquate au niveau du réseau informatique de l'ENIEM. Il consiste à implémenter une politique de sécurité après une étude préalable des différents risques et anomalies, et à concevoir et mettre en place un système de supervision réseaux conforme avec les fondements de cette politique de sécurité, ce système permettra à la fois, de **collecter** des données sur les routeurs, les serveurs et les commutateurs et autres, **afficher** une cartographie du réseau, et **notifier** en cas de panne d'un équipement ou en cas d'éventuelles tentative d'intrusion.

Les responsables informatiques de l'ENIEM m'ont donc proposé pour palier aux différents problèmes coexistants au tour du réseau de cette entreprise, de réaliser un outil d'observation et de contrôle réseau où la sécurité et la supervision seront couplées, qui s'adaptera à la fois avec la topologie du réseau existant et avec les applications et les systèmes qui tournent sur ce réseau.

Le présent travail est structuré en cinq chapitres :

Dans le premier chapitre je décris le cadre et le contexte de mon projet. Tout d'abord je présente mon organisme d'accueil et l'architecture du réseau de cette entreprise, en me basant plus sur mon champ d'études qu'est le département informatique, d'où j'extraie le problème de mon projet. Ensuite, je traite le sujet du travail à réaliser.

Dans le second chapitre, troisième, et quatrième chapitre, je spécifie les différents besoins, respectivement en termes de réseaux informatiques d'entreprise, puis sur la sécurité informatique, et enfin, en supervision des réseaux informatiques.

Dans le cinquième et dernier chapitre, je présente les spécifications de ma solution, l'étude conceptuelle de cette application, ainsi que la description de l'implémentation et les testes de mon application sur une plateforme de tests que je réaliserais.

En fin, Je conclus ce mémoire en présentant les avantages apportés par l'application réalisée.

Les formats des PDU (Protocol data Unit) et le lexique des commande Cisco sont décrit dans les annexes de ce mémoire.

CHAPITRE 1

Cadre du projet

Introduction

Ce chapitre représente une mise dans le contexte du projet de fin d'étude intitulé conception et test d'une infrastructure de supervision couplée avec une politique de sécurité adéquate aux réseaux informatiques de l'ENIEM.

La première partie se focalise sur le cadre du projet à travers une présentation de l'organisme d'accueil. La deuxième et la troisième partie, une définition du travail demandé et les problématiques qu'il doit résoudre.

I.1. Cadre et contexte du projet

I.1.1. Présentation de l'organisme d'accueil « ENIEM »

I.1.1.1. Situation géographique

L'entreprise ENIEM (Entreprise Nationale des Industries de Electroménagers) se trouve à la zone industrielle AISSAT - IDIR OUED - AISSI à 10 Km de TIZI - OUZOU, elle s'étale sur une surface totale de 55 Hectares, sa direction générale se trouve au Chef lieu de TIZI - OUZOU à proximité de la gare ferroviaire.

I.1.1.2. Activités et objectifs de l'entreprise

- **Activités :** Les activités de l'ENIEM sont concentrées sur la production, le montage, la commercialisation, le développement et la recherche dans les différentes branches de l'électroménager. Ces activités sont assurées par ses cinq unités:
  - ***Unité Froid (***Produit des Réfrigérateurs et congélateurs).
  - ***Unité Cuisson (***Assure la production des cuisinières).
  - ***Unité Climatisation (***Produit des climatiseurs, machines à laver, et des chauffes eau).
  - ***Unité Commerciale*** (Assure la distribution et l'exportation des produits ENIEM, ainsi que le service après-vente).
  - ***Unité Prestations Techniques*** (Assure les fonctions de soutien aux autres unités).

- **Objectifs :**

  - L'amélioration de la qualité et l'augmentation du volume de production.
  - La maitrise des coûts de production.
  - L'augmentation des capacités d'études et de développement.
  - Amélioration de la maintenance de l'outil de production des installations.
  - La valorisation des ressources humaines.

I.1.2. Organisation de l'entreprise

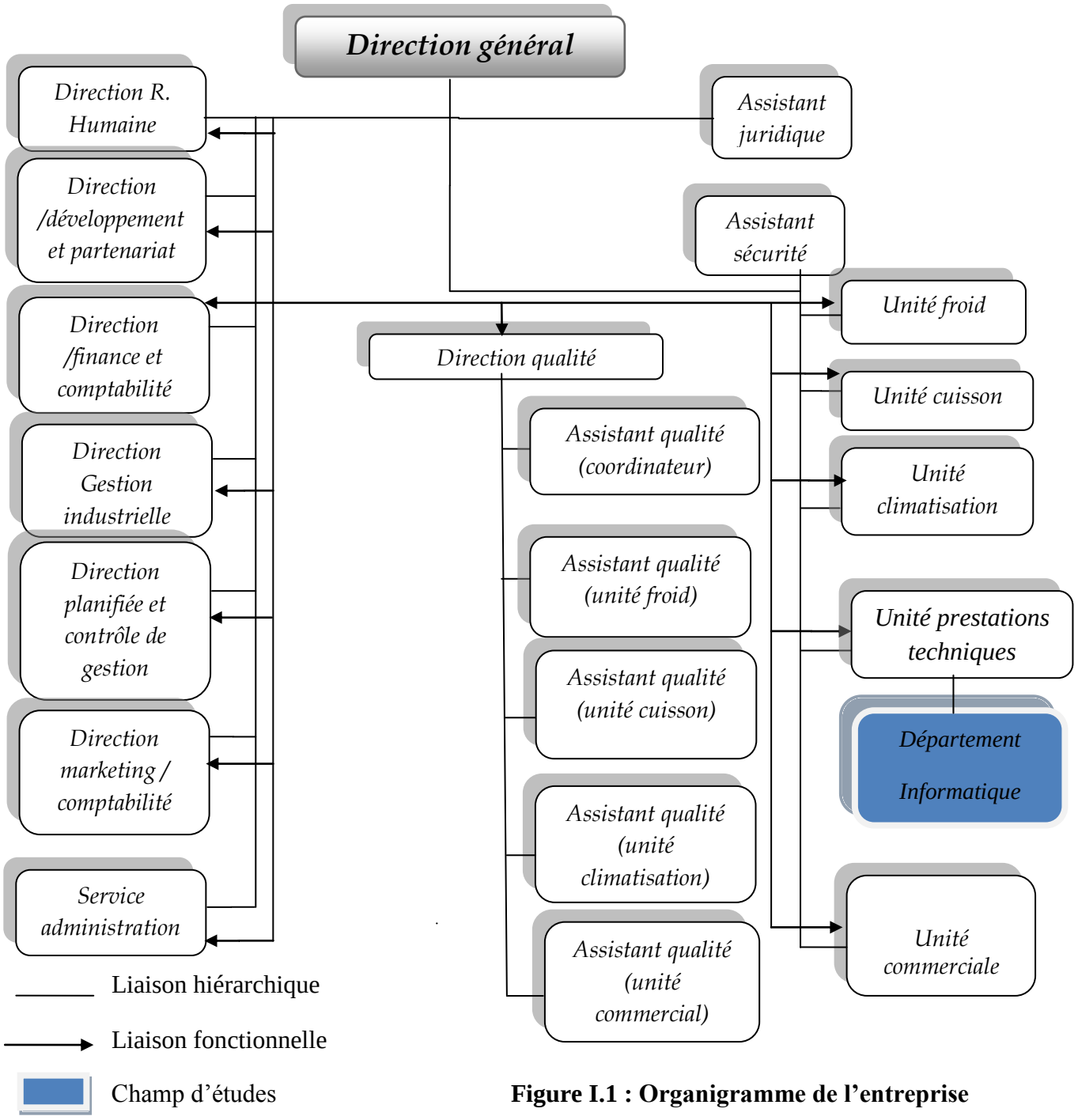

Figure I.1 : Organigramme de l'entreprise

I.1.3. Le champ d'études

I.1.3.1. Organigramme de l'unité de prestations techniques

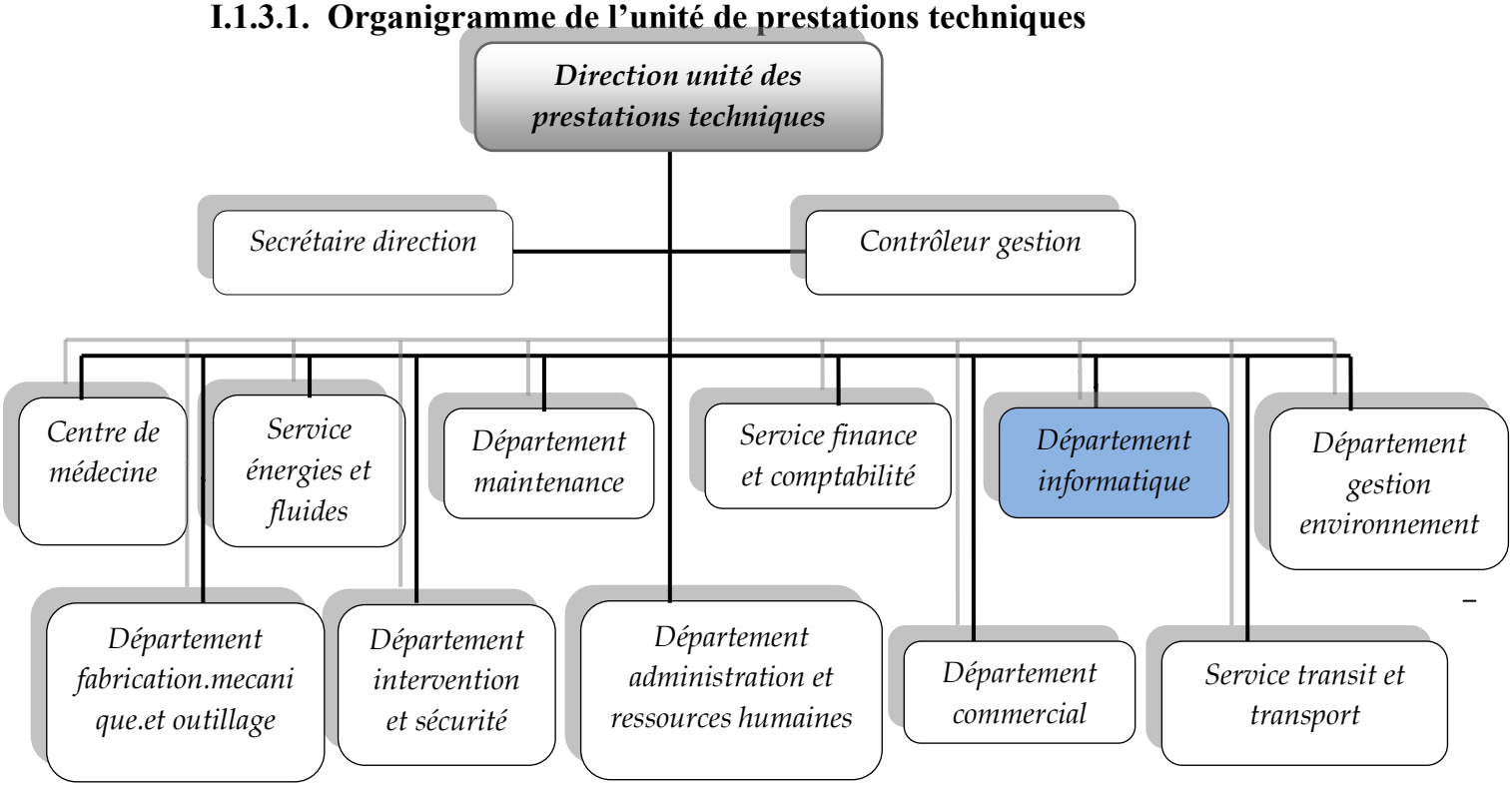

Figure I.2 : Organigramme de l'unité des prestations techniques

I.1.3.2. Organigramme du département informatique (champ d'études)

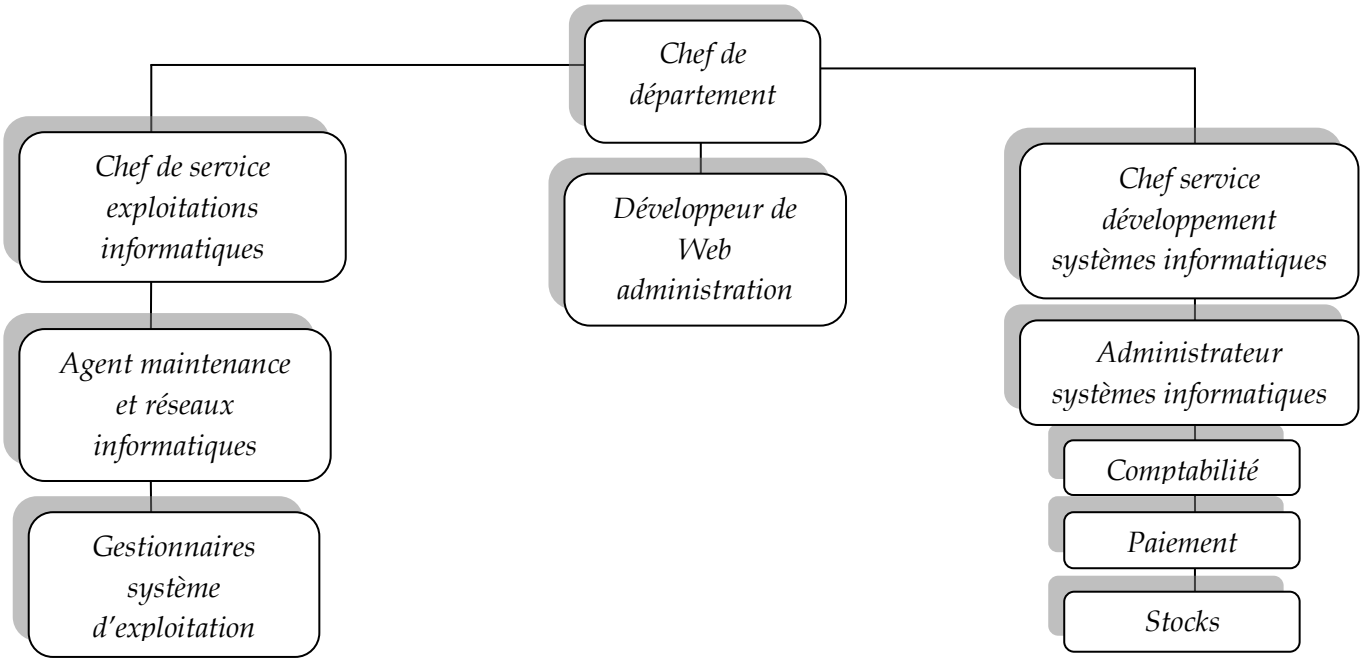

Figure I.3 : Organigramme du champ d'études

I.1.3.3. Description du département informatique

Le département informatique assure les prestations qui répondent aux attentes des utilisateurs internes en termes de fiabilités, sécurités et délai. Il dispose de :

- 12 postes (type: HP, CPU: 2, 40GHz, Disque dur: 40 à 80 Go, RAM: 128 Mo à 1 Go).
- Imprimantes : 04 de type HP petite taille, 04 de grande taille (03 de type **PRINTRANIX** et 01 de type **MAGNA L182OC**).
- **02** grandes stations de climatisation pour la salle-machine (types **AIRWELL 3900**).
- Grand onduleur (type **Emerson Network Power**)

Le département informatique se départage en deux services :

- Service développement du système informatique (**SDSI**).
- Service exploitation informatique (**SEI**).

1. **Service développement informatique :**

Ce service s'occupe du développement des applications et des programmes informatiques. Il est constitué de deux sous services, le premier est chargé de la conception développement informatique et le deuxième s'occupe de l'administration des systèmes informatiques.

2. **Service exploitations informatiques :**

S'occupe de la gestion de l'ensemble des moyens informatiques, de saisie, de traitement, de transmission et de restitution de l'information et assistance aux utilisateurs. Ce service est composé de deux sous services, l'un est celui du chef de la salle machine qui est le responsable du système, à son siège, on trouve des «gestionnaires système ». L'autre est le chef de section gestion des systèmes d'exploitation qui est le responsable du système hardware Software et des réseaux, il doit assurer le bon fonctionnement des équipements (suive des contrats de maintenance et procède au planning maintenance préventive), procède à des évolutions techniques, réseau, télétraitement, base de données, logiciels de bases etc, celui-ci doit aussi assurer la fonction de conseille et d'interfaçage avec l'utilisateur (attaché au chef de salle machine), à son siège on trouve des « Agents réseau informatique ».

I.1.3.4. Missions et activités du département informatique

Le département informatique s'occupe :

- De traiter des commandes d'achats ;
- De la comptabilité générale ;
- Du lancement des commandes en fabrication ;
- De la gestion des stockes de matière première et composant ;
- De la gestion de paie ;
- De l'établissement des procédures de sauvegarde et de restauration des données ;
- D'informer et de former les utilisateurs à l'exploitation optimale des applications.

I.1.4. Le réseau informatique de l'ENIEM

L'entreprise est dotée d'un réseau intranet, et comme cella est constituée des ateliers et du bloc administratif, elle englobe deux types de réseaux : réseau point à point des ateliers ; réseau local Ethernet(en étoile) du bloc administratif.

I.1.4.1. Réseau des ateliers

Le réseau utilisé au niveau des ateliers est un **réseau point à point** (pear to pear), il est composé d'environ 39 terminaux dont 27 écrans HP (modèle 700/92 A, 2392A) et 12 imprimantes HP (modèle 2563B, 2934 A, Rugged Writer 480) reliés au serveur (HP3000/A500) par des liaisons :

- Directes (distances inférieures ou égales à 1200 mètres).
- Modem-modem (pour les distances supérieures à 1200 mètres).
- Multiplexeur-modem (pour les installations de plusieurs terminaux distants).

I.1.4.2.Réseau du bloc administratif

Le réseau informatique intranet de l'ENIEM est un réseau ouvert basé sur la famille des protocoles TCP/IP. Un **réseau Ethernet** dont la topologie choisie est « étoile », vue la configuration du site, à savoir deux bâtiments associés donnant une formes T.

Toutes les prises d'un même étage sont reliées à un Switch contenu dans une armoire dite « armoire d'étage », cette dernière est reliée à son tour avec un câble fibre optique à un Switch dit « fédérateur » contenu dans l'armoire centrale installée au niveau de la salle machine au sous-sol du bâtiment B où le Switch du département informatique es aussi inclue.

Le réseau est composé au total de 06 armoires départagées dans 02 bâtiments, deux à chaque étage. L'emplacement est dicté par la distance maximale entre un Switch et un poste de travail, qui ne doit pas dépasser 100 mètres.

- **Description du matériel utilisé dans le réseau local**
  - **L'armoire de brassage centrale (voir figure I.2) :**

C'est l'armoire principale, toutes les armoires d'étage sont reliées à celle-ci, l'interconnexion est assurée grâce au Switch fédérateur. Elle est constituée des éléments suivants :

- 02 panneaux de brassage à 16 ports : contiennent des connecteurs RJ45.
- 01 Switch d'étage Cisco : contient des ports RJ45 et des ports GBIC (pour câble fibre optique).
- 01 onduleur: pour avoir le temps à sauvegarder les données.
- 01 Switch fédérateur: contient 7 ports GBIC.
- 03 tiroirs optiques: qui relient les armoires des blocs.
- 01 Panneau électrique à 06 prises sous onduleur: pour alimenter les périphériques actifs.

Cette figue présente l'armoire centrale située au département informatique au sous-sol (salle machines) :

Figure I.4 : L'armoire de brassage centrale

- **L'armoire d'étage (voir figure I.5)**

Elle est constituée des éléments suivants :

- ✧ Switch Cisco.
- ✧ panneau de brassage, le grand à 16 ports.
- ✧ 01 tiroir optique.
- ✧ 01 multi-prise.

Figure I.5: L'armoire d'étage

- **Description du système du serveur HP3000/A500 :**

a- La face arrière (voir figure I.6)

Le serveur est composé de DTC (Data Terminal Circuit) qui gère deux types de panneaux, DDP (Panneau de Distribution Direct) et MDP (Panneau de Distribution Modem).

- ✧ Les ports sur le DDP sont du type RJ45 (norme RS423) et numérotés de 100 à 115, 200 à215 pour les ports écrans et de 300 à 315 pour les ports imprimantes.
- ✧ Les ports sur le MDP sont du type DB25 (norme RS232) et numérotés de 400 à 415, de 500 à 515 pour les ports écrans et de 600 à 615 pour les ports imprimantes.

La face arrière des ports DTC est composée des ports AUI et des ports BNC T (Thinlan port) et chacun de ces derniers sont connectés entre eux avec un câble coaxial qui est connecté à son tour au convertisseur Ethernet (10 base 2 to 10 base T). La sortie du convertisseur est un port RJ45, qui est connecté à l'armoire centrale.

Il est aussi équipé d'une unité centrale dont la face arrière est rassemblée de :

- ✧ Console UPS port qui peut être connecté à 3 consoles sorties DB9 avec des câbles HP24252 :
  - ✦ UPS : pour brancher l'onduleur.

- ✦ Rempote : c'est une console secondaire, elle est mise en marche lorsque la console principale se bloque.
- ✦ Console principale.

✧ Une console LAN 10 base T (console réseau).
✧ Le dérouleur : pour lire les cartes de l'ancien système.

b- La face avant (voir figure I.7)

Elle est composée des éléments suivants :

✧ Lecteur de cassettes DLT.
✧ Lecteur DVD.
✧ Lecteur DDS.

Figure I.7 : La face avant du serveur

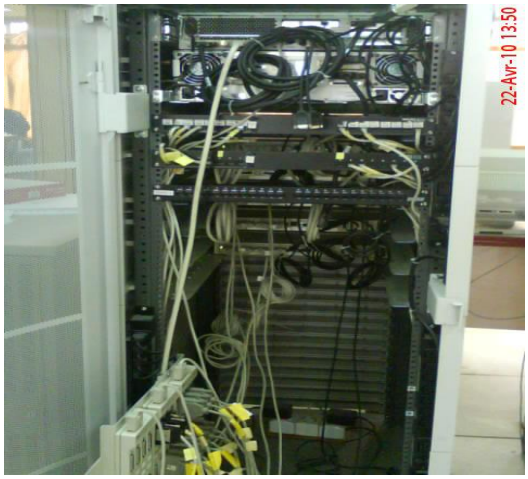

Figure I.6 : La face arrière du serveur

I.2. Étude et analyse de l'existant et problématiques

Cette partie permet de mieux définir le domaine d'étude, ainsi qu'à relever les éventuels manques et anomalies dans le système existant.

I.2.1. L'architecture du réseau existant

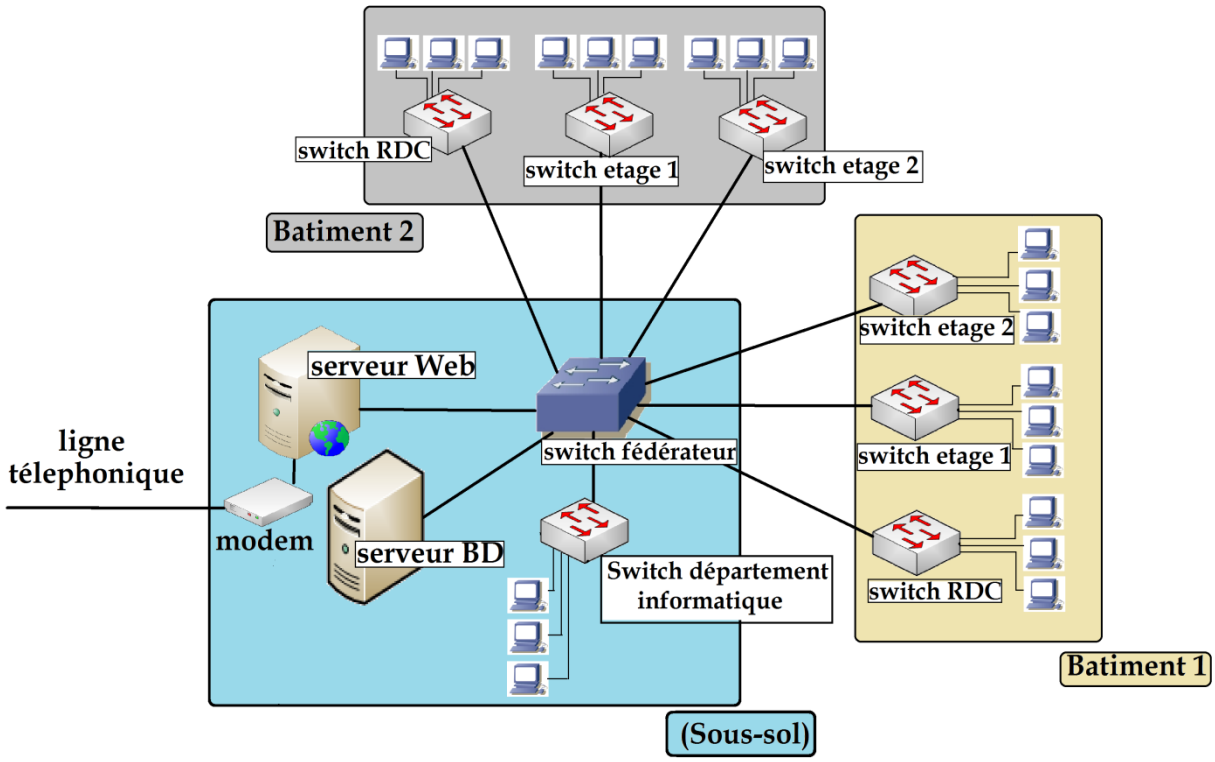

Figure I.8 : Architecture du réseau informatique existant

I.2.2. Présentation du réseau existant et analyse des manques (besoins)

I.2.2.1. Présentation

Le réseau existant est principalement composé de:

- 07 Switch Cisco de niveaux 2 ou de niveau 3.
- 01 Switch Cisco fédérateur (multilayer Switch).
- Un serveur de base de données (HP 3000).
- Un serveur web publié qui peut être vu depuis Internet.
- Un modem (reliant le réseau à internet).
- Des postes de travail (de type HP).

Avec l'aide de mon encadreur, et grâce aux visites au niveau du site, nous avons pus avoir une idée sur l'architecture actuelle du réseau informatique de l'entreprise et en dégager les points suivants :

- Les différentes structures à savoir les blocs administratifs, les Directions d'unités, la structure Informatique, et le Service Commercial des unités, dépendent d'un serveur situé au niveau du département informatique.
- Le réseau local englobe des Switchs Cisco de niveau deux et trois, dotés d'une configuration par défaut, cela implique que l'utilisation de ces équipement est limitée

aux VLAN 1. Ce qui induit que tous les postes se trouvent dans un seul sous-réseau, ceci fait que les communications et les accès sont illimités (aucune politique d'accès).

- Vulnérabilité au niveau organisation interne : la répartition et la multiplication des systèmes du pôle informatique avec sa solution soit disant moins couteuse, et vu que toutes les unités et leurs fonctions appartiennent au même sous-réseau, entraine une complexité voir même une impossibilité à gérer la sécurité de ces systèmes.
- Les serveurs, de web, de messagerie et de partage de connexion sont assurés par une seule machine, celle-ci est directement connectée à internet, sachant que le seul moyen de sécurisation utilisé est un firewall logiciel, cella indique une forme de sécurité minimum et insuffisante. En premier lieu, la sécurité de ses serveurs est mise en jeu, mais aussi celle du réseau interne et du serveur de base de données.
- Absence d'outils permettant la surveillance système et réseau (de hôtes et de services spécifiés), et alertant lorsque les systèmes ont des dysfonctionnements, ce qui peut provoquer la rupture des services (exemple : l'indisponibilité d'un serveur ou de la base de données sans prévention…) et par cela une dégradation des performances.
- Le réseau local a été conçu aux débuts, dans une logique de réseau ouvert. Concrètement, cette logique ouverte se traduit par un certain nombre de problèmes :
  - ✧ Toute prise réseau, qu'elle soit accessible en débranchant un poste de travail ou mise à disposition pour des prestataires extérieurs par exemple, est une menace potentielle, car l'accès réseau sera, dans tous les cas, donné à la machine connectée.
  - ✧ un poste mobile, infecté par un ver, pourra en se reconnectant au LAN contaminer le périmètre interne.
  - ✧ Le serveur de base de données contient des données sensibles mais il peut être accessibles par n'importe qui en privilège et en droits (alors qu'il est impératif que l'accès soit interdit de l'extérieur et limité de l'intérieur).
  - ✧ L'architecture du réseau n'est pas maîtrisée, car rien n'empêche un employé d'ajouter un équipement réseau non autorisé à la place de son poste de travail (un point d'accès WiFi par exemple).
- Absence d'un moyen qui puisse relier l'ENIEM à sa direction de façon sûre et sécurisée.

I.2.2.2. Les besoins en terme de sécurité

Vue l'existant, nous avons pu distinguer les besoins en terme de:

- Confidentialité : assurer que seuls les tiers autorisés aient accès aux informations de l'entreprise considérées comme étant discrètes, et empêcher par cela toute divulgation de celle-ci.

- Disponibilité : toujours garantir la continuité de l'accès aux services offerts par le réseau local, à des informations ou à des ressources.
- Intégrité : garantir que les données stockées dans la base de données ou en transit sur le réseau ne soient pas altérées (de manière intentionnelle ou accidentelle).
- Authentification : garantir la justesse de l'identité des utilisateurs ou des équipements du réseau informatique de l'ENIEM.
- Contrôle d'accès : contrôler les autorisations de toutes les entités dans le but de limiter les accès aux ressources et aux services protégés (base de données…).

I.3. Travail demandé

Et donc le but de ce projet est de trouver une solution optimale et facile à utiliser spécialement pour la sécurisation et la gestion du réseau et des systèmes le composant et y remédier avec ça aux problèmes rencontrés.

Afin de pouvoir réaliser ce travail, il est strictement nécessaire de réorganiser le réseau existant de façon à éclaircir tout les repères et de prendre en mains le control total de celui-ci en premier lieu. Après l'ordonnancement, viens en second lieu le couplage entre les deux processus sécurisation et supervision afin d'exploiter aux mieux les biens de leurs implémentation, offrir la possibilité de devenir proactif face aux problèmes rencontrés, et finalement et le plus important, de pouvoir détecter et interpréter en un simple coup d'œil les causes et origines des problèmes rencontrés afin de les fixer le plus rapidement possible.

Conclusion

Cette partie nous a permis d'avoir une idée globale sur l'organisme d'accueil du point de vue organisation, missions et activités, mais aussi de pouvoir présenter le domaine d'étude ainsi que de décrire son réseau informatique existant, Ce qui nous à permis de mieux s'approcher de la réalité de l'entreprise, et ainsi de se confronter aux problèmes existants, et essayer par cela de les résoudre.

CHAPITRE 2

Les réseaux informatiques d'entreprises

Introduction

Afin de rependre aux conformités des nouvelles technologies réseaux et satisfaire leurs besoins propres en informatique distribuée, les entreprises mettent en œuvre au sein de leurs établissements des réseaux locaux d'entreprise, les RLE (Réseaux Locaux d'Entreprise) ou LAN d'entreprises. Aujourd'hui, il y'a deux types de RLE qui dominent, les réseaux poste à poste, et les réseaux locaux avec serveurs, ces derniers représentent l'essentiel du parc installé en raison de leurs niveau de sécurité ainsi que de leurs adaptabilité et flexibilité. En effet, les distances couvertes par les réseaux informatiques d'entreprises ont pus être étendues grâce à l'interconnexion de RLE, afin de fournir des ressources distantes en temps réel.

II.1. La notion de réseau

II.1.1. Définition d'un réseau

Le terme générique « réseau » définit un ensemble d'entités interconnectées les unes avec les autres de façon bien ordonnée. Un réseau permet ainsi de faire circuler des éléments matériels ou immatériels entre chacune de ces entités selon des règles bien définies. Toutefois, selon le type d'objets interconnectés, on trouve des réseaux téléphoniques, des réseaux sociaux, des réseaux électriques, des réseaux informatiques etc.

II.1.2.Définition d'un réseau informatique

Ensemble d'équipements informatiques interconnectés les uns avec les autres grâce à des supports de connexion conditionnant les différents échanges. Le réseau informatique est devenu une ressource indispensable (voir vitale) pour toute organisation ou entreprise.

II.1.3. définition d'un réseau informatique d'entreprise

C'est une infrastructure de communications et d'administration qui repose sur des services réseaux critiques (annuaires LDAP, DNS, routage de trafic), où des ressources mises en réseau (exemple : serveurs) sont chargées de gérer les accès, le stockage, et le travail collaboratif, etc.

II.2. Esquisse sur les réseaux informatiques d'entreprise

II.2.1. Buts d'un réseau informatique d'entreprise

Au début c'été le partage des ressources les plus couteuses. Mais d'autres besoins émergent :

- ***Interconnexion des utilisateurs***: pour la communication et la collaboration.
- ***Gestion des données***: faciliter les sauvegardes et les mises à jour grâce aux serveurs.
- ***Besoins en logiciels***: les logiciels sont moins couteux en version multipostes qu'en version monoposte, ils sont faciles à faire évoluer (avec mises à jour sur le serveur).
- ***Partages de ressources plus étendus***: garantie l'unicité de l'accès à l'information (bases de données) et aux ressources.
- ***Sécurité***: sécuriser l'accès aux données grâce aux serveurs (avec mots de passe et accès sélectifs), et une politique de sécurité et un système de prévention efficace.

II.2.2. Caractéristiques fonctionnelles

Les fonctionnalités souhaitées et attendues des réseaux informatiques d'entreprise sont :

- ***La facilité:*** amélioration de la réactivité dans l'entreprise, avec une gestion du temps de connexion, ainsi que le dialogue en temps réel.
- ***La capacité:*** désigne le débit que procure un réseau et le type d'information qu'il peut transporter.
- ***La connectivité:*** la capacité de raccorder des équipements aux médias, et d'assurer leurs compatibilités au niveau du dialogue.
- ***L'interconnexion :*** définit la possibilité de relier des réseaux entre eux.
- ***La configuration:*** possibilité de gérer le réseau et de définir des accès aux ressources.
- ***La diffusion:*** possibilité de désigner tout l'ensemble des hôtes par un envoie.
- ***La fiabilité:*** désigne la continuité des fonctionnalités réseaux, et la disponibilité.

II.2.3. Les constituants essentiels d'un réseau informatique d'entreprise

II.2.3.1. Les constituants matériels

❖ **Schéma type d'un réseau informatique d'entreprise**

Le fait que les réseaux soient ordonnés permet de les considérer aisément d'un point de vue algorithmique et les représenter typiquement sous forme de graphes. On distingue deux environnements principaux dans un réseau informatique d'entreprise :

-**Environnement planétaire** : correspond à l'ensemble des sites raccordés à l'Internet.

-**Environnement local** : correspond à la mise en commun de ressources au sein d'un site d'exploitation.

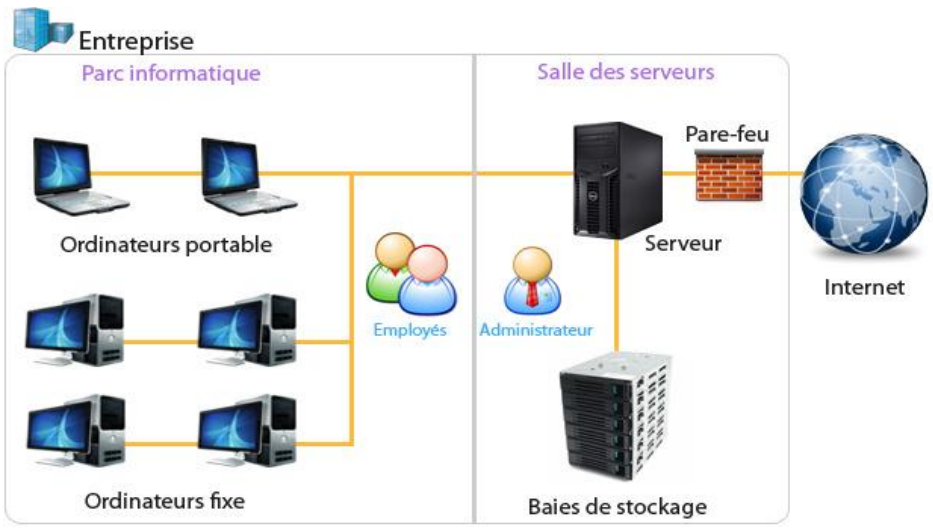

Figure II.1 : Schéma type d'un réseau informatique d'entreprise

❖ **Schéma type d'une liaison**

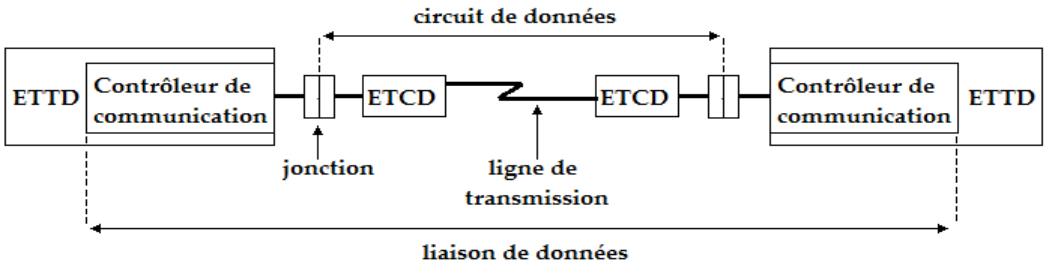

Figure II.2 : Schéma type de liaison dans un réseau

Un réseau informatique d'entreprise est donc constitué du matériel suivant :

- Equipements informatiques.
- Supports de transmission.
- Interfaces de connexion.

II.2.3.1.1. Les équipements informatiques [8]

Il existe deux catégories :

- **Catégorie des équipements d'utilisateur final** : ce sont des équipements informatiques de traitement ETTD (Equipement Terminal de Traitement de Données), ils fournissent des services directement à l'utilisateur comme l'ordinateur.
- **Catégorie des équipements de réseau**: ce sont les équipements qui interconnectent les équipements d'utilisateur final. Example: Switch, routeur, hub…

II.2.3.1.2. Les canaux de transmission (média)

Un canal de transmission est le moyen ou le support mis en place afin d'acheminer les signaux entre les nœuds du réseau. Celui-ci doit être adapté à l'application. Les médias les plus utilisés au niveau des réseaux informatiques d'entreprise, sont :

- ***Le câble coaxial***
- ***Le câble à paires torsadées***
- ***Le câble optique***
- ***Les liaisons sans fils***

II.2.3.1.3. Les interfaces de connexion

Appelés aussi équipements terminaux de circuit de données (ETCD), les équipements informatiques sont reliés au media par l'intermédiaire de ces interfaces via des jonctions ou ce qu'on appel les connectiques (ports et connecteurs), dans le cas d'un réseau local elles peuvent s'agir de cartes réseau, de modems ou aussi d'adaptateurs.

II.2.3.2. Les constituants immatériels

Parmi les principaux constituants immatériels d'un réseau informatique d'entreprise :

II.2.3.2.1. Les logiciels réseau

Ce sont des logiciels spécifiques, conçus pour pouvoir utiliser les équipements mis en réseau, ces logiciels interviendront à de différents niveaux pour bien mener les différents services réseaux. Exemples : logiciels de messagerie, navigateurs…

II.2.3.2.2. Les NOS (Network Operating System)

Souvent nommés « gestionnaires de réseaux », ce sont des systèmes d'exploitation conçus pour réseaux, résident dans les différentes stations du réseau local, par exemple Windows NT de Microsoft, et Unix. Ils fournissent une interface entre les applications des utilisateurs et les fonctions du réseau auxquelles ils font appel. Ce type de systèmes d'exploitation est à l'origine de la gestion de toute la mise en œuvre du réseau (adresses, ressources, partage, sécurité, droits d'accès), et supportent des applications client/serveur comme la messagerie électronique, agendas partagés…

II.2.3.2.3. Les protocoles réseaux [1]

Un protocole de réseau est un ensemble de règles et de procédures à respecter pour pouvoir émettre et recevoir des données dans un réseau.

- ***Protocoles orientés connexion et non orientés connexion***

✧ **Protocole orienté connexion :** il définit un chemin unique entre l'hôte source et l'hôte destination, et inclus un contrôle de transmission pendant la communication.

✧ **Protocole non orienté connexion :** il ne définit pas de chemin unique pour acheminer les paquets. Exemple: protocole IP.

- ***Protocoles routés***

Ce sont des protocoles de communication de niveau 3 d'OSI. Un protocole de routage a toutes les informations pour envoyer des paquets sur le segment spécifié et à l'hôte spécifié. Toutefois, il peut être routable ou non routable :

✧ **Routable:** les messages envoyés à l'aide de ce protocole peuvent sortir de leur réseau (via un routeur). En effet, le format du paquet comprend une distinction entre la partie hôte et la partie réseau.

✧ **Non routable :** les messages envoyés à l'aide de ce protocole ne peuvent pas sortir de leur réseau. En effet, le format du paquet ne comprend pas de mécanisme permettant à un élément réseau de faire suivre ces paquets au travers différents réseaux. Ce type ne convient pas aux réseaux hétérogènes.

- ***Familles de protocoles de routage***

✧ ***Les IGP (Interior Gateway Protocol) :*** ils réalisent le routage à l'intérieur d'un système autonome.

✧ ***Les EGP (Exterior Gatway Protocol):*** protocoles qui effectuent le routage entre deux systèmes autonomes différents.

II.2.3.2.4. Systèmes de stockage

On donnera deux exemples de systèmes de stockage basiques :

a- Les bases de données

Ensemble organisé de données, généralement contrôlées par un système de gestion permettant d'effectuer la recherche, le tri ou la fusion de données, ainsi que toute autre requête relative à ces données. Elles comptent de nombreux domaines de mise en pratique : gestion de stocks, suivi commercial, gestion électronique de documents, gestion de clientèle...

b- Les annuaires LDAP (Lightweight Directory Access Protocol)

Un annuaire électronique est une base de données spécialisée qui peut contenir toute sorte d'information que se soit des coordonnées de personnes ou des données système. Un annuaire LDAP organise les données de façon arborescente. La fonction principale est de retourner un ou plusieurs attributs d'un objet grâce à des fonctions de recherche multicritères. Il peut servir d'entrepôt pour centraliser des informations et les rendre disponibles via le réseau à des utilisateurs, des applications, ou des systèmes d'exploitation. Le protocole d'accès aux services d'annuaires est LDAP.

❖ Les concepts du protocole LDAP

LDAP est un protocole d'annuaire sur TCP/IP. Il définit comment s'établit la communication client-serveur. Il fournit à l'utilisateur des commandes pour se connecter ou se déconnecter, pour rechercher, comparer, créer, modifier ou effacer des entrées. Des mécanismes de chiffrement et d'authentification, couplés à des mécanismes de règles d'accès (ACL) permettent de protéger les transactions et l'accès aux données.

❖ Caractéristiques comparées entre les annuaires et les bases de données

- ✧ Rapport lecture/Ž écriture (beaucoup plus élevé pour les annuaires).
- ✧ Annuaires plus facilement extensibles.
- ✧ Distribution des données entre serveurs plus facile avec les annuaires.
- ✧ Plus grande duplication des informations des annuaires (plus fiable, performant, et plus proche des clients).
- ✧ Importance des standards LDAP (ceci procure une capacité d'interopérabilité).
- ✧ Performances globales des annuaires plus élevées (en lecture).

II.2.3.2.5. Les ports logiciels

Correspond à la couche de transport du modèle OSI, la notion de **port logiciel** permet, sur un ordinateur donné, de distinguer différents interlocuteurs. Ces interlocuteurs sont des programmes informatiques qui, selon les cas, écoutent ou émettent des informations sur ces ports. Cependant, on considère les ports comme des portes donnant accès au système d'exploitation. Les programmes les ouvrent pour fonctionner.

Afin que plusieurs communications puissent circuler en même temps, TCP et UDP utilisent des numéros de ports sur 16bits (soit 65536 numéro) attribués par le système d'exploitation sur demande d'une application. Des conventions ont été établies pour chaque application :

Plage de ports	Utilisation
de 0 à 1023	réservés aux applications publiques
de 1023 à 65535	attribués aux entreprises pour les applications commerciales et utilisés par le système d'exploitation pour l'attribution dynamique des ports source.

Tableau II.1 : Attribution des numéros de ports

❖ **Principe :**

Lorsqu'un logiciel client veut dialoguer avec un logiciel serveur, aussi appelé service, il a besoin de connaître le port écouté par ce dernier. Les principaux services utilisent des ports dits réservés. Par convention, ce sont ceux compris entre **0** et **1 023** inclu. Les services utilisant ces ports sont appelés **services bien connus** (Well-Known Services) comme FTP, DHCP, HTTP...

II.3. Organisation des réseaux informatiques d'entreprise

II.3.1. L'étendue des liaisons

L'étendue des liaisons est les distances couvertes par les réseaux, on distingue trois classes de réseaux selon ces zones de couverture :

. Les LAN (**L**ocal **A**rea **N**etwork): indiquent les réseaux intra-entreprises (RLE), pour des distances de couvertures allant de quelques dizaines de mètres jusqu'à plusieurs centaines de mètres. Toute fois, on peut distinguer les sous-partitionnements suivants :

- ✧ ***Les DAN*** (**D**epartemental **A**rea **N**etwork): relie les utilisateurs d'un département d'entreprise (à l'échelle d'un étage d'immeuble).
- ✧ ***Les BAN*** (**B**uilding **A**rea **N**etwork): à l'échelle d'un bâtiment ou établissement.
- ✧ ***Les CAN*** (**C**ampus **A**rea **N**etwork) : c'est un réseau à l'échelle d'un site ou terrain.

. Les MAN (**M**etropolitain **A**rea **N**etwork) : relient plusieurs bâtiments, dans le même quartier ou à l'échelle d'une ville, étendus sur plusieurs dizaines de kilomètres.

. Les WAN (Wide Area Network) : c'est à l'échelle d'un pays, ou d'un groupe de pays.

II.3.2. Les réseaux locaux d'entreprise (RLE)

Il existe une grande variété de réseaux locaux qui se distinguent par leurs structures, leurs protocoles d'accès, leurs supports de transmission et leurs performances en termes de capacité et de fiabilité. Les MAN d'entreprise et WAN résultent de l'interconnexion de RLE :

II.3.2.1. Les typologies des systèmes

II.3.2.1.1. Les systèmes ouverts

Un système ouvert est un système capable de communiquer et donc échanger des informations avec d'autres systèmes conformément aux normes OSI. Selon le type de matériels, on distingue :

- **Système Homogène:** tous les équipements du réseau sont d'un même constructeur, régies par les mêmes règles.
- **Système Hétérogène:** les équipements du réseau sont de constructeurs différents.

II.3.2.1.2. Les systèmes autonomes (AS)

Un système autonome AS (Autonomous System) est un réseau ou ensemble de réseaux sous un contrôle administratif commun, interconnectés par des routeurs homogènes (ayant les mêmes règles et fonctions). Au sein d'un AS, un protocole interne est utilisé (IGP), tandis qu'entre AS, c'est un protocole externe qui est utilisé (EGP), des sessions BGP (Border Gateway Protocol) sont établies entre les routeurs de bord d'AS. Chaque AS est identifié par un numéro ASN (AS Number) sur 16bits soit de 1 à 65535.

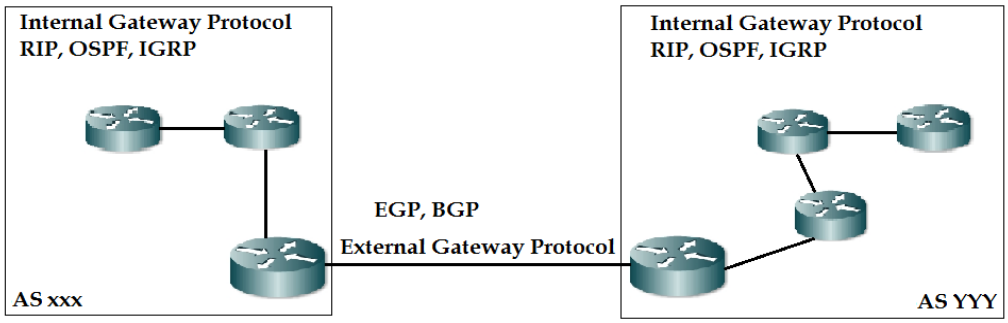

Figure II.3 : Interconnexion de systèmes autonomes

II.3.2.2. Les topologies

Il convient de distinguer :

- **Une topologie physique (topologie de câblage) :** c'est le chemin de câblage apparent, représente la façon avec laquelle les équipements sont interconnectés.
- **Une topologie logique (topologie d'accès) :** c'est la façon avec laquelle les données transitent dans le support de transmission (façon de communication).

On distingue trois topologies physiques et logiques basiques :

1.Topologie en bus :

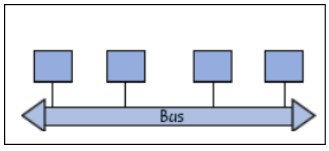

Figure II.4 : topologie en Bus

2.Topologie en étoile :

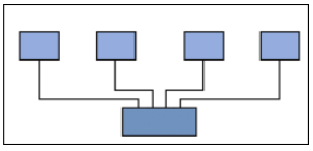

Figure II.5 : Topologie en étoile

3.Topologie en anneau :

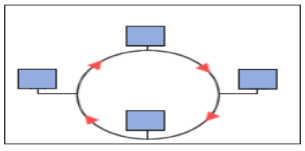

Figure II.6 : Topologie en anneau

II.3.2.3. Les méthodes d'accès [2]

Afin de mettre de l'ordre dans un réseau local, où plusieurs nœuds se partagent le même média, et par cella allouer équitablement la bande passante média, ils doivent respecter des méthodes (règles) régissant l'usage de ce support. Deux sont le plus souvent appliquées :

a- La contention (accès aléatoire)

Connue sous l'acronyme **CSMA** (Carier Sense Multiple Access), c'est une méthode qui consiste à écouter le canal avant d'émettre, Elle est dite aléatoire en sens qu'on ne peut prévoir le temps nécessaire à un message pour être émis, transmis et reçu. Il existe deux variantes :

- **CSMA/CD (Collision Detection) :** écoute avant et pendant l'émission.
- **CSMA/CA (Collision Avoidance)** : emploi de temporisateurs et accusés de réception.

b- L'anneau à jeton (accès déterministe)

C'est une méthode déterministe, car le temps que prendra un message pour atteindre son destinataire peut être déterminé en fonction du nombre de stations et la longueur de câbles.

Un jeton (trame) circule en permanence de station en station. Une station qui veut émettre bascule l'un des octets en position « occupée » et émet son message. Reçu par le destinataire, il remet le jeton à l'état « libre ».

II.3.2.4. Les principales architectures

a- Les réseaux Ethernet (IEEE 802.3)

L'architecture Ethernet repose sur la méthode d'accès CSMA/CD, et varie en fonction du câble utilisé et de la topologie physique, la topologie logique quand à elle est toujours de type bus. Celle-ci offre des débits allant de 10 à 100 Mbps.

b- Token-Ring (IEEE802.5)

Elle repose sur la technique d'accès du jeton. Le débit était de 4Mbps à l'origine, puis 16Mbps. Sa topologie logique est basée sur l'anneau, mais les stations sont connectées selon une topologie physique en étoile. Utilise un câblage à paires torsadées, chaque segment est muni de deux lignes distinctes pour la transmission de/vers les stations, ce qui permet de former un anneau logique.

II.3.2.5. Modes de fonctionnement

Il existe 2 modes de fonctionnement des réseaux selon deux environnements principaux:

- ***a- Client/serveur :*** dans lequel un ordinateur central (serveur dédié) fournit des services réseaux aux autres ordinateurs appelés dans ce cas clients (centralisation).
- ***b- Poste à poste :*** ou égal à égal, dans lequel il n'y a pas d'ordinateur central et chaque ordinateur a un rôle similaire (décentralisation).

II.3.2.6. Modes de communication

a- Mode connecté : exige une connexion entre l'émetteur et le récepteur (principe du téléphone), donc toute transmission doit être précédée d'une demande de connexion réussie.

b- Mode non connecté : ce mode ne demande pas de connexion (principe du courrier).

Les communications sont basées sur un principe de commutation :

- ***Commutation de circuits:*** Création d'un circuit physique reliant les deux extrémités lors de l'établissement de la connexion.
- ***Commutation de paquets:*** L'information est découpée en paquets qui sont transportés de nœud en nœud. Chaque nœud redirige ces fragments selon sa table de routage.
- ***Commutation de cellules :*** commutation de paquets particulière, un paquet est sur 53 octets (5 d'en-tête + 48 de données) appelé cellule. C'est un mélange de la commutation de circuits et de paquets (émission de paquets en mode connecté).

II.3.3. L'adressage IP [3]

Une adresse IP est un moyen d'identification (valeur représentant une position dans un réseau), représentée en décimal pointé et constituée de 4 nombres de 8 bits, compris chacun entre 0 et 255. Elle est constituée de deux parties, une partie identifiant le réseau, et une autre identifiant les hôtes dans ce réseau, et appartient à une classe (A, B, C, D ou E) selon la valeur de son premier octet :

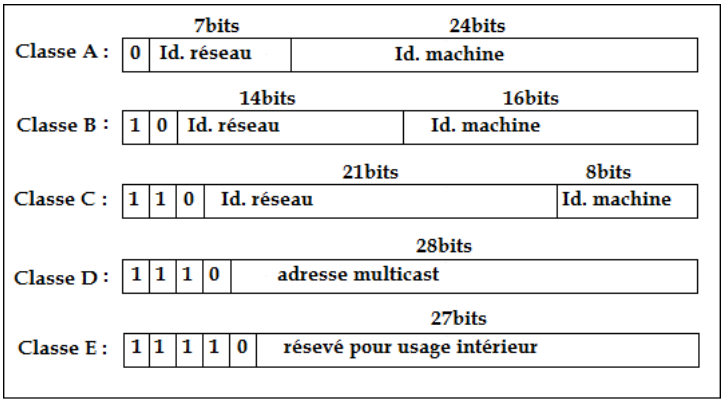

Figure II.7 : Représentation des classes d'adresses IP

Les deux champs de l'adresse IP (netID et hostID) vont varier suivant la classe d'adresse IP. L'espace d'adresses possibles pour chaque classe est représenté dans ce tableau:

Classes	Espace d'adresses IP
Classe A	De 0.0.0.1 à 126.255.255.254
Classe B	De 128.0.0.1 à 191.255.255.254
Classe C	De 192.0.0.1 à 223.255.255.254
Classe D	De 224.0.0.0 à 239.255.255.255
Classe E	De 240.0.0.0 à 247.255.255.255

Tableau II.2 : Les plages d'adresses IP

II.3.3.1. Les adresses IP spécifiques

- ***o.X.Y.Z et <netID=0>.<hostID> :*** Utilisées par une machine pour savoir son adresse, lors d'un processus d'amorçage (boot) par exemple.
- ***<netID>.<hostID tous ses bits à 0>* :** désigne le réseau lui-même (ex : 145.32.0.0).
- ***<netID>.<hostID tous ses bits à 1>*** : adresse de diffusion, désigne toutes les machines du réseau concerné.
- ***255.255.255.255:*** adresse de diffusion locale, désigne toutes les machines du réseau. Mais l'émetteur n'est pas obligé de connaître l'adresse du réseau.
- ***127.X.Y.Z:*** adresse de rebouclage (loopback ou localhost). Un message envoyé à cette adresse ne sera pas envoyé au réseau, il sera retourné à l'application par le logiciel de pilote de la carte. L'adresse **127.0.0.1** est utilisée pour tester le bon fonctionnement d'une carte réseau.

II.3.3.2. Les adresses IP privées

Elles sont réservées à la constitution de réseaux privés, autrement appelés intranet :

- de classe A : de **10.0.0.0** à **10.255.255.255**.
- de classe B : de **172.16.0.0** à **172.31.255.255**.
- de classe C : de **192.168.0.0** à **192.168.255.255**.

II.3.3.3. Subdivision en sous-réseaux (segmentation)

Afin d'optimiser l'utilisation (séparer les machines les plus sensibles, limitation de congestions, prévision de l'évolution) et la sécurité du réseau on le segmente (création de sous-réseaux), un masque de sous-réseaux de longueur variable est utilisé afin d'exploiter plus efficacement l'espace d'adressage. La segmentation induit un découpage de la partie hostID de l'adresse IP en 2 parties, identifiant sous-réseaux (subnetID) et identifiant hôtes (hostID).

II.4. L'interconnexion

Les mécanismes d'interconnexion de réseaux ont plusieurs objectifs, soit :

- La séparation d'un réseau local en plusieurs sous-réseaux.
- Le raccordement de réseaux locaux initialement isolés, ou l'extension de celui-ci au delà de ces limites.
- La réalisation d'un seul grand réseau étendu sur plusieurs sites.
- Le raccordement du réseau local au réseau public (internet) ou à un site distant.

II.4.1. Les modèles de communication OSI et TCP/IP [2]

II.4.1.1. Le modèle OSI (Open System Interconnexion)

Signifie l'interconnexion des systèmes ouverts, permet de résoudre le problème des communications hétérogènes. Il propose donc la manière dont deux éléments communiquent, en décomposant les différentes opérations à effectuer en 7 étapes, ce qui fait un modèle à 7 couches, les protocoles utilisés sont répartis selon ces couches.

a- Les couches du modèle OSI

Les trois couches inférieures sont orientées communication et regroupent des dispositifs matériels. Les quatre supérieures sont orientées application et regroupent des dispositifs logiciels.

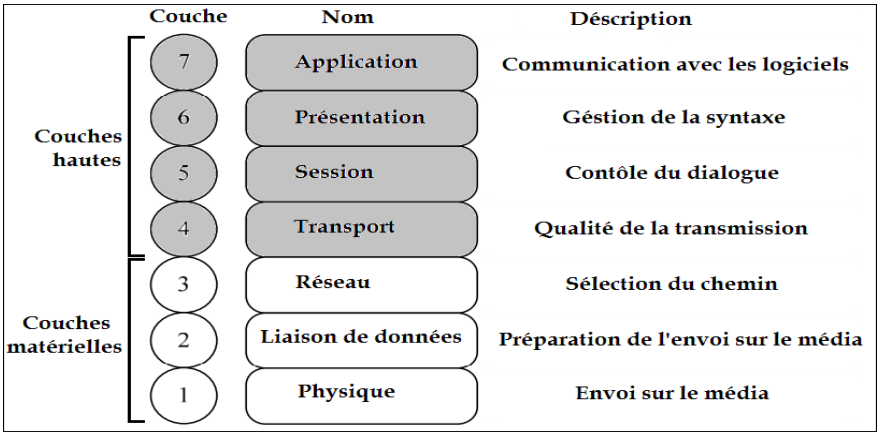

Figure II.8 : Le modèle OSI

Chaque couche communique avec la couche inférieure et supérieure, ce qui permet l'empilement des couches entre elles grâce à des interfaces (sous forme d'unités de données). Pour cela, OSI a recourt au principe d'encapsulation.

b- Encapsulation

Processus de conditionnement des données consistant à leurs ajouter un en-tête de protocole déterminé (par chaque couche) avant d'être transmises à la couche inférieure :

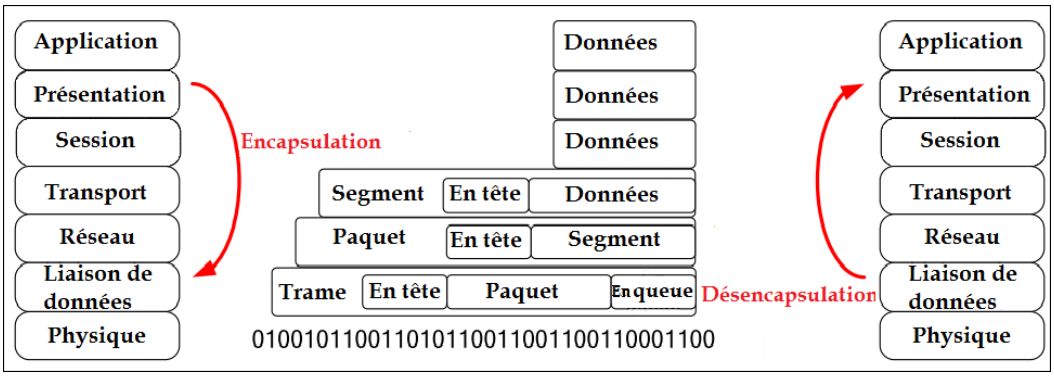

Figure II.9 : Encapsulation de données

Remarque : Pour identifier les données lors de leur passage au travers d'une couche, une appellation PDU (Protocol Data Unit ou Unité de données de protocole) est utilisée, exemple : données, trame...

II.4.1.2. Le modèle TCP/IP

Appelé aussi **modèle Internet,** TCP se charge du transport de bout en bout, tant dit qu'IP est responsable du routage à travers le réseau. Il présente aussi une approche modulaire (utilisation de couches) avec quatre couches.

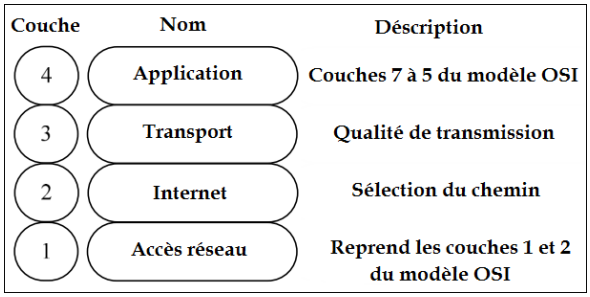

Figure II.10 : Le modèle TCP/IP

II.4.2. Les protocoles HDLC et FrameRelay [3]

. HDLC (High-level Data Link Control)

Protocol de niveau 2, Son but est de définir un mécanisme pour délimiter des trames de différents types, on ajoutant un contrôle d'erreur. C'est un protocole orienté bits, fonctionne en mode synchrone, liaisons point à point ou multipoints, en full-duplex.

. FrameRelay (relais de trames) [3]

Le relais de trame**,** protocole de réseau étendu qui intervient dans les couches 1 et 2 d'OSI, basé sur la commutation de paquets, il sert à véhiculer les données entre les réseaux. C'est un protocole standard pour l'interconnexion des LAN.

II.4.3. Les matériels d'interconnexion

✧ **Les concentrateurs (hubs)**

Le hub (répétiteur) assure la liaison, en se contentant de transférer les données qui lui arrivent vers tous les autres éléments du réseau tout en le régénérant (répétant).

✧ **Les ponts (bridges)**

Equipements de niveau 2 d'OSI permettant de relier des réseaux identiques (travaillant avec les mêmes protocoles et ayant des méthodes d'accès similaires). Ils permettent de filtrer les trames entre les segments en utilisant une table de correspondance port/adresse MAC des stations. Il existe deux techniques de pontage :

. *Source routing :* méthode où la station émettrice détermine le chemin.

. *Spaning-tree :* chaque pont communique avec les ponts voisins en indiquant ses voisins (auto-conception d'un arbre).

✧ **Les commutateurs (switches)**

Travaillent au niveau de la couche 2 d'OSI, leurs tables de routage sont construites à partir des adresses MAC, ils permettent de relier divers éléments tout en segmentant le réseau. Il existe deux modes de fonctionnement:

. *On the fly :* pas de contrôle de trames, dès que l'adresse du destinataire est reçue, la trame est commutée sur le segment correspondant.

. *Store and forward :* la trame est entièrement réceptionnée, analysée et contrôlée puis acheminée vers la destination.

✧ **Les passerelles (gateways)**

Ce sont des systèmes matériels et/ou logiciels permettant de relier des réseaux de protocoles différents. La passerelle réalise une transition en convertissant les protocoles de communication de l'un vers l'autre (fonctionne comme un translateur ou traducteur de formats de trames et de services).

✧ **Les routeurs**

Fonctionnent au niveau de la couche 3 du modèle OSI, Leurs rôles est d'acheminer les données entre réseaux différents en prenants des décisions logiques d'optimisation afin de choisir la meilleur route. Un routeur doit posséder une adresse IP dans chaque réseau IP qu'il interconnecte, on dit qu'il est multi-domicilié. Ces équipements sont dotés d'une part d'interfaces réseaux, et d'autre part de logiciels assurant les fonctions de routage (filtrage, translation d'adresses, firewall).

II.5. La fonction de routage [8]

II.5.1. L'acheminement dans les réseaux

Consiste à assurer le transit des blocs d'un point d'entrée à un point de sortie. Des « tables de routage » indiquent la route à suivre. Une table est un triplet (adresse destination/route à prendre/coût), elle est construite par un protocole en cas de routage dynamique, ou l'administrateur si routage statique.

II.5.2. Les modes de routage

II.5.2.1. Routage statique

La table de routage est initialisée manuellement par l'administrateur, les chemins sont prédéfinis et les routeurs intermédiaires ne prennent aucune décision de routage.

II.5.2.2. Routage dynamique

La première route est souvent configurée manuellement. Au passage de chaque routeur, le meilleur chemin est choisi (routage automatique effectué par les protocoles spécialisés).

II.5.3. Les principaux protocoles de routage

. RIP (Routing Information Protocol)

Protocole à vecteur de distance, C'est-à-dire que les routeurs voisins s'échangent des distances, sa permet de réactualiser les tables de routage. Il utilise un métrique (le principale point de contrôle déterminant le chemin à emprunter pour transmettre, utilisé par les protocoles de transmission, c'est un critère de comparaison) simple : la distance entre une source et une destination est égale au nombre de sauts qui les séparent, elle est comprise entre 1 et 15, la valeur 16 représente l'infini. Pour cela, RIP n'est pas valable aux grands réseaux.

. OSPF (Open Shortest Path First)[1]

Protocole de routage dynamique qui comble les insuffisances de RIP. C'est un protocole d'état de liens, c'est-à-dire qu'un routeur n'envoie pas des distances à ses voisins, il teste plutôt l'état de la connectivité qui le relie à son entourage. Il envoie cette information aux routeurs voisins, qui ensuite la propagent. Ainsi, chaque routeur possède une carte de la topologie du réseau qui se met à jour très rapidement lui permettant de calculer des routes précises.

. IGRP (Interior Gateway Routing Protocol)

Considéré comme un protocole de routage à vecteur de distance, mais il a également été référencé comme hybride. Il possède des caractéristiques qui le distinguent des autres, comme son insensibilité à la taille du réseau, une réponse rapide aux modifications de réseaux.

. EGP ou BGP (External ou Border Gateway Protocol)

C'est un protocole à vecteur de chemin conçu pour les grands réseaux, utilisé pour transporter des informations de routage entre systèmes autonomes. Pour éviter une boucle dans le réseau, ce protocole fait transiter toute la « carte » du réseau à tous les routeurs qui le composent, notamment avec les chemins. Toutefois, si un élément du réseau est présent plus d'une fois, il y'a donc une boucle, ce qui fait une erreur à traiter.

II.6. Protocoles standardisés de base

. Protocole TCP/IP (Transfer Control Protocol/Internet Protocol) [2]

TCP/IP est adapté aux réseaux hétérogènes, **TCP** est un protocole de transport qui gère les sessions de communication orienté connexion, souvent relié au **protocole IP**, un protocole orienté non connexion qui permet l'échange de données sous forme de paquets à travers un ensemble de réseaux.

. Protocole UDP (User Datagram Protocol)

Protocole non orienté connexion résidant à la couche 4, utilise une information complémentaire qu'est le numéro de port, la trame contient donc un numéro de port source et destination. Ce protocole n'offre pas de fonction de contrôle du bon acheminement, et il nécessite moins de bande passante que TCP.

. HTTP (HyperText Transfer Protocol)

Protocole de communication client-serveur développé pour le World Wide Web, il sert pour le transfert hypertexte (contenant des nœuds liés par des hyperliens). C'est un protocole de la couche application. Un serveur HTTP utilise le port 80. Les clients HTTP les plus connus sont les navigateurs Web.

. ICMP (Internet Control Message Protocol[1]

Permet de gérer les informations relatives aux erreurs générées au sein d'un réseau IP. ICMP permet, non pas de corriger ces erreurs, mais de faire part de ces erreurs(Ex : machine destination déconnectée, durée de vie du datagramme expirée, congestion de passerelles intermédiaires) . Ainsi, il est utilisé par tous les routeurs, pour reporter une erreur appelée Delivery Problem. Un exemple d'utilisation d'ICMP est le « Ping », qui donne le temps mis par un paquet pour atteindre une adresse, ou bien un éventuel problème de routage pour atteindre un hôte. Un autre exemple, Si une passerelle détecte un problème sur un datagramme IP, elle le détruit et émet un message ICMP pour informer l'émetteur initial. Les messages ICMP sont véhiculés dans des datagrammes IP.

. TELNET [1]

Protocole standard permettant l'interfaçage de terminaux et d'applications à travers Internet. Ce protocole fournit les règles de bases pour permettre de relier un client (système composé d'un affichage et d'un clavier) à un ordinateur distant (coté serveur). Toutefois, ce protocole de transfert est non sûr, c'est-à-dire que les données circulent en clair sur le réseau.

Conclusion :

Dans ce chapitre, nous avons pris connaissance des différentes notions sur les réseaux informatiques d'entreprises. Ce qui va nous a permis d'avoir une idée sur ce sujet, cela va nous servir par la suite.

CHAPITRE 3

La Sécurité des réseaux informatiques

Introduction

La sécurité du réseau informatique d'une entreprise entre dans la sécurisation globale du système d'information (SI) de celle-ci. Plus formellement, elle consiste à respecter des procédures, au niveau humain, technique et organisationnel. L'objectif est de protéger le réseau de l'entreprise et de se prémunir contre tout type de risques pouvant dégrader ses performances. La sécurité du réseau consiste également à mettre en place des politiques de sécurité, comme la gestion des accès, ou encore des plans d'adressage, pour garantir l'intégrité ainsi que les autres objectifs de sécurité des données critiques de l'entreprise.

Ce chapitre présente dans sa globalité des généralités sur la sécurité, ses faiblesses, mais aussi les menaces et les risques, et propose de ce qu'il est possible d'entreprendre pour protéger efficacement un réseau en exploitant au mieux les possibilités offertes par les équipements couramment utilisés par les entreprises.

III.1 Les vulnérabilités dans les réseaux[5]

Appelées aussi failles ou brèches ou encore trou de sécurité, ce sont toutes les faiblesses ou défauts des ressources ou infrastructures informatiques ou même des humains qui peuvent être exploités par des menaces dans le but de compromettre. Plus le niveau de l'exposition aux menaces est élevé, plus le système est vulnérable. Il convient de distinguer quatre grandes familles de vulnérabilités :

III.1.1. Les vulnérabilités au niveau technologique :

Cette famille comprend toutes les failles liées à l'utilisation des technologies (faiblesse de protocoles, de systèmes d'exploitation, et des équipements informatiques), mais aussi toutes celles liées aux problèmes d'interopérabilités, aux nécessités de migration et à l'introduction de nouveaux produits.

III.1.2. Les vulnérabilités au niveau physique :

Toutes les failles liées aux événements imprévisibles comme les pannes, les accidents ou encore les atteintes intentionnelles aux matériels. C'est en réponse à cette famille que les caractéristiques physiques des salles et équipements informatiques sont analysées et qu'un « plan de continuité » est élaboré (sureté de fonctionnement).

III.1.3. Les vulnérabilités au niveau organisationnel (management) :

C'est les failles liées à l'absence d'une gestion correcte des systèmes informatiques (des listes d'accès, des règles de routage et des logiciels mal configurés ou des paramètres par défaut par exemple). En effet, c'est au niveau de la gestion des solutions, que doivent être définies les règles d'utilisation et d'implémentation de ces dernières. C'est également à ce niveau que doivent être mis en place les contrôles permettant de veiller au respect des

règlements, ainsi que la création et la distribution des procédures régissant le bon fonctionnement de la solution.

III.1.4. Les vulnérabilités dues à l'utilisateur

Ce sont les failles d'origine humaine, elles sont dues à la naïveté et les actions de l'utilisateur sans réflexions ni précautions, à cause du manque de sensibilisation de celui-ci des différents risques encourus.

III.2. Les menaces de sécurité

Une menace de sécurité informatique désigne toute action susceptible de nuire, en exploitant les failles existantes dans l'infrastructure informatique, toutefois, celle-ci peut être accidentelle ou intentionnelle.

- **Menaces accidentelles :** Elles sont causées de manière fortuites et inattendues, celle-ci peuvent s'agir par exemple de catastrophes naturelles ou d'inattention ou erreur humaine. En effet, ce type de menace résulte de l'environnement dans lequel se trouve le système.
- **Menaces intentionnelles :** Ce sont des actions causées par des entités d'intentions malveillantes dont le but est de nuire. En effet, une menace intentionnelle représente « une attaque » contre la sécurité.

III.3. Les risques [5]

Un risque, est la conséquence qui peut être engendrée à cause de l'exposition au danger, c'est-à-dire tout péril ou dommage pouvant survenir de l'exposition aux menaces de sécurité. En effet, une vulnérabilité exploitable plus des menaces constituent (engendrent) un risque. Le niveau de risque dépend des trois paramètres suivants :

- La vulnérabilité : qui représente le niveau d'exposition face à la menace.
- La sensibilité :qu'est la valeur de l'objet (exemple : confidentialité d'une information).
- La menace : qui peut être passive ou active, et plus ou moins néfaste.

III.4. Les contre-mesures[5]

III.4.1. La sureté de fonctionnement (Safety)

Consiste à protéger le système contre les accidents et tout type de menace visant à son dysfonctionnement, tout en garantissant sa disponibilité et fiabilité et donc la continuité de ses services.

III.4.2. La sécurité informatique (Security)

C'est l'ensemble des moyens et techniques mis en œuvre afin de minimiser les vulnérabilités d'un système, en prévention des menaces accidentelles ou intentionnelles.

III.5. Les besoins en sécurité informatique

Ces besoins représentent des services de sécurité, en effet un service utilise un ou plusieurs mécanismes de sécurité. Il convient de distinguer:

- **Confidentialité :** consiste à assurer que seuls les tiers autorisés aient accès aux informations (sur le réseau ou en transit) considérées comme étant discrètes, et empêcher par cela toute divulgation de celle-ci.
- **Disponibilité :** consiste à toujours garantir la continuité de l'accès à un service, à des informations ou à des ressources, c'est-à-dire maintenir le bon fonctionnement du système d'information.
- **Intégrité :** consiste à garantir que les données stockées ou en transit sur le réseau ne soient pas altérées (de manière intentionnelle ou fortuite), et que celles-ci sont bien celles que l'on croit être.
- **Authentification :** consiste à garantir la justesse de l'identité d'un utilisateur ou d'un équipement. En effet, un système doit être sûr de l'identité d'une entité pour lui données un accès, il doit vérifier que le sujet est bien celui qu'il prétend être.
- **Contrôle d'accès :** permet de contrôler les autorisations d'une entité en se basant sur son identité ou son rôle dans le but de limiter les accès à des ressources ou services protégés. Le contrôle d'accès ne peut être efficace sans une authentification.
- **Non-répudiation :** consiste à garantir l'inaptitude de nier une transaction entre des correspondants, donc la transmission sur le réseau ne pourra pas être remise en cause.

III.6. Politique de sécurité [5]

✧ **Définition d'une politique de sécurité :**

Une politique de sécurité est un document confidentiel contenant une collection de directives de sécurité classées par thèmes. Bien évidement, la mise en pratique de cette politique est l'application de ces directives aux thèmes couverts par le projet. Dans les faits, une politique de sécurité consiste à :

- ✧ Connaître les besoins de l'entreprise en matière de sécurité et évaluer les risques.
- ✧ Proposer à tous les départements des outils, des processus et des règles en ligne avec les risques considérés primordiaux pour l'entreprise.
- ✧ Elaborer une série de procédures et d'actions à mener en cas de dangers (vulnérabilité ou menaces d'attaques informatiques par exemple).

III.7. Les attaques informatiques [6]

Une attaque désigne n'importe qu'elle action intentionnelles malveillante visant à compromettre la sécurité d'un système. Il existe plusieurs types selon leurs provenances (les failles) et leurs méthodes, mais aussi leurs objectifs.

III.7.1. Classification des attaques

Les attaques peuvent être classées en attaques passives et attaques actives.

III.7.1.1. Attaques passives

Elles visent la confidentialité, consistent à s'introduire dans un réseau ou simplement l'écouter, afin de collecter des informations, sans engendrer d'altération ou de modification.

. Les méthodes possibles :

- L'écoute.
- Injection de code.
- Usurpation d'identité.
- Intrusion.
- Abus de droits.

III.7.1.2.Attaques actives

Consistent à s'en prendre au système, et changer son comportement, afin d'altérer son bon fonctionnement. Il y'a plusieurs attaques actives, selon les objectifs :

- ***Attaques sur l'intégrité*** *:*

  .Objectifs : modification ou destruction de données ou de configurations.

  . Méthodes possibles :

  - Injection de code
  - Action physique
  - Intrusion

- ***Attaques sur l'authentification*** *:*

  .Objectifs : utilisation des ressources de façon clandestine sur un système.

  . Méthodes possibles :

  - Abus de droits
  - Intrusion

- ***Attaques sur la disponibilité :***

  .Objectifs : perturbation d'un échange par le réseau, d'un service ou d'un accès à un service.

  .Méthodes possibles :

- Abus de droits
- Action physique
- Intrusion

❖ **Description des méthodes**

- Ecoute : Ecoute passive sur le réseau dans le but de récupérer des informations. Exemples d'attaques : analyseurs de réseau, ingénierie sociale …
- Usurpation d'identité : Utilisation d'une fausse identité. Exemple d'attaque : usurpation d'adresse IP (IP spoofing).
- Intrusion : Exploitation des vulnérabilités pour s'introduire dans un système pour récolter des informations et/ou exécuter des commandes nuisibles. Exemples d'attaques : exploitation des erreurs de configuration, exploitation des bugs…
- Abus de droits légitimes *:* Utilisation d'une fonctionnalité du système de façon abusive. Exemples d'attaques : sniffer, ou trop de requêtes pour saturer un serveur.
- Action physique : Destruction, altération ou changement physique de composants.
- Injection de code : Installation et exécution d'un module clandestin sur un système. Exemples d'attaques : virus, bombes logiques, cheval de Troie, ver…

III.7.2. L'anatomie d'une attaque

Plus connue sous « les 5 P », caractérisée par cinq verbes anglophones représentant les cinq étapes formant le squelette d'une attaque : Probe, Penetrate, Persist, Propagate, Paralize .

- **Probe :** consiste à collecter des informations sur le système cible avec différentes manières, comme par exemple, l'usage du programme Nmap afin de scanner des ports et connaitre la version des logiciels utilisés ainsi que le système d'exploitation et les services ouverts, et le programme Nessus qui scan les vulnérabilités, ou encore des outils comme firewalk, hping ou SNMP Walk pour découvrir la nature d'un réseau.
- **Penetrate** : consiste à utiliser les informations collectées afin de pénétrer un réseau, avec des techniques d'outrepassement des protections par mots de passes et d'exploitation de failles, et bien d'autres.
- **Persist :** il s'agit de créer un compte avec des droits d'un utilisateur afin de pouvoir se réinfiltrer ultérieurement, ou bien d'installer une application de contrôle à distance comme par exemple, un cheval de Troie. On parle d'extension de privilège.
- **Propagate :** consiste à parcourir le réseau en observation, à la recherche de ce qui est disponible et accessible dans celui-ci.
- **Paralize :** cette étape consiste à passer en action dans le réseau cible, c'est là que l'intrus exécute son plan d'attaque, il peut par exemple violer l'intimité des informations, endommager des données sensibles, causer un déni de service...

III.7.3. Les attaques les plus connues [6]

III.7.3.1. Attaques par injection de codes

Ce sont des attaques dues au manque de vigilance de l'utilisateur lors de son utilisation de certains outils logiciels et documents avec macros qui sont téléchargés sur Internet sans précaution. Ce type d'attaques utilise des *malware*, qui sont des codes ou des parties de codes destinés à perturber le bon fonctionnement de programmes essentiels au système :

. Les virus

Ce sont des programmes nuisibles(écrits dans n'importe quel langage) placés dans des programmes sains, capables d'infecter d'autres programmes en les modifiant de façon à ce qu'ils puisse se reproduire à leurs tour. Il existe des virus capables d'attaquer n'importe quel type de machine (routeurs, serveur web, etc) équipés de n'importe quels systèmes et logiciels.

. Les vers réseau

Les vers réseau sont des programmes malicieux qui peuvent se reproduire sans avoir à infecter d'autres programmes, et peuvent aussi se déplacer à travers un réseau. En effet, ils sont capables de saturer la bande passante, voir même créer un déni de service.

. Les chevaux de Troie (trojan horse)

On appelle cheval de Troie un programme informatique nuisible ouvrant une porte dérobée (backdoor) dans un système (port réseau) à un intrus ou d'autres programmes indésirables, dans le but d'exécuter des actions nuisibles, comme le vol de mots de passe, copie de données sensibles, contrôle à distance, et bien d'autres.

Une infection par cheval de Troie est traduite parfois par les symptômes suivants :

- Activité anormale du modem ou de la carte réseau : des données sont chargées en l'absence d'activité de la part de l'utilisateur.
- Des ouvertures non envisagées de programmes.
- Des réactions anormales de la sourie et plantages à répétition.

. Les spyware (espiologiciels)

Ce sont des programmes chargés de recueillir des informations de l'ordinateur dans lequel ils sont installés et les envoyer au pirate. Les récoltes d'informations peuvent ainsi être des adresses web des sites visités, des mots-clés saisis dans le moteur de recherche, ou même des analyses des achats via Internet. Outre le préjudice causé par la divulgation d'informations, ces logiciels peuvent être une source de nuisance comme la consommation de mémoire vive et d'espace disque et le plantage d'autres application.

III.7.3.2. Attaques par ingénierie sociale

Une attaque par ingénierie sociale exploite la naïveté de l'utilisateur non sensibilisé, elle permet parfois à un pirate de palier à l'absence de faille et d'extraire ainsi des informations de l'utilisateur sans que ce dernier ne s'en aperçoive d'une mal-intension. Pour ce faire le pirate usurpe par exemple une identité de confiance au téléphone, ou encore utilise les réseaux sociaux, afin de collecter des données personnelles, qui peuvent lui permettre de trouver des mots de passe ou de se faire passer pour les personnes que la victime connait.

II.7.3.3. Attaques réseaux

Ces attaques se basent principalement sur l'exploit des faiblesses liées aux protocoles ou à leurs implémentations en réseau. Les attaques réseaux proviennent généralement du:

. **Scan**

Le scan est une attaque passive, visant la confidentialité en utilisant la méthode d'écoute, elle consiste seulement à récolter des informations. Bien évidement, il y'a différentes techniques de scan. Idéalement, la meilleure est celle qui est la plus furtive afin de ne pas alerter les soupçons de la future victime. Les plus répandues sont:

. *Le scan avec des programmes de scan* : les plus connus, Nmap, qui détermine les ports ouverts, et donc les services exécutés sur la machine cible (exemple : le port 21/TCP pour un service FTP). Il existe un autre type de scanneur, le mappeur passif (exemple : Siphon), permet de connaître la topologie réseau du brin physique sur lequel les paquets sont analysés.

. *Le scan furtif :* aussi appelé scan SYN. Il n'établit pas complètement la connexion TCP: pas de commande ACK après avoir reçu l'accord de se connecter. Grâce à ceci, la méthode est bien plus furtive.

. *Le scan à l'aveugle :* avec usurpation d'une machine intermédiaire. Le système attaqué pense que le scan est réalisé par la machine intermédiaire et non par un pirate.

. *Le scan passif :* est la méthode la plus furtive. Consiste à analyser les champs d'en-tête des paquets et les comparer avec une base de signatures qui pourra déterminer les applications qui ont envoyé ces paquets.

. Intrusion

Signifie pénétration des systèmes d'information ou des réseaux mais aussi tentatives des utilisateurs locaux d'accéder à de plus hauts privilèges que ceux qui leur sont attribués, ou tentatives des administrateurs d'abuser de leurs privilèges.

. Usurpation d'adresse IP (IP spoofing)

Consiste à se faire passer pour une machine appartenant au réseau en truquant les paquets IP (paquets spoofés) en remplaçant l'adresse IP de l'expéditeur (pirate) par l'adresse

IP d'une machine (de confiance) déjà existante dans le réseau après avoir rendu celle-ci invalide, cette technique d'attaque est utile dans le cas d'une authentification basée sur une adresse IP. En effet, elle permet à un pirate de faire passer des paquets sur un réseau, sans que ceux-ci soient interceptés par le système de filtrage de paquets.

Cependant, en spécifiant une adresse IP différente de la sienne, le pirate ne recevra pas les réponses du serveur, puisque celui-ci répondra à l'adresse spoofée. Il existe toutefois deux méthodes permettant de récupérer les réponses :

- *Source routing :* technique consistant à placer le chemin de routage directement dans le paquet IP. Cette technique ne fonctionne plus de nos jours.
- *Reroutage :* consiste à envoyer des paquets RIP aux routeurs afin de modifier les tables de routage. Les paquets avec l'adresse spoofée seront ainsi envoyés aux routeurs contrôlés par le pirate.

. Le sniffing

Un sniffer (renifleur) est un dispositif matériel ou logiciel capable d'écouter un trafic. Le sniffing consiste à l'écoute passive par surveillance des paquets IP qui transitent sur un réseau à l'aide d'un sniffer. L'un des buts finals est de récolter illégalement des informations et des mots de passe. Cette écoute de données en transit peut conduire à des intrusions illicites.

Une protection peut être apportée aux mécanismes de transfert de mots de passe, leur chiffrement. Ceux-ci chiffrés devront alors être « cassés ». Deux possibilités :

- *l'attaque en force :*essayer toutes les permutations possibles pouvant constituer une clé pour déchiffrer le mot de passe en connaissant l'algorithme utilisé.
- *l'attaque par dictionnaire* : deviner le mot de passe chiffrés par comparaison avec des listes de mots de passe eux aussi chiffrés contenus dans des dictionnaires.

III.7.3.4. Attaques contre la communication

Une attaque contre la communication peut s'agir des cas suivants :

- **Interruption :** vise la disponibilité des informations. consiste à accéder à l'information (destruction ou détournement), ce qui fait qu'elle ne sera pas transmise.
- **Interception :** vise la confidentialité des informations, et consiste en un écoute passif.
- **Modification :** vise l'intégrité et la disponibilité des informations.
- **Fabrication :** vise l'authenticité des informations. Appelée aussi mascarade. Consiste à envoyer des informations stipulant qu'elles viennent d'une source connue.

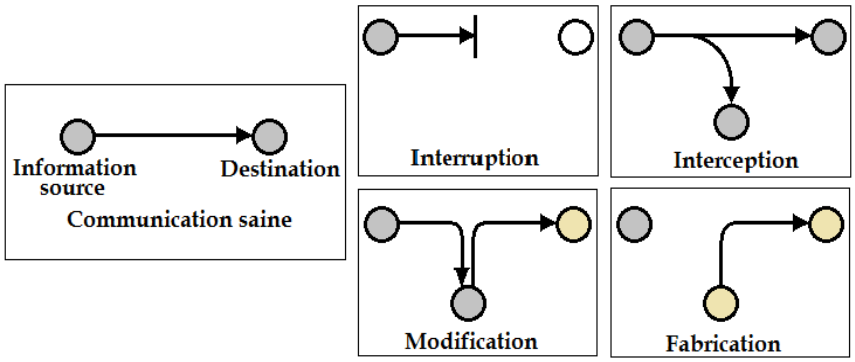

Figure III.1 : Les attaques contre la communication

III.7.3.5. Attaques Man In The Midle (MITM)

L'attaque de l'homme au milieu encore appelée attaque de l'intercepteur permet de détourner le trafic entre deux stations. Pour ce faire, le pirate écoute la communication entre deux machines et falsifie les échanges en se mettant au milieu de la communication, ainsi tous les paquets passent par lui, et les retransmet en toute transparence à l'autre machine. Parmi les attaques man in the midle les plus connues, on trouve :

. ARP spoofing (ARP cache poisoning)

C'est une attaque qui exploite les failles du protocole ARP. L'objectif est de permettre de retrouver l'adresse IP d'une machine en connaissant l'adresse MAC de celle-ci.

✧ ***Le principe* :**

L'attaquant s'interpose entre deux machines du réseau, il envoie à chacune d'elles un paquet ARP falsifié (spoofé) indiquant que l'adresse MAC de l'autre machine a été changée, et que la nouvelle est celle de l'attaquant. Les deux machines cibles vont ainsi mettre à jour leurs tables dynamiques appelées cache ARP, c'est pour sa qu'on parle de ARP cache poisoning ou ARP redirect. De cette façon, quand une des deux machines envoie des paquets à l'autre, ils seront transmis à l'attaquant qui les retransmettra de manière transparente à la machine destinatrice.

. Détournement de session TCP (TCP session hijaking)

Le vol de session TCP est une technique qui consiste à intercepter une session TCP initiée entre deux machines afin de la détourner. En effet, le contrôle d'authentification s'effectuant uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.

✧ ***Principe :***

Dans un premier temps, le pirate écoute le réseau, et lorsqu'il estime que l'authentification a pu se produire, il désynchronise la session entre l'utilisateur et le serveur. Pour ce faire, il construit un paquet avec, comme adresse IP source, celle de la

machine de l'utilisateur et le numéro d'acquittement TCP attendu par le serveur. Le pirate prend possession de la connexion en cours, et peut dresser ses commandes.

III.7.3.6. Attaques par failles applicatives

Ces attaques se basent sur l'exploitation des vulnérabilités des programmes utilisés ou aussi des erreurs de configuration. Pour exploiter ces bogues, le pirate fait appel à des «exploits » qui sont de petits programmes permettant d'exploiter une faille dans un but précis (obtenir un interpréteur de commandes, accéder à certains fichiers, augmenter ses droits...) :

. Les injections SQL

Les données sont envoyées par le client par l'intermédiaire d'un script sur le serveur web. Il s'ensuit une connexion au serveur SQL, puis l'envoi des données de la requête du client. La requête est exécutée par le serveur SQL. La réponse est reçue par le client et est affichée sous la forme d'une page web.

L'attaque par SQL-Injection consiste à injecter des caractères spéciaux ou des chaînes de caractères particulières dans les requêtes SQL du client. Ces caractères peuvent être interprétés par le serveur SQL comme des commandes permettant d'obtenir un accès sans mot de passe, de récupérer des fichiers ou des informations de la base de données (exemple : mots de passe) ou encore détruire des données, etc..

III.7.3.7. Attaques Déni de service

Elles visent à rendre indisponible un service, on distingue deux types de déni de service. Les attaques déni de service les plus connues sont :

. UDP flooding

Le flood consiste à envoyer très rapidement de gros paquets d'information (attaque massif) à une machine avec une fréquence d'envoie élevée, de telle sorte que la victime ne pourra plus répondre aux requêtes (paralyser).

✧ ***Principe d'UDP flooding :***

Le trafic UDP est prioritaire sur TCP. Le but de UDP flooding est donc d'envoyer un grand nombre de paquets UDP, ce qui va occuper toute la bande passante et ainsi rendre indisponible toutes les connexions TCP. Exemple : faire une requête chargen (port 19 / service de génération de caractères) à une machine en spoofant l'adresse et le port source, pour rediriger vers echo (port 7 / service qui répète la chaîne de caractères reçue) d'une autre machine.

. TCP SYN flooding

Toute connexion fiable (utilisant TCP) s'effectue en utilisant le mécanisme de poignée de main en trois temps (Three Way Handshake) : SYN / SYN-ACK / ACK. Une connexion ne peut s'effectuer que lorsque ces trois étapes ont été franchies :

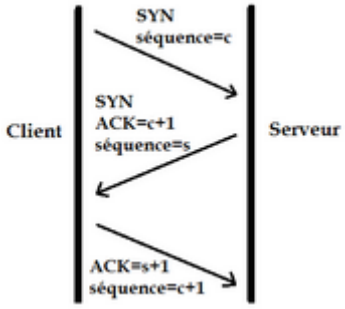

Figure III.2 : La connexion TCP en trois temps

Cependant, ce mécanisme possède une faiblesse, lorsque le serveur renvoie un accusé de réception (*SYN-ACK*) pour un client qui demande d'établir une connexion (bit SYN activé), mais ne reçoit aucun accusé (*ACK*) en retour de ce client. Dans ce cas le serveur crée une structure de données (en mémoire) contenant toutes les connexions semi-ouvertes en attente.

✧ ***Principe de l'attaque :***

Le TCP SYN flooding, exploite la faille de connexion en trois temps. Le pirate envoie de nombreuses demandes de connexion (SYN), des SYN-ACK sont renvoyés, mais il n'y aura jamais de réponse avec ACK car l'adresse source fournie par le pirate est non fonctionnelle, ce qui fait un grand nombre de connexions TCP en attente. Il y a un mécanisme d'expiration permettant de rejeter les paquets SYN au bout d'un certain délai, et libérer l'espace pour d'autres connexions, mais le système agresseur envoie des paquets plus vite que le temps nécessaire au serveur pour faire expirer les demi-connexions. Sa occupe des ressources mémoire, ce qui va entraîner un état instable pouvant conduire à un plantage.

. Attaques ICMP

Le protocole ICMP contrôle l'acheminement des paquets de données IP, et si un problème de transmission est détecté par un routeur, celui-ci informe l'émetteur du paquet en lui envoyant un paquet ICMP.

L'attaque ICMP, consiste à envoyer de faux messages ICMP pour surcharger le réseau, le rendre inutilisable, et entraîner certains dénis de service.

Autres exemples :

- Paralyser le réseau en rédigeant des paquets IP vers une fausse destination.

- Augmenter la charge des systèmes en faisant traiter un grand nombre de messages ICMP.
- Empêcher un émetteur d'envoyer des données, en exploitant la facilité offerte par ICMP pour contrôler le flux d'émission des paquets.

. Attaque par réflexion (Smurf)

Attaque basée sur l'utilisation de serveur broadcast. Un serveur brodcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines du réseau.

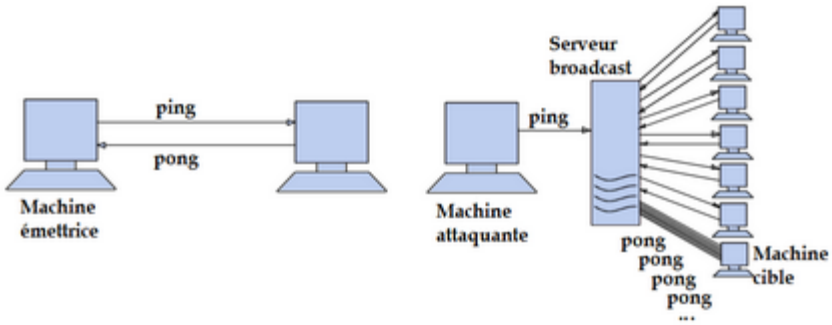

Figure III.3 : L'attaque par réflexion

Le pirate fait des requêtes ICMP ECHO (ping) à un ou plusieurs serveurs de broadcast en spoofant l'adresse source (en indiquant l'adresse de la machine cible). Cette machine cible va recevoir un nombre énorme de réponses, car toutes les machines vont lui répondre, et ainsi utiliser toute sa bande passante et causer son instabilité.

III.8. Les mécanismes de défense [8]

Parmi les mécanismes de défense :

• **La veille technologique :** être en actualité sur les failles, les correctifs, et les nouvelles procédures publiés dans les sites spécialisés (en s'abonnant aux alertes de sécurité des CERT par exemple). Et faire ainsi évoluer la sécurité au cours du temps afin de maintenir un niveau suffisant de protection du système d'information.

• **Sensibilisation des utilisateurs :** mettre les utilisateurs au courant des risques.

• **La protection physique :** consiste à sécuriser l'environnement du système.

• **Antivirus :** logiciel conçu pour protéger l'ordinateur contre les malware.

• **Signature numérique**: données ajoutées pour vérifier l'intégrité ou l'origine des données.

• **Contrôle d'accès :** consiste à vérifier les droits d'accès d'une entité aux ressources.

• **Journalisation (logs) :** Enregistrement des activités de chaque acteur. Permet de constater que des attaques ont eu lieu.

• **Chiffrement :** utiliser des algorithmes basés sur des clés pour transformer les données.

• **Inspection dynamique et filtrage des paquets (pare feu):** un élément (logiciel ou matériel) du réseau contrôlant et filtrant les communications qui le traversent.

• **Système de détection d'intrusion** : repère les activités anormales ou suspectes sur le réseau surveillé. Ne détecte pas les accès incorrects mais autorisés par un utilisateur légitime.

• **Analyse des vulnérabilités** : identification des points de faiblesse du système.

• **Contrôle du routage :** sécurisation des chemins (liens et équipements d'interconnexion).

• **Contrôle d'accès aux communications :** le moyen de communication n'est utilisé que par des acteurs autorisés. Par VPN ou tunnels.

• **Désactivation des services inutiles :** Pour rendre l'accès plus difficile aux pirates.

Remarque : ces mécanismes peuvent néanmoins provoquer une gêne pour les utilisateurs, et les consignes et règles deviennent compliquées si le réseau est étendu. En effet, la sécurité doit être étudiée de façon à ne pas présenter un handicape. C'est la raison pour laquelle il est nécessaire de définir et de suivre dans un premier temps une **politique de sécurité**.

III.9. Cycle d'une politique de sécurité [5]

. La planification : consiste à identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences. Puis élaborer des règles et des procédures à mettre en œuvre dans les différents sévices de l'organisation pour les risques identifiés. Cette phase peut donc être récapitulée en trois étapes :

- ✧ Identification des besoins en termes de sécurité.
- ✧ Analyse de risques.
- ✧ Définition de la politique de sécurité.

. La mise en œuvre : consiste à déployer des mécanismes et des dispositifs de sécurité visant à protéger le réseau (sécurisation) tout en faisant appliquer les règles et les procédures élaborées dans la politique de sécurité.

. Le suivi : consiste en :

- ✧ Les audits de sécurité : l'objectif est de vérifier que chaque règle de la politique de sécurité est correctement appliquée et que l'ensemble des dispositions pris forme un tout cohérent et sûr.
- ✧ Les tests d'intrusion : consiste à éprouver les moyens de protection en essayant de s'introduire dans le système en situation réelle. Le test comprend :
  - Des tests de maintenance : **ping** pour vérifier la connectivité, et **traceroute** pour déterminer le chemin entre deux nœuds avec détails…
  - Des tests logiciels : **crack et COPS** pour tester les mots de passe, et **SATAN** ou **MBSA** pour analyser les vulnérabilités, et **Nmap** pour le scan de ports.

- ✧ Détection des incidents : grâce à des mesures permettant de détecter les incidents de sécurité, comme par exemple, les systèmes de détection d'intrusion.

. La réaction : modifier ou mettre à jour la politique de sécurité de façon à ce qu'elle puisse repondre aux nouvelles exigences de sécurité en essayant de combler les nouvelles failles.

III.10. Description des principaux dispositifs de défense

Les pare-feux et les autres dispositifs à filtrage, les tunnels et les systèmes de détection d'intrusion sont des outils indispensables pour détecter, parer ou éviter de nombreuses attaques. Nous les décrirons, en incluant la manière de les utiliser de façon optimale :

III.10.1. La cryptographie

III.10.1.1. Définitions :

- ✦ **Cryptographie :** Ce mot est dérivé du mot grecque « kripto » qui veut dire caché, et « graphos » qui veut dire écrire, donc c'est l'ensemble des techniques permettant de chiffrer des données pour les rendre inintelligibles sans une action spécifique afin d'assurer l'intégrité et confidentialité ainsi que leur authenticité des informations.
- ✦ **Cryptologie :** Elle est basée sur l'arithmétique, il s'agit dans le cas d'un texte de transformer les lettres en une succession de chiffres, puis de faire des calculs sur ces chiffres pour :
- ➢ Les modifier de telle sorte à les rendre incompréhensibles (le résultat de la modification s'appel cryptogrammes).
- ➢ Faire en sorte que le destinataire saura les déchiffrer.
- ➢ **Chiffrement et déchiffrement :** Chiffrer un texte en clair consiste à le transformer en cryptogramme utilisant des méthodes évoluées (algorithmes, clé…). La technique inverse consiste à retrouver le message original, appelée déchiffrement. Le chiffrement se fait à l'aide d'une clé de chiffrement, et le déchiffrement bien entendu avec une clé de déchiffrement.

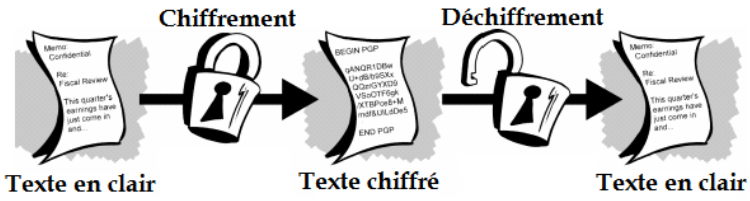

Figure III.4 : Le chiffrement et le déchiffrement

- ✦ **Cryptanalyse :** C'est la reconstruction d'un message (déchiffrement), lorsque la clé de déchiffrement n'est pas connue de l'attaquant**.** Lorsqu'une méthode de cryptanalyse réussi à déchiffré un message, on dit alors que l'algorithme de chiffrement a été cassé.

III.10.1.2. Les cryptographies basiques

- **La cryptographie à clé secrète (symétrique) :** une seule clé suffit pour le chiffrement et le déchiffrement.

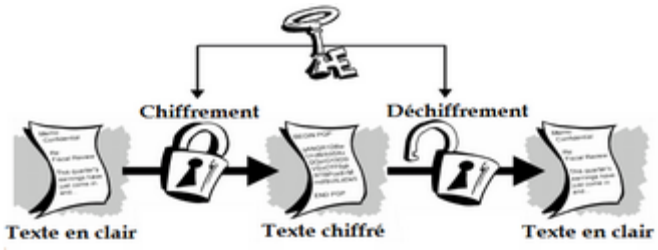

Figure III.5 : Le cryptage symétrique

- Avantage : Une cryptographie simple à utiliser et ne nécessite pas beaucoup de temps.
- Inconvénients : l'échange des clés de déchiffrement (présence de risque). Et l'utilisation d'autant de clé qu'il y'a d'interlocuteurs.

La solution consiste à adopter une autre cryptographie, c'est celle à clés publiques.

- **La cryptographie à clé publique (asymétrique) :** Les clés existent par paires (bi-clés). Une clé publique pour le chiffrement, et une clé privée pour le déchiffrement.

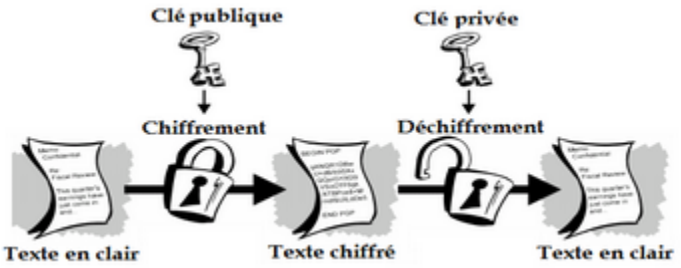

Figure III.6 : La cryptographie asymétrique

- **Principe :**

. Les utilisateurs choisissent une clé aléatoire qu'ils sont seuls à connaitre (clé privée).

. A partir de cette clé, ils déduisent chacun un algorithme automatiquement (clé publique).

. Les utilisateurs s'échangent ces clés publiques.

. Lorsqu'un utilisateur désir envoyer un message à un autre, il lui suffit de le chiffrer au moyen de la clé publique du destinataire, qu'il trouvera dans un serveur de clés tel qu'un annuaire LDAP. Le destinataire le déchiffrera avec sa clé secrète.

- Avantage : permet d'échanger des messages de manière plus sécurisée. Il n'y a plus de besoin de partager des clés secrètes via une voie de transmission.

- Inconvénients : la lourdeur, mais aussi problème de gestion des clés en l'absence d'une autorité de certification. Il faut s'assurer de l'authenticité des individus désirant communiquer avec le gestionnaire de clés pour enregistrer leur clé publique.

La solution est la signature numérique des clés publiques, permettent au destinataire de vérifier l'*authenticité* des acteurs. Elle garanti l'*authentification* et l'*intégrité* des données. Elles fourni également une fonctionnalité de *non répudiation*. Une signature manuscrite peut être imitée, alors qu'une signature numérique est pratiquement infalsifiable. Seul le possesseur est capable de générer la signature, mais toute personne ayant accès à la clé publique correspondante peut la vérifier.

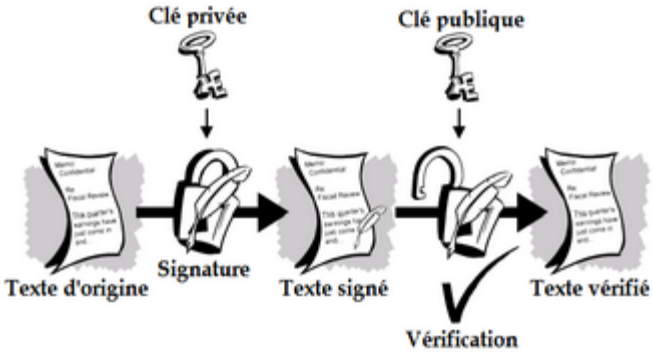

Figure III.7 : La signature numérique

En réalité, signer consiste à calculer une empreinte (par application d'une fonction de hachage) du message à signer et à ne chiffrer que cette empreinte.

III.10.1.3.Fonctions de hachage

C'est une fonction qui permet d'obtenir un condensé (appelé aussi haché) d'un texte, c'est-à-dire une suite de caractères assez courte représentant le texte qu'il condense. En envoyant un message accompagné de son haché (ou condensât), il sera possible de garantir son intégrité, et cela par le simple calcul du haché du message reçu et puis la comparaison de ce dernier avec le haché accompagnant le document. Si le message a été altéré durant la communication, les deux empreintes ne correspondront pas. Et pour vérifier l'authenticité, le haché est signé, ce haché signé est nommé sceau. Ce mécanisme est appelé scellement.

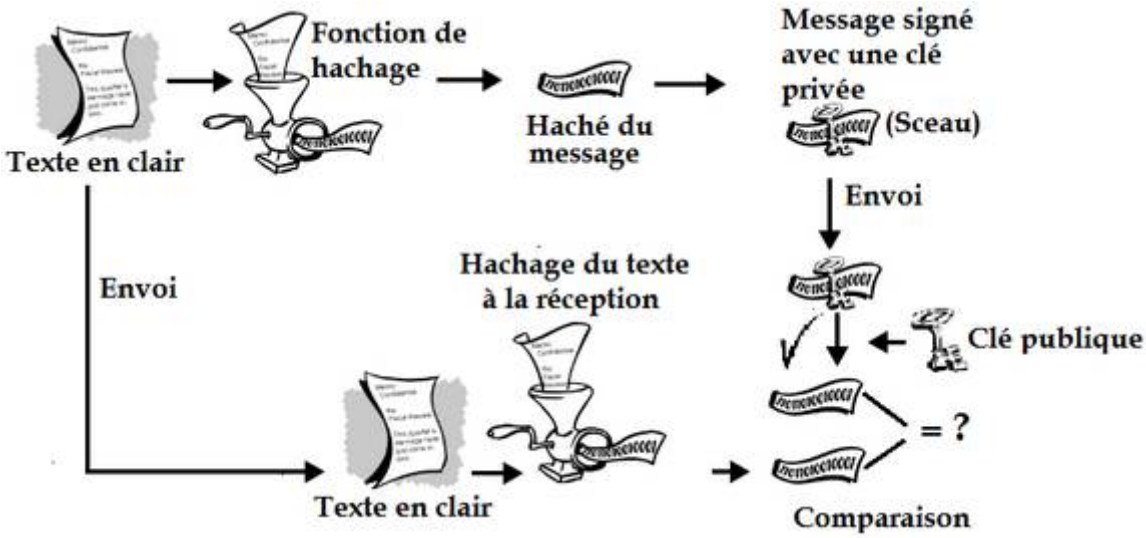

Figure III.8 : La vérification de l'intégrité et l'authenticité d'un message

III.10.1.4.Les protocoles sécurisés [5]

La plupart des protocoles de la suite TCP/IP ne sont pas sécurisés. Ainsi, des protocoles de plus haut niveau (dits protocoles sécurisés) ont été mis au point afin d'encapsuler des données dans des paquets chiffrés, les principaux sont :

- **SSL** (**S**ecure **S**ocket **L**ayer) : ou couche de sockets sécurisée, c'est un procédé de communication assez bas niveau (mais plus haut que IP Sec) sécurisé. Permet d'établir des connexions cryptées afin d'assurer la sécurité des transferts sur réseau. Le système SSL est indépendant du protocole utilisé, ce qui fait qu'il peut sécuriser des transactions faites par les protocoles HTTP, FTP, POP. SSL agit comme une couche supplémentaire (dans le niveau 4) assurant la sécurité.
- **HTTPS** (**H**yper**T**ext **T**ransfer **P**rotocol **S**ecure) : Technique de communication sécurisée basée sur HTTP et SSL.
- **SSH** (**S**ecure **Sh**ell) : permet à un utilisateur ou des services TCP/IP d'accéder à une machine distante via une communication chiffrée incluant l'authentification.
- **IP Sec** (**I**nternet **P**rotocol **Sec**urity) : Procédé de communication bas niveau (couche IP) sécurisé. Permet d'établir des connexions réseau cryptées. Les protocoles d'IPsec :

Les avantages des protocoles sécurisés :

- Les données circulant entre client et serveur sont chiffrées, ce qui garantie la confidentialité, il n'est donc pas possible d'écouter avec un analyseur de trame.
- Le client et le serveur s'authentifient mutuellement, il n'est donc pas possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

III.10.2. Les technologies de contrôle d'accès en réseau

III.10.2.1. Les pare-feux (firewalls) [6]

C'est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre un réseau interne et réseau externe, qui permet de protéger contre certaine attaques en contrôlant et filtrant les communications qui le traversent grâce à une politique de contrôle d'accès. Les firewalls sont donc utilisés pour les fins qui suivent :

- ✓ Le contrôle : Gérer les connexions sortantes à partir du réseau local.
- ✓ La sécurité : Protéger le réseau interne des intrusions venant de l'extérieur.
- ✓ La vigilance : Surveiller/tracer le trafic entre le réseau local et internet.

III.10.2.1.1. Principe de fonctionnement d'un firewall [6]

Des règles bien prédéfinies dans les firewalls permettent d'exécuter des méthodes de filtrage. L'ensemble de ces règles permettent ainsi soit, d'autoriser la connexion (permit), soit de bloquer la connexion (deny), ou de rejeter la demande de connexion (drop). Deux stratégies de configurations du filtrage dans les pare-feux sont habituellement distinguées:

- ✓ Tout ce qui n'est pas explicitement interdit est autorisé.

- ✓ Tout ce qui n'est pas explicitement permis est interdit.

La première stratégie est moins utilisée. En effet, par défaut tous les services TCP/IP sont autorisés. C'est pourquoi la seconde stratégie est préférée à la première et est souvent implémentée par défaut dans les équipements de filtrage.

III.10.2.1.2. Découpage en zones de sécurité (périmètres sécurisés) [5]

Un firewall permet non seulement de concentrer l'administration de la sécurité en des points d'accès limités au réseau mais aussi de créer des périmètres de sécurité (zones à différents niveaux de confiance), ce qui permet d'isoler les différents réseaux de l'entreprise on parle ainsi de « cloisonnement de réseaux » afin d'assurer une connectivité contrôlée et sécurisée en facilitant les tâches de surveillance et d'administration, mais aussi rependre au besoin de créer une nouvelle infrastructure vers un réseau à part dès lors que certaines machines ont besoin d'être accessible de l'extérieur du réseau (exemples : serveur web, serveur FTP public, serveur de messagerie…), on parle ainsi de zone démilitarisée (DMZ, Demilitarized Zone). Une politique de sécurité sera établie :

- ➢ Entre la DMZ et l'extérieur (internet)
- ➢ Entre le réseau externe et le réseau interne
- ➢ Entre la DMZ et le réseau interne (pour des mises à jours sur les serveurs de la DMZ, envoie et réception de messages…).

Remarque : Il existe une règle d'or concernant les DMZ, celle qui recommande de ne pas laisser une zone initialiser des communications vers une zone dont le niveau de sécurité est supérieur au sien. C'est le principe du moindre privilège.

III.10.2.1.3. Types de filtrage [6]

- ✧ **Filtrage simple de paquets (stateless packet filtering)**

C'est un filtrage sans état, le firewall analyse les en-têtes des paquets transitant (couche 3), et vu les règles de filtrage il autorise / interdit le passage d'un paquet selon: le port source/destination, le protocole UDP/TCP, l'adresse source/destination, e type de paquet ICMP, Interface d'entrée / de sortie.

Toutefois, vu l'utilisation de ports ouverts dynamiquement (aléatoirement), il est impossible avec ce type de filtrage de prévoir les ports à laisser passer ou à interdire. Pour y remédier, on a recours au système de filtrage dynamique.

- ✧ **Filtrage dynamique (statefull packet filtering)**

C'est un filtrage à état, il est basé sur l'inspection des couches 3 et 4 du modèle OSI. Un dispositif pare-feu est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets (état d'une connexion et/ou des drapeaux TCP) pour appliquer les règles de filtrage, c'est-à-dire adapter dynamiquement à ces règles.

Si ce type de filtrage est plus performant, il ne protège pas pour autant de l'exploitation des failles applicatives (liées aux vulnérabilités des applications).

✧ **Filtrage applicatif (proxy)**

En fonction du contenu de la couche 7 du modèle OSI, ce type de filtrage impose une connaissance des applications utilisées ainsi que la manière dont les données sont échangées, car celui-ci filtre les communications application par application, de plus, il permet la destruction des en-têtes précédant le message applicatif.

III.10.2.2. Implémentation des règles de sécurité dans les dispositifs à filtrage

Les ACL et les VLAN sont deux technologies adoptées pour leurs niveau de sécurité :

III.10.2.2.1. ACL (Access Control List) [9]

Une ACL, est une liste de règles d'accès implémentées sur un matériel réseau disposant des fonctionnalités de filtrage. Elle fourni un moyen de filtrer les flux en fonction d'informations appartenant aux couches 3 et 4 du modèle OSI. C'est-à-dire que l'autorisation ou l'interdiction des flux sont basées sur des critères d'adresse IP ou de port TCP ou UDP.

A. Les types d'ACL

Il existe plusieurs types d'ACL. Les listes d'accès Cisco sont soit standards, soit étendues :

- **ACL standards (IP standard access list) :** permettent d'autoriser ou de refuser le trafic selon les adresses IP source (le seul critère de filtrage est l'adresse IP source).
- **ACL étendues (IP extended access list) :** permettent de filtrer les paquets IP en fonction de plusieurs attributs, le type de protocole, l'adresse IP source, l'adresse IP destination, les ports TCP/UDP source et destination.

Remarque : Chaque ACL est identifiée avec un numéro unique d'une plage précise valable pour le protocole. Tel que :

- ACLs standards : les plages de numéros assignés sont **<1-99>**, et **<1300-1999>**
- ACLs étendues : les plages de numéros sont **<100-199>**, et **<2000-2699>**

B. Fonctionnement d'une ACL

Quand une ACL est appliquée à une interface d'un dispositif à filtrage, les en-têtes de niveau 3 et 4 des paquets transitant sur le réseau sont analysées pour voir s'il remplissent les conditions du test. Toutefois, une liste d'accès peut être soit entrante, soit sortante :

- ✓ Les ACL Inbound (entrantes) : s'appliquent sur les paquets entrants à une interface. Ceux-là sont traités et testés avant d'être routés vers l'interface de sortie. Une ACL Inbound réduit la charge des recherches de routage en cas d'abandon du paquet.
- ✓ Les ACL Outbound (sortantes) : appliquées sur les paquets sortants d'une interface. Les paquets entrants sont routés vers l'interface de sortie puis traités par le biais de la liste de contrôle d'accès sortante.

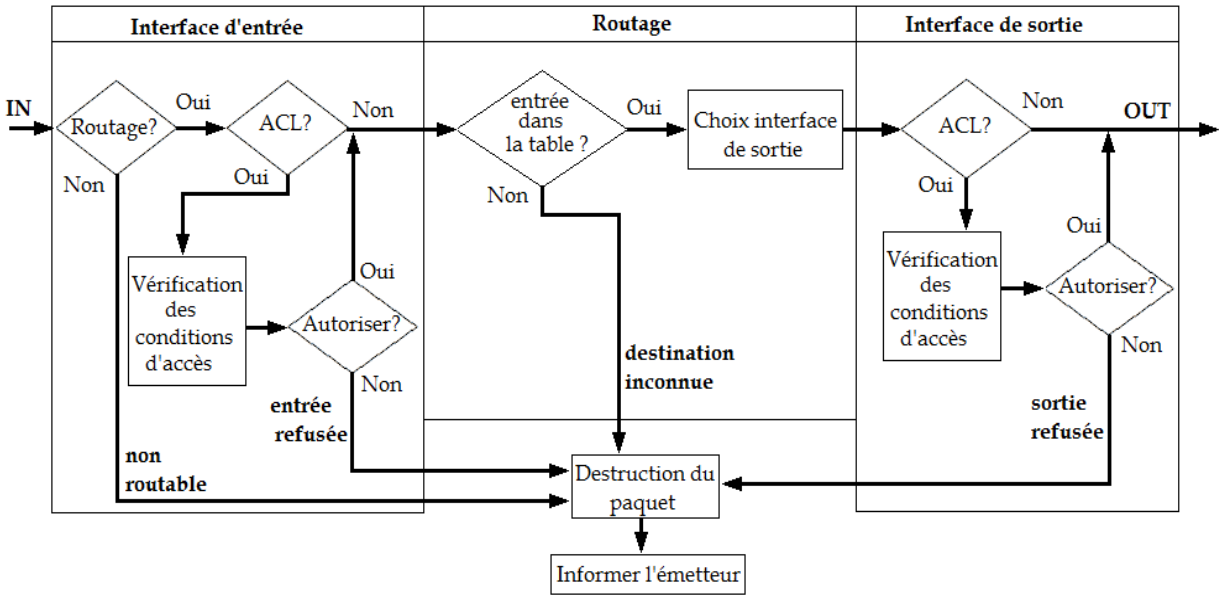

Figure III.9 : Le fonctionnement des ACL

Les règles sont parcourues dans l'ordre. Dès qu'une règle correspond (match) on saute vers la chaîne indiquée (permit, deny, ou drop). Si aucune règle ne correspond on applique la stratégie par défaut.

C.Configuration des ACL [17]

La configuration se fait en deux étapes, créer la liste d'accès puis l'assigner aux interfaces :

1. Créer la liste d'accès, c'est-à-dire définir les critères de filtrage :

L'ACL est crée en mode de configuration global. La syntaxe globale est la suivante:

```
Firewall(config)#access-list  access-list-number {deny | permit}  {les conditions de test}
```

→ **access-list** : commande permettant de créer des listes d'accès.

→ **access-list-number** : numéro qui identifie l'ACL selon le type.

→ **deny | permit** : indiquent la manière (interdire/autoriser) dont les paquets seront traités par le logiciel IOS selon le résultat des conditions à tester.

→ **les conditions de test** : spécifie les conditions à vérifier par l'instruction.

2. Appliquer la liste d'accès sous une ou plusieurs interfaces niveau 3(serial, ou vlan) d'un routeur, un firewall, ou Switch niveau 3:

Les ACL sont affectées à une ou plusieurs interfaces et peuvent filtrer du trafic entrant ou sortant, l'assignement se fait dans le mode config-if avec la syntaxe suivante :

```
Firewall(config-if) #{protocol} access-group access-list-number {in|out}
```

→ **in|out** : indique si l'ACL s'applique sur les parquets entrants ou sortants.

❖ **Création d'une ACL standard :**

Voici la structure d'une ACL standard:

```
Access-list access-list-number {deny | permit} source [source-wildcard mask]
```

→ **Source** : identifie l'adresse IP source, on peut trouver deux cas :
- *Host adresse IP* : pour spécifier un seul hôte
- *Any* : pour n'importe quelle machine

→ **wildcard mask**: le masque générique. Pour spécifier une ou plusieurs adresses IP.

❖ **Création d'une ACL étendue :**

```
access-list acces-list-number { deny | permit } protocol source source-wildcard [operator port] destination destination-wildcard [operator port] [established] [log]
```

→ **Protocol :** spécifie le protocole sur lequel on filtre (filtrer soit sur IP, soit sur TCP…)
→ **operator:** un opérateur sur les ports, c'est-à-dire on peut spécifier exactement le port avec l'opérande **eq** (equal), ou inférieur avec **lt** (less than), ou bien supérieur avec **gt** (great than), ou différent avec **neq** (not equal).
→ **port :** spécifie le port (source/destination).
→ **Established :** autorise le trafic TCP si les paquets utilisent une connexion établie (bit de ACK).
→ **Log :** obtenir du log à chaque fois qu'une adresse IP vérifie la liste de contrôle.

D. Principe du wildcard mask (masque générique)

Un masque de bits générique est une quantité binaire de quatre octets. Ce masque est jumelé à une adresse IP. Les chiffres 1 et 0 sont utilisés pour indiquer la façon de traiter les bits de cette adresse :

- 0 permet de vérifier la valeur du bit correspondant dans l'adresse IP.
- 1 permet de ne pas vérifier (ignorer) la valeur du bit correspondant.

Les ACL utilisent le masquage générique pour identifier une adresse unique ou plusieurs adresses dans le but d'effectuer des vérifications visant à accorder ou interdire l'accès. Pour trouver le wildcard mask d'une adresse, en soustrait son masque de sous-réseau de 255.255.255.255.

E. Postions optimales des listes d'accès

Pour placer les ACL de façon optimale afin d'obtenir un grand impact sur les performances, il faut :

- Placer les listes de contrôle d'accès étendues le plus près possible de la source du trafic refusé. Ainsi, le trafic indésirable est filtré sans traverser l'infrastructure réseau.
- Positionner les ACL standards le plus près possible de la destination, puisqu'elles ne précisent pas les adresses.

Remarque : Une seule ACL est permise par port, par protocole et par direction, c'est-à-dire qu'on ne peut pas par exemple définir deux ACL sur l'interface Ethernet0 pour le trafic IP sortant. Par contre, on peut définir deux ACL pour le trafic IP mais, une pour le trafic entrant et l'autre pour le trafic sortant…

III.10.2.2.2. Les VLAN (virtual LAN) [2]

Un VLAN est un réseau regroupant les machines de manière logique et non plus physique. Sur un Switch, un VLAN est un groupe de ports, les machines connectées à ces ports (même identifiant VLAN) peuvent communiquer entre elles librement. En revanche, toute communication est impossible avec un port étranger au VLAN, ces communications inter-VLAN doivent transiter par un routeur. En fait, les VLAN introduisent la notion de segmentation virtuelle, qui permet de constituer des sous-réseaux logiques selon des critères prédéfinis (ports, adresses MAC, adresses réseau...).

Les VLAN optimisent l'utilisation de la bande passante car ils limitent les domaines de diffusion, et autorisent une répartition et un partage optimal des ressources de l'entreprise. En plus des nouvelles exigences de sécurité qui découlent de l'utilisation de ceux-ci.

A. Les types de VLAN

On distingue trois types de VLAN :

- VLAN par port : niveau 1.
- VLAN par adresse MAC : niveau 2.
- VLAN par sous-réseau / protocole : niveau 3.

B. La gestion centralisée des VLAN [5]

- **Le protocole VTP (VLAN Trunking Protocol) :**

Il permet de réaliser une gestion centralisée des VLAN sur un modèle de type maître/esclave, et donc configurer un Switch qui propagera les configurations VLAN aux

autres Switchs du domaine. Il mémorise les configurations VLAN dans la base de données VLAN des Switchs (vlan.dat). Un domaine VTP est composé de Switchs interconnectés. Pour échanger les configurations entre ces Switchs, il utilise l'« annonce VTP » ou « information VTP » à l'aide de liens « trunk ». Une configuration VTP par default d'un switch induit à: une version VTP de 1, un VTP Domain Name valant « null », un mode VTP « serveur », tout les ports dans VLAN1.

Remarques :

1. Un trunk représente le canal par lequel transitent les trames des différents VLAN entre commutateurs (lien point-à-point entre deux ports). Pour que les commutateurs sachent à quel VLAN appartient une trame, un étiquetage est nécessaire. Les protocoles d'étiquetage utilisés sont ISL (Cisco) et IEEE 802.1q. C'est ce dernier qui est utilisé, sous la dénomination dot1q.

2. Par défaut, Cisco utilise le VLAN1 pour assigner les ports du commutateur ainsi que son administration. Ce VLAN est utilisé par défaut pour faire transiter sur des trunks des protocoles tels que CDP et VTP.

III.10.3. Translation d'adresses (NAT, PAT)

La croissance rapide d'Internet est surprenante. Sans le développement de nouvelles méthodologies d'assignation d'adresses IP, cette croissance rapide aurait épuisé la réserve existante d'adresses IP. Pour pallier à cette pénurie d'adresses IP, plusieurs solutions ont été développées, leurs principe est de masquer plusieurs adresses (ou ports) privées avec un nombre limité d'adresses (ou ports) publiques. Ces solutions, largement mise en œuvre, sont la traduction d'adresses réseau (NAT) et la traduction d'adresse de ports (PAT).

III.10.3.1. La NAT (Network Adress Translation)

C'est un mécanisme permettant de simplifier la gestion de l'adressage IP utilisée pour se connecter à l'extérieur tout en conservant les adresses IP enregistrées dans les réseaux privés. Lorsqu'un paquet est routé par un équipement de réseau (routeur ou pare-feu) vers des réseaux externes, une adresse IP publique routable est attribuée par la passerelle NAT à l'adresse source, c'est-à-dire l'adresse réseau interne privée (non routable). L'adresse publique de la réponse est ensuite retraduite en l'adresse interne privée. Cela, permet de sécurisé, en empêchant de voir les adresse IP privées du réseau interne, les requêtes sembleront ainsi parvenir de la passerelle NAT. On distingue deux types de NAT :

III.10.3.1.1.NAT statique

Utilise un mappage qui reste constant. C'est un mécanisme utile pour les serveurs Web ou les hôtes qui doivent disposer d'une adresse permanente, accessible depuis Internet. Ces hôtes internes peuvent être des serveurs d'entreprise ou des périphériques réseau. Cependant, ce mécanisme permet de connecter des machines à internet de façon transparente, mais sans

pour autant résoudre le problème de la pénurie d'adresses dans la mesure où chaque machine requis une adresse IP publique à elle seule.

III.10.3.1.2.NAT dynamique

Permet de traduire un grand nombre d'adresses privées au moyen d'une adresse publique externe unique (prise parmi un pool) puis de retraduire dans l'autre sens, mais sa ne résous toujours pas le problème de pénurie d'adresses. Pour sa, le NAT dynamique utilise le mécanisme PAT (surcharge). **Le PAT** mappe plusieurs adresses IP privées à une seule adresse IP publique ou à quelques adresses. Lorsqu'un client ouvre une session TCP/IP, le routeur NAT translate son adresse source en publique et attribut un numéro de port au port source. Lorsqu'une réponse revient du serveur, le numéro de port source, devient le numéro de port de destination du client auquel appartiennent les paquets. Il confirme également que les paquets entrants étaient demandés, ce qui ajoute un niveau de sécurité à la session.

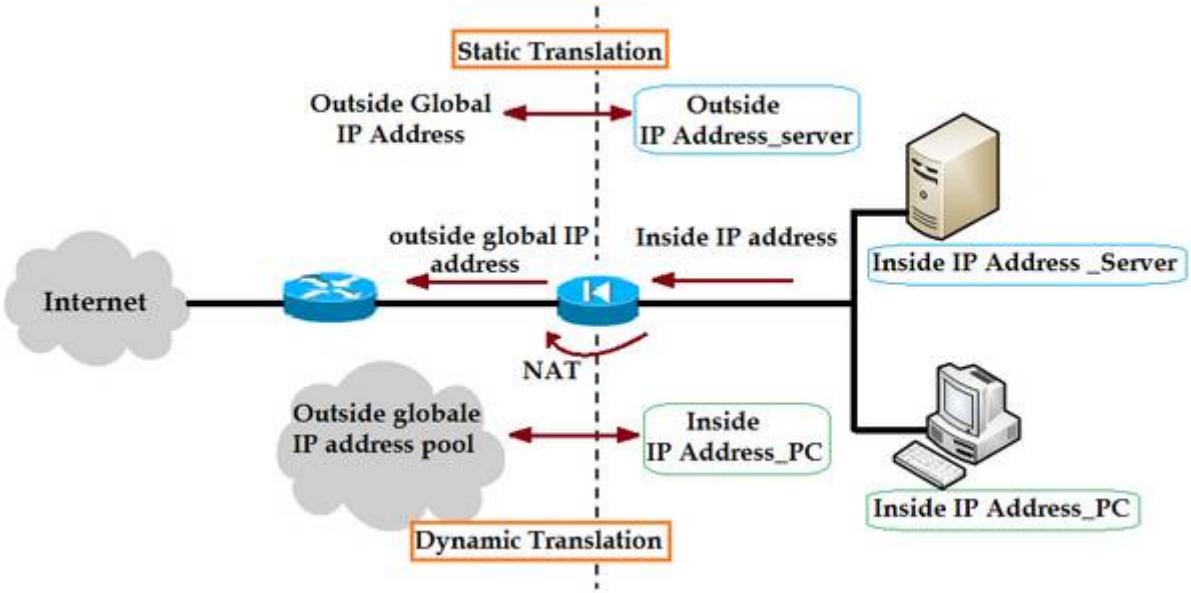

Figure III.10 : Principe du mécanisme de translation

III.10.3.2. Tables NAT et PAT

Les dispositifs (firewall, routeur ,..) configurés pour la NAT utilisent une table appelée table NAT qu'il mettent à jour :

Tableau III.1 : la table NAT statique

Adresse IP privée source	Adresse IP publique source
…	…

Tableau III.2 : la table NAT dynamique

@ IP privée source	Port privé source	@ IP publique source	Port public source	@ IP publique destination	Port public destination
…	…	…	…	…	…

III.10.3.3. Configuration de translation d'adresses [17]

A. Configuration du NAT statique :

Etapes à suivre	Instruction	Indication
1. Etablir la traduction statique entre une adresse locale interne et une adresse globale interne	Routeur(config)#**ip nat inside source static** ip-locale ip-globale	pour supprimer la traduction source statique : **no ip inside source static**
2. Spécifier l'interface interne	Routeur(config)#**interface** numéro type	on passe de Routeur(config) à Routeur(config-if)
3. Signaler l'interface comme connectée à l'intérieur	Routeur(config-if)#**ip nat inside**	
4. quitter le mode configuration d'interface	Routeur(config)#**exit**	
5. spécifier l'interface externe	Routeur(config)#**interface** numéro type	
6. signaler l'interface comme connectée à l'extérieur	Routeur(config-if)#**ip nat outside**	

Tableau III.3 : configuration de NAT statique

B. configuration du NAT dynamique

Tableau III.4 : configuration du NAT dynamique

Etapes à suivre	Instruction
1. définir un pool d'adresses globales à attribuer selon les besoins	Routeur(config)#**ip nat pool** nom ip-début ip-fin **{netmask** masque-réseau | **prefix-length** longueur-préfixe}
2. définir une ACL standard des adresses qui peuvent être traduites	Routeur(config)#**access-list** numéro-liste **permit** source [wildcard mask]
3.établir une source dynamique de traduction, en spécifiant l'ACL précédente	Routeur(config)#**ip nat inside source list** numéro-liste **pool** nom
4. spécifier l'interface interne	Routeur(config)#**interface** numéro type
5. signaler l'interface comme connectée à l'intérieur	Routeur(config-if)#**ip nat inside**
6. spécifier l'interface externe	Routeur(config)#**interface** numéro type
7. signaler l'interface comme connectée à l'extérieur	Routeur(config-if)#**ip nat outside**
8. quitter le mode configuration d'interfaces	Routeur(config)#**exit**

C. Configuration du PAT :

Tableau III.5 : Configuration du PAT

Etapes à suivre	Instruction
1. définir une ACL standard qui autorise les adresses qui doivent être traduites	Routeur(config)#**access-list** numéro-liste-contrôle **permit** source [wildcard mask]
2. spécifier l'adresse globale en tant que pool, à utiliser pour la surcharge	Routeur(config)#**ip nat pool** nom ip-début ip-fin **{netmask** masque-réseau | **prefix-length** longueur-préfixe}
3. établir la traduction de surcharge	Routeur(config-if)#**ip nat inside source list** numéro-liste-contrôle **pool** overload
4. spécifier l'interface interne	Routeur(config)#**interface** numéro type Routeur(config-if)#**ip nat inside** Routeur(config)#**exit**
5. spécifier l'interface externe	Routeur(config)#**interface** numéro type Routeur(config-if)#**ip nat outside** Routeur(config)#**exit**

Remarque : Les attaques distribuées seront toujours redoutables. Ce qui nous amène à comment détecter et empêcher ces attaques ?. En effet, Le fait d'installer un firewall n'est bien évidemment pas signe de sécurité absolue. Les firewalls ne protègent en effet que des communications passant à travers eux. La mise en place d'un firewall doit donc se faire en accord avec une véritable politique de sécurité. D'autre part la mise en place d'ACL n'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système, et ne protège pas d'une attaque venant du réseau interne (qui ne traverse pas le dispositif à filtrage). Ceci induit à utiliser d'autres dispositifs comme les IDS.

III.10.4. Les systèmes de détection d'intrusion (IDS-Intrusion Detection System) [6]

Appelées aussi sondes, c'est un ensemble de composants logiciels et matériels, placé de façon stratégique sur le réseau afin de bien analyser le trafic transitant et détecter ainsi toute activité suspecte, technique de sondage (balayage de ports), activités virales, ou encore audit des fichiers de journaux (logs).

Les IDS sont classé selon deux modes de fonctionnement, selon qu'ils se basent sur des signatures d'attaques ou sur des modèles comportementaux :

. IDS à bibliothèque de signature : consiste à rechercher dans l'activité de l'élément surveillé les empreintes (ou signatures) d'attaques connues (enregistrés dans la base de données des codes malicieux de ce IDS).

. IDS à modèles comportementaux : détectent les anomalies. Leur utilisation comprend une phase d'apprentissage, où ils découvrent le fonctionnement normal des éléments surveillés, puis ils signaleront les divergences par rapport à ce fonctionnement de référence.

Les IDS peuvent aussi être classés selon qu'ils surveillent le trafic réseau ou l'activité de machines :

III.10.4.1. Les systèmes de détection d'intrusion réseaux (NIDS-Network IDS)

Un NIDS nécessite un matériel dédié, il écoute et analyse automatiquement de manière passive les flux en transit sur le réseau et détecte (grâce à sa base de données de codes malicieux) les intrusions en temps réel et génère des alertes si des paquets semblent dangereux. Un NIDS met en place une ou plusieurs cartes réseau en mode promiscuité afin qu'elles n'aient d'adresses IP et de pile de protocole attachée.

III.10.4.2. Les systèmes de détection d'intrusion de type hôte (HIDS-Host IDS)

Un HIDS réside sur un hôte et se comporte comme un démon ou service particulier sur le système de celui-ci. Il analyse en temps réel les flux entrants/sortants d'une machine ainsi que les journaux afin de détecter des signaux d'intrusion (Dos, trojan horce, tentative d'accès non autorisée, exécution de codes malicieux, attaque par buffer overflow…).

Remarque : Lors de la mise en place d'un IDS au sein d'un réseau, il est important de le déployer correctement d'une part, mais aussi de comprendre son fonctionnement interne pour pouvoir le configurer efficacement.

Conclusion :

L'objectif d'une sécurité bien gérée et ciblée consiste à protéger les éléments critiques d'une entreprise. Toute erreur sur la cible à protéger conduit à une analyse erronée de la situation et peut mettre en péril l'entreprise. La détermination de ces éléments critiques et de ces objectifs de sécurité est donc primordiale pour élaborer une politique de sécurité cohérente.

CHAPITRE 4

La Supervision des réseaux informatiques

Introduction

Toute entreprise a besoin d'information lui permettant de comprendre l'état de la sécurité et de l'intégrité de son réseau, et d'identifier les problèmes potentiels avant qu'ils ne se déclarent. En effet, les meilleurs dispositifs de sécurité ne peuvent pas protéger de façon optimale un réseau s'ils ne sont pas correctement supervisés. Ainsi, la sécurité d'un réseau repose d'une part sur l'architecture et son adéquation aux besoins des composants qui le constituent, mais aussi sur l'administration et la supervision au jour le jour de ces équipements.

IV.1.Administration de réseaux

C'est tous les moyens mis en œuvre (connaissances, techniques, outils) qui permettent de superviser, exploiter des réseaux informatiques et planifier leur évolution en respectant les contraintes de coût et de qualité mais aussi assurer la réactivité face aux besoins de changement et d'évolution (C'est le fait de gérer). Il est souhaitable d'appuyer autant que possible son administration de réseaux sur des standards: le protocole SNMP est actuellement la technologie de base qui permet d'administrer un réseau TCP/IP.

IV.1.1.Architecture d'administration et principe général

Une architecture classique d'administration se repose sur le modèle Gérant/Agent (Manager/Agent). Le système se compose :

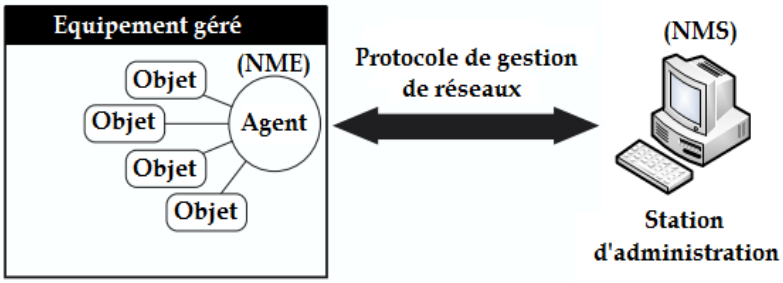

Figure IV.1 : composants du système de gestion réseau

- ✧ D'une entité d'administration NMS (Network Management System) qui est le gérant.
- ✧ Des entités de gestion NME (Network Management Entity) appelés agents qui sont gérées par le NMS.
- ✧ Un protocole pour la gestion.

❖ **Principe général :**

Un système de réseau informatique se compose d'un ensemble d'objets (ces objets et les informations relatives sont stockés dans des bases de données MIB) qu'un système d'administration surveille et contrôle (via un protocole de gestion reposant sur UDP) grâce à un processus appelé manager ou gérant. Pour ce faire, chaque objet est géré localement par un processus appelé agent qui en effet transmet régulièrement ou sur sollicitation les informations de gestion relatives à son état et aux événements qui le concernent au manager.

Le principe se repose donc sur les échanges :

-D'une part : entre une MIB (Management Information Base) et l'ensemble des éléments administrés.

-D'autre part : entre les éléments administrés et le système d'administration.

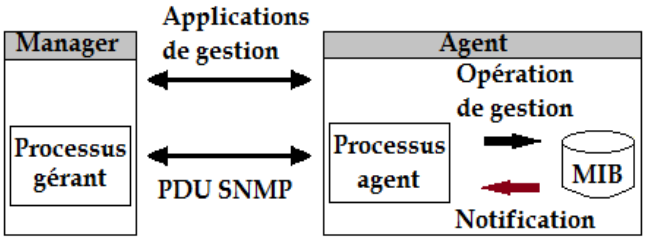

Figure IV.2 : structure fonctionnelle d'administration

De ce fait, on peut modéliser l'architecture d'un système d'administration par :

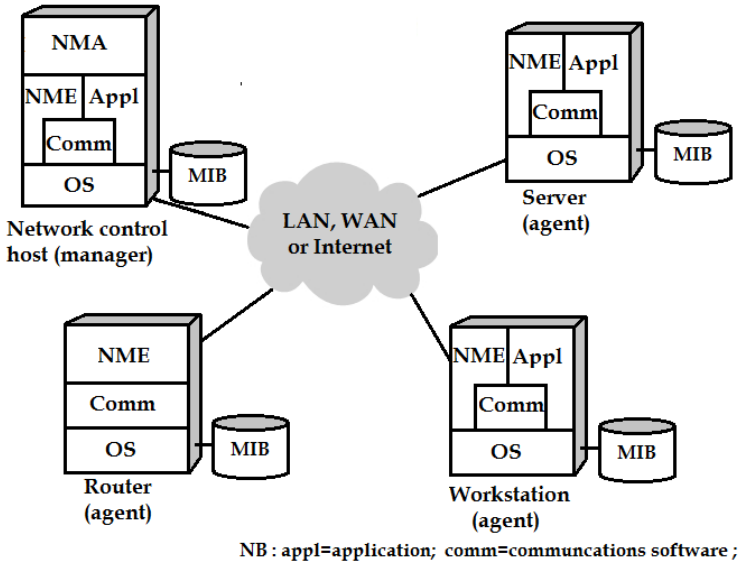

Figure IV.3 : Architecture de système d'administration réseau

Remarque : L'entité d'administration a sa propre entité de gestion NME (Network Management Entity) et aussi un logiciel pour gérer le réseau appelé NMA (Network Management Application) contenant une interface via laquelle les activités d'administration son effectuées.

IV.1.2.Les activités d'administration de réseaux [10]

L'ISO (International Standard Organization) a regroupé les activités d'administration de réseaux en cinq domaines fonctionnels :

- **La gestion des anomalies :** détecte les problèmes réseaux (logiciels ou matériels) et les archive accompagnés d'une solution dans une base de données.

- **La gestion des comptabilités** : permet d'établir des coûts d'utilisation des ressources (la consommation réseau) voir même une facturation.
- **La gestion des performances :** analyse de manière continue les performances du réseau afin de le maintenir dans un état de performance acceptable. Pour ce faire :
  - → des variables contenant des informations significatives quant aux performances sont récupérées (exemple : le temps de réponse d'une station, ou le taux d'utilisation d'un segment réseau…)
  - → les variables sont analysées.
  - → Si elles dépassent un seuil de performance fixé préalablement, une alarme est envoyée à l'administrateur.
- **La gestion des configurations :** effectue un suivi des différentes configurations sur le réseau. De ce fait, elle permet une identification et un contrôle des systèmes et une collecte d'informations.
- **La gestion de la sécurité :** contrôle l'accès aux ressources en fonction des politiques de sécurité (met en application les politiques de sécurité).

Ces activités sont communément classées selon la façon suivante :

- **Supervision** : consiste à surveiller, et collecter toutes sortes d'informations.
- **Gestion :** consiste à gérer le réseau (gestion configurations, ressources, sécurité, dysfonctionnement, les remontées d'alarmes et leurs rapports...)
- **Exploitation** : consiste à traiter les problèmes opérationnels sur le réseau (maintenance, assistance technique…)

IV.2.La supervision

Ensembles de moyens consistant à surveiller les systèmes et à récupérer des informations sur leur état et leur comportement, ce qui peut être fait par interrogation périodique ou par remontée non sollicitée d'informations de la part des équipements de réseaux eux-mêmes.

IV.2.1.Objectifs de la supervision

Les différentes orientations de la supervision réseau doivent être décrites afin d'effectuer les choix de paramétrages adéquats :

- Prévention des pannes : grâce aux Statistiques de la qualité de service et aux Collectes et mesures de performances.
- Diagnostic et résolution rapide de problèmes (la reprise sur incidents).
- Détection d'intrusion.

IV.2.3.Les modules de la supervision

Autour de la supervision, plusieurs modules coexistent :

- La supervision réseau : s'occupe de composants matériel tels que serveur, imprimante, pare-feu …

- La supervision système : s'occupe des applications et logiciels.
- La notification : permet l'envoi d'alertes par email, par sms, par téléphone, par avertissement sonore, …
- L'exécution de commandes : permet de relancer une application qui fait défaut.
- La retranscription d'état du système : permet de voir à tout moment l'état de tous les composants et applications supervisés sous forme d'un graphique, d'une carte ou d'un tableau. Son but est de rendre les résultats plus lisibles.
- La cartographie : visualise le réseau supervisé par l'intermédiaire de carte, de graphique, de tableau, …
- Le reporting : consiste en un historique complet de la supervision.

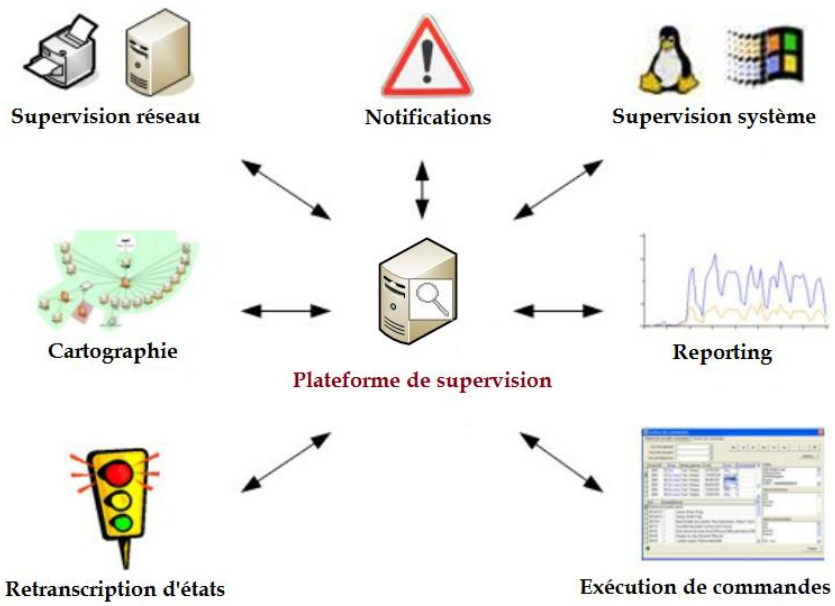

Figure IV.4 : les modules coexistant autour de la supervision

IV.2.4.Les événements et les indicateurs à superviser

Il est important de choisir les événements correspondants aux besoins du service ou du métier ainsi que les informations d'état à superviser, le plus souvent :

- Table ARP.
- Tables de session.
- L'équipement est-il opérationnel ?
- Quelle est la charge CPU ?
- Quelle est la charge réseau ?
- Quel est le temps de réponse ?
- Les disques sont-ils proches de la saturation ?
- La connectivité est-elle toujours assurée ?
- Y'a-t-il des activités suspectes ?
- …

IV.2.5.Architectures de supervision [11]

On distingue deux architectures de supervision :

- Architecture centralisée : la surveillance se fait par un serveur de supervision global, et les remontées d'informations et d'alarmes se font directement vers ce serveur.
- Architecture décentralisée : les remontées d'information se font dans un premier temps vers les serveurs de supervision locaux, puis de ces derniers vers le serveur global.

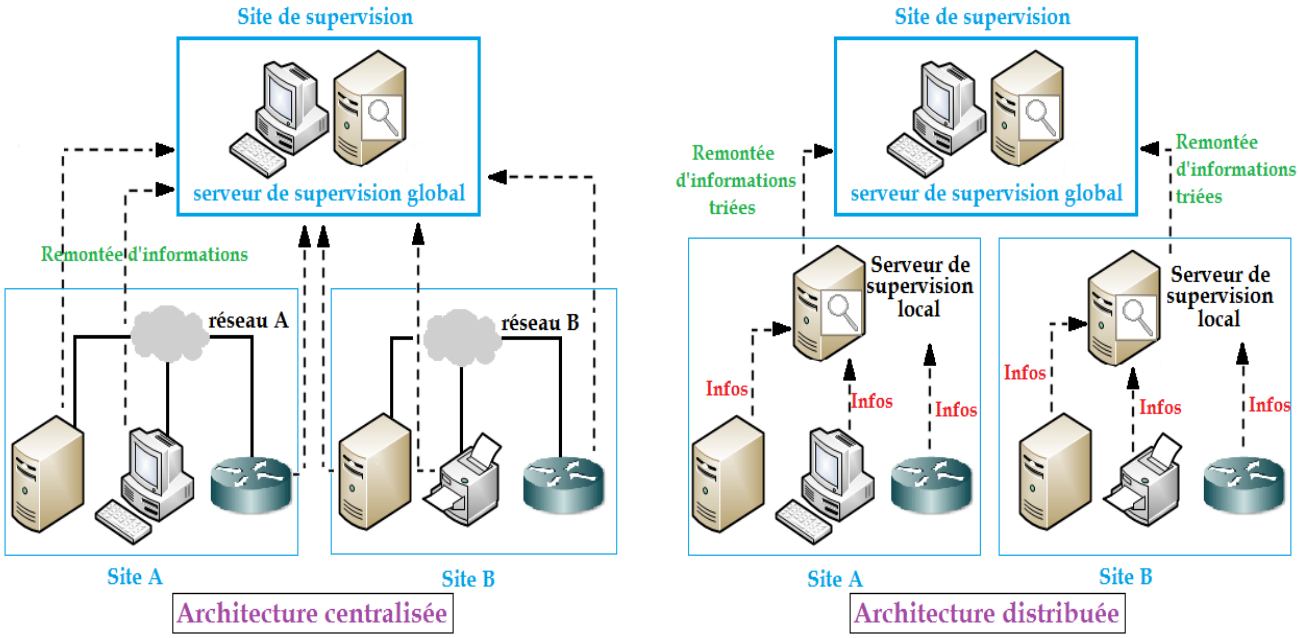

Figure IV.5 : Les architectures de supervision

IV.2.6.Les méthodes possibles de supervision [11]

Les principales méhodes de supervision sont les suivantes :

- Analyser les fichiers log (fichiers journaux) en consultation ou avec remontée.
- Récupérer des résultats de commandes et de scripts locaux ou distants.
- Utiliser le protocole SNMP (Simple Network Management Protocol).

Pour ce faire deux modes sont utilisés, le temps réel et le temps différé :

IV.2.6.1. Supervision en temps réel

Ce mode de supervision est utilisé selon les événements et les indicateurs à superviser et selon leur criticité, les outils les plus souvent utilisés sont :

- Tripwire : outil de scellement de configuration. Selon une fonction de hachage, le fichier de configuration est haché puis signé, et on vérifie l'intégrité en comparant à ce haché.

- MBSA (Microsoft Baseline Security Analyzer) : outil fourni par Microsoft pour vérifier le niveau de sécurité des machines Windows à distance ou en local.
- Sonde IDS : système servant à détecter des attaques.
- Antivirus : programmes pour surveiller et lutter contre les virus.
- SMS (System Management Server) : utilisé pour gérer des machines Windows.

IV.2.6.2. Supervision en temps différé

Une supervision en temps différé s'effectue en parallèle avec la supervision en temps réel, elle constitue le plus souvent une analyse manuelle, mais lorsque le volume des données est important, des outils de traitement de logs sont utilisés. En pratique, tous les équipements génèrent pour chaque événement important des lignes de log, ces fichiers journaux sont archivés et centralisés sur des serveurs afin de les analyser à posteriori pour :

- Evolution à long terme.
- Détection des tendances et anomalies à suivre sur le réseau.
- Suivi de la qualité de service.
- Intervention sur des incidents de sécurité à posteriori.

On peut citer :

- **Analyse d'attaques :**

L'analyse des fichiers log permet de récolter des compléments d'information lors du traitement d'un événement de sécurité (action non autorisée détectée par l'analyse). Afin d'identifier et diagnostiquer cet événement et lancer les procédures de sécurité adéquates.

Remarque : un événement de sécurité peut être une mauvaise manipulation, une préparation d'attaque ou même une attaque. Par exemple une ligne de logs signalant une tentative échouée de connexion d'un utilisateur pour erreur de mot de passe, cela est traduit par une mauvaise manipulation. Cet événement est plus grave si cette ligne de code est répétée plusieurs fois.

Afin d'obtenir des informations sur l'origine d'une attaque, on utilise :

.traceroute : utilitaire permettant d'afficher la route suivie par les paquets IP depuis le point d'émission jusqu'à la destination, en donnant la liste de tous les équipements traversés.

Whois : un outil qui permet de lister la plage d'adresses IP à laquelle appartient une adresse IP entrée ainsi que des informations (nom, coordonnées postales et téléphoniques) sur le propriétaire de cette plage.

.dig, host, Nslookup : des outils qui permettent d'effectuer des requêtes DNS.

- **Tableau de bord de sécurité [8]**

Permet d'avoir une vue d'ensemble de la sécurité opérationnelle d'une plateforme ou d'un réseau (détection des anomalies, des attaques et des évolutions à mener sur le périmètre considéré pour effectuer une prévention des pannes et des attaques). Dans un tableau de bord, figure les éléments qui suivent :

- ✧ Information sur les événements marquants survenus dans la période de référence.
- ✧ Etat d'avancement des mécanismes de sécurité du domaine sécurité.
- ✧ Synthèse des événements de sécurité que subit le réseau accompagnés de leurs niveaux de sévérité :

    - ✦ Nombre de machines impactées, nature de l'impact (visant la disponibilité, l'intégrité...), sévérité de l'impact.
    - ✦ Origine de l'attaque (son adresse source).
    - ✦ Caractérisation de l'événement (virus, DoS…).
    - ✦ La réaction face à l'incident.

Remarque : dès qu'il est question de tâches de plus langue haleine, l'emploi de tableaux de bord devient fastidieux. Pour cette raison, les fichiers log sont traités par des outils tel que les produits de type ESM (Entreprise Security Management), ou des outils de supervision libres.

IV.2.7.Formats de données de la supervision [11]

Il s'agit des fichiers de journalisation :

IV.2.7.1.Syslog

C'est un standard pour tout ce qui concerne les messages de notification d'événements définissant à la fois le format de ces données et le mécanisme de transport de ces messages.

Pour tout événement survenant sur un système peut être logé, pour ce faire, un message est ne dépassant pas 1024 octets généré pour chacun d'eux, comme par exemple, une erreur d'authentification, un message du noyau ou d'une application, ou une connexion à un service.

Remarque : deux propriétés caractérisent un message, sa facilité et sa sévérité, qui peuvent être présentées par des entiers. La facilité permet de distinguer quel est le processus ou démon tournant sur le système à l'origine du message. La sévérité concerne le coté critique (urgence, erreur, avertissement, information, alerte...

IV.2.7.2.Netflow

Technologie conçue par Cisco, elle permet de collecter des données sur le trafic traversant des équipements réseau, et de ce fait effectuer des mesures de ce trafic dans un cadre de supervision ou de facturation.

Un flux IP est caractérisé par les adresses IP, le protocole utilisé, les ports, les interfaces d'entrée et de sortie ainsi que le champ TOS. Au premier passage d'un paquet, le routeur consulte ses tables afin de déterminer vers quel nœud le router (ceci consomme des ressources CPU). Cependant, les paquets qui suivent bénéficient du cache Netflow lors de leur entrée sur le routeur, cela permet à celui-ci d'accéder à l'information de routage plus rapidement.

Quand le routeur libère son cache Netflow d'une entrée, un datagramme peut être envoyé à un superviseur en incluant les informations de routage. Ces données sont rassemblées par un collecteur générique qui effectue souvent des prétraitements basiques permettant l'émission de rapports. Les données qui peuvent être pertinentes pour la supervision de la sécurité sont

les données de comptage (Netflow accounting). Leur analyse est judicieuse dans de nombreux cas, comme par exemple dans la détection d'attaques, cela grâce aux regroupements des logs, qui permet d'observer des comportements et expliquer de événement de sécurité.

IV.3.Protocole de gestion de réseau dans le modèle TCP/IP : SNMP [11]

SNMP (Simple Network Management Protocol) est un protocole de communication qui a été crée pour être une couche utilisant TCP/IP à un niveau supérieur. Il opère en accord avec UDP et IP, et permet de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseau et matériels à distance. C'est l'un des protocoles les plus utilisés pour la gestion (management, monitorage) des réseaux.

SNMP est utilisé pour:

- Administrer les équipements et échanger des éléments de configuration.
- Surveiller le comportement des équipements et les performances réseaux.
- Modifier le paramétrage de certains composants.

Comme son nom l'indique, il est relativement simple tout en étant très complet. En effet, sa simplicité ne lui empêche pas de pouvoir gérer des réseaux hétérogènes complexes. Son utilisation est basée sur 3 éléments. Les voici :

- Les agents, placés sur les éléments actifs du réseau.
- Les managers.
- La MIB.

Toutefois, il y'a deux modes de fonctionnement :

- Le polling : dans lequel la station de supervision interroge les agents à tour de rôle.
- Les traps SNMP : où l'équipement remonte lui-même une alarme afin de signaler une anomalie au superviseur.

IV.3.1. Concepts fondamentaux

IV.3.1.1. Station d'administration (NMS-Network Management Station)

Entité utilisée par l'administrateur pour gérer son réseau, dispose d'un outil dit "manager". C'est un client, dans la mesure où c'est lui qui envoie les requêtes aux divers agents SNMP du réseau. Il devra aussi disposer d'une fonction serveur, car il doit rester à l'écoute (sur le port UDP 162) des alertes que les équipements sont susceptibles d'émettre à tout moment. Toutefois, l'administrateur peut observer le comportement de la totalité de son réseau depuis sa station d'administration. Une NMS doit obligatoirement posséder :

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

IV.3.1.2. Agent de gestion

Chaque équipement que l'on voudra "manager" à distance devra disposer d'un agent SNMP, C'est-à-dire une application de gestion résidant dans un périphérique et chargée de transmettre les données locales de gestion de celui-ci au format SNMP. Cet agent est un serveur, qui reste à l'écoute du port UDP 161 pour des requêtes provenant de l'administrateur. L'agent devra éventuellement pouvoir agir sur l'environnement local, si l'administrateur souhaite modifier un paramètre. Par ailleurs, l'agent SNMP pourra émettre des alertes de sa propre initiative, s'il a été configuré pour ça. Un agent assume ainsi les travaux ci-dessous :

- Collecter des informations statistiques concernant la communication, et les opérations de réseau.
- Stocker les informations localement dans les MIB.
- Répondre aux commandes de la station d'administration, inclus : Transmet des informations statistiques à l'entité d'administration, modifie les paramètres…

Remarque : Pour les serveurs et les stations il existe probablement un logiciel à installer, quelque soit le système. Pour Linux, c'est "NET-SNMP". Windows XP professionnel, Windows 2000 "pro" et "server" permettent d'installer un agent SNMP.

IV.3.1.3. Les communautés

La communauté définit le domaine de gestion (groupe). L'authentification entre le NMS et l'agent utilise donc la communauté comme une sorte de mot de passe. Une entité peut avoir l'accès en lecture seule, en lecture/écriture, ou encore en lecture seule mais sur certaines branches seulement... En général, la communauté "public" est celle qui a le droit de lecture sur les informations non sensibles.

L'inconvénient est qu'avec SNMP v1, qui est actuellement la seule version vraiment stabilisée et reconnue par tous, ce mot de passe circule en clair. Toutefois, SNMP est évolué pour un minimum de sécurité. SNMP v2 utilise l'algorithme MD5 (message Digest5) pour hacher les noms de communautés. La sécurité a été étudier plus en avant avec SNMP v3, qui intègre des mécanismes de vérification d'intégrité des messages et d'authentification avec des algorithmes de hachage et de chiffrement.

IV.3.1.4. Les alarmes

Il est possible de demander (en configurant) aux stations d'émettre de temps en temps (une fois par heure par exemple) un rapport, sur les anomalies et pourquoi pas quelques statistiques sur son état. Cela permet de soulager le travail de la station d'administration qui n'a plus qu'à écouter ses protégés.

IV.3.1.5. Les objets

Dans SNMP, un objet peut être des informations matérielles, des paramètres de configuration, des statistiques de performance et autres variables qui sont directement liés au comportement en cours de l'équipement. Les objets sont classés dans une sorte de base de donnée appelée MIB. Les données de la MIB peuvent être adressées par un OID (Object

IDentifier) qui correspond au chemin depuis la racine de l'arborescence des données de gestion jusqu'à l'objet, chaque nœud étant marqué par un identifiant (nombre et nom). 1.5.3.2.4 est un OID possible. Cette séquence se lit de gauche à droite et correspond à des nœuds dans l'arborescence des noms.

IV.3.1.6. Les MIB (base d'informations de gestion)

La MIB se présente comme une base de données normalisée (sous forme de variables et de tables) d'objets, qui permettra de lire et d'écrire sur les équipements distants, de façon également normalisée. Chaque MIB est propre à l'agent. Il ya donc une MIB pour chaque équipement supervisé. Un agent stocke deux grandes classes de données:

- Données d'état de la machine (nombre de paquets reçus sur une interface, ...).
- Données correspondant à la configuration de la machine (politique de sécurité ou de routage par exemple).

Cette MIB contient donc:

- Des informations à consulter.
- Des paramètres à modifier.
- Des alarmes à émettre.

IV.3.1.6.1. Structure d'une MIB

- Elle est organisée hiérarchiquement avec une structure arborescente, où une branche représente la catégorie logique et une feuille les informations sur un objet.
- Elle contient une partie commune à tous les agents SNMP en général, une partie commune à tous les agents SNMP d'un même type de matériel et une partie spécifique à chaque constructeur.
- Chaque nœud d'un arbre (niveau de la hiérarchie) représente un objet. Cet objet est définit avec un OID (Object IDentifier). Cet identifiant est constitué d'une suite de chiffre séparé par des points (index numérique) et SNMP utilise cette façon de faire.
- Pour qu'un client accède à ces objets, il faut qu'il en connaisse l'existence.
- Non seulement la structure est normalisée, mais également les appellations des diverses rubriques (pour rendre les choses plus lisibles).
- Une MIB contient un ensemble d'informations standards, c'est la MIB standard. Or pour la plupart des éléments réseaux, on rajoute un certain nombre d'objet propre a un agent pour en exploité les possibilités : c'est la MIB privée.
- La MIB est un fichier texte écrit en langage ASN 1(Abstract Syntax Notation 1).

Pour la MIB et les commandes de base associées :

- Les outils ont besoin de connaître la version SNMP utilisée (option –v 1 pour SNMP v1).
- Les outils ont besoin de connaître la "communauté" (à voir comme un mot de passe). Par exemple, communauté autorisée en lecture s'appelant "public" (option -c public).
- Les outils doivent savoir la cible (adresse IP de l'agent SNMP interrogé).
- Les commandes ont besoin de savoir à quelle feuille de la MIB on s'intéresse.

Remarques :

- Un gestionnaire SNMP utilise les MIB pour convertir les OID en texte humainement compréhensible. Il importe une MIB SMI (spécification au format ASN.1) puis la compile. Une compilation convertit la MIB depuis un format ASCII vers un format utilisable nativement par le gestionnaire.

- SMI (Structure of Management Information) est une syntaxe qui spécifie comment les données (objets SNMP) sont représentées via ASN.1 (décrit pour chaque objet (avec un OID, une syntaxe, un encodage)).

IV.3.1.6.2. La représentation d'une MIB (Structure et représentation d'objets)

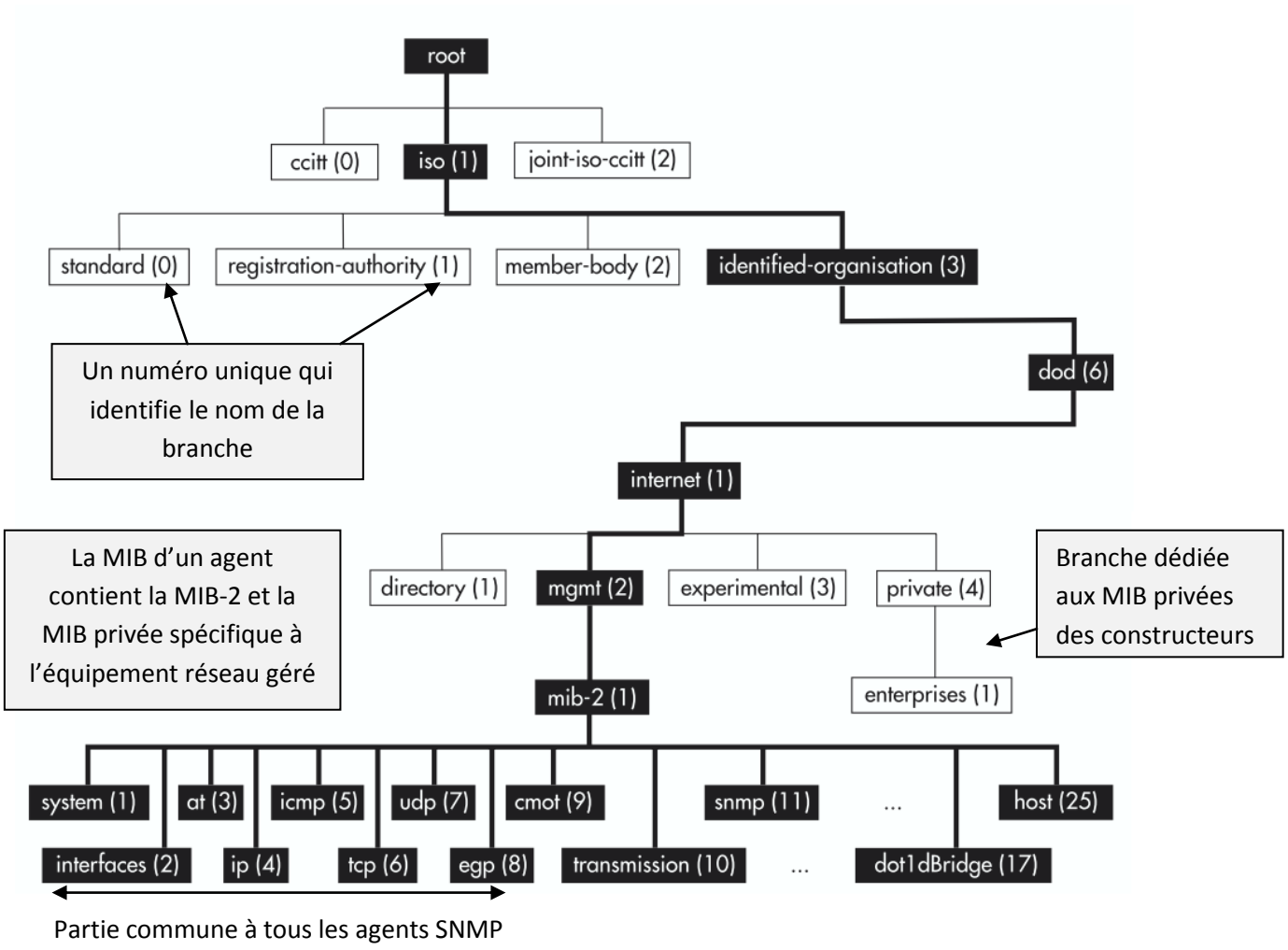

Figure IV.6: Structure de MIB

❖ **Description :**

- iso(1) : branche qui définie La gestion de réseau. Dans cette branche on trouve un certain nombre de définitions d'organisations subordonnées. La gestion de réseau entre dans le nœud identified-organisation(3).

- Sous le nœud dod(6) se trouvent un certain nombre de réseaux subordonnés. La gestion de réseau entre dans le nœud internet(1).

- Sous le nœud internet(1) se trouvent un certain nombre de nœuds subordonnés représentant différents services et tentatives de normalisation. La gestion de réseau standardisée se trouve dans le réseau mgmt(2).

- Sous le nœud mgmt(2) se trouvent un certain nombre de nœuds subordonnés représentant différents services et tentatives de normalisation. La gestion de réseau standardisée se trouve dans le nœud mib-2(1).

- Sous le nœud mib-2(1) se trouvent un certain nombre de nœud subordonnés représentant différents groupement de variables MIB, Ce sont des tables contenant les informations de l'élément du réseau. Ce qu'on appel Les tables MIB, on y trouve :

- Groupe « System » : Informations génériques de configuration.
- Groupe « Interfaces » : Informations concernant les interfaces (type, adresse, nombre d'octets in/out, statut,…)
- at (adress translation) ou Groupe « ARP » : Liaison Adresse Physique – Adresse logique.
- Groupe « IP » : Informations sur le niveau IP (TTL, forwarding?, tables de routage, nombre de paquets, d'octets, de "forward"…)
- Groupe « ICMP » : Informations statistiques sur les messages ICMP (Nombre de messages, de messages Echo, …)
- Groupe « TCP » : Informations sur les connexions TCP (connexions en cours, nombre de messages, de circuits ouverts, TTL, …)
- Groupe « UDP », « EGP », « SNMP »…

Remarque : mib-2 est une base d'objets commune à tous les équipements. Correspond à des informations TCP/IP.

Exemple de variables :

Sous le nœud system(1), on trouve par exemple deux variables MIB sysDescr(1) et sysLocation(2). Les identifiants d'objets de ces variables (chemin d'accès à ces variables) s'obtiennent en écrivant de gauche à droite les différents nœuds, séparés par des points :

sysDescr : .1.3.6.1.2.1.1.1

sysLocation : .1.3.6.1.2.1.1.2

Remarque : (.1.3.6.1.2.1), autrement dit .iso.org.dod.internet.mgmt.mib est le début de chemin le plus souvent employé. Si le chemin indiqué commence par un point (.1.3.6.1.2.1.1.1) il s'agit d'un chemin absolu, s'il ne commence pas par un point (1.1), il est considéré comme relatif à ce qui manque, à savoir (.1.3.6.1.2.1).

Quelques éléments de données de la MIB pour en clarifier le contenu :

Variable MIB	Catégorie	Description
sysUpTime	Système	Durée écoulé depuis dernier démarrage
ifNumber	interfaces	Nombre d'interfaces réseau
ipDefaultTTL	ip	Valeur utilisée dans le champ TTL
ipInReceives	ip	Nbre de datagrammes reçus
ipForwDatagrams	ip	Nbre de datagrammes acheminés
ipOutNoRoutes	ip	Nbre d'erreurs de routage
ipReasmOKs	ip	Nbre de datagrammes réassemblés
ipFragOKs	ip	Nbre de datagrammes fragmentés
ipRoutingTable	ip	Table de routage IP
icmpInEchos	icmp	Nbre de demandes d'echo ICMP reçues
tcpMaxConn	tcp	Nbre maxi de connexions TCP autorisées
tcpInSegs	tcp	Nbre de segments reçus par TCP
udpInDatagrams	udp	Nbre de datagrammes UDP reçus

Tableau IV. 1: Exemple d'éléments d'une MIB

IV.3.1.7. Les proxies

L'utilisation de SNMP nécessite que tous les agents supportent un protocole commun, tel que UDP et IP. Cependant, il est aussi possible de monitorer des équipements n'utilisant pas TCP/IP ou n'ayant pas d'agent SNMP. Pour cela, un proxy SNMP doit être installé sur une machine TCP/IP. Ces proxies suppléent les machines inadaptées car ils connaissent les objets de la MIB nécessaires pour la gestion du système mandaté. La communication entre le proxy et la machine suppléée ne peuvent pas utiliser SNMP pour dialoguer et il faut donc, pour le proxy, s'adapter aux protocoles connus par la seconde machine (faire la translation entre les données d'un agent de supervision privée et SNMP. Puis transmettre ces données à un superviseur SNMP). L'utilisation de ces proxies permet ainsi à SNMP de s'adapter facilement à des réseaux très hétérogènes et prouve la grande flexibilité de ce protocole.

IV.3.2.Les messages SNMP

Il existe trois messages SNMP différents : les requêtes, les réponses et les alarmes (trapes). Les requêtes SNMP sont les suivantes :

- GetRequest : recherche d'une variable sur un agent.
- GetNextRequest : recherche la variable suivante.
- GetBulk : recherche un ensemble de variables regroupées.
- SetRequest : change la valeur d'une variable sur un agent.

L'agent répond aux requêtes par un message GetResponse. En cas d'erreur, le message sera accompagné d'un des codes d'erreurs suivants :

- NoAccess : accès non autorisé.
- WrongLength : erreur de longueur.

- WrongValue : erreur de valeur.
- WrongType : erreur de type.
- WrongEncoding : erreur d'encodage.
- NoCreation : objet inexistant.
- ReadOnly : seule la lecture est autorisée.
- NoWritable : interdiction d'écrire.
- AutorisationError : erreur d'autorisation.

Les alarmes sont envoyées par l'agent lorsqu'un événement survient sur la ressource monitorée. Elles peuvent prendre les formes suivantes :

- ColdStart (0) : redémarrage du système à froid.
- WarmStart (1) : redémarrage du système à chaud.
- LinkDown (2) : le lien n'est plus opérationnel.
- LinkUp (3) : le lien est à nouveau opérationnel.
- AuthentificationFailure (4) : Tentative d'accès à l'agent avec un mauvais nom de communauté.
- EgpNeighborLoss (5) : la passerelle adjacente ne répond plus.
- EntrepriseSpecific (6) : alarme spécifique aux entreprises.

IV.4.Les menaces et besoins de sécurité de SNMP

La hausse continuelle des attaques par le réseau a fait apparaître le besoin de sécuriser le protocole SNMP. On a donc proposé une nouvelle version (SNMPv3) qui vise à apporter des outils pour sécuriser les échanges SNMP. Deux des objectifs principaux étaient de conserver un protocole simple d'utilisation et de rester compatible avec les anciennes versions de SNMP (v1 et v2). SNMPv3 apporte une nouvelle architecture qui répond à plusieurs besoins de sécurité correspondants à des menaces identifiées :

- Modification de l'information (intégrité).
- Usurpation d'identité (authentification).
- Modification de flux (rejeu).
- Affichage des données (confidentialité).

Dans le cadre de la gestion de réseau, la confidentialité est aussi importante que l'intégrité et l'authentification dans la mesure où les données échangées sont sensibles. Le besoin d'authentification est fort car on veut se protéger d'un attaquant qui se ferait passer pour un manager qui reconfigurerait un équipement au détriment des utilisateurs. Le contrôle d'accès est également une des priorités. Certaines données ne doivent être accédées (que ce soit en lecture ou en écriture) que par des utilisateurs dûment autorisés.

Conclusion

Ce chapitre nous a permis de présenter le principe général d'administration réseau et d'identifier les besoins fonctionnels et non fonctionnels de notre système. Le chapitre suivant sera consacré à la spécification et la conception de la plateforme d'administration réseau.

CHAPITRE 5

Conception et test de l'infrastructure de solution

Introduction

A l'issu d'une étude préalable du réseau informatique de l'ENIEM (chapitre I), et avec l'aide de mon encadreur nous avons pu dégager les insuffisances aux quelles nous devions apporter une solution ; qui consiste à la supervision ainsi qu'à la conception d'un plan de sécurité plus pertinent qui sera capable de rependre au contraintes de sécurité du millenium du réseau Informatique de l'entreprise.

Dans ce chapitre, nous allons donc, présenter les spécifications de notre solution de sécurité et d'administration de la maquette du réseau vulnérable, dont la conception se base sur un plan de couplage entre sécurité et supervision. En effet, les tests se feront sur des maquettes de test.

V.1. Les solutions retenues

Après avoir pris connaissances des failles existantes dans la maquette présentée et des besoins (chapitre I), nous avons opté pour les solutions suivantes :

- Agencement et administration du réseau local sous vlan (l'organiser méthodiquement), et mise en place d'un plan de sécurité rependant aux besoins prédéfinis.
- Intégration de la fonctionnalité de supervision au réseau.

V.2. Présentation du projet

Mon stage s'est déroulé au sein de l'équipe informatique. Ce service comme nous l'avons vu auparavant a la responsabilité de la mise en œuvre et de l'administration des systèmes, et du réseau local reliant les bâtiments qui abritent l'ensemble des équipes de l'entreprise.

Ce stage comprend le programme suivant les solutions retenues, qui est le suivant :

- Implémentation d'un plan de sécurité et ajout de nouvelles fonctions.
- Interconnexion sécurisée entre l'entreprise et sa direction.
- Mise en place d'une solution de supervision.

- **Présentation des différentes étapes du programme :**

1. Choix de l'infrastructure du réseau après couplage entre sécurisation et supervision

Avant toutes autre action, il faut décider de la nouvelle architecture (faire évoluer l'existant), en cohérence avec le programme de la solution et en fonction des besoins en :

- **Interconnexion :** installation d'un routeur.
- **Sécurité** : implémentation d'un firewall matériel (PIX 515), et déplacement du serveur web.
- **Supervision et administration :** déploiement d'un serveur de supervision global.

2. Etapes de conception pour le projet de sécurisation :

- Réorganiser par VLAN et administrer ces VLAN et leurs accès après avoir déterminé un plan d'adressage adéquat.
- Installer un firewall et découper en périmètres (zones) de sécurité.
- Implémenter des mécanismes de sécurité selon périmètres : définir les règles de filtrage, les translations d'adresses et de ports.

3. Etapes de conception pour le projet d'interconnexion :

- Implanter deux routeurs reliant de façon sécurisée l'ENIEM à sa direction.
- Faire le choix du protocole de routage.
- Choix du protocole d'encapsulation.
- Configurer les deux routeurs (routage, encapsulation, vty…)

4. Etapes de conception pour le projet de supervision :

- Implémentation du système de supervision sous SNMP et installation des outils de supervision de la sécurité.
- Activation du service SNMP et des paramètres dans chacun des équipements du réseau à superviser.

5. Mise en œuvre de plateformes de test

- Conception de maquettes virtuelles en se servant d'outils de simulation, émulation et de virtualisation permettant de tester et d'illustrer les configurations.
- Utilisation des outils de base de diagnostique réseau (ping…).
- Réalisation de test avec les différentes méthodes de sécurisation.
- Réalisation de test sur la supervision.
- Réalisation de test de vulnérabilité et de scan.

V.3. Les démarches de la conception

V.3.1. Le design de la nouvelle infrastructure

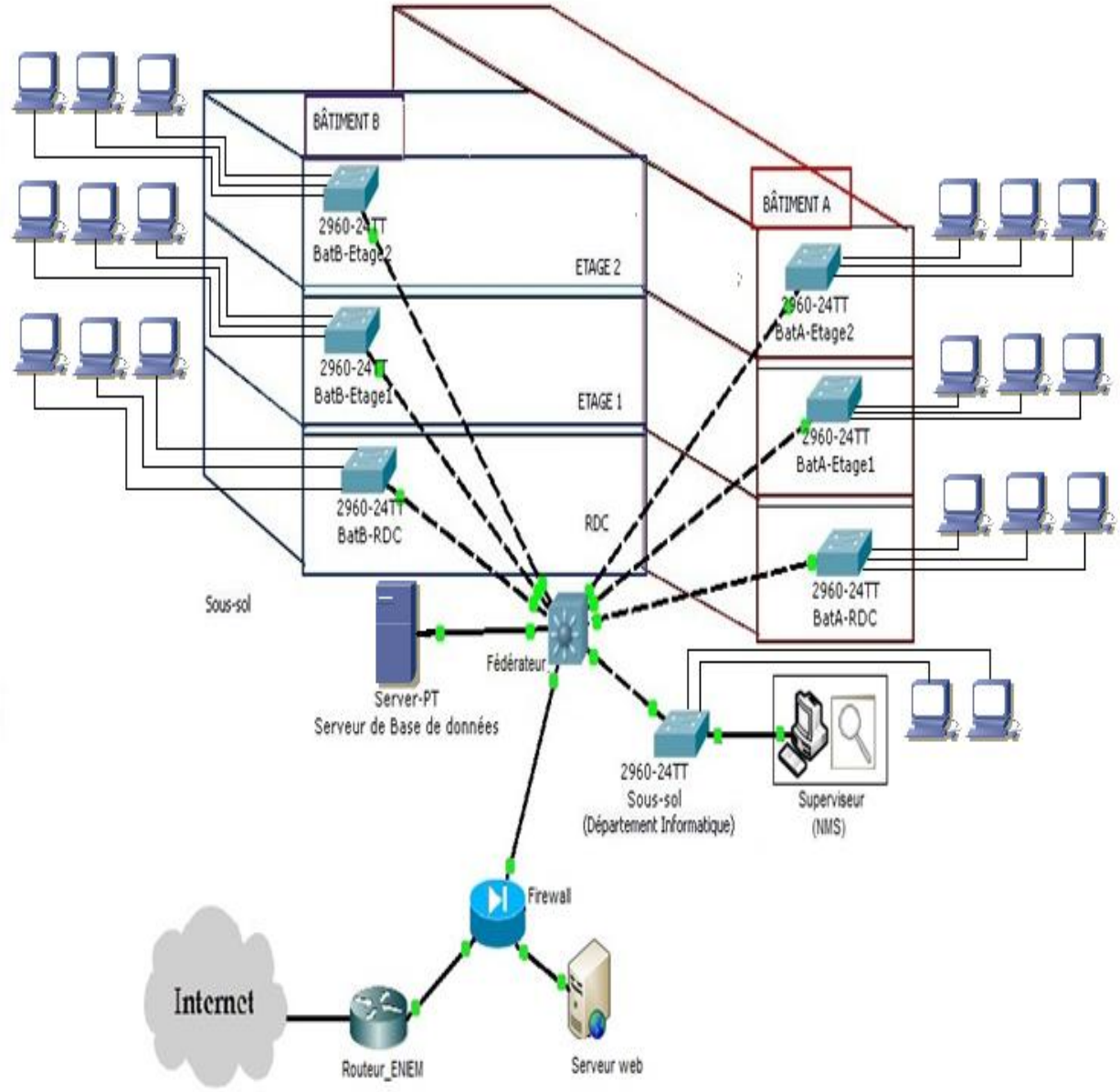

Figure V.1 : Design de l'infrastructure de solution

V.3.2. La sécurisation de l'infrastructure

V.3.2.1. Administration et agencement du réseau local sous VLAN

Etant dans le même réseau, ses activités sont dispersées, c'est pour pallier à cela que nous utiliserons les VLAN, cela permettra de faciliter le travail de l'administrateur et l'accroissement de la sécurité. En effet, la segmentation par VLAN permet de créer des domaines de diffusion gérés par les commutateurs indépendamment de l'emplacement où se

situent les nœuds, et aussi de regrouper les utilisateurs qui ont besoins d'accéder aux mêmes ressources. Cela va nous permettre d'avoir un réseau bien ordonné.

Nous allons donc proposer un plan d'adressage et désigner des sous-réseaux, puis configurer les Switchs selon les besoins convenables en utilisant un réseau VLAN pour chaque unité (VLAN niveau 3) et spécifier le serveur avec un VLAN, et le département informatique avec un, et un VLAN (vlan 9) dédié au firewall, voici les étapes :

V.3.2.1.1. Elaborer un nouveau plan d'adressage

Les objectifs du plan d'adressage sont :

- Eviter la duplication accidentelle d'adresses.
- Contrôler le fonctionnement du réseau.
- Organiser l'exploitation de l'intranet.

A. Adressage de l'intranet et segmentation par VLAN :

Nous aurons besoin pour le réseau local (dont l'adresse est 192.168.1.0) de 8 sous-réseaux, le masque variable sera 255.255.255.224. Nous désignerons ces sous-réseaux selon les besoins :

	8 sous-réseaux de 32 (-2) adresses	VLAN correspondant	Désignation
Plages d'adresses au sein du sous-réseau	0-31	/	Switchs
	32-63	VLAN 2	Serveur
	64-95	VLAN 3	Département Informatique
	96-127	VLAN 4	Unité Prestations Techniques
	128-159	VLAN 5	Unité Commerciale
	160-191	VLAN 6	Unité Cuisson
	192-223	VLAN 7	Unité Climatisation
	224-240	VLAN 8	Unité Froid
Masque	255.255.255.224 (**/27**)		

Tableau V.1 : Le plan d'adressage et les VLAN du RLE

Remarques 1 : Il est possible d'étendre les plages d'adresses affectées si le nombre de stations devient plus important que prévu, pour ce faire nous diminuons le masque.

Remarque 2 : pour sortir du VLAN, la route de sortie doit être connue, et doit être pointée sur l'adresse IP de la carte de commutation sur chaque VLAN. La passerelle par default des PC pointe donc sur l'adresse IP de l'interface logique (du VLAN d'appartenance).

❖ **Adressage des interfaces logiques des Switchs :** Voici un aperçu sur l'adressage des interfaces VLAN au niveau des Switchs :

	Switchs	Interfaces	Adresses IP
Sous-sol	Switch Fédérateur	VLAN 1	192.168.1.1/27
		VLAN 2	192.168.1.33/27
		VLAN 3	192.168.1.65/27
		VLAN 4	192.168.1.97/27
		VLAN 5	192.168.1.129/27
		VLAN 6	192.168.1.161/27
		VLAN 7	192.168.1.193/27
		VLAN 8	192.168.1.225/27
		VLAN 9	192.168.2.1 /24
	Switch département Informatique	VLAN 1	192.168.1.2/27
RDC	Switch Bâtiment A	VLAN 1	192.168.1.3/27
	Switch Bâtiment B	VLAN 1	192.168.1.4/27
Etage 01	Switch Bâtiment A	VLAN 1	192.168.1.5/27
	Switch Bâtiment B	VLAN 1	192.168.1.6/27
Etage 02	Switch Bâtiment A	VLAN 1	192.168.1.7/27
	Switch Bâtiment B	VLAN 1	192.168.1.8/27

Tableau V.2 : attribution d'adresses aux interfaces VLAN

❖ **Adressage des équipements du réseau local et VLAN d'appartenance :**

Position	Equipements		Adresses IP	VLAN d'appartenance
Sous-sol	Switch Fédérateur		**192.168.1.1 /27**	/
	Serveur de base de données		**192.168.1.34 /27**	**VLAN 2**
	Switch Département Informatique	PC Superviseur	**192.168.1.66 /27**	**VLAN 3**
		PC Maintenance	**192.168.1.67 /27**	**VLAN 3**
		PC Comptabilité UPT	**192.168.1.100/27**	**VLAN 4**
RDC	Switch Bâtiment A	PC1-UPT	**192.168.1.98 /27**	**VLAN 4**
		PC2- UPT	**192.168.1.99 /27**	**VLAN 4**
	Switch Bâtiment B	PC1-département commerciale	**192.168.1.130/27**	**VLAN 5**
		PC- ressources Humaines	**192.168.1.120/27**	**VLAN 4**
Etage 01	Switch Bâtiment A	PC6-Froid	**192.168.1.231**	**VLAN 8**
		PC7-Froid	**192.168.1.232**	**VLAN 8**
	Switch Bâtiment B	PC1-Climatisation	**192.168.1.194**	**VLAN 7**
		PC5-Climatisation	**192.168.1.198**	**VLAN 7**
Etage 02	Switch Bâtiment A	PC1-Froid	**192.168.1.226**	**VLAN 8**
		PC-Gestion stocks	**192.168.1.135**	**VLAN 5**
	Switch Bâtiment B	PC1-Cuisson	**192.168.1.162**	**VLAN 6**
		PC3-Cuisson	**192.168.1.164**	**VLAN 6**

Tableau V.3 : Attribution des adresses et VLAN aux équipements

Remarques :

1. Nous nous sommes contenté de deux à trois Postes de travail par Switch pour illustrer l'adressage et le fonctionnement. Pour des raisons de pratique, nous ne pouvons pas représenter tous les postes.

2. Nous pouvons avoir plusieurs réseaux IP sur notre site, mais nous avons limité le nombre à un réseau IP (192.168.1.0) afin de simplifier la connexion à Internet, car le nombre de réseau à translaté deviendra une source de complexité, car nous utiliserons un seul point de sortie vers Internet. Pour nous, le firewall n'aura qu'à prendre un réseau (tout en ayant autant de sous-réseaux nécessaires pour notre intranet) dans ses règles de translations d'adresses.

- **L'infrastructure du réseau local avec le plan d'adressage :**

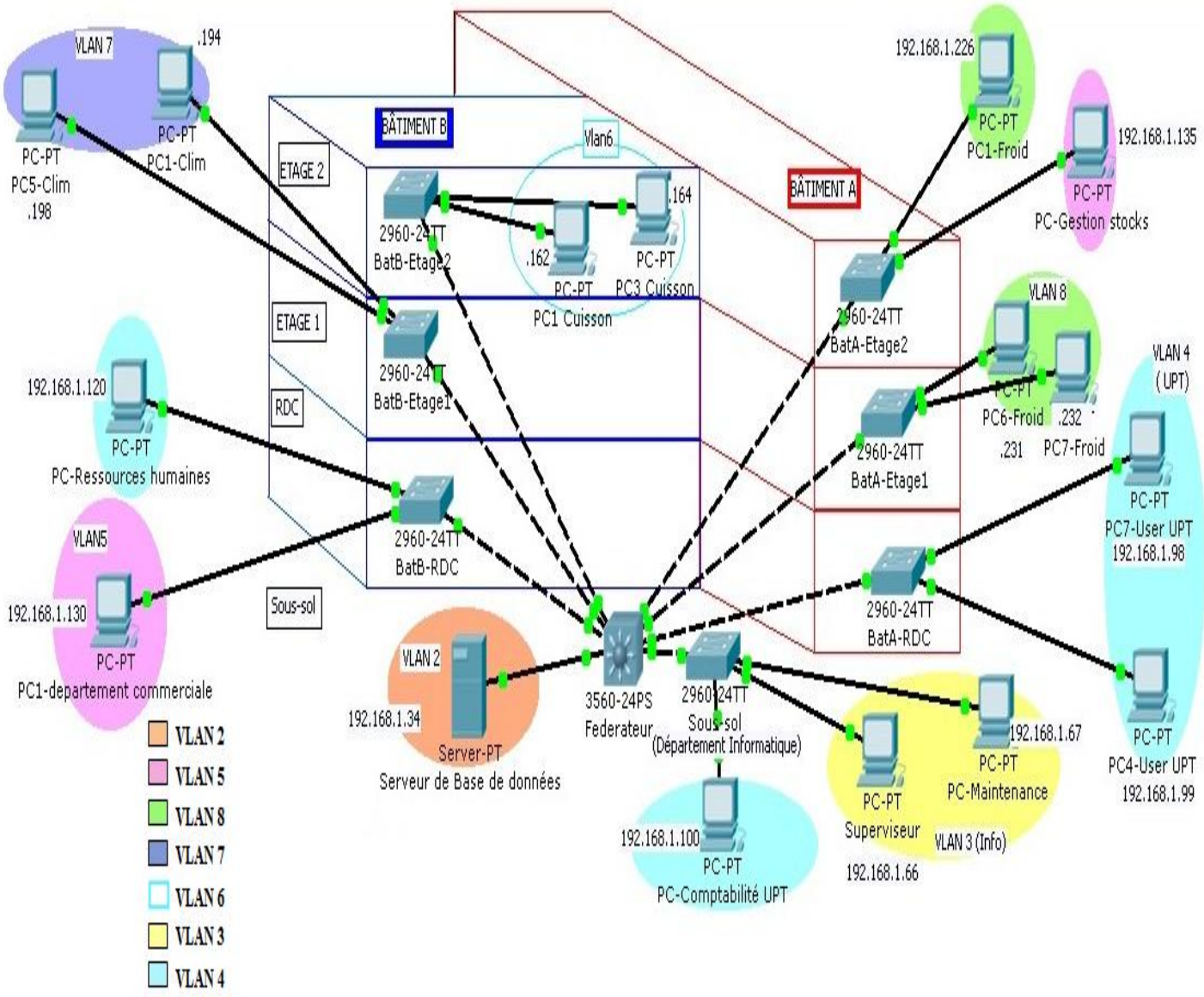

Figure V.2 : la plateforme du réseau local avec le plan d'adressage et les VLAN

B. Adressage du WAN :

Nous utiliserons un réseau IP dédié, et cela pour les raisons suivantes :

- Ces adresses ne sont pas diffusées sur l'ensemble du réseau, elles ne sont connues qu'entre routeurs adjacents.
- Ces adresses n'ont pas besoin d'être connues des utilisateurs.
- Permet de mieux identifier les liaisons WAN.

❖ **L'architecture de la connexion sécurisée WAN et son plan d'adressage:**

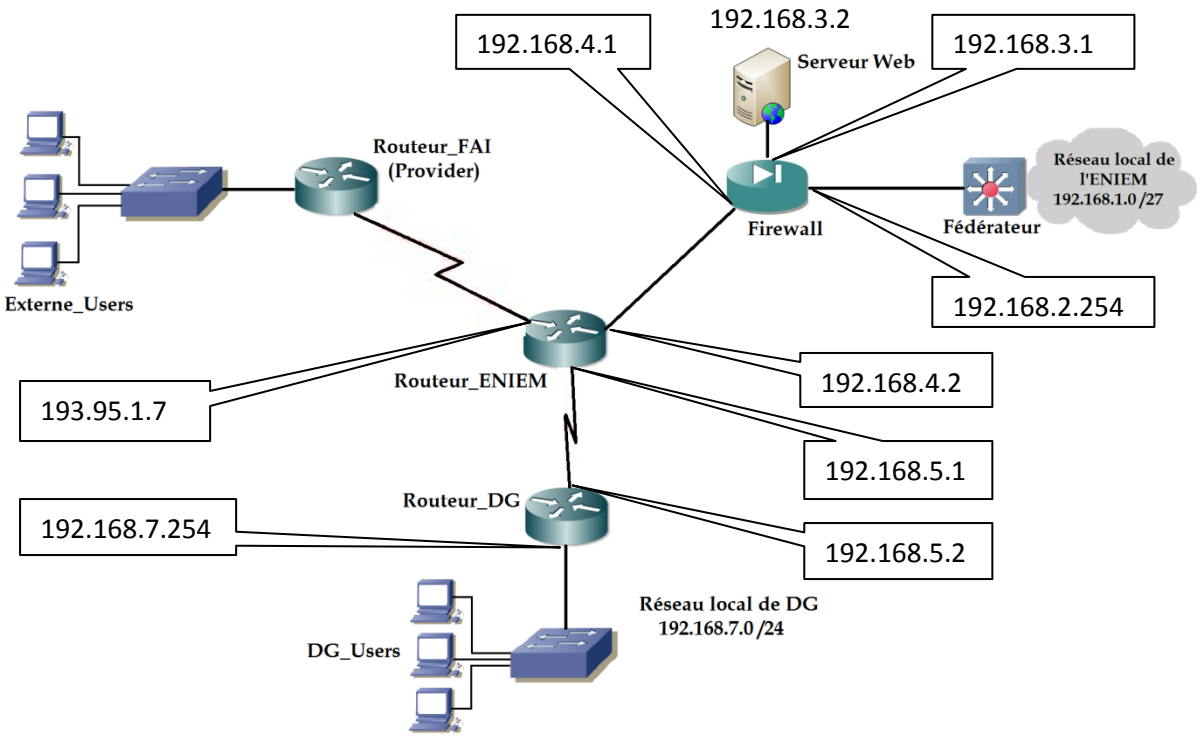

Figure V.3 : Architecture de l'interconnexion des RLE de l'entreprise

V.3.2.1.2. Configurer les Switchs

Les étapes principales de configurations de nos Switchs sont les suivantes :

A. Créer les VLAN

```
Switch(config)# vlan vlan-id
Switch(config-vlan)# name vlan-name
```

B. Assigner les VLAN

```
Switch(config)# interfaces type-interface id-interface
Switch(config-if)#switchport mode [access | trunk]
Switch(config-if)#switchport access vlan vnal-id
```

C. Créer des ACL pour gérer les communications entre VLAN (routage inter-VLAN) :

- **ACL 1:**
  - Autoriser l'accès de l'administrateur (superviseur) à tous les postes, donc à tous les VLAN.
  - Autoriser l'accès du PC-Maintenance à tous les postes.
- **ACL 2:** interdire tous accès à l'administrateur et au PC maintenance sauf si c'est un echo-reply, c'est-à-dire une réponse à un ping (pong).
- **ACL 3:** autoriser l'accès de tous les sous-réseaux du réseau local 192.168.1.0 au serveur de base de données et interdire l'accès d'autres.
- **ACL 4:** interdire la communication entre les postes du VLAN 7 avec ceux du VLAN 5 et autoriser les autres communications.
- **ACL 5 :** interdire les communications entre VLAN 6 et VLAN 8.

D. configurer la route d'accès à internet

Nous indiquons le point de sortie, qui correspond à l'interface 192.168.2.254 :

```
switch(config)#ip route 0.0.0.0  0.0.0.0 192.168.2.254
```

.Configurations correspondante en lignes de commandes :

✓ **Configuration du Switch fédérateur :**

```
switch>enable                                    //passer du mode non privilégié en mode Exec
switch#configure terminal                        // passer en mode configuration global
switch(config)#enable password Eniem7            //attribuer un mot de passe
switch(config)#hostname Federateur               //attributer un nom au Switch
Federateur(config)#interface vlan 1              //passer en mode configuration de l'interface vlan1
Federateur(config-if)#ip address 192.168.1.1  255.255.255.224    //attribuer une addresse
Federateur(config-if)#no shutdown                //activer l'interface
Federateur(config-if)#exit                       //quitter le mode configuration actuel
Federateur(config)# vtp mode server              //configurer le Switch en serveur VTP
Federateur(config)# vtp domain Eniem.fr
Federateur(config)# vtp version 2
Federateur(config)#vlan 2                        //créer le vlan 2
Federateur(config-vlan)#name serveur             //attribuer un nom au vlan 2
Federateur(config-vlan)#exit
Federateur(config)#interface vlan 2              //configurer l'interface vlan2
Federateur(config-if)#ip address  192.168.1.33  255.255.255.224
 Federateur(config-if)#no shutdown
```

```
Federateur(config-if)#exit
Federateur(config)#vlan 3                    //créer le vlan 3
Federateur(config-vlan)#name Informatique    //attribuer un nom au vlan 3
Federateur(config-vlan)#exit
Federateur(config)#interface vlan 3          //configurer l'interface vlan3
Federateur(config-if)#ip address  192.168.1.65  255.255.255.224
 Federateur(config-if)#no shutdown
Federateur(config-if)#exit
      //pour créer les autre vlan (4, 5, 6 , 7, 8), on suit les même étapes que pour vlan 2 et 3
Federateur(config)#interface fastEthernet 0/2
Federateur(config-if)#switchport mode access    //definer l'interface en mode access
Federateur(config-if)#switchport access vlan 2  //assigner l'interface au vlan 2
Federateur(config-if)#no shutdown
Federateur(config-if)#exit
Federateur(config)#interface fastEthernet 0/9
Federateur(config-if)#switchport mode access    //definer l'interface en mode access
Federateur(config-if)#switchport access vlan 9  //assigner l'interface au vlan 9
Federateur(config-if)#no shutdown
Federateur(config-if)#exit
                    //Créer les ACL et les attributer aux interfaces vlan
Federateur(config)#access-list 101 permit icmp 192.168.1.66  0.0.0.0  any
Federateur(config)#access-list 101 permit icmp 192.168.1.67  0.0.0.0  any
Federateur(config)#access-list 101 permit icmp any  192.168.1.34
Federateur(config)#access-list 102 permit icmp any 192.168.1.66  0.0.0.0  echo-reply
Federateur(config)#access-list 102 permit icmp any 192.168.1.67  0.0.0.0  echo-reply
Federateur(config)#interface vlan 3
Federateur(config-if)#ip access-group 101 in
Federateur(config-if)#ip access-group 102 out
Federateur(config-if)#exit
Federateur(config)#access-list 103 permit icmp 192.168.1.0  0.0.0.255  host 192.168.1.34
Federateur(config)#interface vlan 2
Federateur(config-if)#ip access-group 103 out
Federateur(config-if)#exit
Federateur(config)#access-list 104 deny icmp host 192.168.1.194 host 192.168.1.130
Federateur(config)#access-list 104 deny icmp host 192.168.1.194 host 192.168.1.135
```

```
Federateur(config)#access-list 104 deny icmp host 192.168.1.198 host 192.168.1.130
Federateur(config)#access-list 104 deny icmp host 192.168.1.198 host 192.168.1.135
Federateur(config)#access-list 104 permit any any
Federateur(config)#access-list 104 permit icmp any any
Federateur(config)#interface vlan 7
Federateur(config-if)#ip access-group 104 in
Federateur(config-if)#exit
Federateur(config)#access-list 105 deny icmp host 192.168.1.162 host 192.168.1.226
Federateur(config)#access-list 105 deny icmp host 192.168.1.164 host 192.168.1.226
Federateur(config)#access-list 105 deny icmp host 192.168.1.162 host 192.168.1.231
Federateur(config)#access-list 105 deny icmp host 192.168.1.164 host 192.168.1.231
Federateur(config)#access-list 105 deny icmp host 192.168.1.162 host 192.168.1.232
Federateur(config)#access-list 105 deny icmp host 192.168.1.164 host 192.168.1.232
Federateur(config)#access-list 105 permit icmp any any
Federateur(config)#interface vlan 6
Federateur(config-if)#ip access-group 105 in
Federateur(config-if)#exit
Federateur(config)#exit
Federateur#write terminal      // sauvegarder la configuration
```

✓ **Configuration du Switch du département informatique :**

```
switch>enable
switch#configure terminal
switch(config)#enable password Eniem7
switch (config)#hostname Informatique
Informatique(config)#interface vlan 1
Informatique(config-if)#ip address 192.168.1.2 255.255.255.224
Informatique(config-if)#no shutdown
Informatique(config-if)#exit
Informatique(config)#vtp mode client
Informatique(config)#interface fastEthernet 0/1
Informatique(config-if)#switchport mode trunk
Informatique(config-if)#switchport  trunk encapsulation dot1q
Informatique(config-if)#no shutdown
```

```
Informatique(config-if)#exit
Informatique(config)#interface fastEthernet 0/2
Informatique(config-if)#switchport mode access
Informatique(config-if)#switchport access vlan 3
Informatique(config-if)#no shutdown
Informatique(config-if)#exit
Informatique(config)#interface fastEthernet 0/3
Informatique(config-if)#switchport mode access
Informatique(config-if)#switchport access vlan 3
Informatique(config-if)#no shutdown
Informatique(config-if)#exit
Informatique(config)#interface fastEthernet 0/4
Informatique(config-if)#switchport mode access
Informatique (config-if)#switchport access vlan 4
Informatique(config-if)#no shutdown
Informatique(config-if)#exit
Informatique(config)#exit
Informatique#write terminal
```

✓ **Switch RDC Bâtiment A :**

```
switch>enable
switch#configure terminal
switch(config)#enable password Eniem7
switch(config)#hostname BatA_RDC
BatA_RDC(config)#interface vlan 1
BatA_RDC(config-if)#ip address 192.168.1.3 255.255.255.224
BatA_RDC(config-if)#no shutdown
BatA_RDC(config-if)#exit
BatA_RDC(config)#vtp mode client
BatA_RDC(config)#interface fastEthernet 0/1
BatA_RDC(config-if)#switchport mode trunk
BatA_RDC(config-if)#switchport  trunk encapsulation dot1q
BatA_RDC(config-if)#no shutdown
BatA_RDC(config-if)#exit
BatA_RDC(config)#interface fastEthernet 0/2
```

```
BatA_RDC(config-if)#switchport mode access
BatA_RDC(config-if)#switchport access vlan 4
BatA_RDC(config-if)#no shutdown
BatA_RDC(config-if)#exit
BatA_RDC(config)#interface fastEthernet 0/3
BatA_RDC(config-if)#switchport mode access
BatA_RDC(config-if)#switchport access vlan 4
BatA_RDC(config-if)#no shutdown
BatA_RDC(config-if)#exit
BatA_RDC(config)#exit
BatA_RDC#write terminal
```

✓ **Switch RDC Bâtiment B :**

```
switch>enable
switch#configure terminal
switch(config)#enable password Eniem7
switch(config)#hostname BatB_RDC
BatB_RDC(config)#interface vlan 1
BatB_RDC(config-if)#ip address 192.168.1.4 255.255.255.224
BatB_RDC(config-if)#no shutdown
BatB_RDC(config-if)#exit
BatB_RDC(config)#vtp mode client
BatB_RDC(config)#interface fastEthernet 0/1
BatB_RDC(config-if)#switchport mode trunk
BatB_RDC(config-if)#switchport  trunk encapsulation dot1q
BatB_RDC(config-if)#no shutdown
BatB_RDC(config-if)#exit
BatB_RDC(config)#interface fastEthernet 0/2
BatB_RDC(config-if)#switchport mode access
BatB_RDC(config-if)#switchport access vlan 4
BatB_RDC(config-if)#no shutdown
BatB_RDC(config-if)#exit
BatB_RDC(config)#interface fastEthernet 0/3
BatB_RDC(config-if)#switchport mode access
BatB_RDC(config-if)#switchport access vlan 5
```

```
BatB_RDC(config-if)#no shutdown
BatB_RDC(config-if)#exit
BatB_RDC(config)#exit
BatB_RDC #write terminal
```

✓ **Switch étage 01 Bâtiment A :**

```
switch>enable
switch#configure terminal
switch(config)#enable password Eniem7
switch(config)#hostname BatA_Etage1
BatA_Etage1(config)#interface vlan 1
BatA_Etage1(config-if)#ip address 192.168.1.5 255.255.255.224
BatA_Etage1(config-if)#no shutdown
BatA_Etage1(config-if)#exit
BatA_Etage1(config)#vtp mode client
BatA_Etage1(config)#interface fastEthernet 0/1
BatA_Etage1(config-if)#switchport mode trunk
BatA_Etage1(config-if)#switchport  trunk encapsulation dot1q
BatA_Etage1(config-if)#no shutdown
BatA_Etage1(config-if)#exit
BatA_Etage1(config)#interface fastEthernet 0/2
BatA_Etage1(config-if)#switchport mode access
BatA_Etage1(config-if)#switchport access vlan 8
BatA_Etage1(config-if)#no shutdown
BatA_Etage1(config-if)#exit
BatA_Etage1(config)#interface fastEthernet 0/3
BatA_Etage1(config-if)#switchport mode access
BatA_Etage1(config-if)#switchport access vlan 8
BatA_Etage1(config-if)#no shutdown
BatA_Etage1(config-if)#exit
BatA_Etage1(config)#exit
BatA_Etage1#write terminal
```

✓ **Switch étage 01 Bâtiment B :**

```
switch>enable
switch#configure terminal
```

```
switch(config)#enable password Eniem7
switch (config)#hostname BatB_Etage1
BatB_Etage1(config)#interface vlan 1
BatB_Etage1(config-if)#ip address 192.168.1.6 255.255.255.224
BatB_Etage1(config-if)#no shutdown
BatB_Etage1(config-if)#exit
BatB_Etage1(config)#vtp mode client
BatB_Etage1(config)#interface fastEthernet 0/1
BatB_Etage1(config-if)#switchport mode trunk
BatB_Etage1(config-if)#switchport  trunk encapsulation dot1q
BatB_Etage1(config-if)#no shutdown
BatB_Etage1(config-if)#exit
BatB_Etage1(config)#interface fastEthernet 0/2
BatB_Etage1(config-if)#switchport mode access
BatB_Etage1(config-if)#switchport access vlan 7
BatB_Etage1(config-if)#no shutdown
BatB_Etage1(config-if)#exit
BatB_Etage1(config)#interface fastEthernet 0/3
BatB_Etage1(config-if)#switchport mode access
BatB_Etage1(config-if)#switchport access vlan 7
BatB_Etage1(config-if)#no shutdown
BatB_Etage1(config-if)#exit
BatB_Etage1(config)#exit
BatB_Etage1#write terminal
```

✓ **Switch étage 02 Bâtiment A :**

```
switch>enable
switch#configure terminal
switch(config)#enable password Eniem7
switch (config)#hostname BatA_Etage2
BatA_Etage2(config)#interface vlan 1
BatA_Etage2(config-if)#ip address 192.168.1.7 255.255.255.224
BatA_Etage2(config-if)#no shutdown
BatA_Etage2(config-if)#exit
BatA_Etage2(config)#vtp mode client
```

```
BatA_Etage2(config)#interface fastEthernet 0/1
BatA_Etage2(config-if)#switchport mode trunk
BatA_Etage2(config-if)#switchport  trunk encapsulation dot1q
BatA_Etage2(config-if)#no shutdown
BatA_Etage2(config-if)#exit
BatA_Etage2(config)#interface fastEthernet 0/2
BatA_Etage2(config-if)#switchport mode access
BatA_Etage2(config-if)#switchport access vlan 8
BatA_Etage2(config-if)#no shutdown
BatA_Etage2(config-if)#exit
BatA_Etage2(config)#interface fastEthernet 0/3
BatA_Etage2(config-if)#switchport mode access
BatA_Etage2(config-if)#switchport access vlan 5
BatA_Etage2(config-if)#no shutdown
BatA_Etage2(config-if)#exit
BatA_Etage2(config) #exit
BatA_Etage2 #write terminal
```

✓ **Switch étage 02 Bâtiment B :**

```
switch>enable
switch#configure terminal
switch(config)#enable password Eniem7
switch (config)#hostname BatB_Etage2
BatB_Etage2(config)#interface vlan 1
BatB_Etage2(config-if)#ip address 192.168.1.8 255.255.255.224
BatB_Etage2(config-if)#no shutdown
BatB_Etage2(config-if)#exit
BatB_Etage2(config)#vtp mode client
BatB_Etage2(config)#interface fastEthernet 0/1
BatB_Etage2(config-if)#switchport mode trunk
BatB_Etage2(config-if)#switchport  trunk encapsulation dot1q
BatB_Etage2(config-if)#no shutdown
BatB_Etage2(config-if)#exit
BatB_Etage2(config)#interface fastEthernet 0/2
BatB_Etage2(config-if)#switchport mode access
```

```
BatB_Etage2(config-if)#switchport access vlan 6
BatB_Etage2(config-if)#no shutdown
BatB_Etage2(config-if)#exit
BatB_Etage2(config)#interface fastEthernet 0/3
BatB_Etage2(config-if)#switchport mode access
BatB_Etage2(config-if)#switchport access vlan 6
BatB_Etage2(config-if)#no shutdown
BatB_Etage2(config-if)#exit
BatB_Etage2(config)#exit
BatB_Etage2#write terminal
```

V.3.2.2. Implémentation du firewall matériel PIX (Private Internet eXchange)

V.3.2.2.1. Choix du type de firewall PIX Cisco

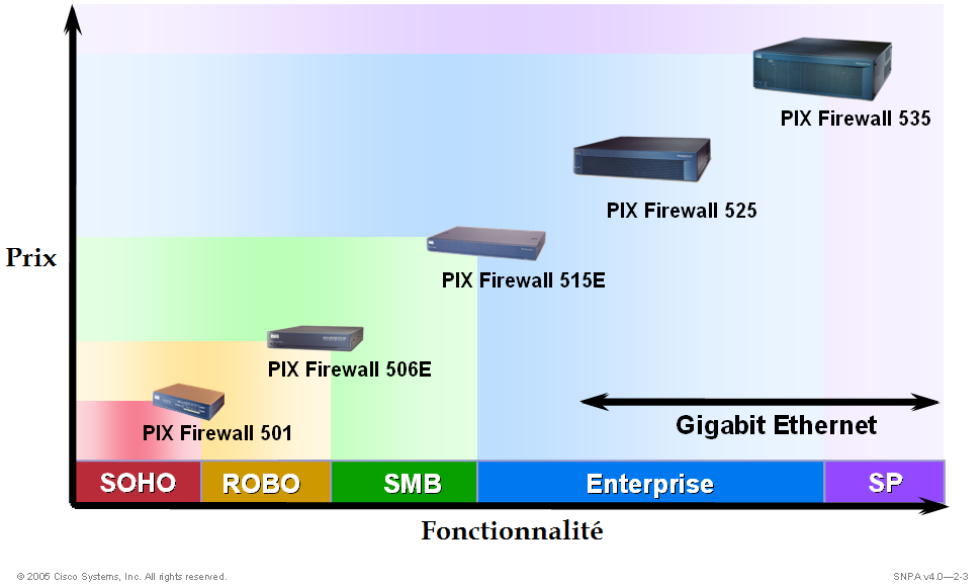

Figure V.4 : Types de firewall PIX Cisco

❖ **Caractéristiques du PIX 515 :**

- Il est désigné pour les petites et moyennes entreprises mais aussi pour les grandes entreprises.
- Interfaces :
  - Supporte jusqu'à six interfaces 10/100 fastEthernet.
  - Supporte jusqu'à 25 VLANS.
- Peut fonctionner en failover: Active/Standbay, Active/Active.
- Supporte jusqu'à 2000 tunnels VPN.

→ Ce qui en fait un excellent choix pour les entreprises nécessitant un bon rapport coût-efficacité, c'est la solution de sécurité résiliente en "zone démilitarisée". Il offre également jusqu'à 188 Mbits / s de débit firewall avec la capacité de traiter plus de 130000 sessions simultanées.

Remarque : les PIX 501 et 506 sont utilisés dans les petits bureaux et pour le télétravail, les PIX 525 et 535, sont conçus pour les grandes entreprises, pour du gigabits Ethernet.

⇨ Nous avons choisi donc pour sécuriser notre réseau, le **firewall PIX 515E**

V.3.2.2.2. Inclure le firewall PIX dans le réseau

Nous plaçons le PIX 515 entre le réseau interne et le réseau externe, Nous allons le doté de trois interfaces réseaux : une connectée au réseau local (Inside, Ethernet1), l'autre à Internet (Outside, Ethernet0) et la troisième au serveur Web (DMZ, Ethernet2) comme le montre la figure :

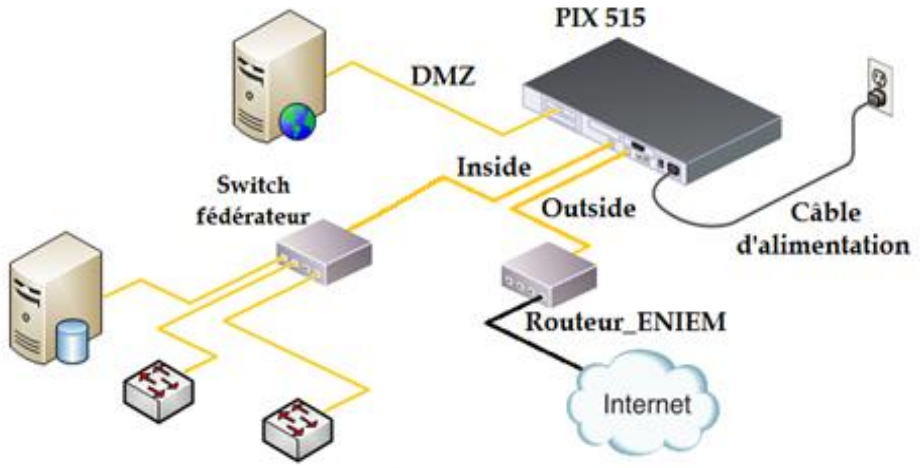

Figure V.5 : schéma de branchement du firewall

Avec sa, trois zones de sécurité différente seront créées:

- La zone interne avec 100% de sécurité (**Inside Network**)→Le réseau local.
- La zone externe avec 0% de sécurité (**Outside Network**) →Internet.
- La zone intermédiaire avec 50% de sécurité (**DMZ**) → Serveur Web.

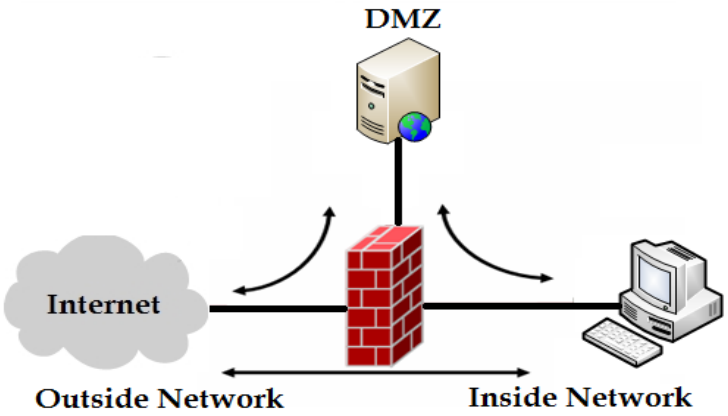

Figure V.6 : Cloisonnement du réseau en trois zones de sécurité

Remarque : dans cette architecture, il y'a différence de protection périmètrique, les flux entre les zones sont ainsi filtrés à différents niveaux, on établie des règles d'accès entre ces trois zones telque:

- Du plus sécurisé vers le moins sécurisé → accès autorisé.
- Du moins sécurisé vers le plus sécurisé → accès interdit (ou limité avec des ACL).

V.3.2.2.3. Les procédures de configuration du firewall PIX 515

Pour configurer le firewall nous devons suivre les étapes suivantes :

- Configurer les interfaces du firewall.
- Configurer les translations d'adresses.
- Configurer le routage.
- Contrôler les accès avec des ACL.

1. Configurer les interfaces du pare-feu : nous suivons les procédures suivantes :

- Donner un nom pour chaque interface.
- Donner une adresse IP.
- Donner le niveau de sécurité.

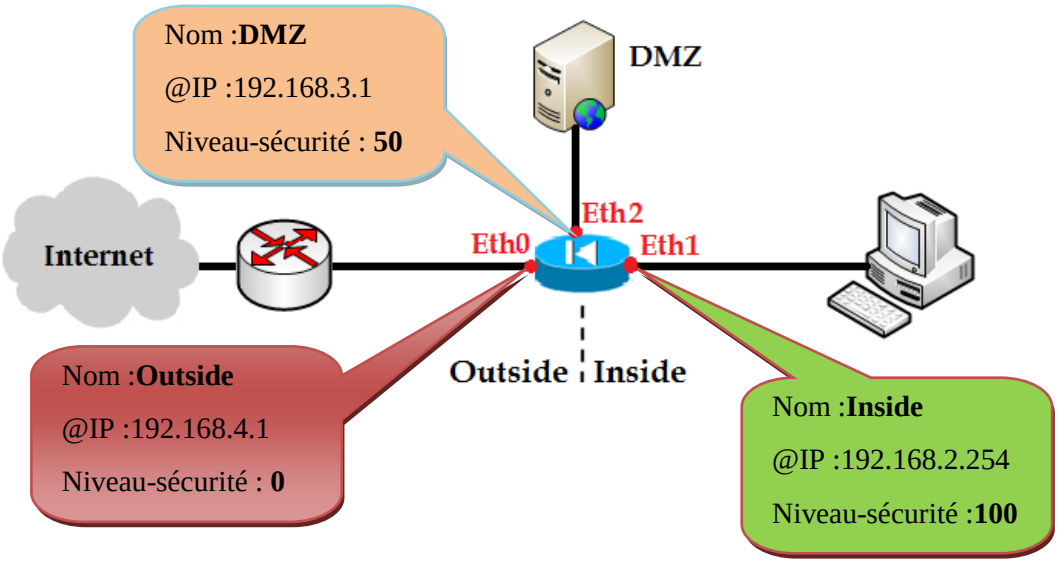

Figure V.7 : Configuration des trois interfaces du firewall

. La configuration en lignes de commandes :

```
Pixfirewall>enable
Pixfirewall #configure terminal
Pixfirewall(config) #enable password Eniem7
Pixfirewall(config)#interface Ethernet 0     //configurer l'interface Ethernet 0
Pixfirewall(config-if)#nameif Outside
Pixfirewall(config-if)#ip address
Pixfirewall(config-if)#Security-level 0
Pixfirewall(config-if)#Duplex auto
Pixfirewall(config-if)#speed auto
Pixfirewall(config-if)#exit
Pixfirewall(config)#interface Ethernet 1       //configurer l'interface Ethernet 1
Pixfirewall(config-if)#nameif Inside
Pixfirewall(config-if)#ip address
Pixfirewall(config-if)#Security-level 100
Pixfirewall(config-if)#Duplex auto
Pixfirewall(config-if)#speed auto
Pixfirewall(config-if)#exit
Pixfirewall(config)#interface Ethernet 2       //configurer l'interface Ethernet 2
Pixfirewall(config-if)#nameif DMZ
Pixfirewall(config-if)#ip address
Pixfirewall(config-if)#Security-level 50
Pixfirewall(config-if)#Duplex auto
Pixfirewall (config-if)#speed auto
Pixfirewall(config-if)#exit
```

2. Translation d'adresses

Pour éviter que nos adresses entrent en conflit avec celles de l'internet, mais aussi pour masquer notre plan d'adressage interne vis-à-vis des utilisateurs situés sur Internet nous utilisons la NAT et la PAT.

Remarque : il y'a garantie que toutes les adresses privées ne seront jamais routées sur Internet

- **Configurer les translations d'adresses :**

.Indiquer l'application PAT à toute machine (0.0.0.0 0.0.0.0) venant de l'interface Inside.

```
Pixfirewall(config)#nat (inside) 1  0.0.0.0  0.0.0.0
```

.Indiquer de faire du PAT avec l'interface outside :

```
Pixfirewall(config)#global (outside) 1  interface
```

. Appliquer un mappage de redirection entre Inside et DMZ et entre DMZ et Outside :

```
Pixfirewall(config)#static (Inside,DMZ) 192.168.3.0  192.168.2.0 netmask 255.255.255.0
```

. Redirection des adresses venant de l'extérieur vers la DMZ :

```
Pixfirewall(config)#static (DMZ,Outside) 192.168.4.1  192.168.3.2
```

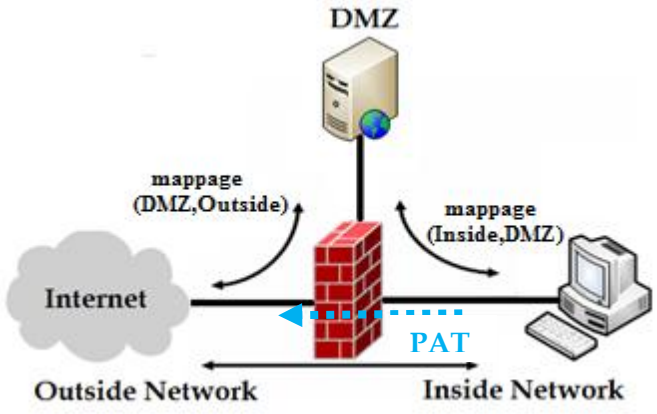

Figure V.8 : configuration du PAT

3. Configurer le routage :

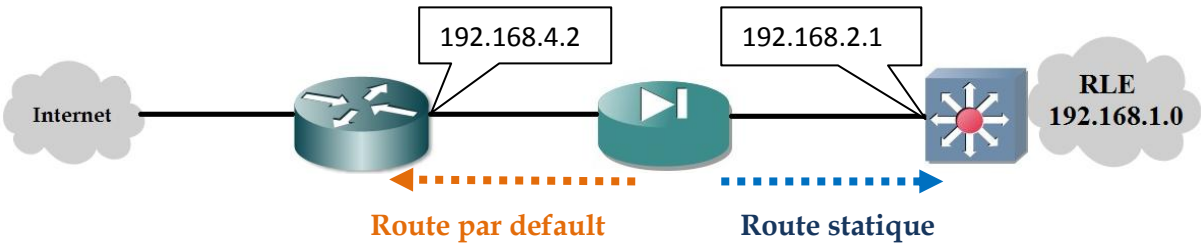

Figure V.9 : Le routage au niveau du firewall

. Indiquer aux adresses appartenant au réseau 192.168.1.0 la route vers l'interface VLAN 9 (192.168.2.1) :

```
Pixfirewall(config)#route Inside 192.168.1.0  255.255.255.0  192.168.2.1  1
```

.Indiquer la passerelle 192.168.4.2 pour toutes autres adresses (non locale) :

```
Pixfirewall(config)#route Outside 0.0.0.0  0.0.0.0  192.168.4.2  1
```

4. Filtrer les accès au réseau

Dans un firewall, l'accès de plus sécurisé à moins sécurisé est autorisé, et du moins sécurisé vers le plus sécurisé l'accès est interdit. De la, personne ne peut accéder au serveur web pour consulté le site de l'ENIEM, et même la direction générale n'a pas d'accès au RLE. C'est pour cela, que nous allons créer des ACL qui autoriseront certains accès :

.Autoriser le service http de toute machine vers la DMZ :

```
Pixfirewall(config)#access-list 101 permit http any host 192.168.3.2 eq
```

. Autoriser l'accès des PC de la direction Générale aux PC1-Commerciale et pc-ressources humaines ainsi qu'au PC-gestion stocks :

```
Pixfirewall(config)#access-list 101 permit tcp 192.168.7.0  0.0.0.255 host 192.168.1.130 eq

Pixfirewall(config)#access-list 101 permit tcp host 192.168.7.7  host 192.168.1.120 eq

Pixfirewall(config)#access-list 101 permit tcp host 192.168.7.7  host 192.168.1.135 eq

Pixfirewall(config)#access-list 101 deny tcp any any

Pixfirewall(config)#access-group 101 in interface outside
```

V.3.3. Interconnexion entre l'entreprise ENIEM et sa direction générale

Le réseau WAN va interconnecter le RLE de l'entreprise ENIEM (située à la zone industrielle) au RLE de sa direction générale à Tizi-Ouzou, celui-ci utilisera les sévices d'un réseau de transport qui correspond aux couches physique (niveau 1) et logique (niveau 2), tel que Ethernet est utilisée pour le RLE, et FrameRelay pour le WAN.

Cette technologie repend à des contraintes plus larges. Dans ce projet d'interconnexion nous allons :

- Interconnecter des RLE via FrameRelay et Gérer la qualité de service.
- Configurer le routage.
- Sécurisé l'interconnexion.

Les étapes sont comme suite :

V.3.3.1. Choix du routeur

Afin de choisir le bon routeur qui sera cohérant avec nos besoins il faut se baser sur les points suivants :

- Les réseaux supportés (Ethernet, Token-Ring,…)
- Les supports WAN disponibles (RTC, X25, FrameRelay, PPP, HDLC…)
- Les protocoles supportés (TCP/IP…)

- Les protocoles et méthodes de routage (OSPF, RIP, EGRP…)
- Administration (administrabilité)

⇨ Le routeur 2600 supporte les réseaux Ethernet, englobe un support WAN FrameRelay, et supporte le protocole TCP/IP, celui-ci peut utiliser OSPF pour le routage, en plus il est administrable. Nous utiliserons donc le **routeur Cisco C2600**.

V.3.3.2. Le choix de la technologie d'encapsulation

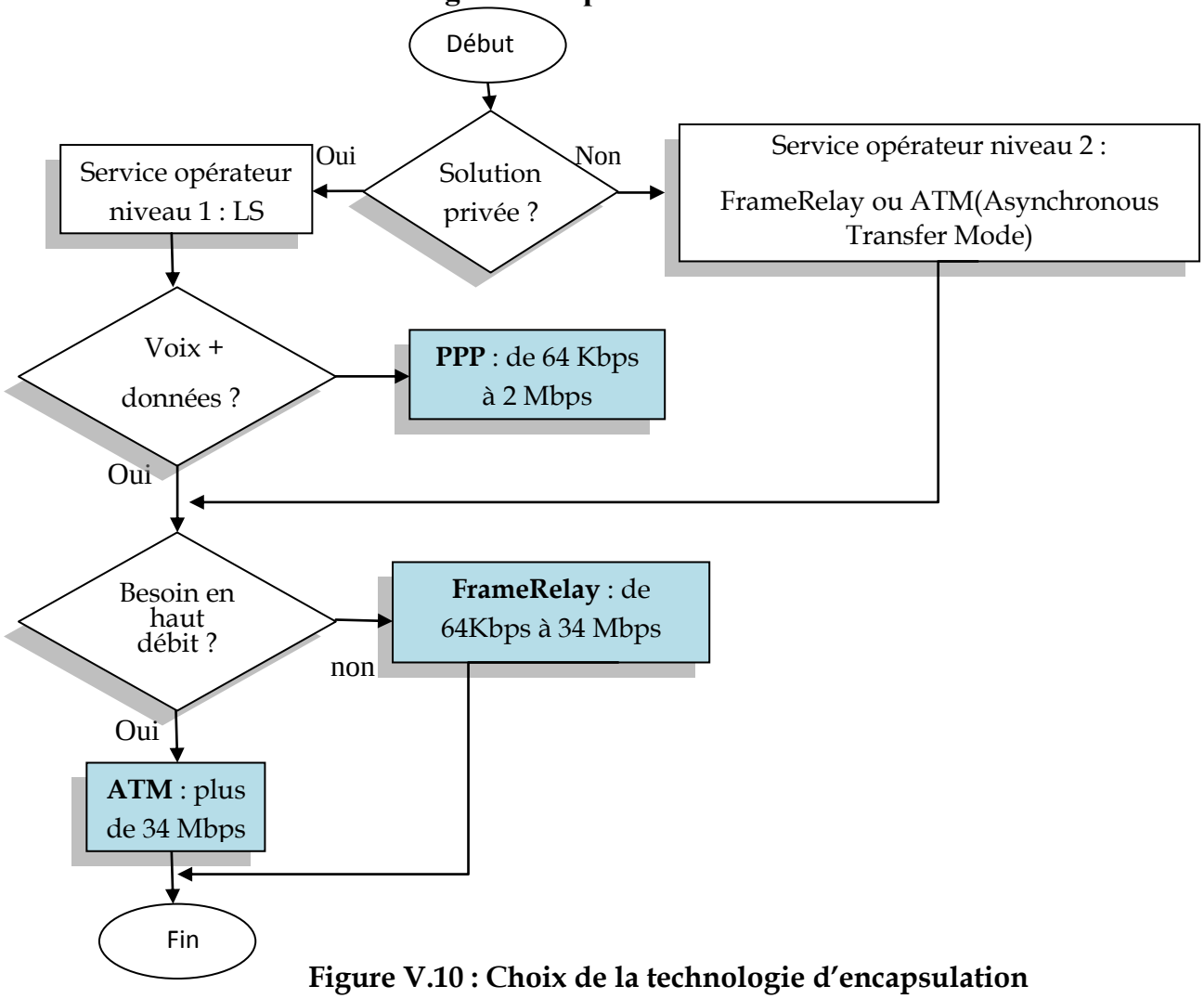

Figure V.10 : Choix de la technologie d'encapsulation

⇨ FrameRelay, revient moins couteux et repend aux besoins de notre réseau, tout en offrant une bonne qualité de services (gérer les congestions et garantir les débits). Nous utiliserons donc l'encapsulation le **protocole Framerelay**.

V.3.3.3. Choix du protocole de routage

Une fois arrivés sur le WAN, les paquets IP provenant du RLE se trouvent face à de multiples routes allant vers la même destination. Il convient d'utiliser un protocole de routage dynamique, nous avons alors le choix entre RIP et OSPF. Ce dernier étant le plus performant et le plus rependu, même s'il est un peut complexe à programmer.

⇨ Nous utiliserons donc **OSPF**.

V.3.3.4. Connecter notre routeur au réseau de transport

La manière la plus simple de raccorder notre routeur consiste à les configurer en FRAD (FrameRelay Access Device). Dans ce cas les trames LAN (Ethernet) seront converties en trame FrameRelay. Une fois mise en place, la liaison FrameRelay permettra aux routeurs de se joindre directement.

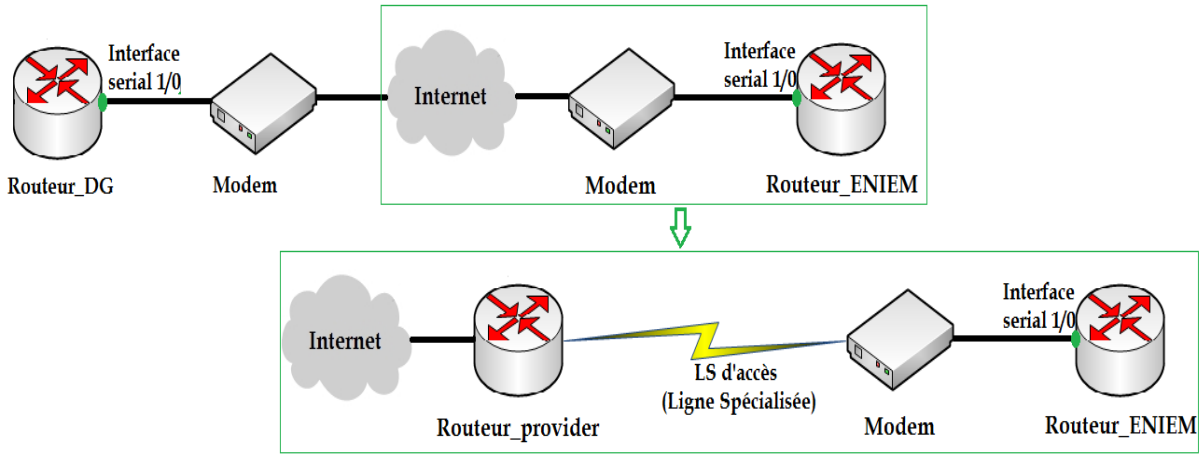

Figure V.11 : Connexion du routeur au réseau de transport

Remarque : si notre routeur ne supportait pas FrameRelay, nous l'aurions connecté à des FRAD de l'opérateur via son interface série.

V.3.3.5. Configurer les routeurs

1. Configurations de base :

```
Router>enable
Router#configure terminal
Router(config)#hostname RouteurENIEM
RouteurENIEM(config) #enable password Eniem7
RouteurENIEM(config) #enable secret Eniem2013        //définir un mot de passe crypté
```

3. configuration de la ligne console :

```
RouteurENIEM(config) #line console 0

RouteurENIEM(config-line) #enable pasword ENIEM2013
```

.Configurer la ligne de console pour exiger un mot de passe à l'ouverture de la session :

```
RouteurENIEM(config-line) #login
```

Rappal : La connexion au routeur s'effectue par le port console en utilisant la ligne associée à ce port ou bien à distance en utilisant les lignes virtuelles

4. Configurer des lignes virtuelles (vty) :

Afin de permettre la connexion telnet ou ssh sur le routeur si nous désirons administrer le routeur à partir d'une liaison Ethernet et non série. Voici la configuration pour chacun des routeurs:

```
RouteurENIEM(config) #line vty 0 4
RouteurENIEM(config-line) #password Eniem7
RouteurENIEM(config-line) #login   //configurer le terminal virtuel pour qu'il exige un
                                   mot de passe à l'ouverture d'une session
```

5. Configuration des interfaces :

Les ports LAN (Ethernet) des routeurs, nous les avons utilisé pour relier les réseaux LAN Ethernet et les port Série pour simuler le réseau WAN. Les configurations sont comme suite :

- **Routeur ENIEM :**
  - **Interfaces Ethernet :**

```
RouteurENIEM(config) #interface Ethernet 2/0
RouteurENIEM(config-if) #ip address 192.168.4.2  255.255.255.0
RouteurENIEM(config-if) #shutdown
RouteurENIEM(config-if) #no shutdown
RouteurENIEM(config-if) #exit
```

  - **Interfaces Séries :**

```
RouteurENIEM(config)#Interface serial 1/0
RouteurENIEM(config) #ip  address  192.168.5.1 255.255.255.0
RouteurENIEM(config-if) #shutdown
RouteurENIEM(config-if) #no shutdown
RouteurENIEM(config-if) #exit
RouteurENIEM(config)#Interface serial 1/1
RouteurENIEM(config-if) #ip  address  193.95.1.7 255.255.255.0
RouterENIEM(config-if) #shutdown
RouteurENIEM(config-if) #no shutdown
```

- **Routeur de la Direction générale :**
  - **Interfaces Ethernet :**

```
RouteurDG(config) #interface Ethernet 2/0
```

```
RouteurDG(config-if) #ip address 192.168.7.254  255.255.255.0
RouteurDG(config-if) #shutdown
RouteurDG(config-if) #no shutdown
RouteurDG(config-if) #exit
```

- **Interfaces Séries :**

```
RouteurDG(config)#Interface serial 1/0
RouteurDG(config) #ip  address  192.168.5.2 255.255.255.0
RouteurDG(config-if) #shutdown
RouteurDG(config-if) #no shutdown
```

6. Mise au point de la fonction de routage :

.Configuration du routage avec OSPF :

. La première tâche est d'activer le routage OSPF. Sur nos routeurs, il faut attribuer un numéro de processus, car plusieurs instances d'OSPF peuvent fonctionner simultanément.

. Le seconde tâche est de définir l'aire, appelé backbone area. Dans notre cas area 0

Remarque : même si de nombreuses configurations d'OSPF sont possibles, il est conseillé de respecter les règles qui suivent :

. L'aire doit couvrir toutes les interfaces WAN du routeur (interfaces séries, RNIS, ATM…)

. Une aire doit être définie par site ou par groupes de sites fédérés. L'intérêt étant de contrôler la diffusion des sites.

- **Routeur ENIEM :**

```
RouteurENIEM(config) #router ospf 1
RouteurENIEM(config-router) #Network 192.168.4.0  0.0.0.255 area 0
RouteurENIEM(config-router) #Network 192.168.5.0  0.0.0.255 area 0
RouteurENIEM(config-router) #Network 193.95.1.7  0.0.0.0 area 0
```

- **Routeur de la Direction générale :**

```
RouteurDG(config) #router ospf 1
RouteurDG(config-router) #Network 192.168.5.0   0.0.0.255 area 0
RouteurDG(config-router) #Network 192.168.7.0   0.0.0.255 area 0
```

7. Configuration de FrameRelay :

- **Routeur ENIEM :**

```
RouteurENIEM(config)#Interface serial 1/0
RouteurENIEM(config-if)#encapsulation frame-relay
```

- **Routeur de la Direction générale:**

```
RouteurDG(config)#Interface serial 1/0
RouteurDG (config-if)#encapsulation frame-relay
```

8. Sécurisation générale des routeurs :

La sécurisation des routeurs est assurée avec :

. Des mots de passe cryptés :

```
Routeur(config) #enable secret password
```

. Interdiction d'accès aux autres terminaux virtuels :

```
Routeur(config)#line vty 5 15
Routeur(config-line) #no login
```

. Désactivation des services non utilisés qui peuvent être exploités pour nuire :

```
Routeur(config)#no service tcp-small-servers
Routeur(config) #no service udp-small-servers
```

→ Désactivent les services TCP et UDP echo, daytime et chargen, qui ne sont pas utilisés de manière générale et peuvent permettre de récolter des informations utiles ou de lancer des attaques par déni de service. Il est préférable que ces services à valeur ajoutée soient assurés par un serveur dédié.

```
Routeur(config)#no ip bootp server
```

→ Désactive le service bootp, qui utilise le routeur pour récupérer des informations réseau et expose de ce fait ce dernier à des attaques par déni de service.

V.3.4. Supervision du réseau

Plus un réseau est important plus il devient difficile à gérer. Même lorsque le réseau est fonctionnel, il y'a des événements et des erreurs qui ne sont pas perceptibles, mais qui peuvent le devenir sous certaines conditions. Il convient donc d'utiliser une maintenance préventive avec des outils qui simplifient sa gestion, et diminuent donc le nombre potentiel de pannes et d'éviter le pire, et garantir avec sa, la fiabilité et la disponibilité, cella entre en relation avec la sécurité.

❖ **La plateforme de supervision sous SNMP :**

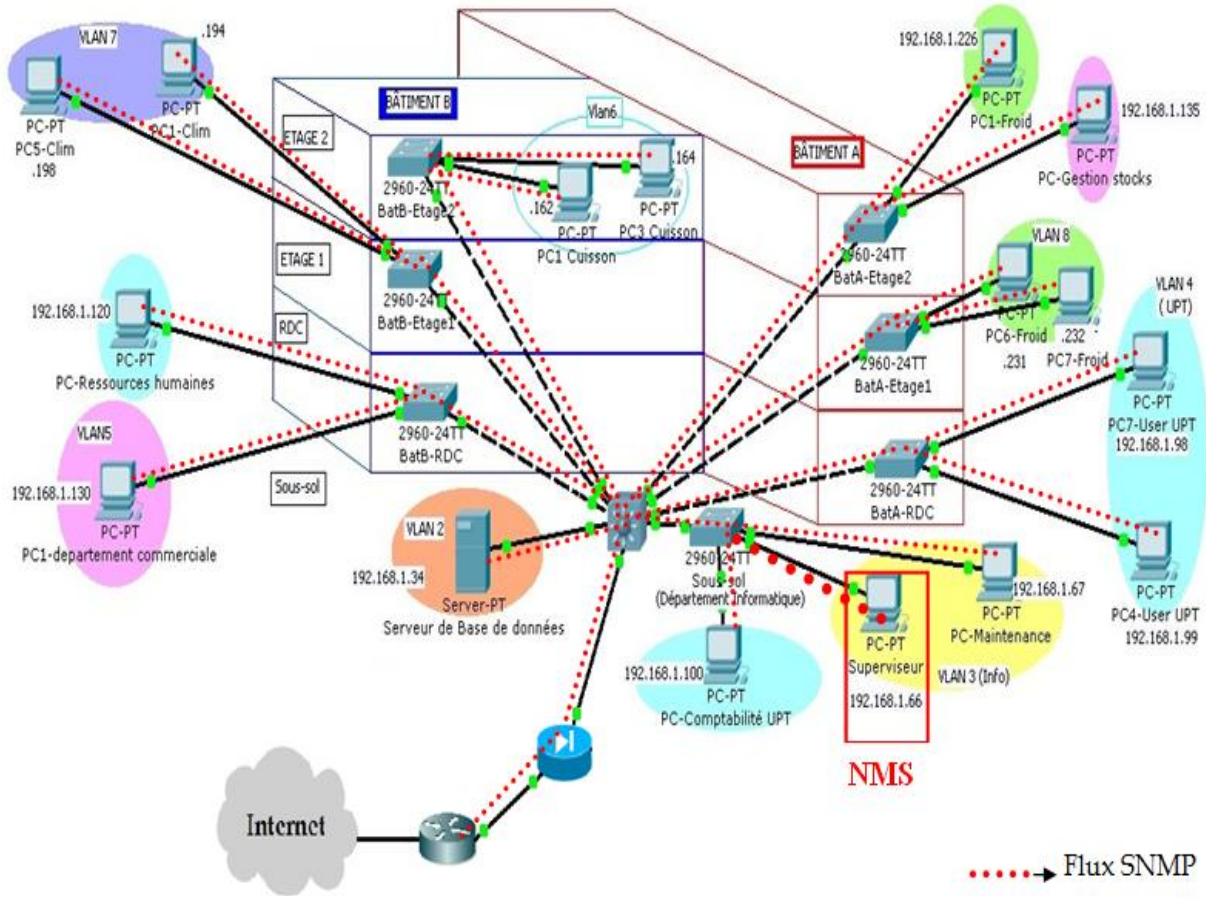

Figure V.12 : la plateforme de supervision et le flux SNMP

Rappel : La NMS (Network Managment Station) gère les NME (Network managment Entity)

Une telle plateforme va fédérer la gestion du parc informatique autour d'une gestion centralisée des alarmes, cela nécessite un paramétrage très important. Et donc, dans le cadre d'une supervision centralisée en temps réel, nous allons:

- Installer et configurer un serveur de supervision global, et installer les outils nécessaires.
- Configurer les équipements pour qu'ils soient supervisés par le manager installé.

V.3.4.1. Installer et configurer un serveur de supervision global :

La mise au point comprend, l'installation d'un NMA, SNMP, et des outils d'analyse et scan **:**

V.3.4.1.1. Installation d'une NMA (Network Management Application) :

Nous utilisons **PRTG** (Paessler Router Trafic Grapher). C'est un outil qui surveille l'utilisation du réseau et de la bande passante ainsi que différents autres paramètres via SNMP, tels que l'utilisation de la mémoire vive et celle de l'unité centrale, fournissant ainsi aux administrateurs système des mesures temps réel et des tendances d'utilisation périodiques leur permettant d'optimiser l'efficacité, l'organisation et la configuration des lignes

permanentes, des routeurs, des pare-feu, des serveurs et autres composants du réseau qui sont compatible SNMP.

PRTG tourne sur un ordinateur Windows, les données statistiques enregistrées sont stockées dans une base de données interne pour être exploitées, celles-ci sont visualisées sur l'interface graphique Windows de PRTG. Voici l'interface graphique de PRTG 13 :

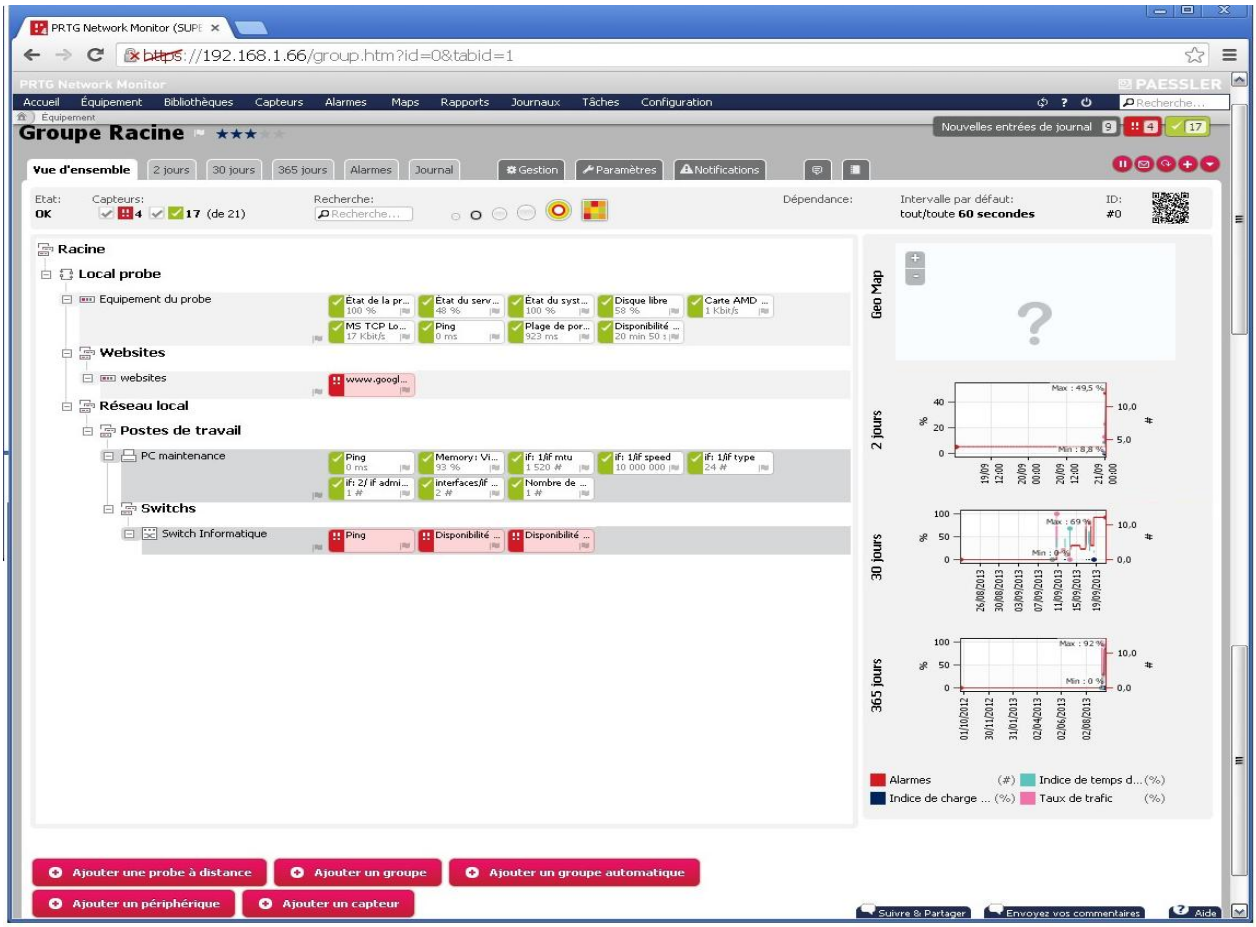

Figure V.13 : L'interface graphique de PRTG

V.3.4.1.2. Installation des outils d'analyse et de gestion réseau (démons SNMP sous Windows XP) :

L'installation se fait sous le système Windows XP. Il faudra juste faire un peu attention à ne pas laisser l'accès à n'importe qui sur n'importe quoi. Les étapes sont les suivantes :

1. Aller dans le panneau de configuration - Ajout/suppression de programmes - ajouter/supprimer des composants Windows :

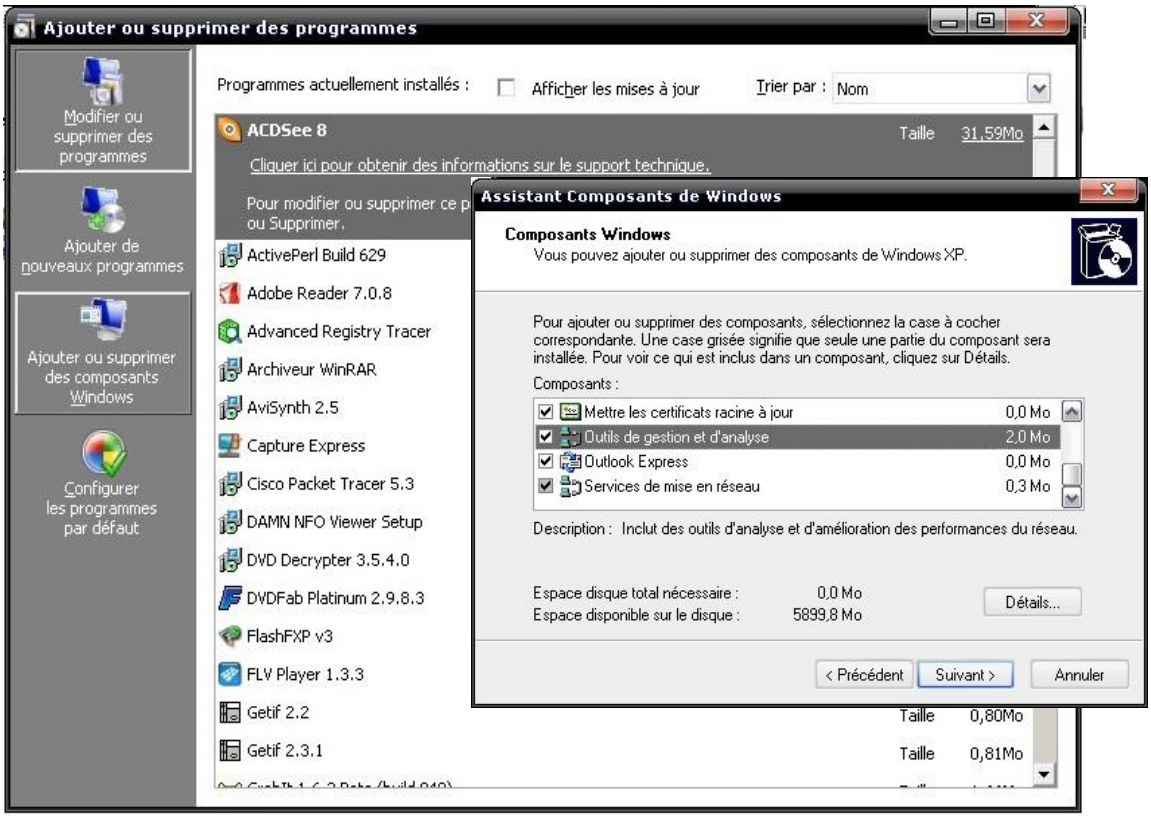

Figure V.14 : Installation des outils d'analyse et de gestion

2. Cocher la case "Outils de gestion et d'analyse".
3. Cliquer sur "Détails" et cocher la case "SNMP ".

V.3.4.1.3. Paramétrer le service SNMP client (superviseur) :

Les procédures sont comme suite :

1. Gérer poste de travail, en cliquant du bouton droit sur "Poste de travail":
2. Développer "Service et applications" et repérer "Service SNMP" :

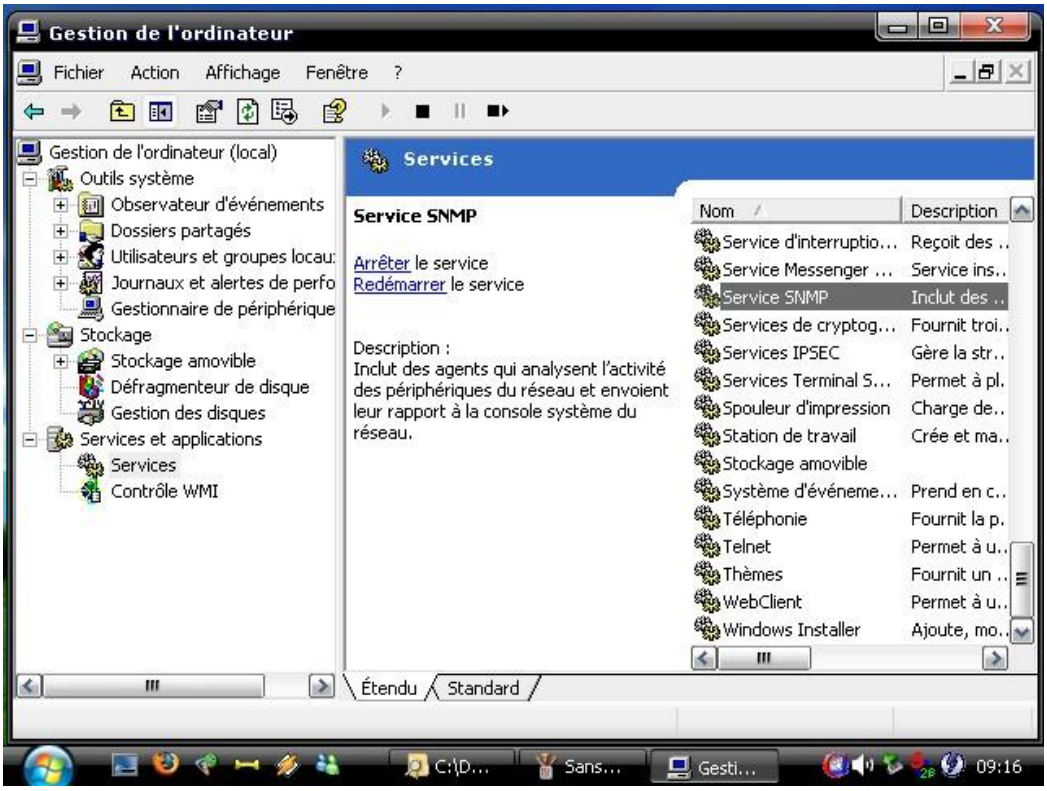

Figure V.15 : Gestion de l'ordinateur

3. Double-cliquer sur service SNMP pour configurer l'agent et la sécurité :

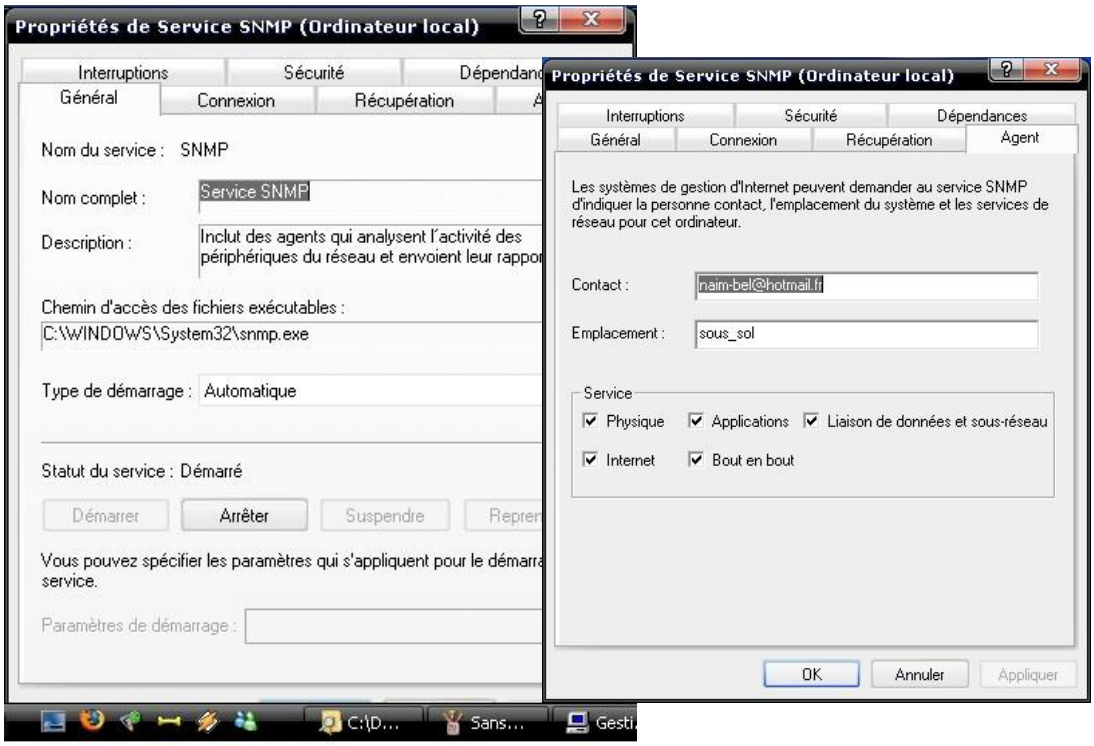

Figure V.16 : configuration de l'agent SNMP

4. Cliquer sur l'onglet sécurité afin de configurer la communauté, et les sources de paquets SNMP autorisés :

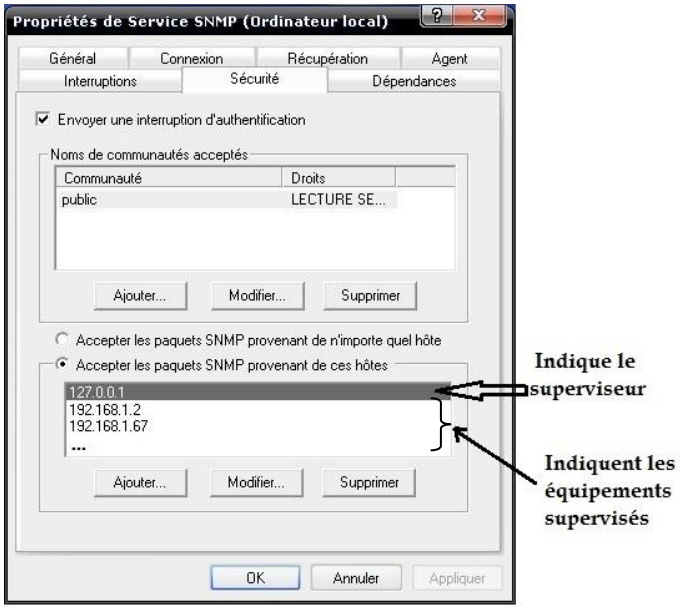

Figure V.17 : configuration de la sécurité du service SNMP

V.3.4.1.4. Déploiement d'un outil d'analyse de vulnérabilités et un outil de scanne pour superviser la sécurité :

Afin de superviser la sécurité du réseau nous avons choisi l'utilisation de :

1. **MBSA (Microsoft Baseline Security Analyzer) :**

C'est un outil conçu par Microsoft pour vérifier le niveau de sécurité des machines Windows à distance ou en local. Et nous avons besoin d'un tel outil.

Ce logiciel va nous offrir de bonne fonctionnalités qui vont nous facilité la supervision de la sécurité de nos postes, il nous permet de donc de:

- Analyser les applications.
- Détérminer les vulnérabilités d'administration Windows : nous permet d'analyser les problèmes de sécurité du système d'exploitation, liés notamment à l'état du compte Invité, au type du système de fichiers, aux partages de fichiers disponibles et aux membres du groupe Administrateurs.
- Rechercher les mots de passes vulnérables.
- Analyser les mises à jour de sécurité : MBSA utilise pour sa base de données des mises à jour, ou un catalogue hors ligne qui est mis à jour par Microsoft dès que des mises à jour de sécurité sont disponibles. Ce catalogue permet de vérifier l'état des mises à jour de sécurité sur les ordinateurs analysés. Si une mise à jour de sécurité figurant dans le catalogue n'est pas installée sur l'ordinateur analysé, MBSA la signale dans le rapport de sécurité. MBSA recherche les mises à jour de sécurité, service packs et correctifs cumulatifs manquants pour tous les produits pris en charge par Microsoft Update.

- Afficher les ressources analysées.
- Afficher les détails des résultats.
- Obtenir des solutions pour corriger les problèmes.

Les détails de rapports sont donnés sous la même forme que cet exemple :

Score	Catégorie	Résultat
	Mises à jour de sécurité	Impossible de charger le fichier CAB de sécurité Comment corriger le problème
	Test des mots de passe des comptes locaux	Certains comptes d'utilisateurs (3 sur 4) ont un mot de passe vide ou simple, ou n'ont pas pu être analysés. Afficher les ressources analysées Détails du résultat Comment corriger le problème
	Mises à jour automatiques	La fonctionnalité de mise à jour automatique est désactivée sur cet ordinateur. Afficher les ressources analysées Comment corriger le problème
	Expiration des mots de passe	Certains comptes d'utilisateurs (3 sur 4) ont un mot de passe n'expirant pas. Afficher les ressources analysées Détails du résultat Comment corriger le problème
	Mises à jour incomplètes	Aucune installation de mise à jour logicielle incomplète n'a été détectée. Afficher les ressources analysées
	Pare-feu Windows	Le Pare-feu Windows n'est pas installé ou configuré, ou n'est pas disponible dans cette version de Windows.
	Système de fichiers	Tous les disques durs (4) utilisent le système de fichiers NTFS. Afficher les ressources analysées Détails
	Autologon	L'ouverture de session automatique n'est pas configurée sur cet ordinateur. Afficher les ressources analysées
	Compte Invité	Le compte Invité est désactivé sur cet ordinateur. Afficher les ressources analysées
	Accès anonymes	Les accès anonymes sont restreints de façon adéquate sur cet ordinateur. Afficher les ressources analysées
	Administrateurs	Pas plus de 2 administrateurs ont été trouvés sur cet ordinateur. Afficher les ressources analysées Détails
	Statut de SQL Server/MSDE	SQL Server et/ou MSDE n'est pas installé sur cet ordinateur

Remarque : les rapports sont donnés avec des scores, ceux-là doivent de préférence être classés par ordre du «plus pire en premier ». Voici les scores :

→ Analyse impossible.

→ Le test a échoué (critique).

→ Le test a échoué (non critique).

→ Recommandations ou informations supplémentaires.

→ Le test à réussi.

→ Le test n'a pas été effectué.

Voici l'interface graphique de MBSA :

Figure V.18 : L'interface graphique de MBSA

Nous pouvons analyser un ordinateur, ou plusieurs à la fois, mais aussi analyser l'ordinateur où MBSA est installé (superviseur) en spécifiant les paramètres suivants:

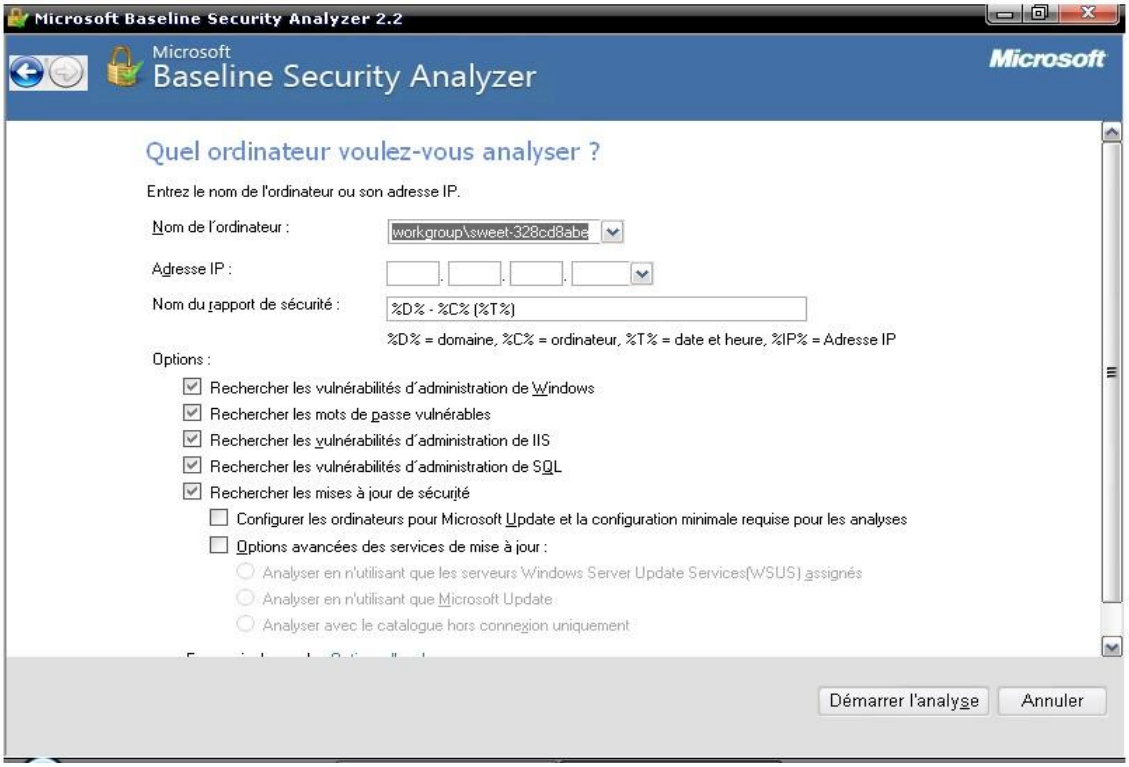

Figure V.19 : Analyse individuelle d'un ordinateur sous MBSA

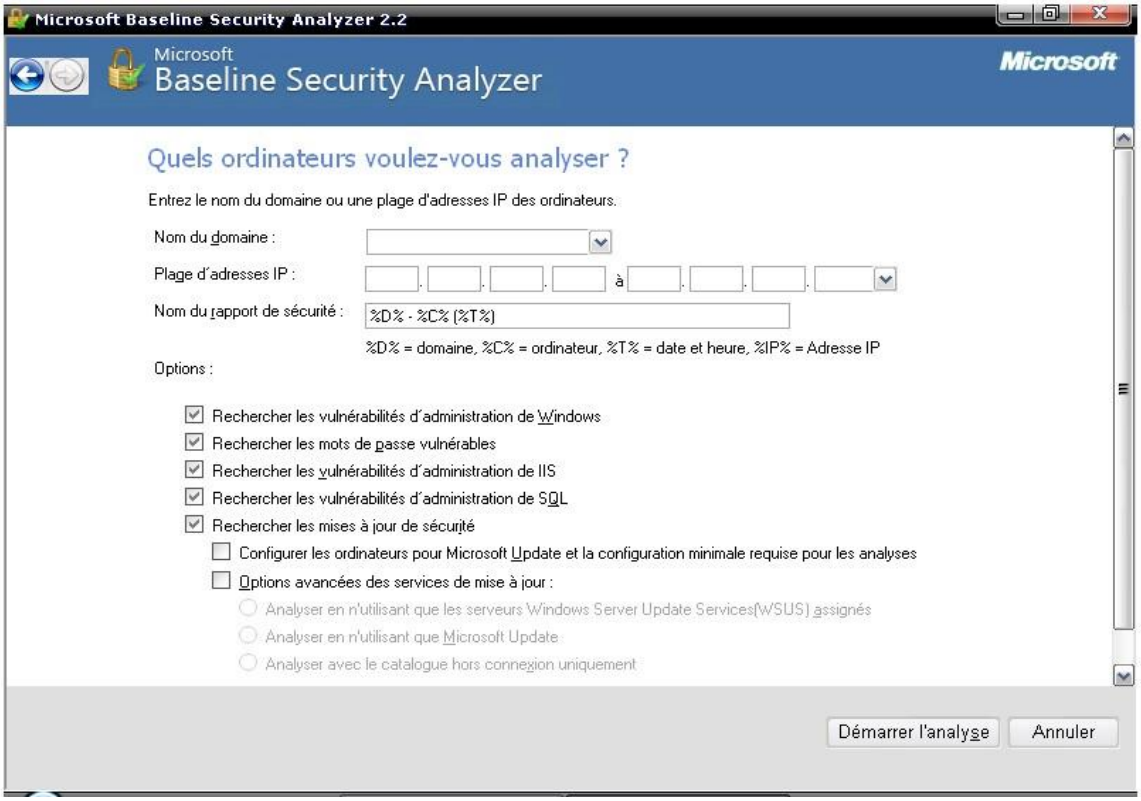

Figure V.20 : Analyse d'un groupe d'ordinateurs sous MBSA

2. Nmap :

Nmap est un scanneur de ports. Nous l'utiliserons pour :

- Détecter les ports ouverts.
- Détecter les services hébergés et ainsi de désactiver ceux qui sont inutilisés, afin d'éviter qu'un malfaiteur puisse exploiter sont port ouvert pour dressé des attaques.
- Récolter des informations sur le système d'exploitation d'un ordinateur distant.

Cela nous permettra donc, d'avoir une idée sur ce que notre système donnera d'informations s'il subit un scanne d'un pirate, et donc connaitre le niveau de sécurité et par cela le niveau d'exposition aux menaces, et en contre partie, prendre les mesures nécessaires.

Ce logiciel est devenu une référence pour les administrateurs réseaux, car l'audit des résultats de Nmap fournit beaucoup d'indications sur la sécurité du réseau de l'entreprise.

Figure V.21 : L'interface graphique de Nmap

Une fois mis en place, nous spécifions les adresses IP des postes à analyser un à un, en spécifiant à chaque fois le profil du scan à effectuer, puis nous lançons le scan :

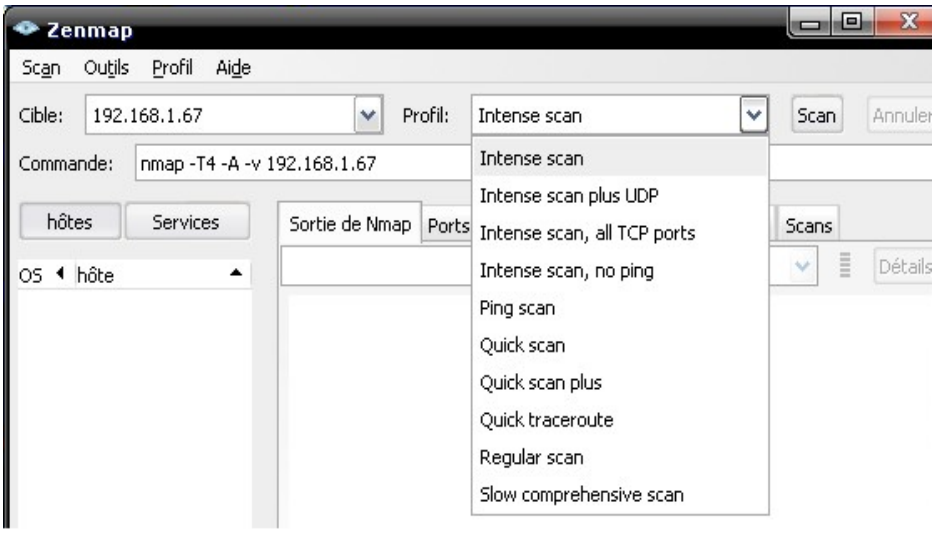

Figure V.22 : Lancer un scanne avec Nmap

V.3.4.2. Configuration des équipements à superviser

Dans cette partie, nous allons configurer le service SNMP serveur (des équipements à supervisés) :

V.3.4.2.1. Paramétrer les Postes de travail

1. **Installation des démons SNMP :**

L'installation se fait sous le système Windows XP. Nous suivrons les mêmes procédures que pour le superviseur :

Aller dans le panneau de configuration - Ajout/suppression de programmes - ajouter/supprimer des composants Windows - Cocher la case "Outils de gestion et d'analyse" - cliquer sur "Détails" - Cocher la case "SNMP (Protocole simplifié de gestion de réseaux)".

2. **Paramétrer le service SNMP serveur :**

Notre configuration va nous servir pour que seule la machine locale « superviseur » puisse lire la totalité de la MIB et aussi écrire, à travers la communauté « public ».

Etapes :

1. Gérer poste de travail, en cliquant du bouton droit sur "Poste de travail":
2. Développer "Service et applications" et repérer "Service SNMP" :
3. Double-cliquer dessus pour configurer l'agent et la sécurité :

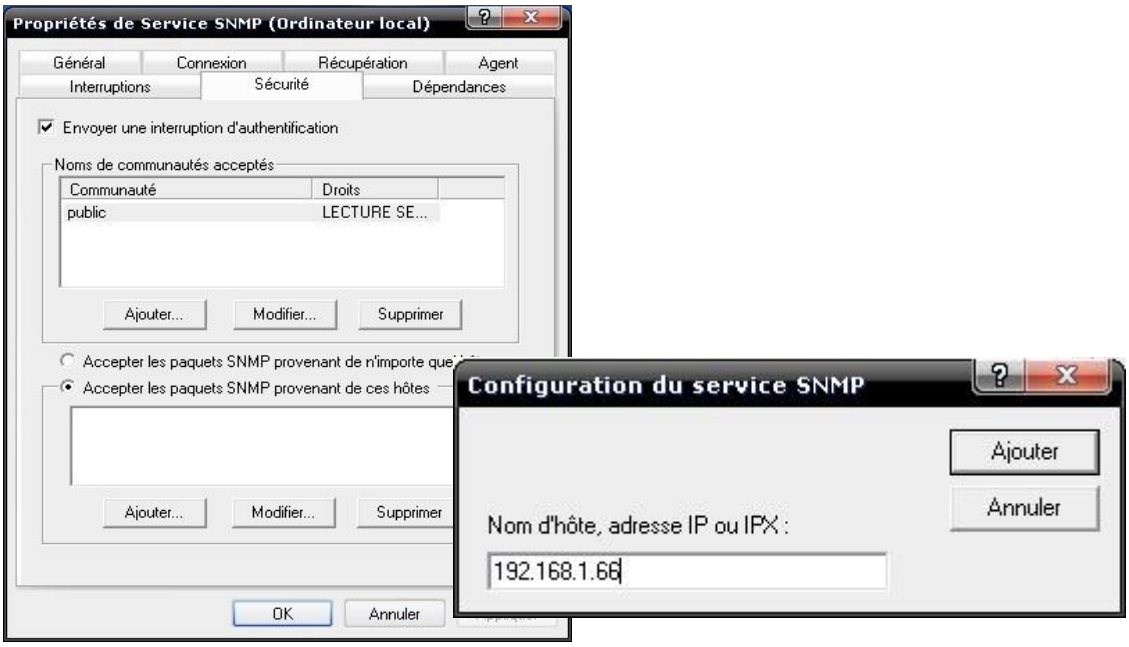

Figure V.23 : Configuration du service SNMP serveur

Remarque : Nous ne créerons donc qu'une communauté « public », qui aura les droits depuis une seule machine (192.168.1.66) qui est le superviseur.

V.3.4.2.2. Configurer le protocole SNMP dans les Switchs et les routeurs et le firewall

Nous donnons si dessous, un exemple de configuration pour le Switch du département informatique. Il suffit de suivre les mêmes étapes pour les autres équipements. Les étapes :

1. **Activer l'accès SNMP :** configurer l'équipement afin qu'il accepte les « get » et « set » SNMP avec la communauté « public » en lecture écriture :

```
Switch(config) # snmp-sever community public rw          // droit d'accès en lecture écriture
```

2. **Configurer l'équipement pour envoyer les paquets SNMP au manager :**

```
Switch(config) # snmp-sever host 192.168.1.66 public
```

3. **Activer l'envoi des traps SNMP de l'équipement vers le manager :**

```
Switch(config) # enable snmp traps {type}
```

→ Cette commande permet aux « traps » d'être envoyées automatiquement au manager, il suffit juste d'indiquer le type de « traps » à activer. Exemple : CPU, VTP…

4. **Définir l'interface qui sera la source des traps :**

```
Switch(config) # snmp-server trap-source fastEthernet 0/2
```

Remarque : pour une meilleure sécurité, nous pouvons créer une liste d'accès qui donne tout les droits au superviseur :

```
Switch(config) #access-list 1 permit 192.168.1.66  0.0.0.0      //le superviseur uniquement

Switch(config) #snmp-server community public RW 1
```

V.3.5. Mise en œuvre de plateformes virtuelles pour les tests

Dans les parties précédentes, Nous avons décris les démarches à suivre pour implémenter notre solution de sécurité et supervision. Dans ce qui suit, nous aborderons les différentes méthodes de tests, en utilisant des logiciels spécifiques pour chaque fonction.

V.3.5.1. Les logiciels utilisés pour simuler la mise en œuvre des solutions

Afin de réaliser nos tests pour chacune des fonctions ci-dessous, nous utilisons pour :

- Test des différentes configurations (Switchs, routeurs, PC) → le logiciel **Packet tracer**.
- Test de configuration du pare-feu → **GNS3**.
- Test de supervision → **GNS3** associé à **VMware**, avec le logiciel de monitoring **PRTG.**
- Analyse des vulnérabilités (repérage des failles) → le logiciel **MBSA** (**M**icrosoft **B**aseline **S**ecurity **A**nalyzer).
- Scanne des ports (services) → le logiciel **Nmap.**
- Capture de trames → **Wireshark** (il s'agit d'un analyseur de protocoles très complet qui permet, entre autres, d'analyser très finement les trames protocolaires SNMP).

V.3.5.2. Les tests de configuration

- **La maquette de test :**

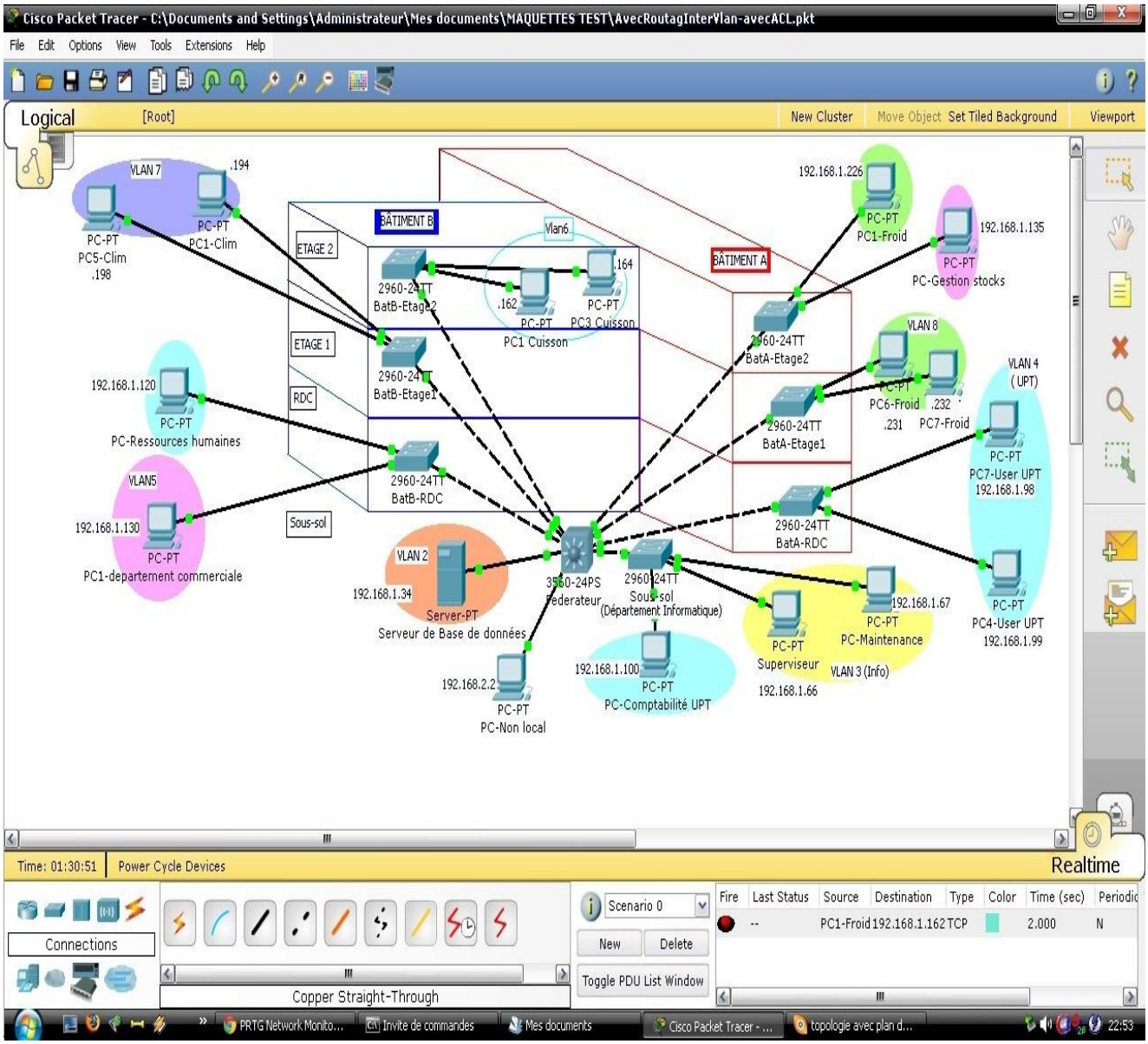

Figure V.24 : La maquette de test du RLE sous Packet tracer

- **Simulation :**

Remarque : nous ne feront que certains tests et visualisations afin de démontrer le fonctionnement du plan.

1. **Les VLAN :**

.Vérification de la création des VLAN :

```
Federateur#show vlan
```

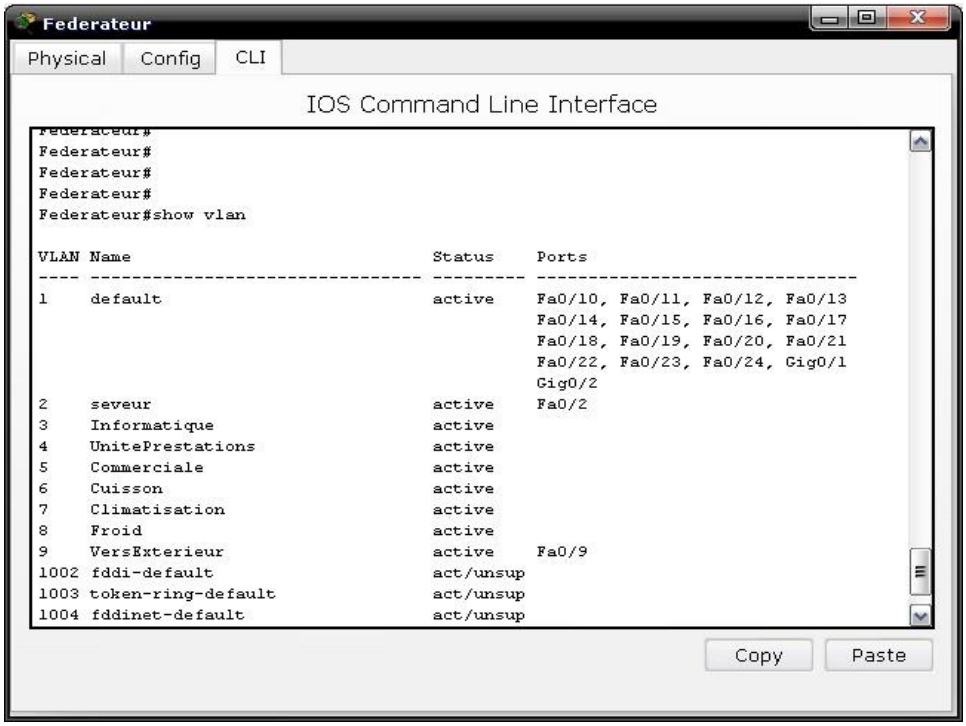

Figure V.25 : La visualisation des VLAN créés

2. **Vérifier la configuration de VTP:**

```
Federateur#show vtp status
```

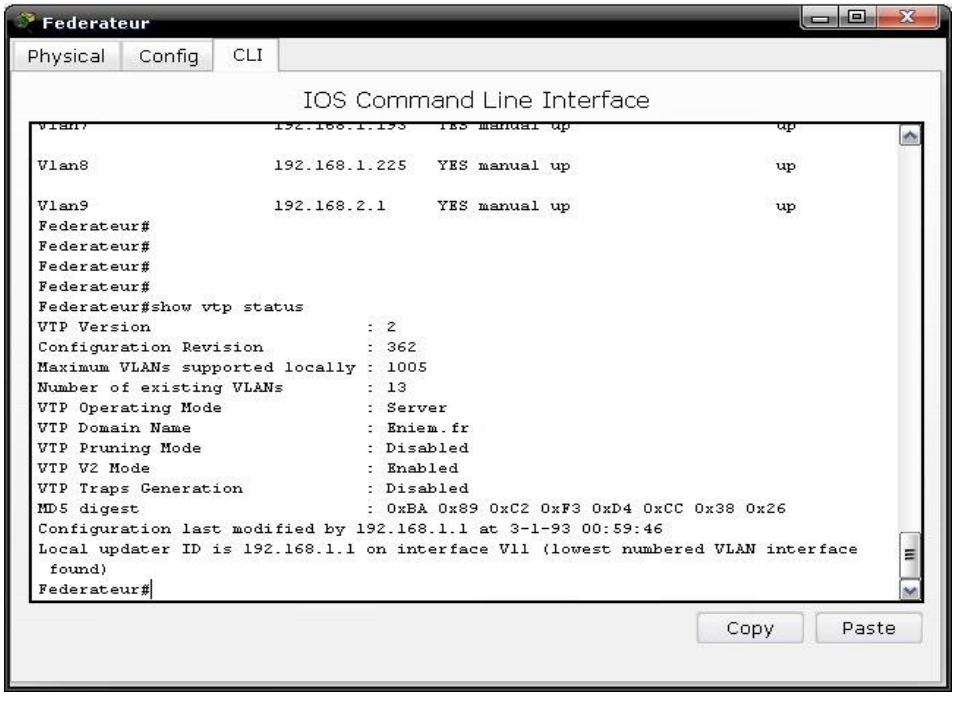

Figure V.26 : La visualisation de la configuration de vtp serveur

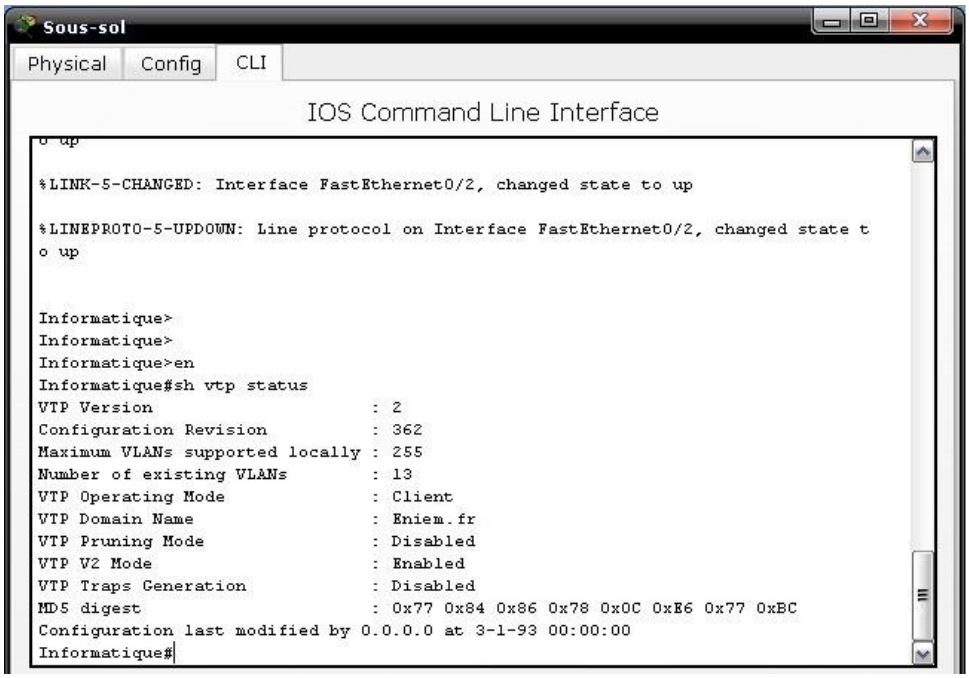

Figure V.27 : La visualisation de la configuration de vtp client sur le Switch Informatique

3. Vérifier la configuration et l'état des interfaces fastEthernet et logiques :

```
Federateur#show ip interface brief
```

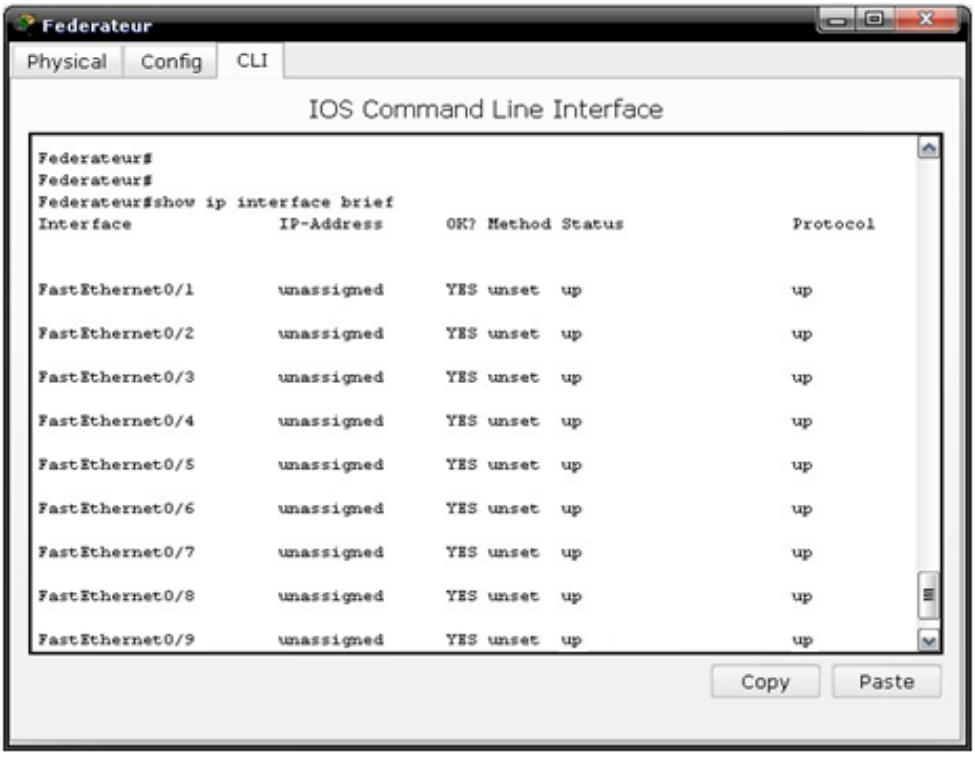

Figure V.28 : La visualisation de la configuration et l'état des interfaces FastEthernet du Fédérateur

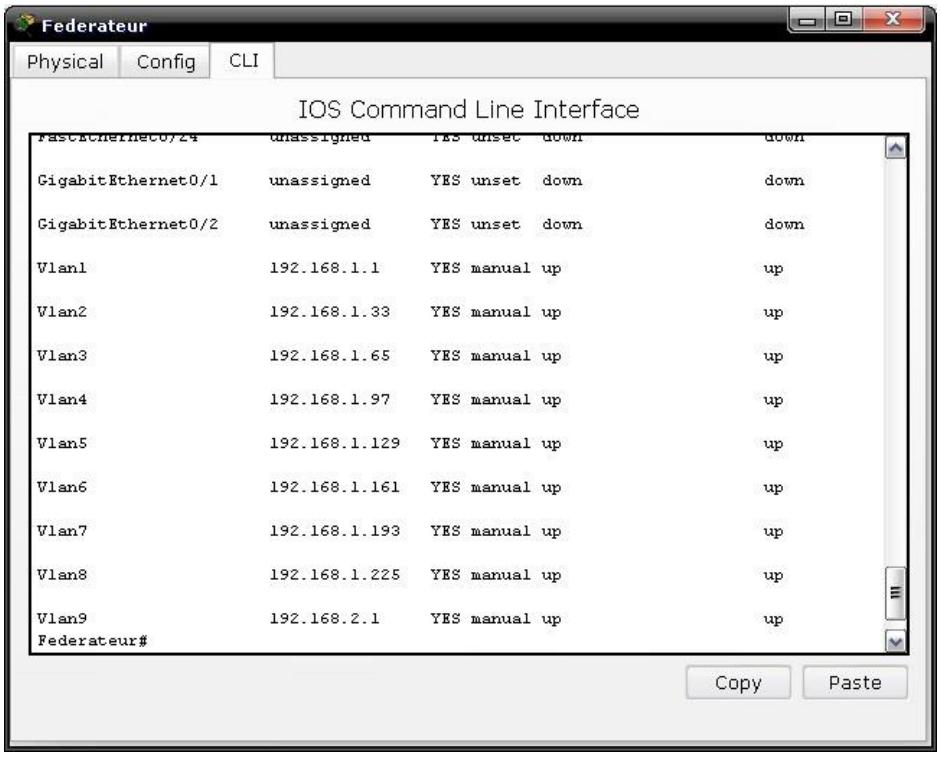

Figure V.29 : La visualisation de la configuration et l'état des interfaces logiques du Fédérateur

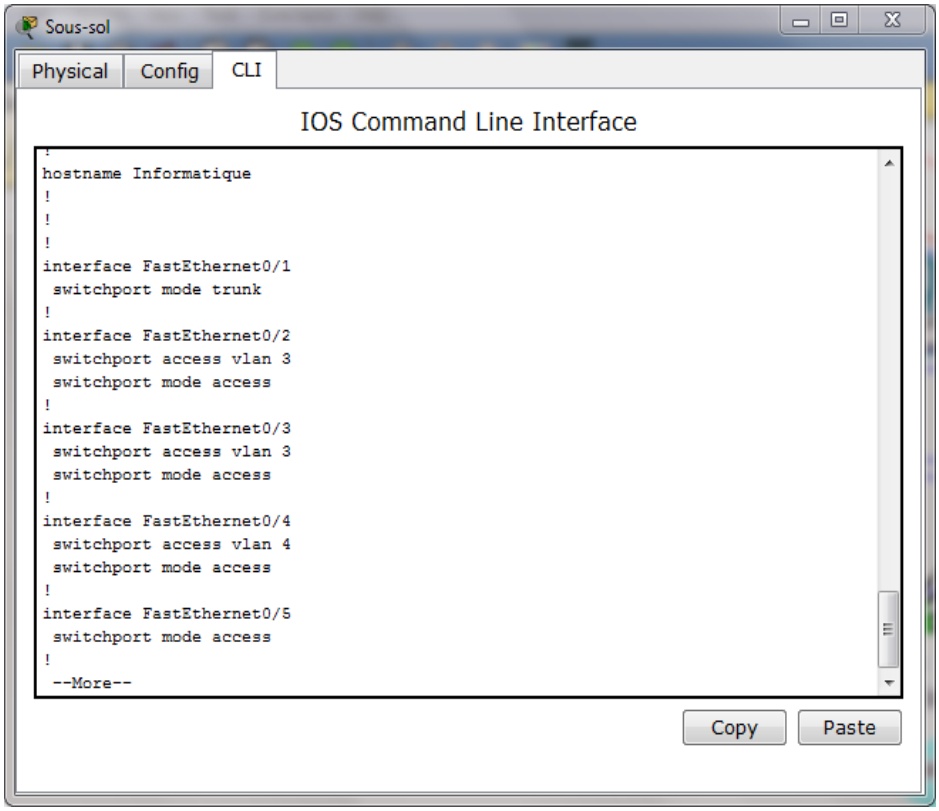

Figure V.30 : La visualisation de l'état des interfaces du Switch du département informatique

4. Vérifier la configuration des ACL :

```
Federateur#show running-config
```

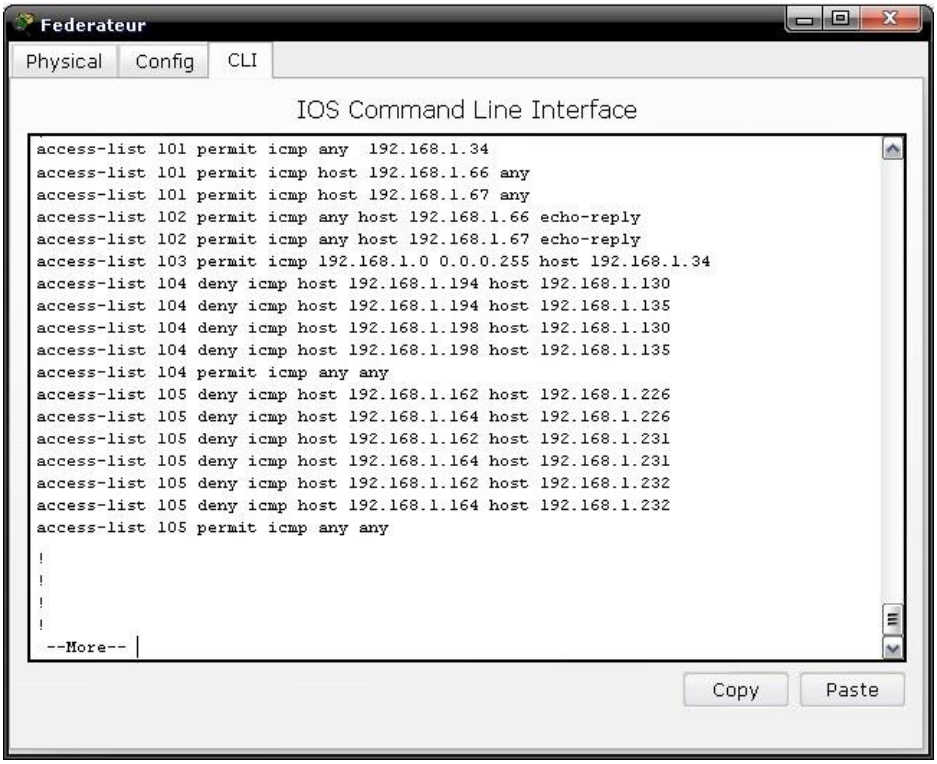

Figure V.31 : La visualisation des ACL configurées

5. Test des ACL :

.ACL1 et ACL2 : Les PC maintenance et superviseur ont l'accès vers tous les autres postes des autres VLAN, mais aucun n'a accès à ces deus postes, voici des exemples de ping:

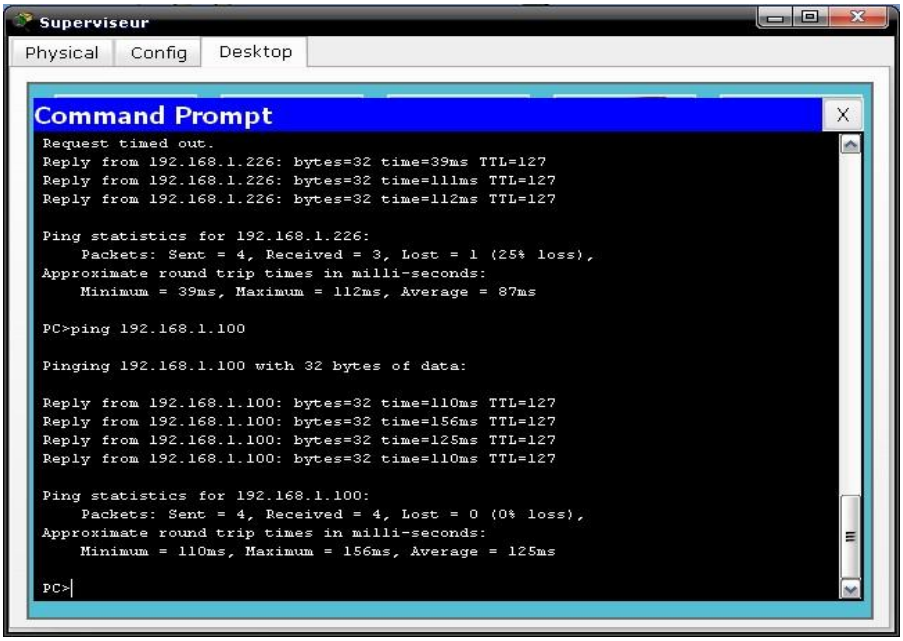

Figure V.32 : Résultat du ping du PC superviseur vers VLAN 8 et VLAN 4

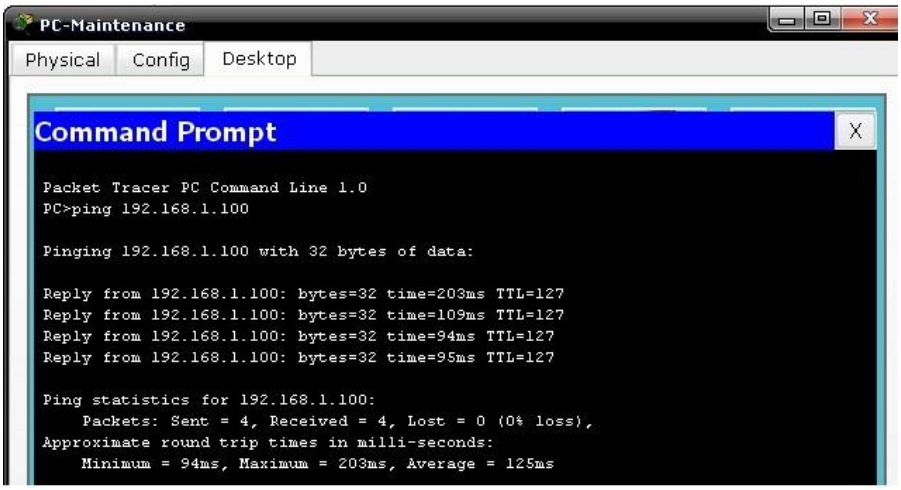

Figure V.33 : Résultat du ping du PC maintenance vers VLAN 4

→ Prise en compte de l'ACL 1. Ces deux PC ping avec succès tout les autres postes.

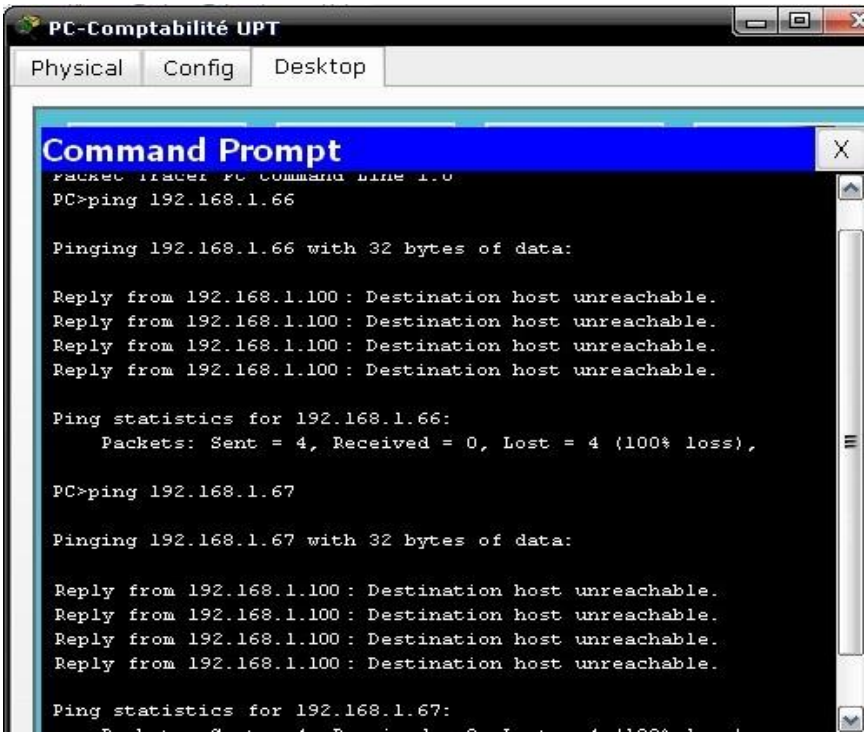

Figure V. 34: Résultat du ping du VLAN4 vers PC superviseur et PC maintenance

→ Prise en compte de l'ACL 2. Aucun PC n'arrive à pinguer le superviseur et le PC maintenance.

. ACL 3 : tout les PC du réseau locale (192.168.1.0 /27) peuvent accéder au serveur. L'accès de l'exterieur est interdit.

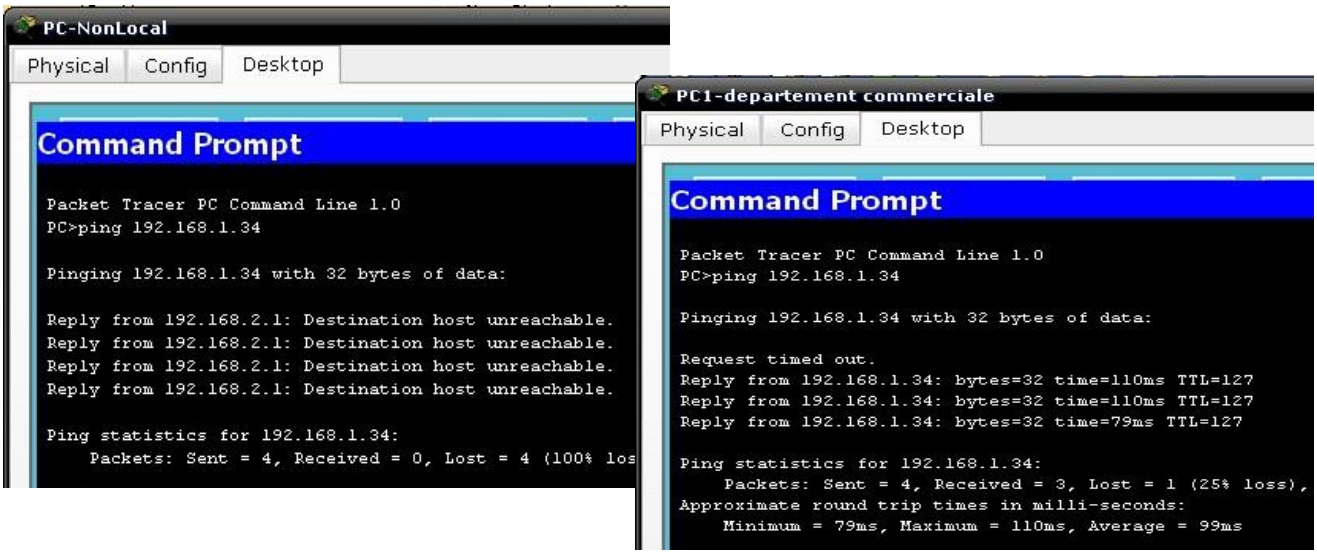

Figure V.35 : Résultat de ping local et non local vers le serveur de base de données

→ Prise en compte de l'ACL 3. C'est seulement les PC du RLE qui ont accès au serveur.

. ACL 4 : les VLAN 7 et VLAN 5 ne communiquent pas entre eux.

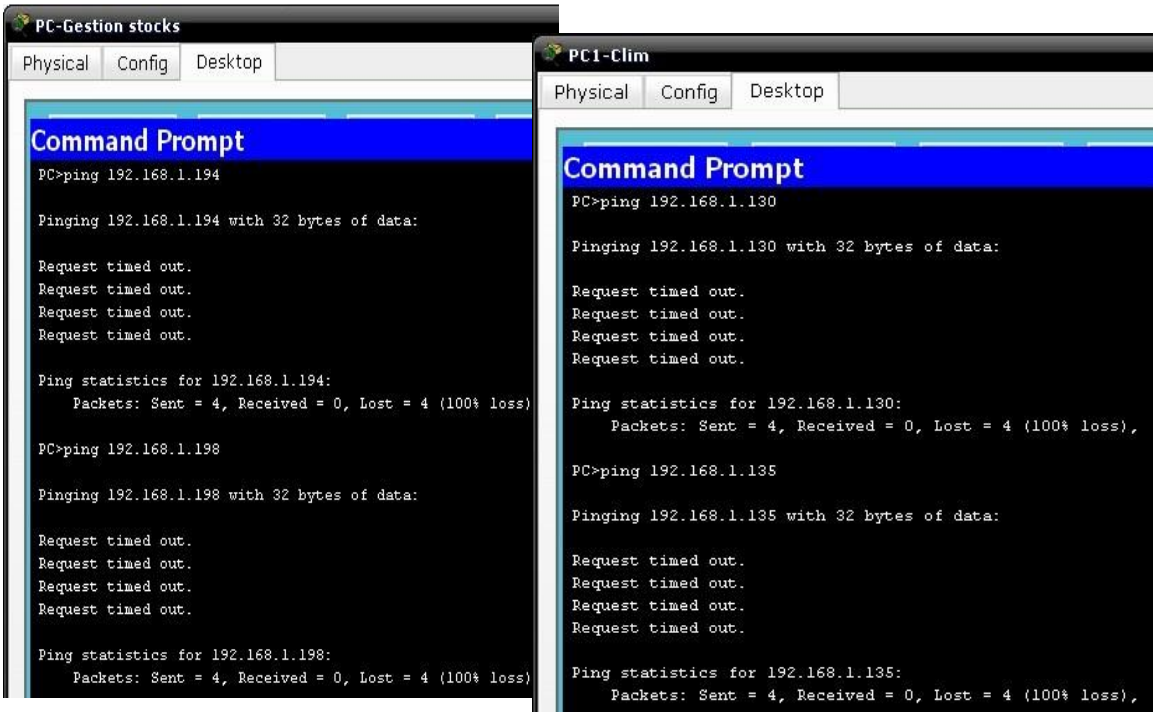

Figure V.36 : résultat des ping entre VLAN 7 et VLAN 5

→ Prise en compte de l'ACL 4.

Remarque :l'ACL 5 est aussi prise en compte, car VLAN 6 et VLAN 8 ne communiquent pas.

6. La route d'accès à internet :

```
Federateur#show ip route
```

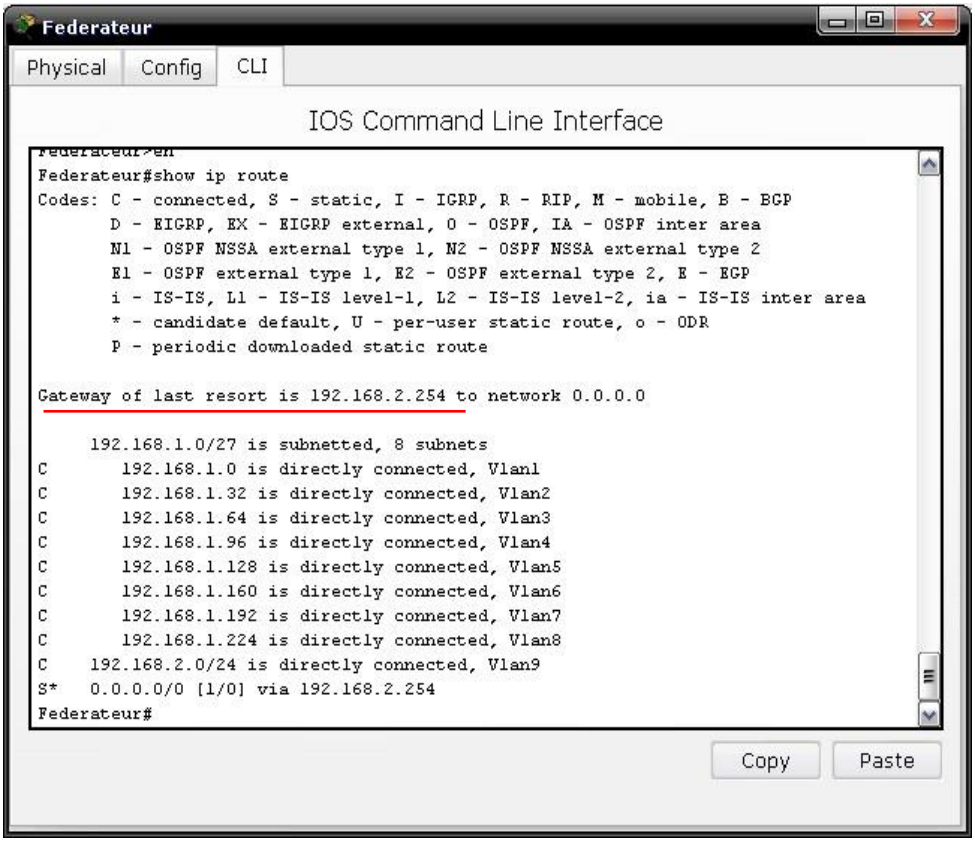

Figure V.37 : visualisation de la route de sortie pour le RLE

7. Vérifier la configuration du routeur :

.Affichage des lignes disponibles :

```
RouteurENIEM(config)#do show line
```

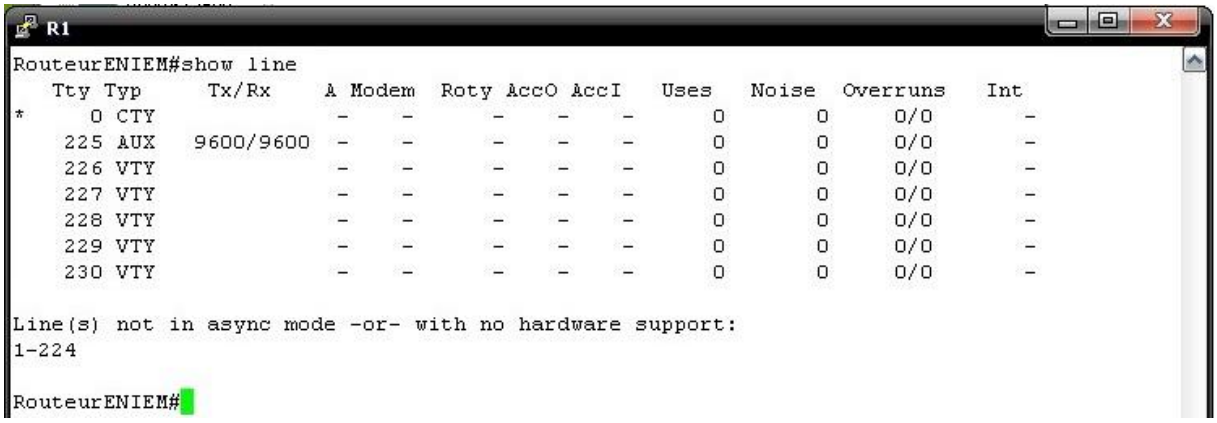

Figure V.38 : visualisation des lignes de configuration disponibles

. Vérifier la configuration des interfaces du routeur :

```
RouteurENIEM#show running-config
```

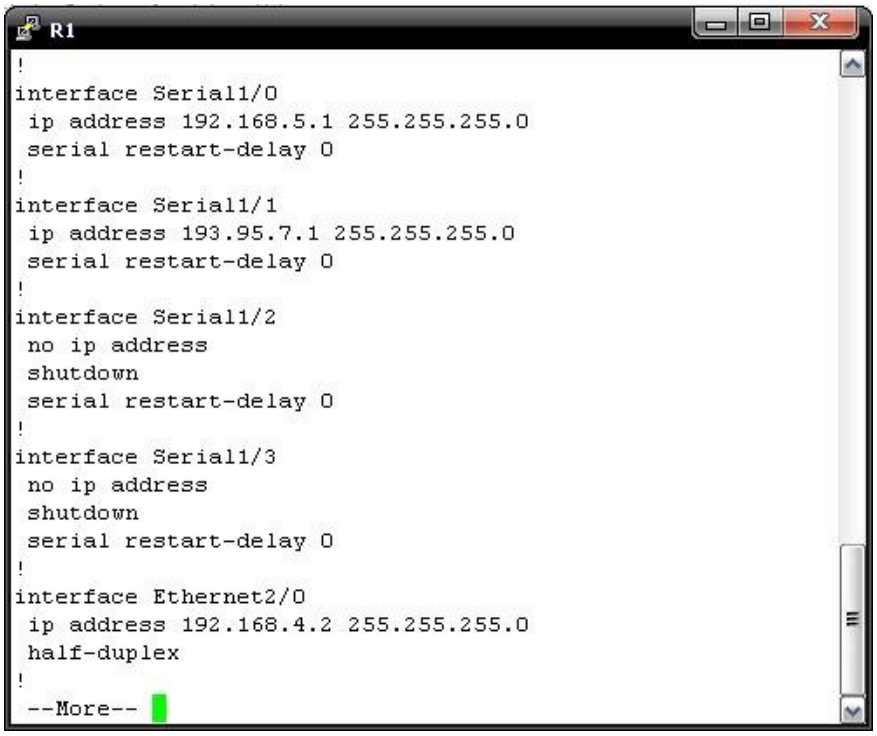

Figure V.39 : vérification de la configuration des interfaces

. Vérifier la configuration d'ospf et de Frame-Relay :

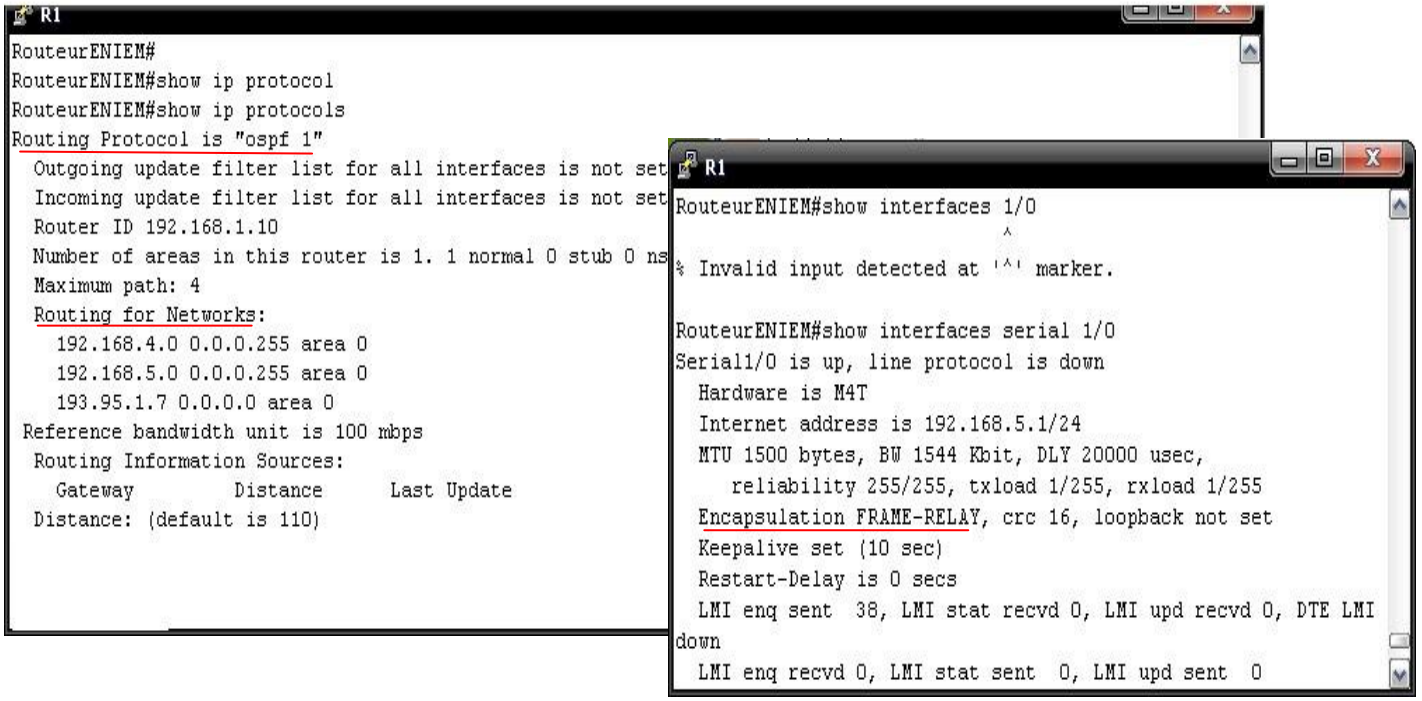

Figure V.40 : vérification de la configuration d'ospf et Frame-Relay

8. Vérifier la configuration du firewall :

.Configuration des trois interfaces du pare-feu :

```
Pixfirewall#show running-config
```

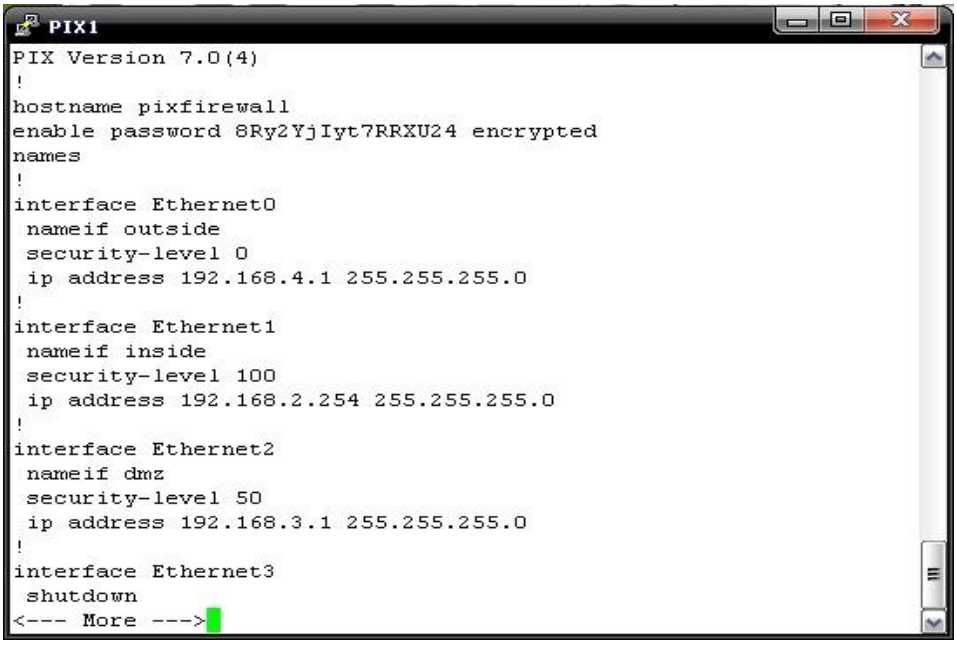

Figure V.41 : Vérification de la configuration des interfaces de PIX

. Translation d'adresses :

```
Pixfirewall#show nat
```

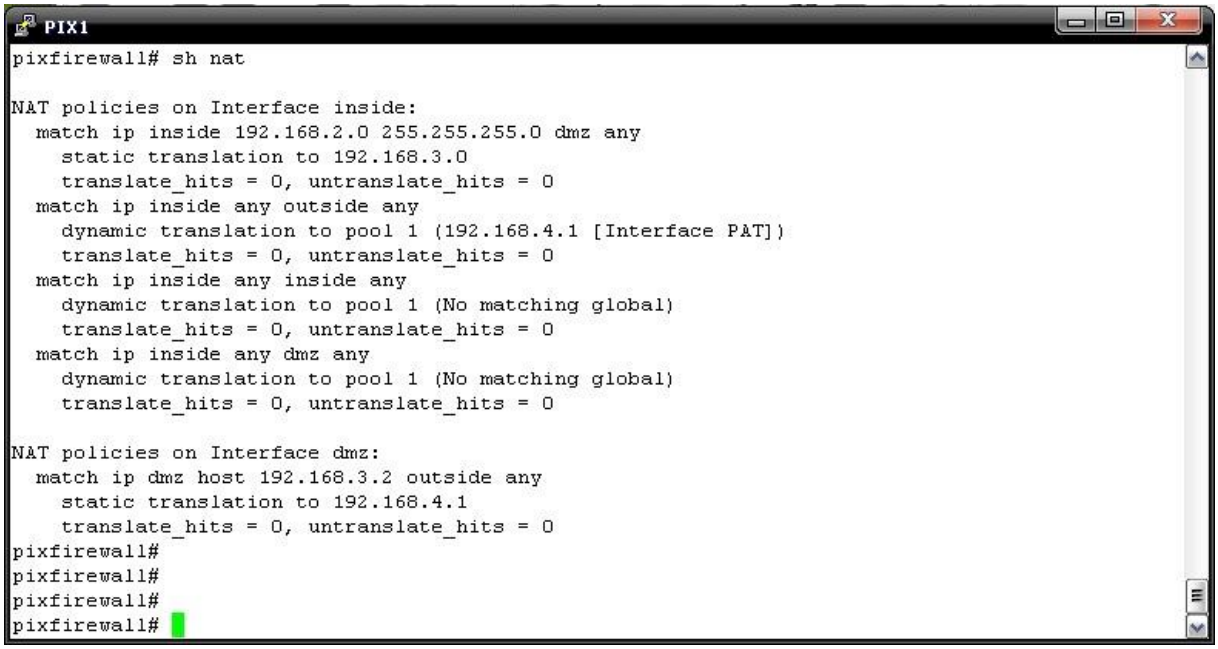

Figure V.42 : Visualisation de la configuration de translation d'adresses

.Le routage :

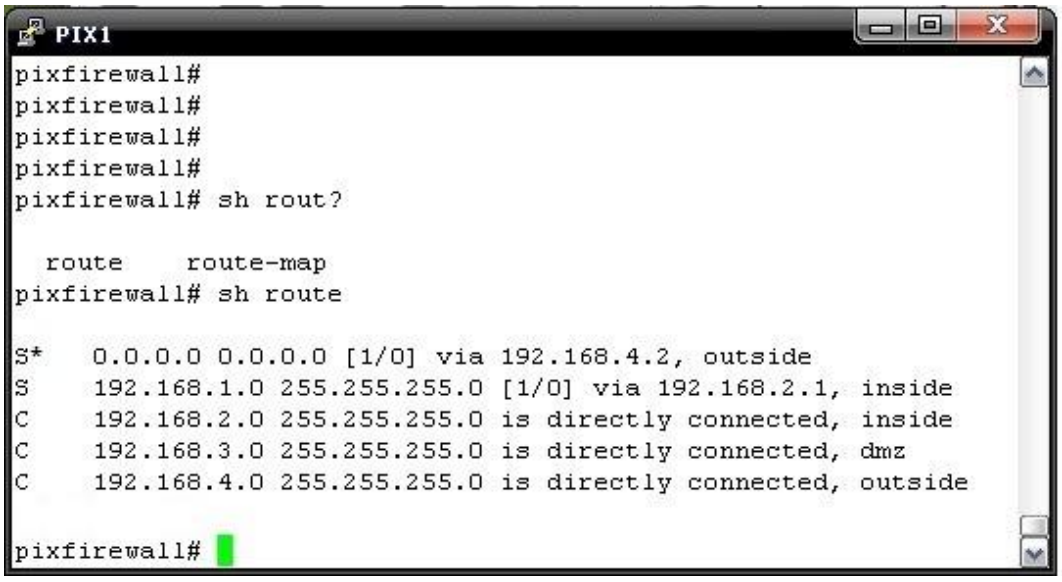

Figure V.43 : Visualisation des routes configurées

Remarque : "S" veut dire "Static", et "C" veut dire "Connected". Et " *" candidate default.

. Les ACL :

```
Pixfirewall#show running-config
```

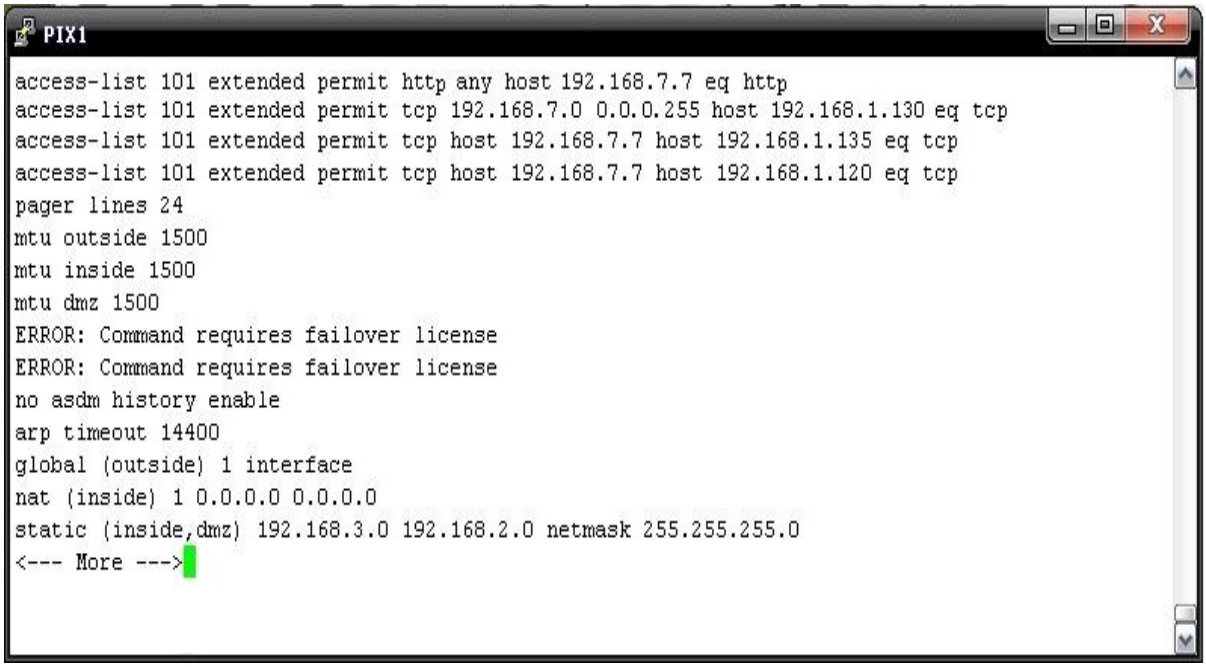

Figure V.44 : Visualisation des listes d'accès configurées

9. Simulation de la solution de supervision

❖ **Mise au point des outils :**

1. Installer VMware afin de créer nos machines virtuelles dotées de Windows XP.
2. Activer et configurer le service SNMP pour une seule communauté que nous appelons « public ». et nous spécifions la réception des paquets en indiquant les adresses comme suite :

   .Pour le superviseur : recevoir des parquets SNMP de tout les équipements à supervisés.

   .Pour les équipements (PC, Switchs, Routeurs, Firewall) : recevoir des paquets SNMP du superviseur (192.168.1.66).
3. Installer PRTG afin de pouvoir automatiser la gestion du réseau sous une interface graphique simple.
4. Installer MBSA et Nmap, afin de mieux superviser la sécurité de notre réseau.
5. Configurer les VMnet (cartes réseau des PC virtuels)
6. Pour pouvoir émuler les PC virtuels crées dans VMware, nous leurs spécifions les cartes réseau correspondantes VMnet (celles de VMware) .

❖ **La maquette virtuelle utilisée pour la supervision :** là aussi, nous ne ferons que quelques exemples afin de démontrer le fonctionnement et la possibilité d'implémentation :

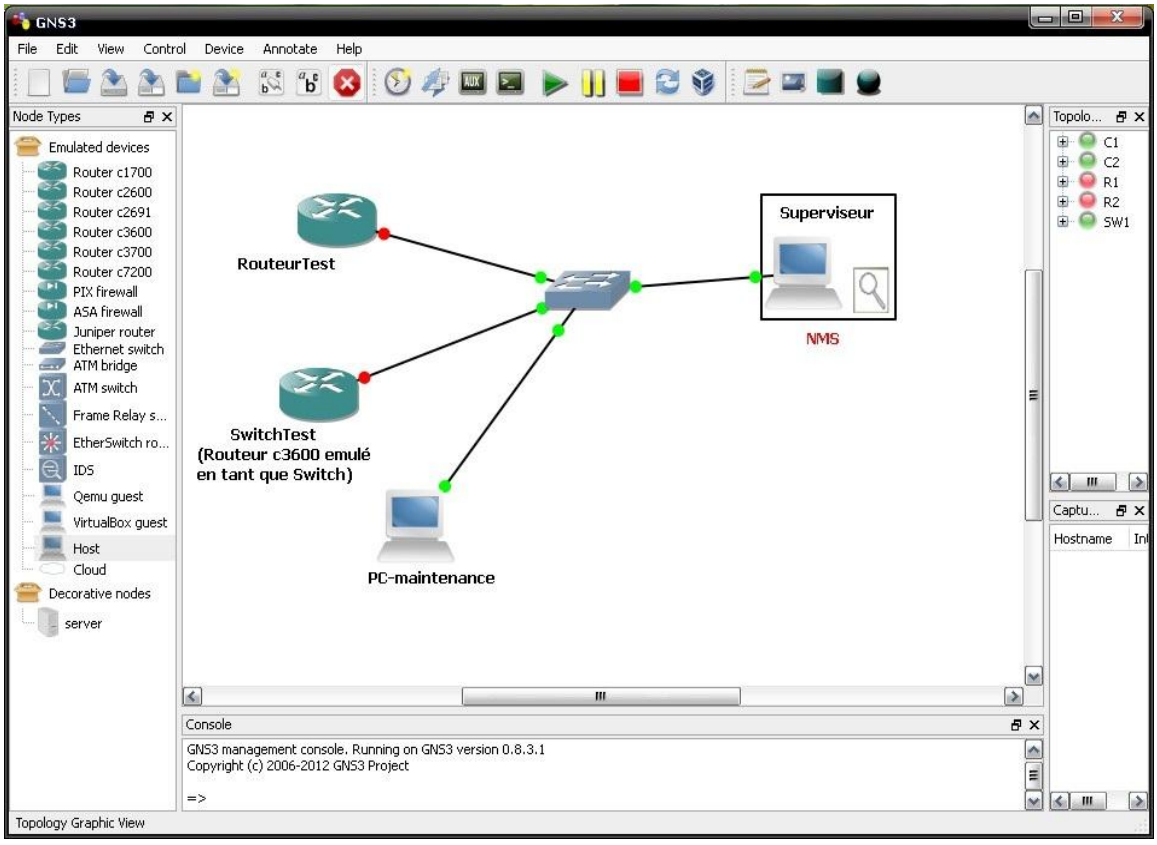

Figure V.45 : maquette pour tester la supervision sous GNS3

Remarque : vu que nous ne pouvons pas émuler un Switch, nous avons émulé un routeur en tant que Switch. Pour ce faire, nous avons inséré un module pour Switch (NM-16ESW : Network Module-16 interfaces) dans le slots 1 du routeur C3600.

❖ **Vérification de la configuration des agents SNMP :**

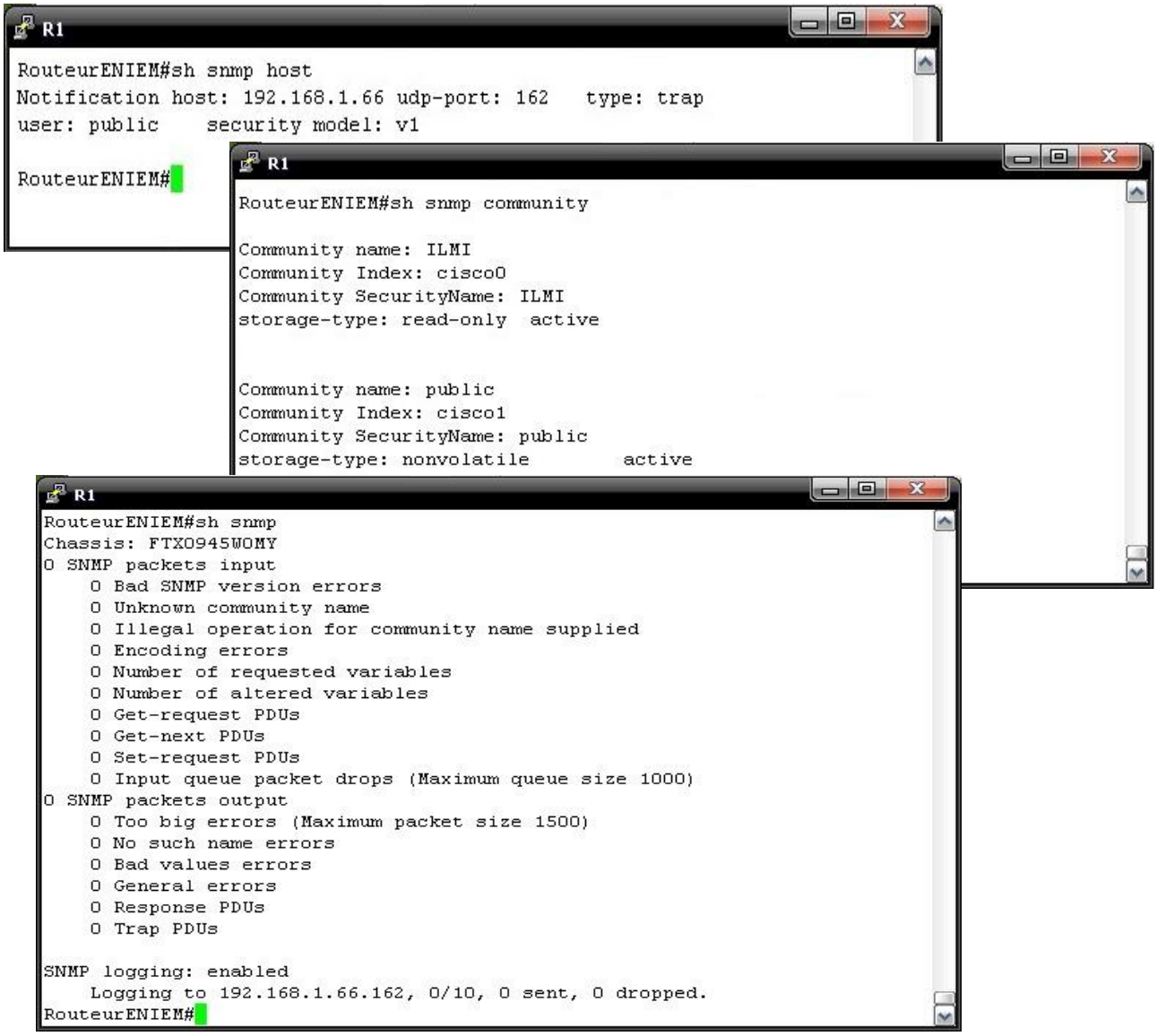

Figure V.46 : Vérification de la bonne configuration des agents SNMP d'équipements

Une fois les configurations vérifiées, nous passons à la supervision via SNMP, avec PRTG, MBSA, Nmap, et Wireshark :

❖ **Superviser avec PRTG :**

.Mise en route :

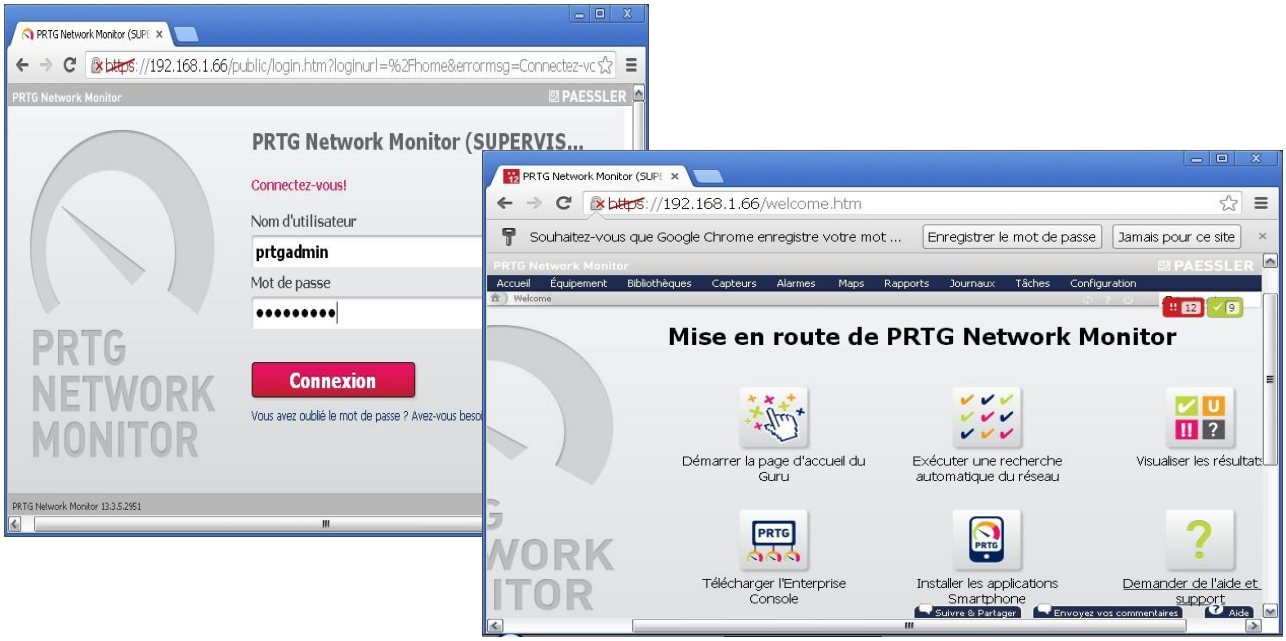

Figure V.47 : Mise en route de PRTG

. Ajouter un groupe : clique droit sur Local probe :

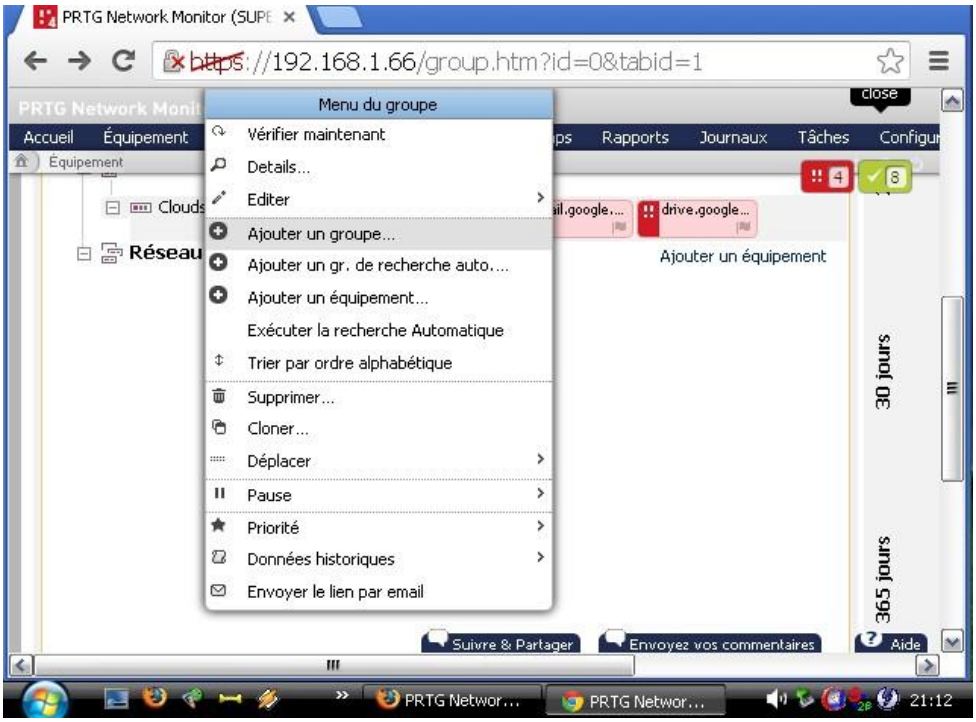

Figure V.48 : Ajouter un groupe d'équipements sous PRTG

Remarque : nous avons besoin de créer un group « Réseau Test », et 3 sous-groupes, un pour les PC, un pour les Switchs, et un autre pour les routeurs. Nous remarquerons que le groupe de la probe et les capteurs associés à l'équipement sont déjà créés (automatiquement).

.Spécifier les données :

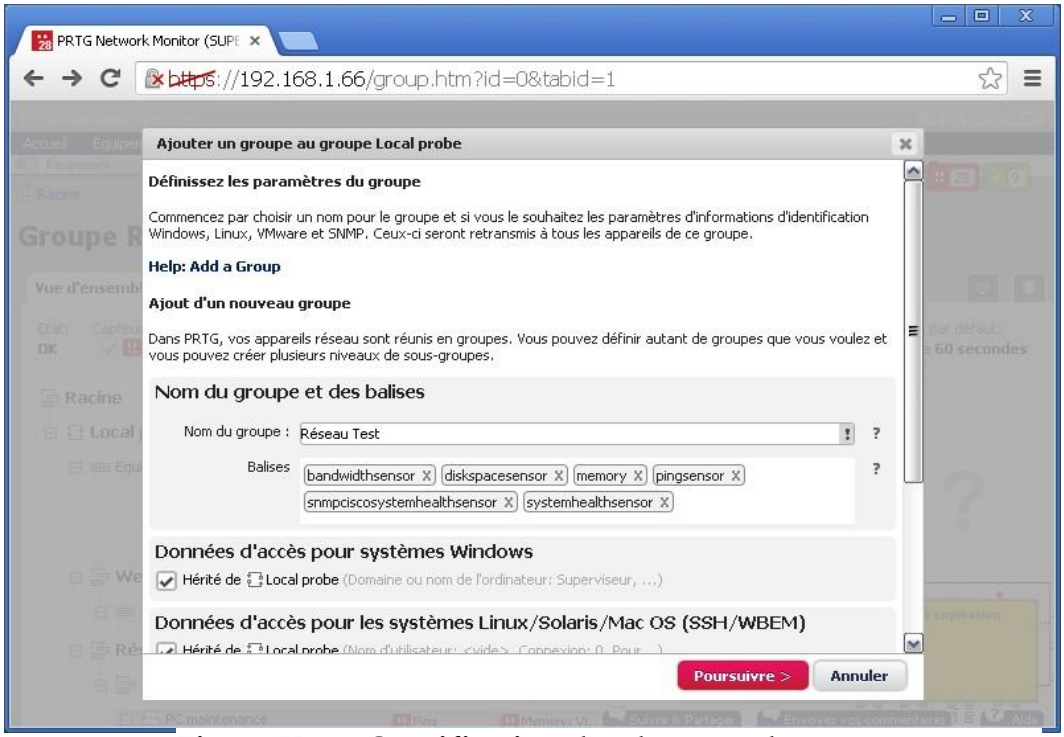

Figure V.49 : Spécification des données du groupe créé

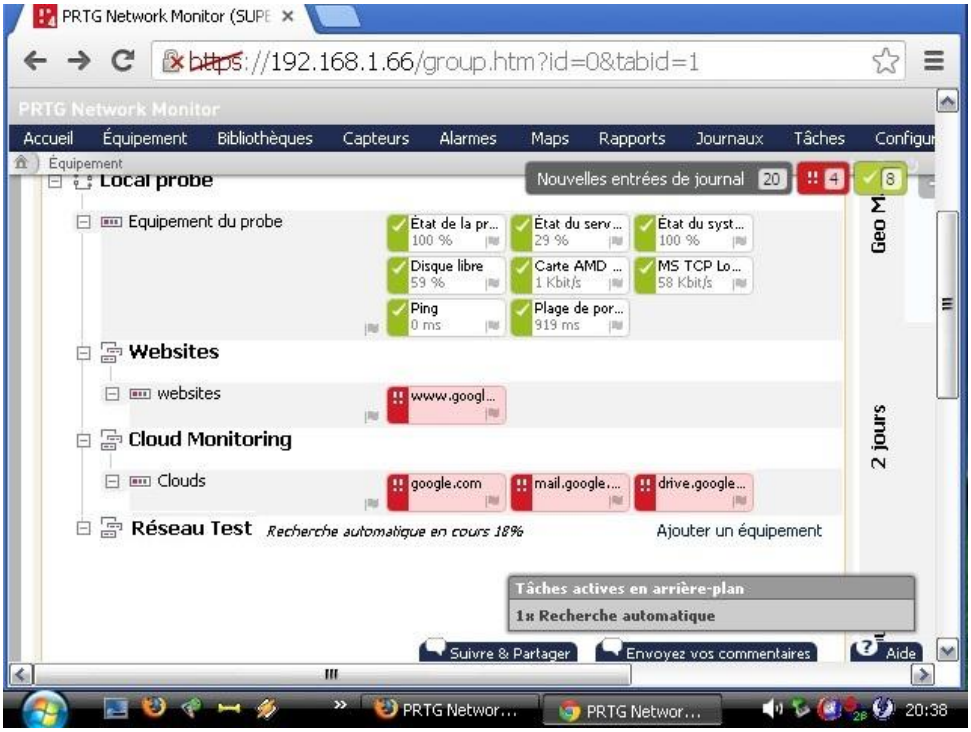

Figure V.50 : Le groupe Réseau Test créé

.Ajouter des capteurs : après avoir ajouter des équipements de la même manière que l'ajout d'un groupe, il nous faut ajouter des capteurs en fonction de ce que nous voulons superviser :

Cliquer sur bouton droite de la sourie sur l'équipement, puis sur ajouter un capteur :

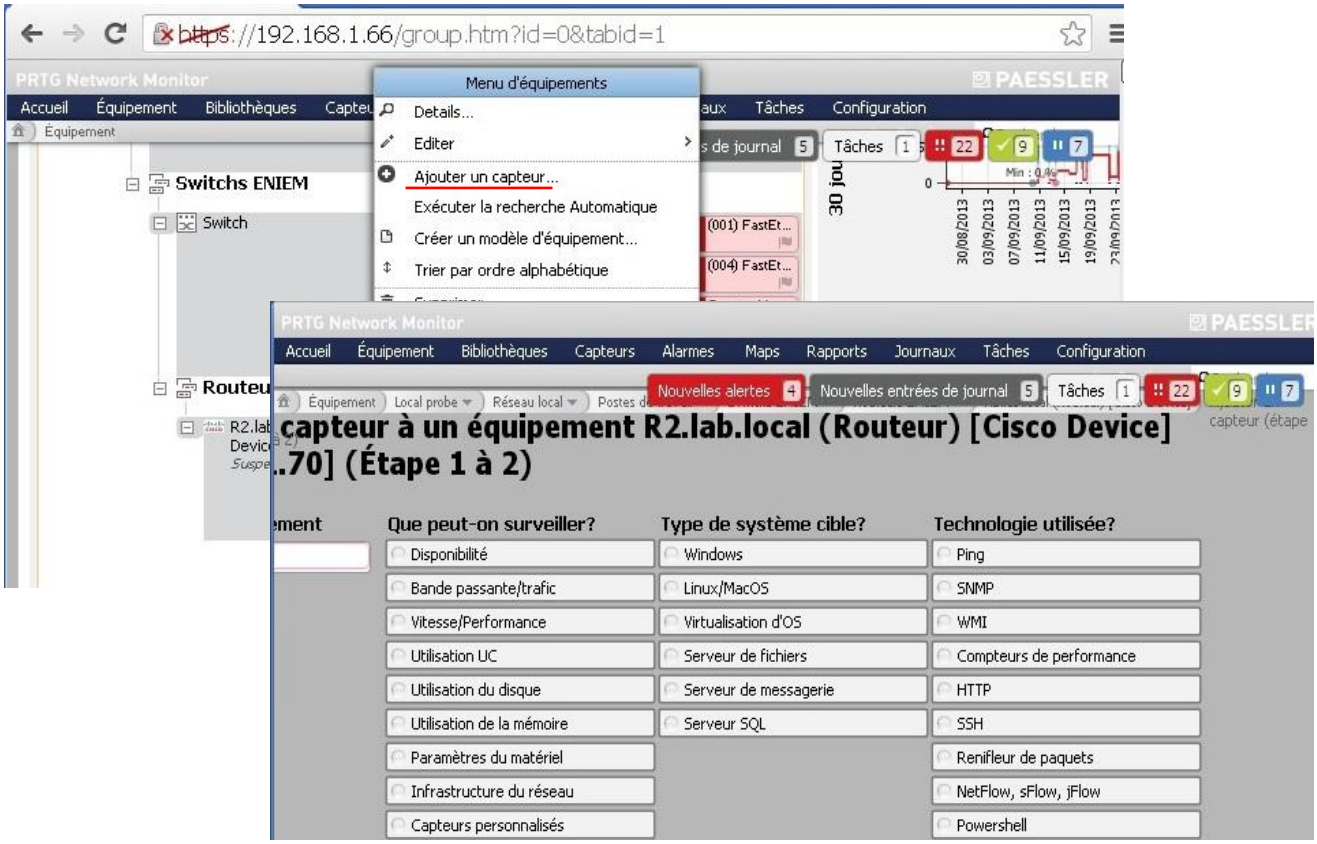

Figure V.51 : Ajouter un capteur

.Voici des exemples de capteurs de supervision de disponibilité :

Figure V.52 : Exemples de capteurs

Remarque : une fois le capteur est ajouter, il prendra une couleur selon son état d'avancement ; vert quand il est fonctionnel, rouge quand il n'est pas fonctionnel, l'orange est un avertissement, et il devient bleu quand il est suspendu.

Figure V.53 : Les états et les notifications des capteurs PRTG

.Nous procédons avec la même manière pour créer les trois groupe, et les trois équipements à supervisé (PC maintenance, Switch test, Routeur test) ainsi que leurs capteurs :

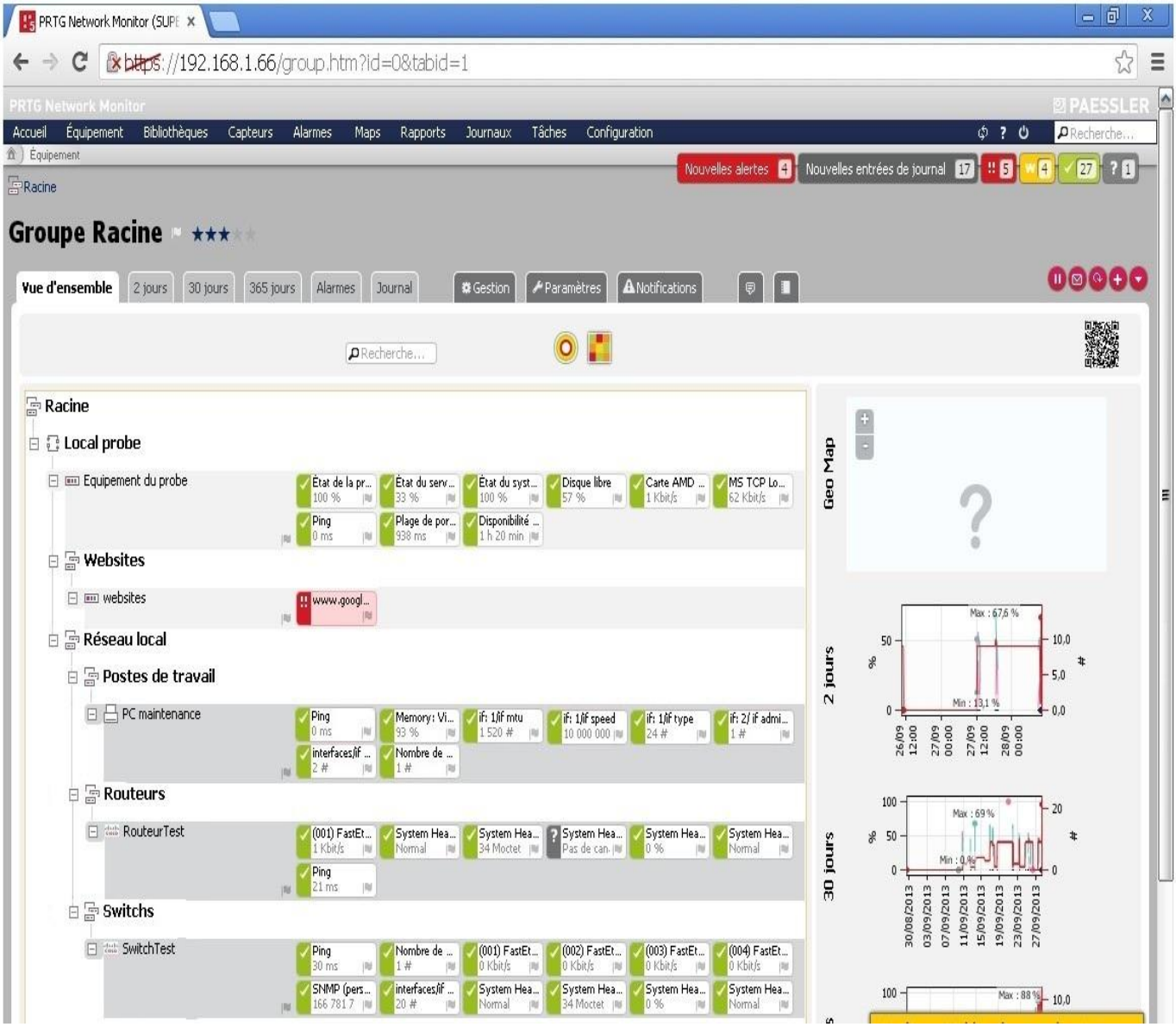

Figure V.54 : La mise au point des groupes

.Nous pouvons consulter chaque capteur en cliquant dessus. Voici un exemple :

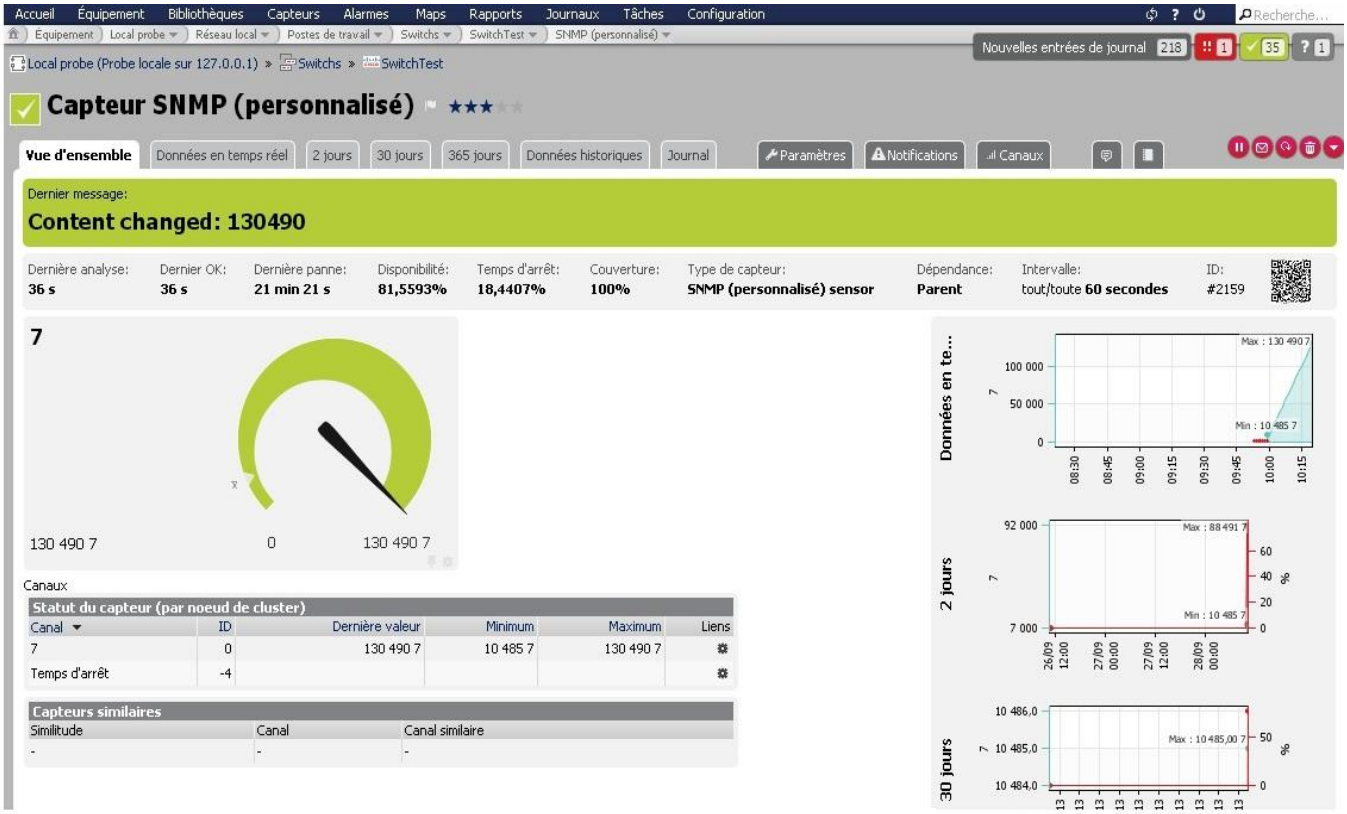

Figure V.55 : Etat du capteur SNMP

. Nous peut observer le mécanisme de la supervision via SNMP, pour ce, nous utilisons Wireshark pour la capture de trame. Clique droit sur l'interface où nous ferons la capture :

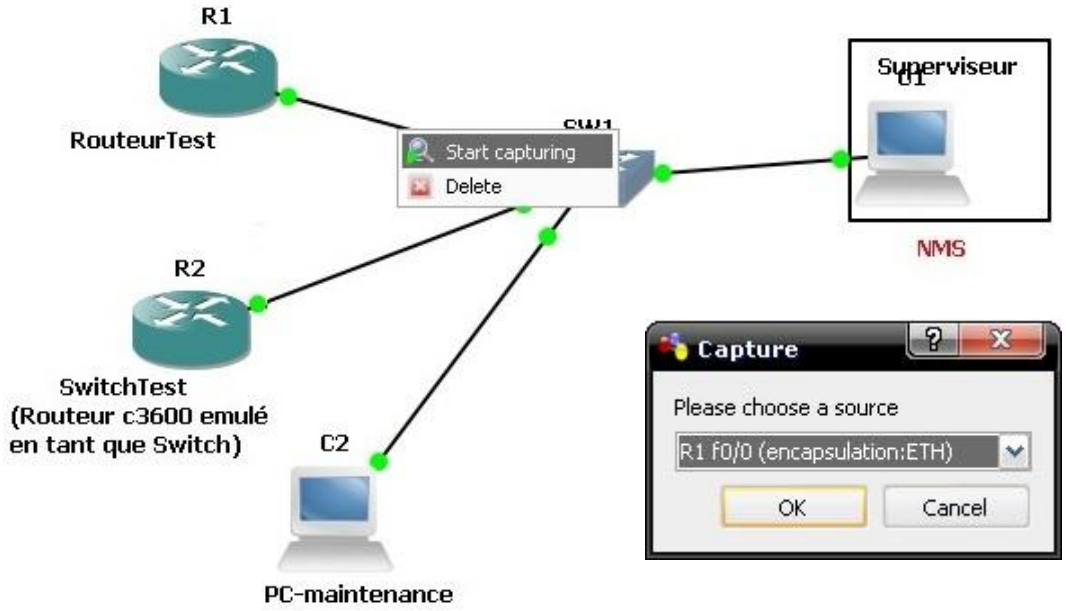

Figure V.56 : lancer la capture de trames

.Voila le résultat :

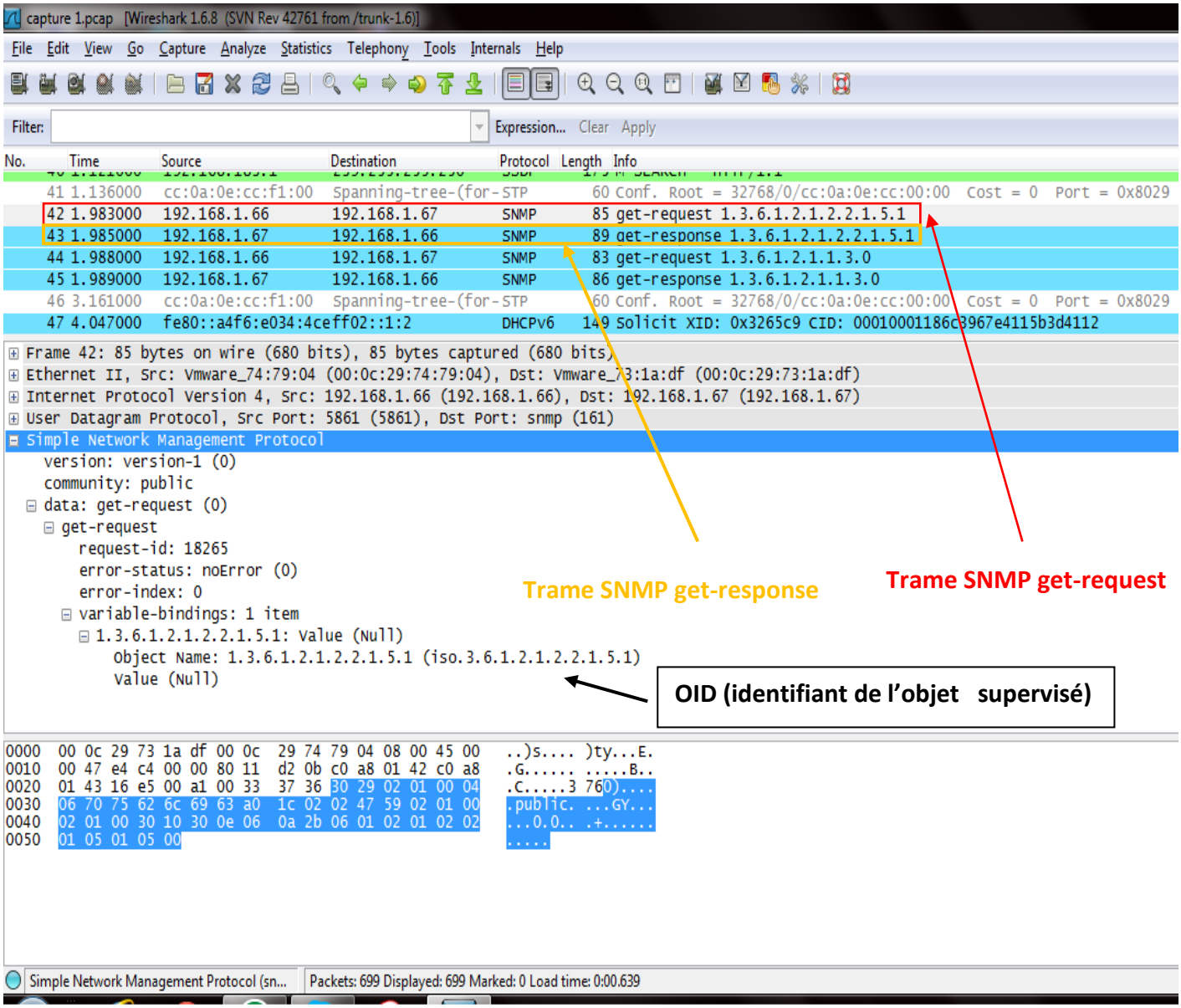

Figure V.57 : Capture de trames SNMP

Remarque : Nous cliquons sur la trame SNMP get-request pour voir le contenu.

Nous cliquons sur la trame SNMP get-response :

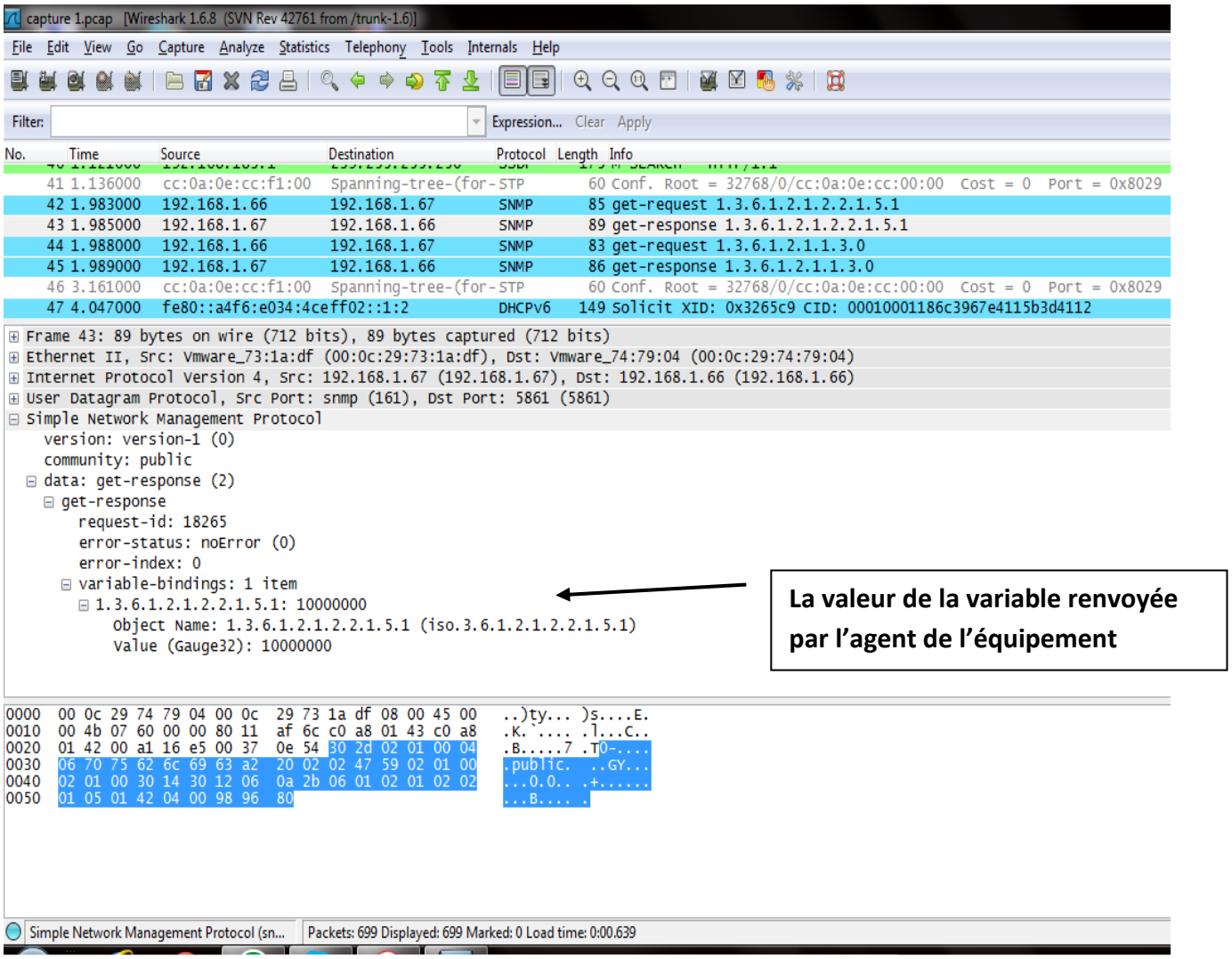

Figure V.58 : Capture de trames SNMP

La MIB liste l'unique identifiant OID de chaque objet supervisé dans le réseau SNMP. Notre Manager SNMP ne peut monitorer notre équipement que s'il compile son fichier MIB (il compile le fichier MIB qui est en syntaxe ASN.1 (fichier texte) en fichier binaire), qu'il intègre par la suite dans le gestionnaire de MIB du NMA (PRTG) :

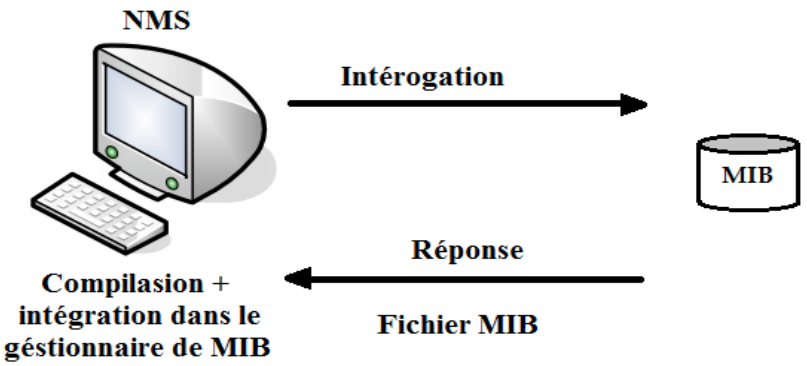

Figure V.59 : Principe d'interrogation de MIB

❖ **Superviser la sécurité avec MBSA :**

.Spécifier le hôte à analyser puis cliquer sur Démarrer l'analyser :

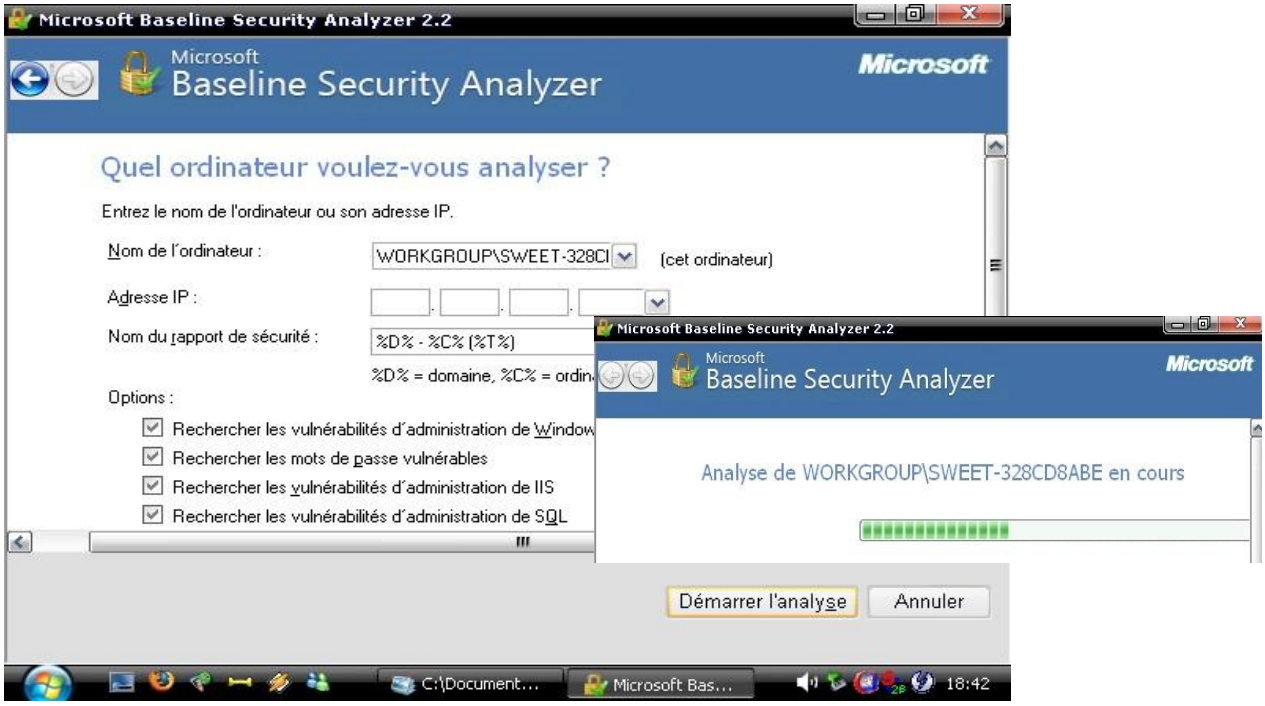

Figure V.60 : Démarrer l'analyse d'un hôte avec MBSA

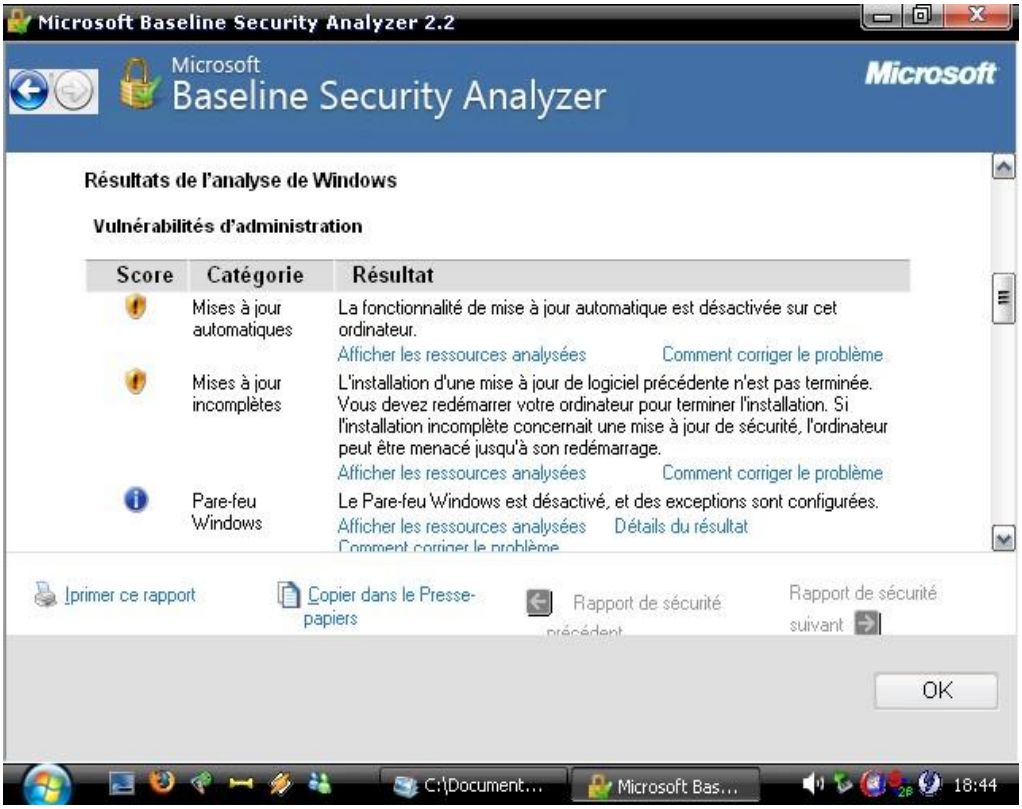

Figure V.61 : Résultat de l'analyse avec MBSA

❖ **Scan de port avec Nmap :**

Démarrer Nmap, entrer l'adresse IP de la cible (post à scanner), par exemple PC maintenance, sélectionner intense scan puis cliquer sur scan pour lancer un scan :

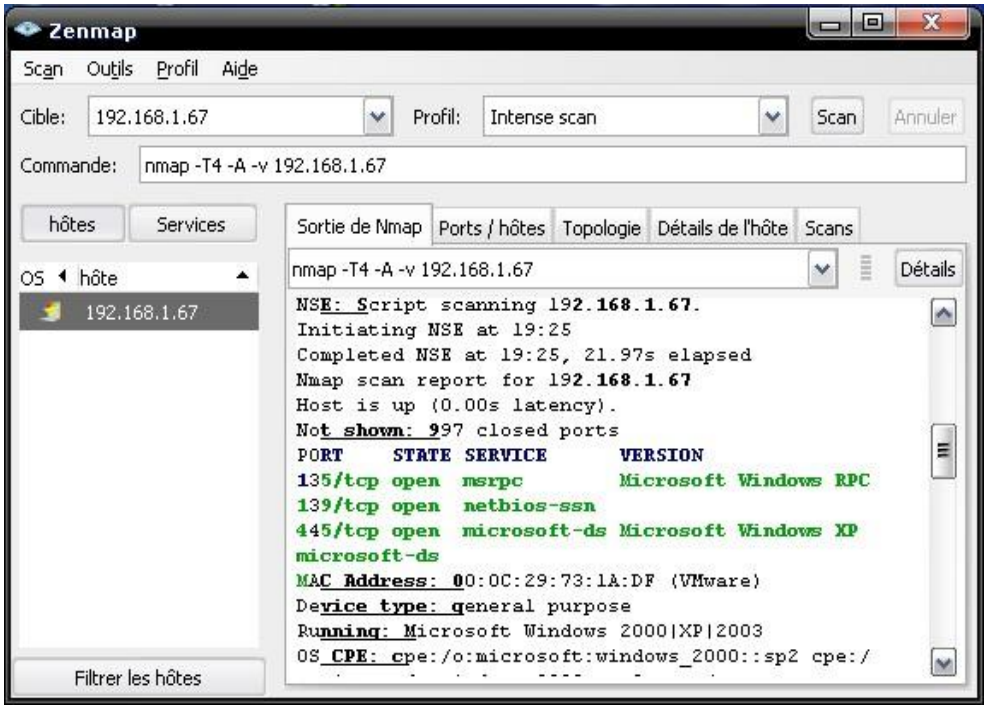

Figure V.62 : Résultat d'un scan avec Nmap

→ Le résultat du scan nous donne les ports ouverts ainsi que des informations sur le système utilisé et l'adresse MAC. Nmap offre aussi d'autres fonctionnalités comme, la visualisation d'hôtes, des services de chaque port, et même du traceroute :

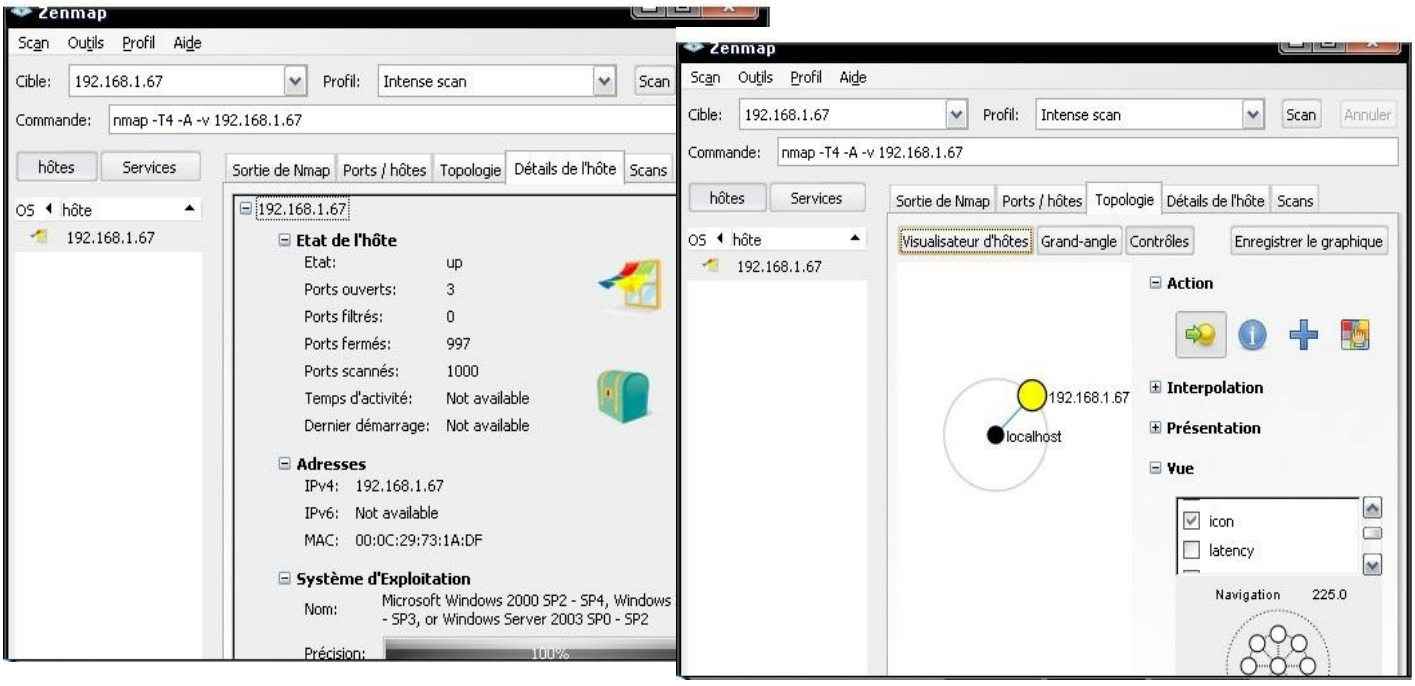

Figure V.63 : Les fonctionnalités offertes par Nmap

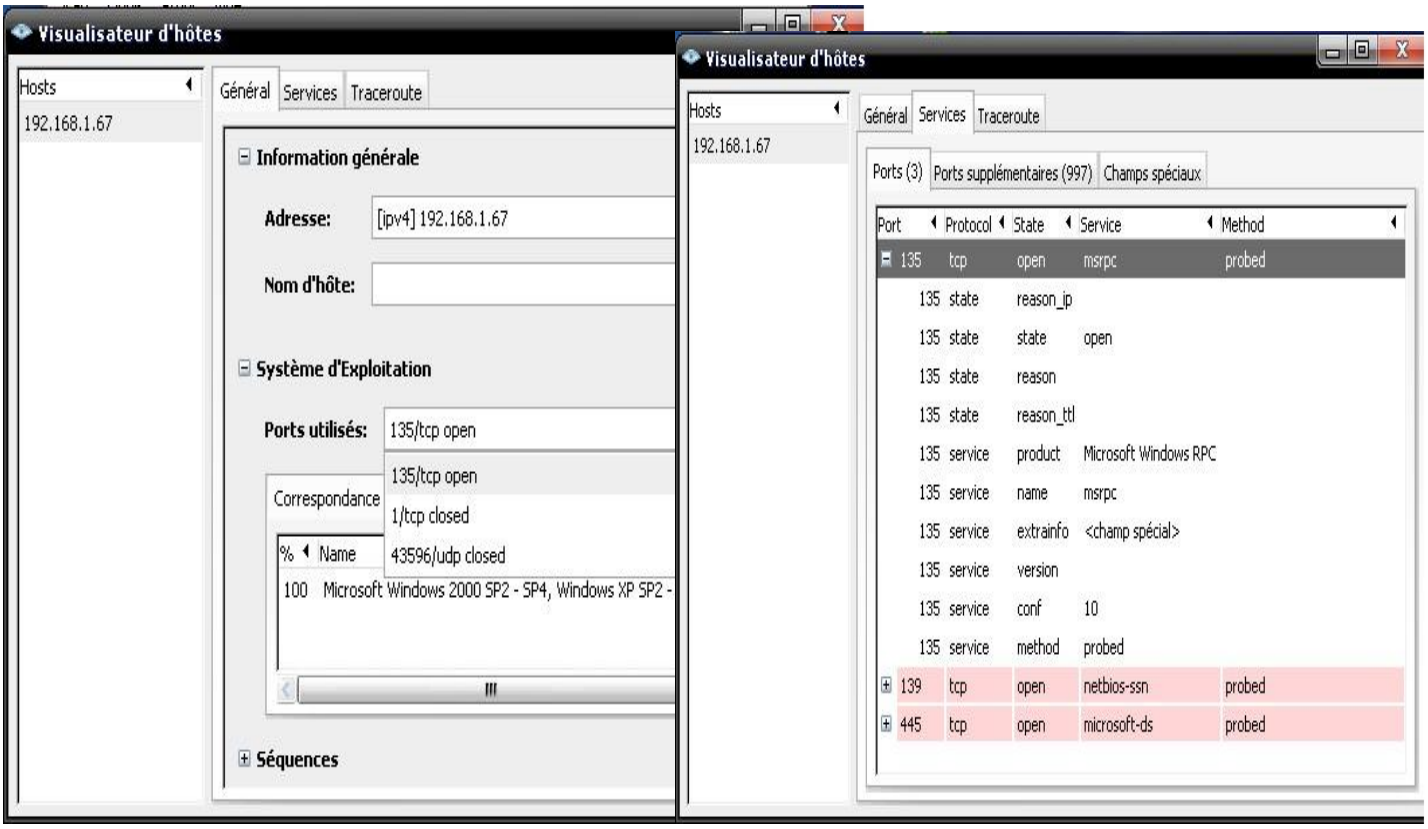

Figure V.64 : La visualisation des hôtes

.Synthèse : nous adoptant le plan de notre conception en se servant des outils de test, nous avons vérifié les points suivants :

- ✓ **Création des VLAN.**
- ✓ **Configuration du VTP serveur et client.**
- ✓ **Les interfaces logiques et fastEthernet sont bien configurables.**
- ✓ **Le routage inter-vlan et les ACL sont respectés et sont bien fonctionnels.**
- ✓ **L'accès au serveur est bien limité (et donc sécurisé).**
- ✓ **Le plan d'adressage offre une bien une souplesse et facilité de manipulation.**
- ✓ **La configuration du firewall.**
- ✓ **La configuration de Frame Relay et d'OSPF.**
- ✓ **La configuration de SNMP.**
- ✓ **La possibilité de récolter des informations sur l'état des systèmes du réseau et diagnostiquer les problèmes de fonctionnement et de sécurité avec notre plan de supervision.**

Conclusion

Dans ce chapitre nous avons présenté les spécifications de ma solution de sécurité et de supervision ainsi que les différentes étapes d'implémentation. Nous également réalisé une série de tests avec différentes options. Il est toutefois important de prendre les résultats avec prudence, car ceux-ci sont dépendants de notre plateforme de tests (processus, mémoire…).

Conclusion générale

Conclusion

Le réseau informatique est au cœur de l'entreprise, quelle que soit son secteur d'activité. On peut facilement comparer la place que joue le réseau informatique au sein d'une entreprise à celle que joue le système nerveux chez l'être humain. En effet, il doit fonctionner pleinement et en permanence pour garantir l'activité. Les problèmes de sécurité doivent donc être réduits au minimum, car une indisponibilité du système d'information ou la perte de son authenticité peut être une cause de pertes pour notre entreprise.

Pour ce, deux phases sont importantes : garantir la sécurité du système et de l'information, mais aussi tenter de prévenir en cas de problème et, le cas échéant, garantir une remontée d'information rapide et une durée d'intervention minimale (c'est le rôle de la supervision).

Dans ce mémoire, nous nous sommes intéressé à la conception d'une solution visant la sécurité du réseau de l'ENIEM y compris son système de gestion, mais aussi la surveillance de ce réseau y compris sa politique et ses systèmes de sécurité (cela contribue à contrôler que la stratégie définie dans la politique de sécurité est mise en œuvre par les niveaux de pilotage et opérationnel, et à la remontée d'informations pertinentes jusqu'aux décideurs).

C'est important de souligner que la stratégie de sécurité adopté ne sera pas uniques, car au fur et à mesure, il y'a de nouvelle attaques qui apparaissent, d'où l'utilité des audits de sécurité. En effet, nous proposons ces perspectives pour mieux atteindre le but de ce mémoire :

Le déploiement d'une façon stratégique d'une unité IDS (Intrusion Detection System) voir même une IPS (Intrusion Prevention System) afin de détecter les attaques et de prévenir des menaces venants se heurter au réseau.

Application de fonction de redondance au niveau du réseau, on installant des liaisons redondantes fonctionnant selon le besoin en mode Active-Active, ou en mode Active - Standby.

Installation et configuration d'une liaison backup entre l'ENIEM et sa direction générale assurant ainsi la permanence d'interconnexion en cas de coupure ou saturation de la liaison existante.

Configuration de la supervision du RLE de la direction Générale via SNMP, tel que les alarmes et notifications seront envoyés par mail au superviseur global.

Par ailleurs, l'étude d'un tel thème, nous a amener à conclure que la supervision et la sécurité sont deux mécanisme dépendants, en effet ceux-là se coalisent pour former une stratégie fiable. Cela nait du besoin de superviser le plan et le système de sécurité (fonctionnement, suivi, anomalies…), mais aussi de sécuriser le système de supervision ainsi que les échanges des données de supervision.

Nous avons pu prouver qu'il est réalisable d'associer à l'infrastructure du réseau informatique vulnérable de l'entreprise ENIEM un plan couplant entre sécurité et supervision, tout en automatisant la remontée des alarmes et des notifications. Nous avons également réalisé une série de tests avec différentes options. Il est toutefois important de prendre les résultats avec prudence, car ceux-ci sont dépendants de notre plateforme de tests (processus, mémoire…).

L'infrastructure conçue pour le réseau de l'ENIEM va permettre de satisfaire les besoins en termes de confidentialité, disponibilité, intégrité, authentification, et contrôle d'accès, et par cela réduire les risques encourus.

Bibliographie

Bibliographie

❖ Livres :

[1] Claude SEVERIN, Préface de Jean-Pierre Arnaud, « RESEAUX & TELECOMS », 2e édition, DUNOD Informatique, 2003.

[2] Tarmo ANTTALAINEN, « introduction to Telecommunications Network Engineering », 2nd edition, Artech House, 2003.

[3] Jean-Luc MONTAGNIER, « Réseaux d'entreprises par la pratique», edition Eyrolles.

[4] Stallings W. « Network Security ». 2nd edition. Prentice Hall, 2003.

[5] Vincent REMAZEILLES, « La sécurité des réseaux avec CISCO». Edition eni.

[6] Jean-François PILLOU, Jean-Philippe BAY, « Tout sur la sécurité informatique ». 2e édition, DUNOD, 2005.

[7] Jean-Luc MONTAGNIER. « Construire son réseau d'entreprise ». Éditions Eyrolles, 2001.

[8] Cédric LIORENS, Laurent LEVIER, Denis VALOIS. « Tableaux de bord de la sécurité réseau ». 2nd edition. Editions Eyrolles, 2003.

❖ Articles :

[9] Cécilien CHARLOT. « Solution NAC de contrôle d'accès au réseau ». [H5845], base documentaire Attaques et mesures de protection des SI (2008). Dans le thème sécurité des systèmes d'information, et dans l'univers technologies de l'information. Edition Techniques de l'ingénieur.

[10] Olivier WILLM. « Administration de réseaux informatiques : protocole SNMP ». [H 2840], base documentaire Architecture des systèmes et réseaux

(2003). Dans le thème Technologies logicielles Architectures des systèmes et dans l'univers technologies de l'information.

[11] Sarah NATAF, Vincent BEL, Franck VEYSSET. « Technique de supervision de la sécurité des réseaux IP ». [H 5820], dans le thème sécurité des systèmes d'information. Edition Techniques de l'ingénieur.

[12] Microsoft Etudes 2008. « Sécurité des réseaux informatiques ». Microsoft corporation, 2007.

❖ Sites :

[10] www.sndl.cerist.dz

[11] www.commentcamarche.com

[17] www.Cisco.com

. www.develloppez.com

. www.dpstelecom.com

. www.wiki.monitoring-fr.org

. http://www.loriotpro.com/

Annexe A

A.1.Structure d'un paquet IPV4

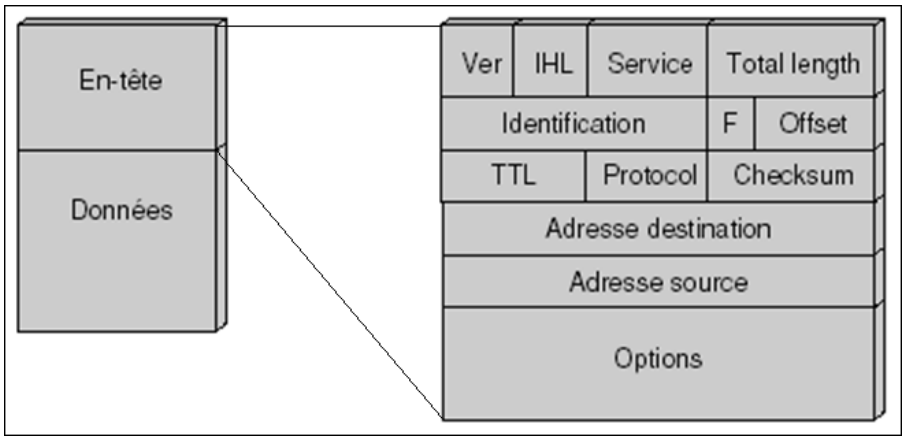

Figure A.1 : Structure d'un paquet IPV4

❖ **Champs et descriptions :**

- **Version (Ver):** Indique la version de protocole IP utilisée (4 bits).
- **HL (Header Length):** taille de l'en-tête avec les options.
- **Service :** type de service pour IP
- **Longueur totale (Total length):** Précise la longueur du paquet IP en entier, y compris les données et l'en-tête, en octets (16 bits).
- **Identification :** identifiant du datagramme, utilisé pour la fragmentation.
- **Flag (F) :** drapeau binaire (sur 3 bits) pour la fragmentation.
- **Offset :** offset du datagramme courant dans le datagramme fragmenté.
- **Durée de vie (TTL):** Un compteur qui décroît graduellement, par incréments, jusqu'à zéro. À ce moment, le datagramme est supprimé, ce qui empêche les paquets d'être continuellement en boucle (8 bits).
- **Somme de contrôle (Checksum):** Assure l'intégrité de l'en-tête IP (16 bits).
- **Adresse d'origine :** Indique le nœud émetteur (32 bits)
- **Adresse de destination:** Indique le nœud récepteur (32 bits).
- **Données:** Cet élément contient des informations de couche supérieure (longueur variable, maximum 64 Ko).
- **Remplissage:** Des zéros sont ajoutés à ce champ pour s'assurer que l'en-tête IP soit toujours un multiple de 32 bits.

A.2. Structure d'un segment TCP

Le protocole TCP encapsule les informations provenant de la couche supérieure dans des segments dont voici les principales informations :

16 bits	16 bits	32 bits	32 bits	16 bits	16 bits	Variable
Port Source	Port Destination	Numéro de séquence	Numéro d'accusé de réception	Fenêtre	Somme de contrôle	Données

Figure A.2 : Structure d'un segment TCP

❖ **Champs et descriptions :**

- **Port source :** Numéro du port appelant
- **Port de destination :** Numéro du port appelé
- **Numéro de séquence :** Numéro utilisé pour assurer le séquençage correct des données entrantes
- **Nº d'accusé de réception :** Prochain octet TCP attendu
- **Somme de contrôle :** Somme de contrôle calculée des champs d'en-tête et de données
- **Données :** Données du protocole de couche supérieur

A.3. Structure d'un datagramme UDP

UDP étant un protocole non orienté connexion, il dispose d'un en-tête de taille réduite par rapport aux en-têtes des segments TCP :

16 bits	16 bits	16 bits	16 bits	Taille variable
Port Source	Port Destination	Longueur	Somme de contrôle	Données

Figure A.3 : Structure d'un datagramme UDP

Le protocole UDP est conçu pour les applications ne devant pas assembler de séquences de segments. Il laisse aux protocoles de la couche application le soin d assurer la fiabilité.

A.4. Structure d'une trame Ethernet II

Les trames Ethernet V2 sont les plus utilisées actuellement :

8 octets	6 octets	2 octets	2 octets	46 à 1500 octets	4 octets
Préambule	Adresse destination	Adresse source	Ether-type	Données	CRC

Figure A.4 : Format d'une trame Ethernet II

❖ **Champs et descriptions :**

- **Préambule :** Annonce le début de la trame et permet la synchronisation.
- **Adresse destination et adresse source:** adresses physiques des cartes Ethernet destination et source.
- **Type :** Indique quel protocole est concerné par le message. La carte réalise un démultiplexage en fournissant les données au protocole concerné.
- **Données** : L'information véhiculée par la trame.
- **CRC (Cyclic Redundancy Code):** Champ de contrôle de la redondance cyclique. Permet de s'assurer que la trame a été correctement transmise et que les données peuvent donc être délivrées au protocole destinataire.

A.5. Format d'une trame 802.1q

Afin qu'une trame Ethernet d'un certain VLAN puisse être identifiée, un code d'identification VLAN (CLI-Tag Control Information) définit par la norme 802.1q est rajouter.

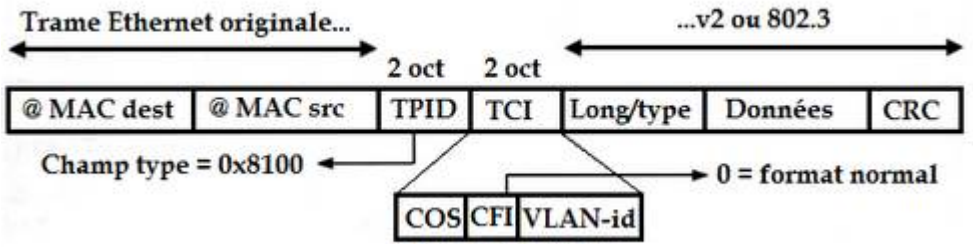

Figure A.5 : Format d'une trame 802.1q

- **Champs et descriptions :**

- **TPID (Tag Protocol Identifier):** type du tag, 0x8100 pour 802.1Q.
- **TCI (Tag Control Information) :** le label 802.1q inséré dans la trame Ethernet.
- **COS (Class Of Service) ou Priorité :** niveaux de priorité définis par l'IEEE 802.1P.
- **CFI (Common Format Identifier) :** Ethernet ou token-ring.
- **VLAN-id:** VLAN identifier (numéro), codé sur 12 bits (jusqu'à 4096 vlans).

. Information : Le standard IEEE 802.1Q

Le standard 802.1Q de l'IEEE est aujourd'hui le standard de fait pour l'identification des trames faisant partie d'un réseau virtuel. Il a succédé à ISL (Inter-Switch Link), protocole propriétaire développé par Cisco (et également repris par quelques autres constructeurs).

Le principe général est de rajouter dans chaque trame Ethernet destinée à être transmise d'un commutateur à un autre quelques en-têtes supplémentaires contenant en particulier l'identifiant du réseau virtuel auquel elle appartient (VID, VLAN Identifier), qui est un numéro sur 12 bits, de 0 à 4094 (4095 est réservé et, en pratique, 0 et 1 sont inutilisés).

A.6. Structure d'une trame SNMP (PDU SNMP)

Le format d'un message SNMP standard :

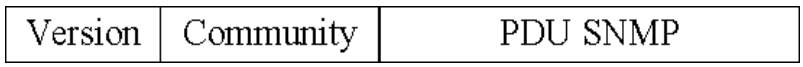

Figure A.6 : Format d'un message SNMP standard

- **Champs et descriptions :**

- **Version :** précise la version du protocole SNMP utilisée.
- **Community :** nom pour identifier le manager et filtrer l'accès aux informations.
- **PDU (Protocol Data Unit) SNMP :** il est constitué de l'une des trois PDU suivants :

✧ PDU GetRequest, GetNextRequest et SetRequest **:**

Type	request-Id	0	0	Affectation des variables

Figure A.7 : Format d'une PDU GetRequest, GetNextRequest et SetRequest

- **Type :** indique s'il s'agit d'une PDU GetRequest, GetNextRequest ou SetRequest.
- **Request-Id** : La réponse à la requête sera retournée avec la valeur fournie par ce champ, afin d'associer la réponse à la requête.
- **Affectation des variables** : est une suite de couples d'identificateurs et de valeurs associées. Les valeurs sont fournies uniquement dans le cas d'une PDU SetRequest.

✧ PDU GetResponse **:**

Type	request-Id	error-status	error-index	Affectation des variables

Figure A.8 : Format de PDU GetResponse

- **Type :** permet de reconnaître une PDU SetResponse des PDU précédentes (dont le format est identique).
- Les champs **error-status** et **error-index :** nous informent sur le résultat de la requête.

✧ PDU Trap :

Type	entreprise	Agent-addr	generic-trap	specific-trap	time-stamp	Affectation

Figure A.9 : Format de PDU trap

Tel que Affectation :

nom1	valeur1	nom2	valeur2	nom3	valeur3

. Champs de PDU trap :

- **Entreprise :** Il est l'identifiant de l'agent ayant généré l'alarme.
- **Agent-addr :** C'est l'adresse IP de l'agent ayant généré l'alarme.
- **Generic-Trap :** Ce champ prend une des sept valeurs possibles de l'alarme :

  - 0 → ColdStart : redémarrage du système à froid.
  - 1 →WarmStart : redémarrage du système à chaud.
  - 2→LinkDown : le lien n'est plus opérationnel.
  - 3→LinkUp : le lien est à nouveau opérationnel.
  - 4→AuthentificationFailure : Tentative d'accès à l'agent avec un mauvais nom de communauté.
  - 5→EgpNeighborLoss : la passerelle adjacente ne répond plus.
  - 6→EntrepriseSpecific : alarme spécifique aux entreprises.

- **Specific-Trap** : Ce champ est un code déterminant la nature de l'alarme. Il est spécifique à chaque agent propriétaire.
- **Time-Stamp :** Ce champ donne le temps écoulé, en millisecondes, entre l'envoi de l'alarme et l'initialisation de l'agent.

Annexe B

Introduction

Cette documentation regroupe des commandes utilisées sur les routeurs et commutateurs CISCO. En introduction seront présentées les commandes permettant de configurer les bases du routeur et du commutateur tels que nom de l'équipement, mots de passe, bannière, commandes de sauvegarde, de visualisation et configuration basique d'interfaces. Par la suite, les commandes spécifiques aux routeurs et aux commutateurs seront présentées respectivement.

B.1. Les conventions d'écriture

Italique	indique des arguments dans lesquels l'utilisateur fournit des valeurs
[X]	indique un élément facultatif
|	indique un choix facultatif ou obligatoire
[X|Y]	indique un choix facultatif
{X|Y}	indique un choix obligatoire

B.2. les commandes de base

B.2.1.Commandes pour changer de mode d'exécution et de configuration :

```
Router> enable  //*passage du mode exec (ou utilisateur ou inprivilégié) au mode privilégié*//
Routeur#  //*mode privilégié*//
Router# configure terminal //*passage en mode de configuration global*//
Router(config)#  //*mode configuration global*//
Router(config)# exit | end | ^C | ^Z  //* quitter le mode actuel*//
Router# disable //*passage du mode privilégié au mode utilisateur*//
Router> //*mode utilisateur*//
Router# ? //*afficher de l'aide sur les commandes*//
```

B.2.2.Outils de diagnostic :

```
Router# ping ip-address
Router# traceroute ip-address
```

B.2.3.Visualisation de l'état de l'équipement :

```
Router# show version
Router# show flash
Router# show memory
Router# show interfaces
Switch# show history
Switch# terminal history {size number }
```

B.2.4.Visualisation et sauvegarde de la configuration :

```
Router# show running-config //*afficher la configuration actuelle (en cours)*//
Router# show startup-config //*afficher la configuration de démarrage (celle enregistrée)
Router# copy running-config startup-config
Router# copy running-config tftp:
Switch# copy system:running-config tftp:[[[//location ]/directory ]/filename ]
Switch# copy nvram:startup-config tftp:[[[//location ]/directory ]/filename ]
```

B.2.5.Suppression du fichier de configuration :

```
Router# erase nvram:startup-config
Router# erase startup-config
```

B.2.6.Configuration de base d'un équipement CISCO :

```
Router(config)# hostname router-name //*nom de l'équipement*//
Router(config)# enable password password //* mot de passe *//
Router(config)# enable secret password //*mot de passe crypté*//
Router(config)# banner motd # message #
Router(config)# banner login # message #
```

B.2.7.Configuration de la console et du terminal virtuel :

```
Router(config)# line console 0
Router(config-line)# password password
Router(config-line)# login
Router(config-line)# logging synchronous
Router(config)# line vty 0 4
Switch(config)# line vty 0 15
Router(config-line)# password password
Router(config-line)# login
Router(config)# service password-encryption
```

B.3. Les commandes spécifique aux routeurs et aux Switchs

B.3.1. Routeurs

B.3.1.1. Configuration des interfaces sur un routeur :

```
Router(config)# interface type port
Router(config-if)# ip address ip-address subnet-mask
Router(config-if)# description description
Router(config-if)# clock rate rate
Router(config-if)# no shutdown
Router(config-if)# exit
```

B.3.1.2. Configuration du routage :

Cisco Discovery Protocol (CDP) :

```
Router# show cdp neighbors
Router# show cdp neighbors detail
Router(config)# no cdp run
Router(config-if)# no cdp enable
```

Configuration de routes statiques et route statique par défaut :

```
Router(config)# ip route prefix mask {ip-address | interface-type interface-number [ip-address ]} [distance ] [name ] [permanent] [tag tag ]
Router(config)# ip route network-address subnet-mask {ip-address |exit-interface }
Router(config)# ip route 0.0.0.0 0.0.0.0 [exit-interface | ip-address ]
```

Configuration d'OSPF :

```
Router(config)# router ospf process-id
Router(config-router)# network network-address wildcard-mask area area-id
Router(config-router)# passive-interface interface-type interface-number
```

Configuration de l'ID du routeur en configurant une interface de bouclage (Loopback) ou avec la commande router-id :

```
Router(config-router)# router-id ip-address
Router(config-if)#ip ospf priority {0  255 }
Router(config)#interface loopback number
Router(config-if)#ip address ip-address subnet-mask
Router#clear ip ospf process
```

Configuration de la bande passante ou du coût pour le calcul de la métrique d'OSPF :

```
Router(config-router)# auto-cost reference-bandwidth value-mbps
Router(config-if)# bandwidth bw-kbps
Router(config-if)# ip ospf cost cost
Router# show interface interface-type interface-number
Router(config-if)# ip ospf hello-interval seconds
Router(config-if)# ip ospf dead-interval seconds
```

Propagation de la route par défaut :

```
Router(config)# ip route 0.0.0.0 0.0.0.0 [exit-interface | ip-address ]
Router(config-router)# default-information originate
```

Visualisation et dépannage d'OSPF :

```
Router# show ip ospf [interface interface-type interface-number ]
Router# show ip ospf neighbor
Router# show interface interface-type interface-number
Router# show ip protocols
```

Commandes de visualisation et de dépannage pour le routage, valable pour tous les protocoles de routage :

```
Router# ping ip-address
Router# traceroute ip-address
Router# show ip route
Router# show ip interface brief
Router# show running-config
Router# debug ip routing
Router# undebug ip routing
Router# undebug all
```

B.3.2. Commutateurs et Commutation

B.3.2.1 Configuration de base d'un commutateur

Configuration de l'interface de gestion sur un commutateur :

```
Switch(config)# interface vlan vlan-id
Switch(config-if)# ip address ip-address subnet-mask
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface type port
Switch(config)# interface range type port - port
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan vlan-id
Switch(config-if)# end
Switch(config)# ip default-gateway ip-address
Switch# show ip interface brief
Switch# show ip interface
```

Configuration d'options sur un port du commutateur :

```
Switch(config-if)# duplex {auto | full | half}
Switch(config-if)# speed {auto | value-bps }
Switch(config-if)# mdix auto
```

Possibilité d'activer l'interface web pour la configuration du commutateur :

```
Switch(config)# ip http authentication enable
Switch(config)# ip http server
```

Gestion de la table d'adresse MAC du commutateur :

```
Switch# show mac-address-table
Switch(config)# mac-address-table static MAC-address vlan {1-4096 | ALL} interface interface-id
```

B.3.2.2. Configuration de la sécurité sur les commutateurs :

Configuration de la sécurité des ports :

```
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum number
Switch(config-if)# switchport port-security mac-address mac-address
Switch(config-if)# switchport port-security mac-address sticky [mac-address ]
Switch(config-if)# switchport port-security violation {shutdown | restrict |protect}
Switch# show port-security [interface interface-id ]
Switch# show port-security address
```

B.3.2.3 Réseaux locaux virtuels VLANs

Configuration de VLANs :

```
Switch(config)# vlan vlan-id
Switch(config-vlan)# name vlan-name
Switch# show vlan [brief | id vlan-id | name vlan-name | summary]
Switch# show interfaces [interface-id | vlan vlan-id ] | switchport
Switch# delete flash:vlan.dat
```

Configuration d'agrégations de VLANs (Trunk) :

```
Switch(config)# interface type port
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan vlan-id
Switch(config-if)# switchport trunk allowed vlan vlan-id [,vlan-id,vlan-id ...]
Switch(config-if)# switchport trunk allowed vlan add vlan-id
Switch# show interfaces id-interface switchport
Switch# show interfaces trunk
```

Dynamic Trunking Protocol DTP :

```
Switch(config)# interface type port
Switch(config-if)# switchport mode access
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport mode dynamic auto
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# switchport nonegociate
Switch# show dtp interface type port
```

VLAN Trunking Protocol VTP

```
Switch(config)# vtp mode {server | client | transparent }
Switch(config)# vtp domain domain-name
```

```
Switch(config)# vtp password password
Switch(config)# vtp version {1 | 2}
Switch(config)# vtp pruning
Switch# show vtp status
Switch# show vtp counters
Switch# show interfaces trunk
```

Routage inter-vlan

Configuration de sous-interfaces sur un Router-on-a-stick :

```
Router(config)# interface type interface-number
Router(config-if)# no shutdown
Router(config-if)# interface type interface-number.subinterface-number
Router(config-subif)# encapsulation dot1q vlan-id
Router(config-subif)# ip address ip-address subnet-mask
```

B.4. Réseaux étendus WAN

B.4.1 Point-to-Point Protocol PPP

Activation du protocole hdlc sur une interface série :

```
Router(config-if)# encapsulation hdlc
```

Activation du protocole ppp sur une interface série :

```
Router(config-if)# encapsulation ppp
Router(config-if)# compress [predictor | stac]
Router(config-if)# ppp quality percentage
Fonction de rappel PPP (A quoi cela sert-il ? ? ?) :
# ppp callback [accept | request]
```

B.4.2. Protocole d'authentification du mot de pass PAP et CHAP :

```
Router(config-if)# ppp authentication {chap | chap pap | pap chap | pap}
[if-needed] [list-name | default] [callin]
Router(config)# username name password password
Router(config-if)# ppp pap sent-username name password password
```

Exemple de configuration de PAP entre deux routeurs R1 et R2 :

```
R1(config)# username User2 password User2-password
R1(config-if)# encapsulation ppp
R1(config-if)# ppp authentication pap
R1(config-if)# ppp pap sent-username User1 password User1-password
R2(config)# username User1 password User1-password
R2(config-if)# encapsulation ppp
R2(config-if)# ppp authentication pap
R2(config-if)# ppp pap sent-username User2 password User2-password
```

Même exemple mais en utilisant CHAP :

```
R1(config)# username User2 password User2-password
R1(config-if)# encapsulation ppp
R1(config-if)# ppp authentication chap
R1(config-if)# ppp chap hostname User1
R1(config-if)# ppp chap password User1-password
R2(config)# username User1 password User1-password
R2(config-if)# encapsulation ppp
R2(config-if)# ppp authentication chap
R2(config-if)# ppp chap hostname User2
R2(config-if)# ppp chap password User2-password
```

Visualisation et dépannage d'une interface série :

```
Router# show interfaces serial interface-number
Router# show controllers
Router# debug ppp {packet | negotiation | error | authentification | compression |cbcp}
```

B.4.3. Frame Relay

Configuration de Frame Relay avec mappage statique :

```
Router(config-if)# encapsulation frame-relay [cisco | ietf]
Router(config-if)# bandwidth bw-kbps
Router(config-if)# no frame-relay inverse-arp
Router(config-if)# frame-relay map protocol protocol-address dlci [broadcast] [ietf] [cisco]
Router# show frame-relay map
```

Interface de supervision locale LMI :

```
Router# show frame-relay lmi
Router# frame-relay lmi-type [cisco | ansi | q933a]
```

Configuration de sous-interfaces Frame Relay :

```
Router(config)# interface serial interface
Router(config-if)# encapsulation frame-relay
Router(config-if)# interface serial subinterface_number [multipoint | point-to-point]
Router(config-subif)# ip address ip-address subnet-mask
Router(config-subif)# frame-relay interface-dlci dlci-number
Router(config-if)# no shutdown
```

Visualisation et dépannage de Frame Relay :

```
Router# show interfaces
Router# show frame-relay lmi
Router# show frame-relay pvc [interface interface ] [dlci]
Router # clear counters
Router # show frame-relay map
Router # clear frame-relay-inarp
Router # debug frame-relay lmi
```

B.5. Sécurité

B.5.1 Sécurisation générale du routeur

Configuration de mots de passe sécurisés et authentification AAA :

```
Router(config)# aaa new-model
Router(config)# aaa authentication login LOCAL_AUTH local
Router(config)# line console 0
Router(config-line)# login authentication LOCAL_AUTH
Router(config-line)# line vty 0 4
Router(config-line)# login authentication LOCAL_AUTH
Router# username username password password
Router# username username secret password
Router(config)# service password-encryption
Router(config)# security passwords min-length number
```

Exemple de chiffrement de mots de passe :

```
R1(config)# username Student password cisco123
R1(config)# do show run | include username username Student password 0 cisco123
R1(config)#
R1(config)# service password-encryption
R1(config)# do show run | include username username Student password 7 03075218050061
R1(config)#
R1(config)# username Student secret cisco
R1(config)# do show run | include username username Student secret 5 $1$z245$lVSTJzuYgdQDJiacwP2Tv/
R1(config)#
```

Désactivation de la ligne auxiliaire :

```
Router(config)# line aux 0
Router(config-line)# no password
Router(config-line)# login
Router(config-line)# exit
```

Configuration des lignes de terminaux virtuels VTY pour Telnet et SSH :

```
Router(config)# line vty 0 4
Router(config-line)# no transport input
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
Router(config)# login block-for seconds attempt tries within seconds
Router(config)# security authentication failure rate threshold-rate log
```

Configuration des lignes de terminaux virtuels VTY uniquement pour SSH :

```
Router(config)# line vty 0 4
Router(config-line)# no transport input
Router(config-line)# transport input ssh
Router(config-line)# exec-timeout number
Router(config)# service tcp-keepalives-in
```

Configuration de SSH :

```
Router(config)# ip ssh version 2
Router(config)# hostname hostname
Router(config)# ip domain-name domain-name
Router(config)# crypto key {generate | zeroise} rsa
Router(config)# username username secret password
Router(config)# line vty 0 4
Router(config-line)# transport input ssh
Router(config-line)# login local
Router(config)# ip ssh time-out seconds
Router(config)# authentification-retries number
Router# show ip ssh
Router# show ssh
```

Désactivation des services non utilisés :

```
Router# show running-config
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
Router(config)# no ip bootp server
Router(config)# no service finger
Router(config)# no ip http server
Router(config)# no snmp-server
Router(config)# no cdp run
Router(config)# no service config
Router(config)# no ip source-route
Router(config)# no ip classless
Router(config-if)# shutdown
Router(config-if)# no ip directed-broadcast
Router(config-if)# no ip proxy-arp
```

Authentification des protocoles de routage

Configuration d'OSPF avec authentification simple du protocole de routage :

```
Router(config)# router ospf process-id
Router(config-router)# area area-id authentification
Router(config)# interface type port
Router(config-if)# ip ospf authentication
Router(config-if)# ip ospf authentication-key string
Router# show ip route
```

Configuration d'OSPF avec authentification md5 du protocole de routage :

```
Router(config)# interface type port
Router(config-if)# ip ospf message-digest-key 1 md5 string
Router(config-if)# ip ospf authentication message-digest
Router(config)# router ospf process-id
Router(config-router)# area area-id authentication message-digest
Router# show ip route
```

B.5.2. Cisco SDM et Simple Network Management Protocol SNMP

Processus de sécurisation automatique du routeur :

```
Router# auto secure
Configuration du routeur pour la prise en charge de SDM :
Router# configure terminal
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
Router(config)# username name privilege 15 secret password
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

Configuration de la consignation via le protocole SNMP vers le serveur Syslog :

```
Router(config)# logging syslog-server-ip-address
Router(config)# logging trap {emergencies | alerts | critical | errors | warnings | notifications | informational | debugging}
```

B.5.3 Liste de Contrôle d'Accès ACL

B.5.3.1. ACL standard

Configuration d'une ACL standard :

```
Router(config)# access-list access-list-number {permit | deny | remark remark } source [source-wildcard ] [log]
Router(config)# no access-list acces-list-number
Router(config-if)# ip access-group {access-list-number | access-list-name } {in | out}
Router# show access-lists [acces-list-number | NAME ]
```

Configuration d'une ACL standard nommée :

```
Router(config)# ip access-list standard NAME
Router(config-std-nacl)# sequence-number [permit | deny | remark] source [source-wildcard ] [log]
Router(config-if)# ip access-group access-list-name {in | out}
Router# show access-lists [NAME ]
```

Utilisation d'une ACL pour contrôler l'accès aux lignes virtuelles VTY :

```
Router(config)# access-list access-list-number {deny | permit} source [source-wildcard ]
Router(config)# line vty 0 4
Router(config-line)# access-class access-list-number in [vrf-also] | out
```

B.5.3.2 ACL étendue

Configuration d'une ACL étendue :

```
Router(config)# access-list access-list-number {permit | deny | remark} protocol source [source-wildcard ] [operator operand ] [port port-number or name ] destination [destination-wildcard [operator operand ] [port port-number or name ] [established]
Router(config)# access-list access-list-number {permit | deny} protocol source source-wildcard destination destination-wildcard {eq | neq | gt | lt | range} protocol-number [established]
Router(config-if)# ip access-group {access-list-number | access-list-name } {in | out}
Router# show access-lists [acces-list-number | NAME ]
```

Configuration d'une ACL étendue nommée :

```
Router(config)# ip access-list extended NAME
Router(config-ext-nacl)# sequence-number [permit | deny | remark] protocol source [source-wildcard ] destination [destination-wildcard ] {eq | neq | gt | lt | range} protocol-number [established]
Router(config-if)# ip access-group access-list-name {in | out}
Router# show access-lists [NAME ]
```

B.5.3.3 ACL dynamique

Exemple de configuration d'une ACL dynamique :

```
Router(config)# username name password password
Router(config)# access-list access-list-number dynamic dynamic-name [timeout
minutes ] permit telnet source source-wildcard destination destination-wildcard
Router(config-if)# ip access-group access-list-number in
Router(config)# line vty 0 4
Router(config-line)# autocommand access-enable host timeout minutes
Router(config-ext-nacl)# evaluate reflect-NAME
Router(config-if)# ip access-group IN-NAME in
Router(config-if)# ip access-group OUT-NAME out
```

B.5.3.4. ACL basée sur le temps

Exemple de configuration d'une ACL basée sur le temps :

```
Router(config)# time-range NAME
Router(config-time-range)# periodic DAYS hh:mm to hh:mm
Router(config)# access-list ACL-number permit protocol source source-wildcard destination destination-wildcard {eq | neq | gt | lt | range} protocol-number time-range NAME
Router(config-if)# ip access-group ACL-number {in | out}
```

B.5.4. Services d'adressage IP

Evolutivité des réseaux avec NAT :

Configuration de la NAT statique :

```
Router(config)# ip nat inside source static local-ip global-ip
Router(config)# interface type number
Router(config-if)# ip nat inside
Router(config)# interface type number
Router(config-if)# ip nat outside
```

Configuration de la redirection de port :

```
Router(config)# ip nat inside source static protocol local-ip port global-ip port
```

Configuration de la NAT dynamique :

```
Router(config)# ip nat pool NAME start-ip end-ip {netmask netmask | prefix-length prefix-length }
Router(config)# access-list access-list-number permit source [source-wildcard ]
Router(config)# ip nat inside source list access-list-number pool NAME
Router(config)# interface type number
Router(config-if)# ip nat inside
Router(config)# interface type number
Router(config-if)# ip nat outside
```

Configuration de la surcharge NAT première configuration possible :

```
Router(config)# access-list access-list-number permit source [source-wildcard ]
Router(config)# ip nat inside source list access-list-number interface interface overload
Router(config)# interface type number
Router(config-if)# ip nat inside
Router(config)# interface type number
Router(config-if)# ip nat outside
```

Configuration de la surcharge NAT deuxième configuration possible :

```
Router(config)# access-list access-list-number permit source [source-wildcard ]
Router(config)# ip nat pool NAME start-ip end-ip {netmask netmask | prefix-length
prefix-length }
Router(config)# ip nat inside source list access-list-number pool NAME overload
Router(config)# interface type number
Router(config-if)# ip nat inside
Router(config)# interface type number
Router(config-if)# ip nat outside
```

Visualisation et dépannage de NAT :

```
Router# show ip nat translations [verbose]
Router# show ip nat statistics
Router(config)# ip nat translation timeout timeout-seconds
Router# clear ip nat translation *
Router# clear ip nat translation inside global-ip local-ip [outside local-ipglobal-ip ]
Router# clear ip nat translation protocol inside global-ip global-port local-ip
local-port [outside local-ip local-port global-ip global-port ]
Router# debug ip nat [detailed]
```

B.6. Le monitoring avec SNMP

Configuration:

```
switch(config)# snmp-server community community-string [ro | rw] [access-list-number]
switch(config)# snmp-server enable traps <type>
switch(config)# snmp-server host ip-address-manager community-string
```

Visualisation et dépannage de SNMP :

```
switch# show snmp
switch# show snmp [user|host|community]
```

∞ Les mots clé ∞

adressage - administration - attaque - ACL - brèche - contre-mesure - cryptographie - cisco - CLI - configuration - connexion - datagramme - entreprise - ENIEM - exploitation - encapsulation - filtrage - firewall - faille - FrameRelay - gestion - HIDS - interconnexion - intrusion - IDS - menace-monitoring - MIB - MBSA - NAT - netflow - NIDS - notification - NMS - NMA - NME - Nmap - OSPF - OID - paquet - pare-feu - PAT - prévention - piratage - PIX 515 - PIX 515 E - protocole - ports - protection - PRTG - PDU - réseaux - risque - routage - sécurité - sécurisation - scan - supervision - surveillance - SNMP - syslog - trame - trunk - vulnérabilité -VLAN - VTP.