REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'enseignement supérieur et de la recherche scientifique
Université Saad Dahlab A Blida
Faculté Des Sciences
Département D'informatique

MEMOIRE DE FIN D'ETUDE EN VUE D'OBTENTION
DU DIPLOME DE MASTER EN :
INFORMATIQUE (ingénierie de logiciel)

THEME

CONCEPTION ET REALISATION D'UN MONITEUR DE SUPERVISION ET GESTION RESEAU

ORGANISME D'ACCEUIL : *DIRECTION GENERALE SONATRACH*

Présenté par :
Mr. DOUGA Yassine
Mr. BENDOUHA Amine

Promoteur et Encadreur :
Mr. BELAAZOUGUE Zahir

PRESIDENT JURÉ : Mm BENSTITI
Juré :
Mm CHORFA
Mm BOUSSETTA

PROMOTION : 2010/2011

Sommaire

Liste des tableaux

Liste des Figures

REMERCIEMENT

Tous d'abord on remercie Dieu qui nous a permis de réaliser un de nos rêves.

On remercie tous le personnel du service approvisionnement pour leurs chaleureux accueils et leur aide et surtout Mme Tire, Mr Belaazougue Zahir pour son encadrement et Mme Benabbass de SONATRACH.

On remercier toutes les personnes qui nous ont aidé de près ou de loin pour la réalisation de ce travail et surtout Mr Ouldaissa et Mr Ferfera de USDB qui nous ont était d'une grande aide par leur suivi et leur suggestion qui ont était très utile a la réalisation de notre projet.

DEDICACES

JE DÉDIE CE MODESTE TRAVAIL

À MES TRÈS CHERS PARENTS QUI N'ONT MÉNAGÉ AUCUN EFFORT POUR QUE JE N'EUSSE BESOIN DE RIEN, POUR LEUR SOUTIEN, PATIENCES AMOUR ET TENDRESSE

À SŒUR AHLEM À MES GRANDS-PARENTS ET SURTOUT DADI QUE DIEU LES GARDES

À TOUT MA FAMILLE

À MON BINÔME, AMI ET FRÈRE BENDOUHA AMINE SA FAMILLE

À MES AMIS ET TOUS LES ÊTRES CHERS DANS MA VIE

À TOUS MES ENSEIGNANTS PENDANT MON CURSUS QUE JE NE REMERCIERAIS JAMAIS ASSEZ

A TOUTE LA PROMOTION 2010.

YASSINE

DEDICACES

Je voudrais dédier cet humble travail

à toute ma famille, a ma chère maman et mon cher père qui m'ont soutenu et encourager.

A mon binôme Yassine.

A mes frères.

A ma sœur.

A mes neveux.

A mes nièces.

A mes amis.

A tous ceux qui m'aiment.

AMINE

Introduction générale

INTRODUCTION GENERALE

Sonatrach, l'une des plus grandes entreprises internationales de produits énergétiques et pétrochimiques au monde a entrepris au cours des dernières années une transformation majeure dans l'ensemble de l'entreprise.

L'implantation d'un environnement de travail commun COE fondé sur les technologies Microsoft, EMC, Cisco, HP, ... en constitue l'un des principaux éléments.

Le standard COE (Common Operating Environment) est une **norme interne** à la Sonatrach qui doit permettre la rationalisation de son infrastructure informatique.

Aujourd'hui, le Système d'information de l'entreprise est devenu un véritable outil de compétitivité. L'entreprise est ainsi connectée en permanence, à travers des sites Internet et Extranet, avec ses clients, ses partenaires et ses sous-traitants. En interne ses employés accèdent ou, afin de pouvoir prendre en temps réel les bonnes décisions.

L'accélération des progrès technologiques a ainsi vu naître de nouvelles applications particulièrement gourmandes en bande passante telles les applications « Peer-to-Peer » et les applications multimédia (Vidéo Streaming, Visioconférence). Venant s'intégrer dans un paysage déjà pourvu d'un grand nombre d'autres services de bases tels que la messagerie, le partage de fichier ou encore l'impression en réseau, elles viennent perturber le fonctionnement sur le réseau d'applications parfois plus stratégiques (Citrix, SAP, ...).

Cette situation engendrée par des problèmes de congestion sur les réseaux, crée une insatisfaction des utilisateurs qui ne peut être résolue qu'en intégrant dans les réseaux des mécanismes permettant, à tout instant, d'offrir aux trafics prioritaires et aux trafics à contraintes de délai de transit, la part de bande passante et les temps de réponse qui leur sont nécessaires. En effet, Comme tous les administrateurs réseau le savent, un réseau est fragile et on peut faire le constat suivant :

- Les utilisateurs : « ça ne marche pas ! »
- Les responsables du réseau : « c'est l'Application ! »

- Les responsables des applications : « c'est le Réseau ! »

L'objectif est donc de concevoir et réaliser une application surveillant continûment le réseau et qui nous permettra de comprendre son comportement.

En effet, le but est de permettre à un administrateur réseau de :

- Visualiser les principales valeurs critiques en manière de performances locales
- Analyser les nouvelles applications et leur impact sur le réseau.
- Réduction des pics de trafic WAN.
- Diagnostique les lenteurs réseau grâce à des reporting.
- Détection du trafic WAN non autorisé et d'anomalies et d'évènements de sécurité.
- D'éviter les goulots d'étranglement de la bande passante et serveurs.
- Déterminer quelles applications accaparent le plus la bande passante, qui les utilisent et quand.
- Validation des paramètres de QoS (qualité de service).
- Contrôle du Flux d'un réseau.

Présentation

PRESENTATION

1. Présentation de l'organisme d'accueil

Sonatrach est la compagnie algérienne de recherche, d'exploitation, de transport par canalisation, de transformation et de commercialisation des hydrocarbures et de leurs dérivés. Elle intervient également dans d'autres secteurs tels que la génération électrique, les énergies nouvelles et renouvelables et le dessalement d'eau de mer. Elle exerce ses métiers en Algérie et partout dans le monde où des opportunités se présentent. [Son10]

2. Historique de l'entreprise national SONATRACH

L'entreprise nationale SONATRACH a été crée le 31.12.1963 son rôle principale était le développement du secteur des hydrocarbures. Les missions prérogatives de l'entreprise nationale SONATRACH ont été élargies le 22.9.1966. Ainsi sa mission s'étend à tous les domaines de l'industrie pétrolière, à savoir la recherche, la production, le transport, la transformation et la commercialisation des hydrocarbures.

Depuis le 24.02.1971, date de nationalisation des hydrocarbures l'entreprise a pris en charge l'ensemble du domaine minier et s'est vue confier le développement de toutes les branches de l'industrie pétrolière.

La SONATRACH est passé de 33 agents en 1964 à 103.000 à la fin des années 1980, pour assurer une meilleure gestion et améliorer les performances dans le cadre de la politique nationale de réorganisation de l'économie du pays, elle entreprend sa restructuration pour donner naissance à 17 entreprises industrielles de réalisation et de service.

Actuellement SONATRACH compte un effectif de 50.000 agents environ et conserve pour sa part la charge des opérations de recherche, de production, de transport par canalisation de traitement de conditionnement et de liquéfaction des hydrocarbures liquides et gazeux.

Dans le cadre de la restructuration des entreprises décidée en 1982 la SONATRACH a fait l'objet d'un découpage qui a donné naissance a d'autre entreprises ASMIDAL, NAFTAL ENPE, ENTP….etc. . Ce découpage a permis de

réduire l'effectif de la SONATRACH et de la ramener à 30.000 agents après ce découpage les taches de la SONATRACH se sont réduite. [Son10]

3. Mission principale de la SONATRACH

Sous l'autorité d'un Président Directeur Générale, la SONATRACH a notamment pour missions essentielles :

- Le développement, la conservation et la valorisation des réseaux énergétique sur tout le territoire national.
- La reconstitution et l'augmentation des réserves d'hydrocarbure.
- L'intensification des efforts d'exploitation et capitalisation des études réalisées dans ce domaine, pour une meilleure connaissance du sous-sol et la mise évidence des réserves d'hydrocarbures.
- La diversification des marchés et des produits destinés a l'exportation
- L'approvisionnement énergétique national à moyen terme, compte rendu de la réserve nationale.
- L'adaptation de l'outil commercial aux exigences du marché énergétique pour une meilleure maîtrise de ses mécanismes et des performances accrues.
- Le développement des techniques modernes de gestion national par le biais de la formation continue. [Son10]

4. Organigramme général de SONATRACH

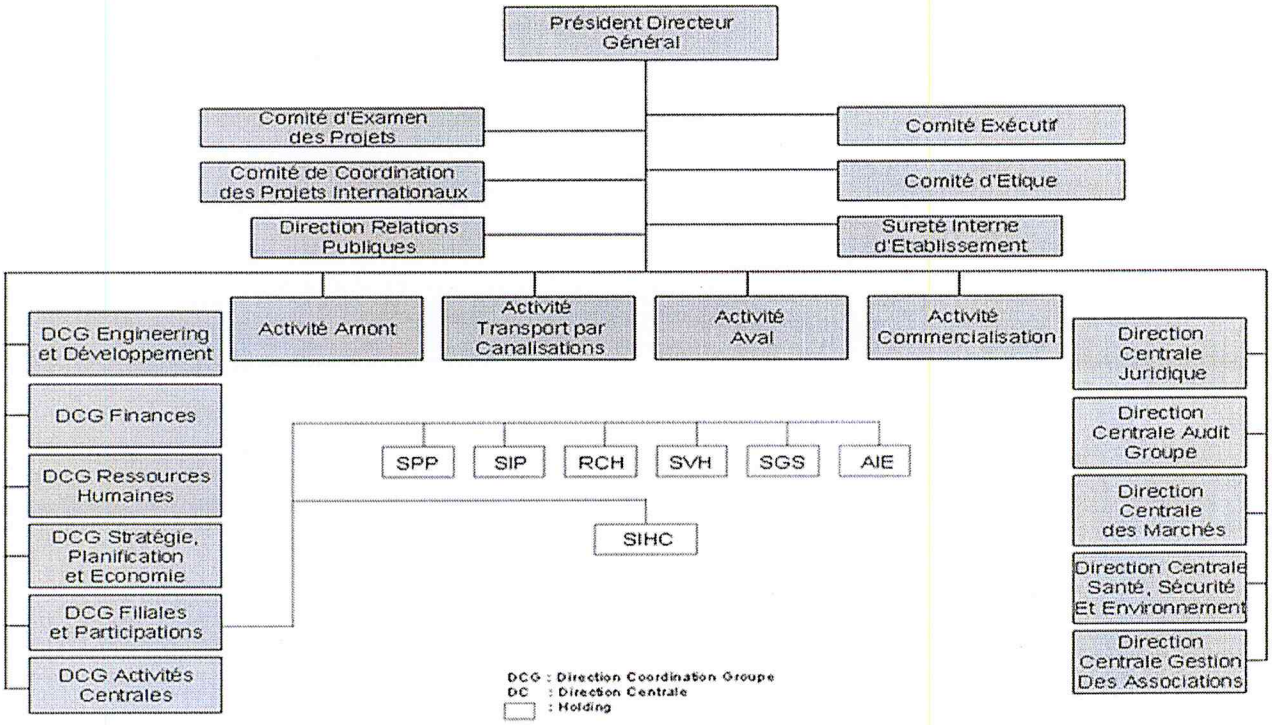


Fig.1 : Organigramme général de SONATRACH

4.1 Légende de l'organigramme général de SONATRACH

SIE : Sûreté Interne d'Etablissement.

SIHC : Holting International

AMT : Activité Amont

TRC : Transport par Canalisation

AVL : Activité Aval

RCH : Coordination général Ressources Humaines

COM : Direction de Communication

FIN : Coordination groupe Finances

ACT : Coordination groupe Activité Central

JUR : Direction Juridique

SPE : Coordination général Stratégie Planification et Economie

ADG : Direction Audit Groupe

HSE : Direction Santé Sécurité, Environnement. [Son10]

4.2 Organigramme d'ACT

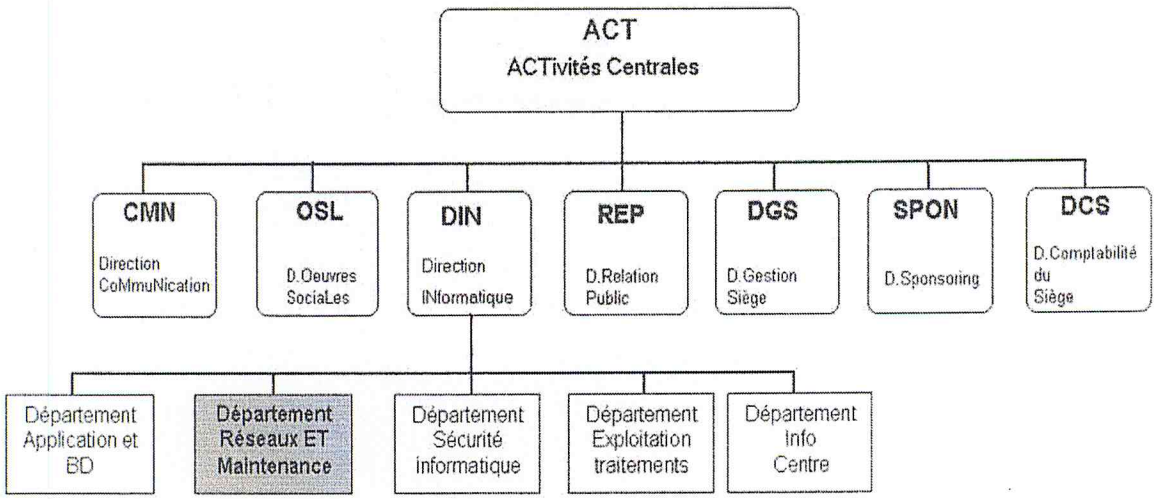


Fig.2 : Organigramme d'ACT

DCG : Direction Comptable Siège OSL : Direction Œuvres Sociales

DGS : Direction Gestion Siége DIN : Direction Informatique REP : Relation Publique [Son10].

5. Présentation de la Direction Informatique :

La Direction INformatique (DIN) est la direction de traitement principal de l'entreprise.

SONATRACH en matière informatique, elle constitue :

- L'outil prévisible de la Direction Générale en matière d'informatique
- Le centre de traitement des directions centrales

- Le prestataire de service qui indique les structures opérationnelles

La DIN n'exerce pas de tutelle directe sur les structures de l'entreprise en matière informatique, elle est interlocuteur de l'entreprise pour toutes relations en matières avec les organismes extérieures.

Son organisation repose sur les activités suivantes :

- La distribution fondamentale entre activités se réalisation de produits informatique et celles de leur utilisation
- Le regroupement en entités homogènes des activités de base pouvant intégrer des ensembles cohérents
- La dotation d'une autonomie de fonctionnement aux structures internes leur permettant la recherche de rentabilité
- La minimisation de la dépendance des structures internes par l'utilisation des équipements et logiciels adéquats
- La promotion continue de l'informatique par la mise à disposition des utilisateurs de compétences et de moyens adaptés
- La possibilité de prendre en charge la gestion des équipements informatique des structures opérationnelles qui seraient confiées. [Son10]

5.1. Mission de la DIN :

La DIN a pour mission :

- Les prestations de service informatique aux structures de l'entreprise
- La réalisation et la mise en place du système d'information
- L'assistance à toutes les structures de l'entreprise a des actions de :
  - Développement de l'information
  - Choix du matériel informatique
  - Réalisation des systèmes d'information
  - Maintenance des équipements
  - La sous-traitance de certaines prestations informatiques au profit des centres de traitements de l'entreprise [Son10].

5.2 Organigramme de la direction informatique :

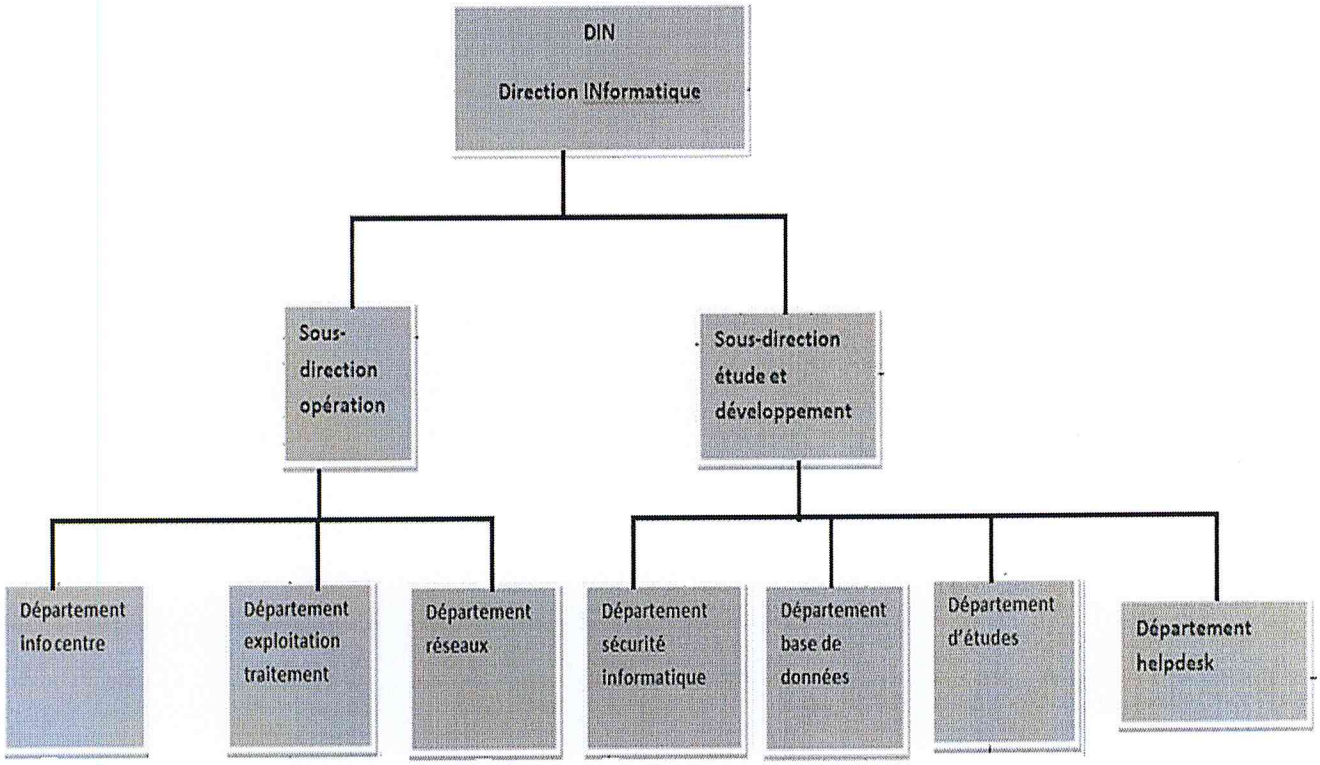


Fig.3 : Organigramme de la direction informatique. [Son10]

CHAPITRE I :

Les notions réseau

CHAPITRE I : LES NOTIONS RESEAUX

INTRODUCTION

Un réseau (Network) est un ensemble d'ordinateurs et périphériques interconnectés. Il permet de faire circuler des données informatiques et ainsi d'échanger du texte, des images, de la vidéo ou du son entre chaque équipement selon des règles et protocoles bien définis. [ADN10]

Intérêt du réseau

- Le partage des fichiers et des périphériques, imprimantes et applications
- La communication entre personnes grâce au courrier électronique, vidéo conférence...
- La communication entre processus.
- La garantie de l'unicité de l'information (bases de données)
- Les jeux en réseau ou sur Internet ...
- Les réseaux permettent aussi de standardiser le développement des applications. [ADN10].

Les avantages:

- Diminution des coûts grâce aux partages des données et des périphériques
- Standardisation des applications
- Accès aux données en temps utile
- Communication et organisation plus efficace. [ADN10].

I.1 LAN

I.1.1 Qu'est-ce qu'un réseau local ?

LAN signifie, Local Area Network (en français Réseau Local). Appelé aussi réseau local d'entreprise ou Privé, Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et souvent reliés entre eux grâce à la technologie la plus répandue, l'Ethernet. Avec à ce type de réseau, l'entreprise ou l'organisation dispose d'un système qui lui permet :

- Le partage des données.
- L'accès aux Ressources du réseau (imprimantes, serveurs)
- L'accès aux applications disponibles sur le réseau (logiciel)

Un réseau local relie des ordinateurs et des périphériques tels que des unités de stockages ou des imprimantes à l'aide de support de transmission par câble (coaxial ou paire torsadée) ou radio fréquences sans fil sur une circonférence d'une centaine de mètres. Au-delà, on considère que le réseau fait partie d'une autre catégorie de réseau appelé (MAN - Metropolitan Area Network), pour laquelle les supports de transmission sont plus adaptés aux grandes distances....[ADN10].

I.1.2 Réseau Local (Ethernet)

La technologie Ethernet utilise le protocole d'accès connu sous le nom de CSMA/CD (Carrier Sense, Multiple Access with Collision Détection). Lorsqu'un équipement sur le réseau cherche à émettre des données, il écoute d'abord l'activité du réseau (par une mesure de la tension électrique), afin de s'assurer qu'aucune autre station n'utilise déjà le réseau. Si le réseau est inutilisé, l'équipement peut alors transmettre une trame dans le cas contraire, il attend un temps aléatoire puis réessaye.

Lorsque deux stations émettent en même temps, une collision se produit et les deux trames sont détruites. Toutes les stations reçoivent alors un signal pour les prévenir. Les deux stations émettrices attendent alors un temps aléatoire avant de retransmettre à nouveau les données. Plus il y a d'élément dans un réseau, plus le nombre de collisions augmente.

L'un des avantages du commutateur par rapport au concentrateur est d'émettre vers le port de la station destinatrice, permettant ainsi la segmentation des collisions... [ADN10].

I.2 MAN

Ce type de réseau est apparu relativement récemment et peut regrouper un petit nombre de réseau locaux au niveau d'une ville ou d'une région. L'infrastructure

peut être privée ou publique. Par exemple, une ville peut décider de créer un 'MAN' pour relier ses différents services disséminés sur un rayon de quelques kilomètres et en profiter pour louer cette infrastructure à d'autres utilisateurs. La bande-passante peut être de quelques centaines de kbits/s à quelques Mbits/s. [ADN10].

I.3 WAN

Ce type de réseau permet l'interconnexion de réseaux locaux et métropolitains à l'échelle de la planète, d'un pays, d'une région ou d'une ville. L'infrastructure est en général publique (PTT, Télécom etc.) et l'utilisation est facturée en fonction du trafic et/ou en fonction de la bande-passante réservée, pour les lignes louées (une ligne louée est réservée exclusivement au locataire, 24h sur 24, pour la durée du contrat).Les modems sont un des éléments de base des WANs. La bande-passante va de quelques kbits/s à quelques Mbit/s. Une valeur typique pour une ligne louée est de 64kbits/s (en fonction des services offerts). [ADN10].

Architecture Client Serveur

Les deux types de réseaux les plus fréquents sont :

- Le réseau local sans serveur, connexion de poste à poste.
- Les réseaux organisés autour d'un serveur (Client/serveur).

Ces deux types de réseau ont des capacités différentes.

Serveurs : application spécialisés dans la fourniture et le stockage des ressources partagées des utilisateurs du réseau

Clients : application qui accèdent aux ressources partagées fournies par un serveur du réseau. [ADN10].

I.4 VLAN

I.4.1 Qu'est-ce qu'un VLAN (Réseau local virtuel)

Réseau dans le cadre duquel la segmentation des groupes ou domaines n'est pas contrainte par des éléments physiques ou géographiques mais par une configuration logique avec l'aide de matériel et logiciel spécifiquement conçu pour le VLAN. [ADN10].

I.4.2 Le principe du VLAN

Indépendamment de la localisation géographique sur le réseau, les stations peuvent communiquer comme si elles étaient sur le même segment. Un VLAN est assimilable à un domaine de diffusion (Broadcast Domain). Ceci signifie que les messages de diffusion émis par une station d'un VLAN ne sont reçus que par les stations de ce VLAN.

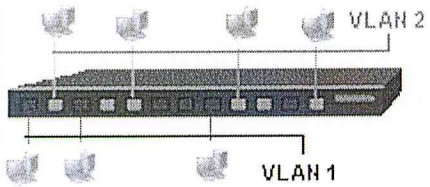
Les VLAN n'ont été réalisables qu'avec l'apparition des commutateurs. Auparavant, pour constituer des domaines de diffusion, il était nécessaire de créer des réseaux physiques, reliés entre eux par des routeurs, cette obligation liée à la localisation géographique des stations était contraignante pour l'administrateur réseau. Les VLAN ont révolutionné le concept de segmentation des réseaux, ils permettent de constituer autant de réseaux logiques que l'on désire sur une seule infrastructure physique, réseaux logiques qui auront les mêmes caractéristiques que des réseaux physiques.[ADN10].

Il existe plusieurs méthodes de construction des VLAN:

- par port (niveau 1)
- par adresse IEEE (niveau 2)
- par protocole (niveau 3)
- par sous réseau (niveau 3)

I.4.2.1 VLAN par port

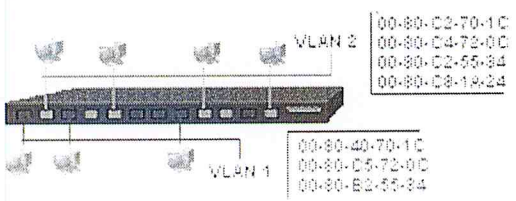
Un VLAN par port, aussi appelé VLAN de niveau 1 (pour physique), est obtenu en associant chaque port du commutateur à un VLAN particulier. C'est une solution simple, qui a été rapidement mise en œuvre par les constructeurs. Les premiers VLAN ne permettaient pas de créer un même réseau sur plusieurs commutateurs.



Depuis une nouvelle génération de commutateurs permet de le réaliser, grâce à l'échange d'informations entre les commutateurs et au marquage des trames. Les VLAN par port manquent de souplesse, tout déplacement d'une station nécessite une reconfiguration des ports. De plus, toutes les stations reliées sur un port par l'intermédiaire d'un même concentrateur, appartiennent au même VLAN. [ADN10].

I.4.2.2 VLAN par adresse IEEE

Un VLAN par adresse IEEE, ou VLAN de niveau 2 est constitué en associant les adresses MAC des stations à chaque VLAN. L'intérêt de ce type de VLAN est surtout l'indépendance de la localisation. La station peut être déplacée, son adresse physique ne changeant pas, il est inutile de reconfigurer le VLAN.



Les VLAN configurables avec l'adresse MAC sont bien adaptés à l'utilisation de stations portables. La configuration peut s'avérer fastidieuse car elle nécessite de

renseigner une table de correspondance avec toutes les adresses MAC et elle doit être partagée par tous les commutateurs. [ADN10].

I.4.2.3 VLAN par protocole

Un VLAN par protocole, ou VLAN de niveau 3, est obtenu en associant un réseau virtuel par type de protocole du réseau. On peut ainsi constituer un réseau virtuel pour les stations communiquant avec le protocole TCP/IP, et un autre pour les stations communiquant avec le protocole IPX... Dans ce type de VLAN, les commutateurs apprennent la configuration. Par contre, elle est légèrement moins performante car les commutateurs doivent analyser des informations. [ADN10].

I.4.2.4 VLAN par sous-réseau

Également appelé VLAN de niveau 3, un VLAN par sous réseau utilise les adresses IP. Un réseau virtuel est associé à chaque sous réseau IP. Dans ce cas, les commutateurs apprennent la configuration et il est possible de changer une station de place sans reconfigurer le VLAN. Cette solution est l'une des plus intéressantes, malgré une petite dégradation des performances de la commutation due à l'analyse des informations. [ADN10].

I.4.3 Le marquage des trames

Le marquage permet de reconnaître les trames. L'appartenance à tel ou tel VLAN peut être déduite des informations contenues dans la trame (adresse IEEE, protocole...) ou insérée dans cette trame.

Plusieurs solutions constructeurs ont été proposées telles Virtual Tag Trunking de 3Com ou encore Inter Switch Link Protocol de Cisco, toutes incompatibles entre elles. Pour cette raison, l'IEEE a défini une norme VLAN sous la référence 802.1Q.[ADN10].

I.4.4 Les avantages du VLAN

- Réduction de la diffusion du trafic
- Création de groupes de travail sans remise en cause de l'infrastructure physique

- Contrôle des échanges entre les différents VLAN.

Les messages de diffusion (broadcast) sont limités à l'intérieur de chaque VLAN. Les broadcasts d'un serveur peuvent être limités aux clients de ce serveur. Le membre d'un groupe peut se déplacer sans changer de réseau virtuel. Les échanges inter VLAN se réalisent tout comme pour tous les échanges inter réseaux, à travers des routeurs. [ADN10].

I.5 Le modèle OSI

Introduction

Lorsque les réseaux informatiques ont pris de l'importance, l'ISO(International Standards Organisation) et l'UIT_T (International Télécommunications Union - anciennement CCITT) ont décidé de créer un modèle de base pour décrire les différentes fonctions que doit remplir un réseau. Ce modèle, baptisé modèle OSI (Open System InterConnect), est basé sur le principe suivant : les fonctions remplies par un système de télécommunication sont segmentées en couches permettant de diviser l'ensemble des fonctions en modules, possèdent chacun une tâche bien définie. Chaque couche excepté la couche la dernière se sert des fonctions remplies par les couches inférieures pour remplir sa propre fonction.[ADN10].

I.5.1 Les fonctions ont été divisées en sept couches

Couches Hautes	logiciel	Application	FTP, NNTP, DNS, SNMP, SMTP, POP3, IMAP, IRC, HTTP, VoIP...	7
	Cryptage & Compression	Présentation	SMB, ASCII, UUCP, NCP, AFP, SSP...	6
	DNS & Transaction	Session	NetBios, AppleTalk, Telnet...	5
Couches Basses	Datagramme	Transport	TCP, UDP, RTP, SPX...	4
	Paquet / routeur	Réseau	IPV4, IPV6, NetBEUI, ICMP, IPX, RIP....	3
	Trame / pont	Liaison	Connexion, Déconnexion, Ethernet, CSMA/CD et CA, PPP, ARP, Token...	2
	Bit	Physique	Modem, Multiplexeur	1

Tab I.1 : Les fonctions des sept couches OSI

L'OSI est un modèle de base normalisé par l'International Standard Organisation (ISO).

▪ Fonctions des sept couches

- **Niveau 7 (application)**: gère le format des données entre logiciels.
- **Niveau 6 (présentation)**: met les données en forme, éventuellement de l'encryptage et de la compression, par exemple mise en forme des textes, images et vidéo.
- **Niveau 5 (session)**: gère l'établissement, la gestion et coordination des communications
- **Niveau 4 (transport)**: s'occupe de la gestion des erreurs, notamment avec les protocoles UDP et TCP/IP
- **Niveau 3 (réseau)**: sélectionne les routes de transport (routage) et s'occupe du traitement et du transfert des messages: gère par exemple les protocoles IP (adresse et le masque de sous-réseau) et ICMP. Utilisé par les routeurs et les switchs mangeables.
- **Niveau 2 (liaison de données)**: utilise les **adresses MAC**. Le message Ethernet à ce stade est la trame, il est constitué d'un en-tête et des informations. L'en-tête reprend l'adresse MAC de départ, celle d'arrivée + une indication du protocole supérieur.
- **Niveau 1 (physique)**: gère les connections matérielles et la transmission, définit la façon dont les données sont converties en signaux numériques: ça peut-être un câble coaxial, paires sur RJ45, onde radio, fibre optique, ...

A chacun de ces niveaux du modèle OSI, on encapsule un en-tête et une fin de trame (message) qui comporte les informations nécessaires en suivant les règles définies par le protocole réseau employé. Le protocole est le langage de communication (la mise en forme) utilisé pour le transfert des données (actuellement TCP/IP mais d'autres ont été utilisés comme NetBeui (antérieur à Windows 98), Novell IPX, ...). Sur le graphique ci-dessous, la partie qui est rajoutée à chaque couche est sur fond blanc. La partie en grisée est celle obtenue après encapsulation (intégration) du niveau précédent.

La dernière trame, celle qu'on obtient après avoir encapsulé la couche physique, est celle qui sera envoyée sur le réseau.[ADN10].

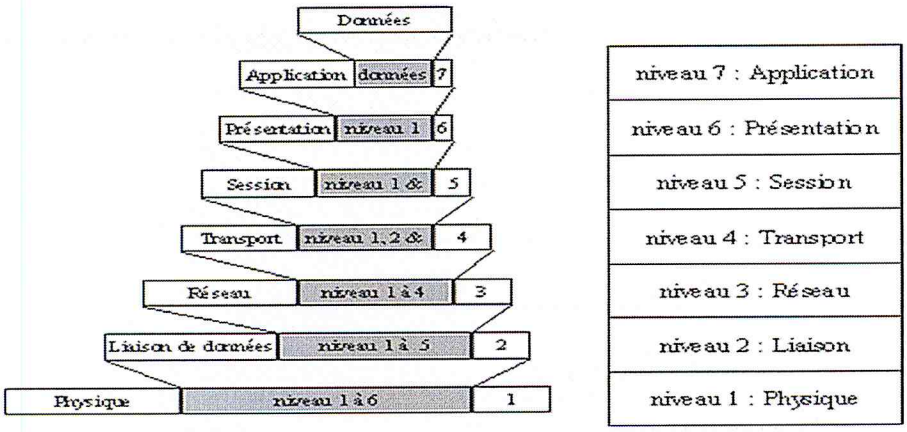


Fig. I.1 : Les sept couches OSI

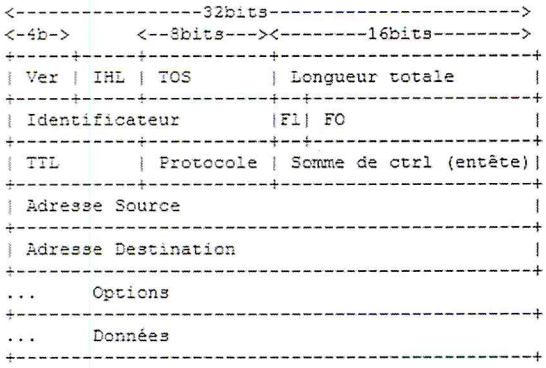
I.6 Les paquets réseau

Regroupement logique d'information comportant un en-tête qui contient l'information de contrôle et (habituellement) les données de l'utilisateur. Le terme paquets est le plus souvent utilisé pour désigner les unités de données au niveau de la couche réseau. Les termes datagramme, trame, message et segment sont aussi utilisés pour décrire des regroupements logiques d'information à différentes couches du modèle de référence OSI ainsi que dans divers cercles technologiques. [ADN10].

I.6.1 Quelques formats de paquets réseau

Comme il était défini un paquet est une unité de transmission utilisée pour communiquer donc le format d'un paquet à un rapport avec le type de protocole avec qui on communique, voici quelques exemples de protocoles usuels avec leur format de paquets :

- **Les paquets IP**

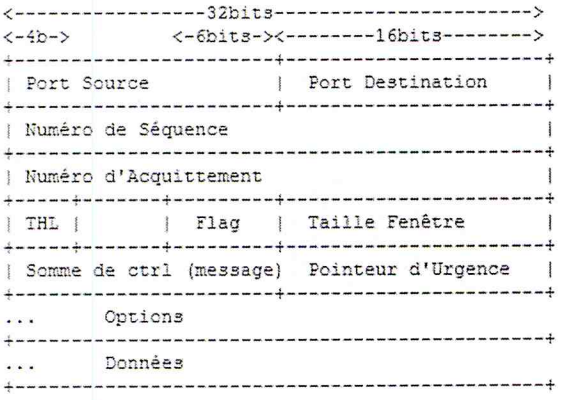



```
Ver = Version d'IP
IHL = Longueur de l'en-tête IP (en mots de 32 bits)
TOS = Type de service
Longueur totale du paquet IP (en octets)
Fl (3 premiers bits) = indicateurs pour la fragmentation
 * 1er = Reservé
 * 2me = Ne pas fragmenter
 * 3me = Fragment suivant existe
FO (13 bits suivants) = Décalage du fragment
 * valeur a multiplier par 8 octets
TTL = Durée de vie restante

Quelques protocoles transportés :
        1 = ICMP                 8 = EGP
        2 = IGMP                11 = DoP
        4 = IP (encapsulation)  17 = UDP
        5 = Stream              36 = XTP
        6 = TCP                 46 = RSVP
```

Fig. I.2 : Format d'un paquet IP

- **Les paquets TCP**




```
THL = Longueur de l'entête TCP sur 4 bits (*32bits)
Flags = indicateur codé sur les 6 bits de droite
        (du plus faible au plus fort)
        * 0 = Fin
        * 1 = Synchronisation (SYN)
        * 2 = Réinitialisation (Reset)
        * 3 = Données immédiates (Push)
        * 4 = Acquittement (ACK)
        * 5 = Données urgentes

Options = suites d'option codées sur
 * 1 octet à 00 = Fin des options
 * 1 octet à 01 = NOP (pas d'opération)
 * plusieurs octets de type TLV
   T = un octet de type:
     2 Négociation de la taille max. du segment
     3 Adaptation de la taille de la fenêtre
     4 Autorisation des acquittements sélectifs
     8 Estampilles temporelles
   L = un octet pour la taille totale de l'option
```

Fig. I.3 : Format d'un paquet TCP

- **Paquets UDP**

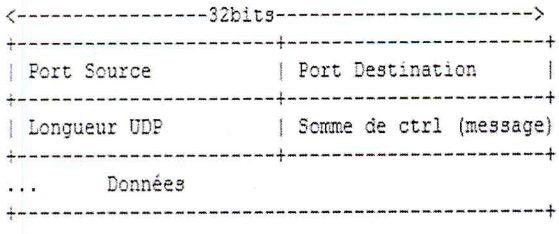


Fig. I.4 : Format d'un paquet UDP

- **Paquets ICMP**

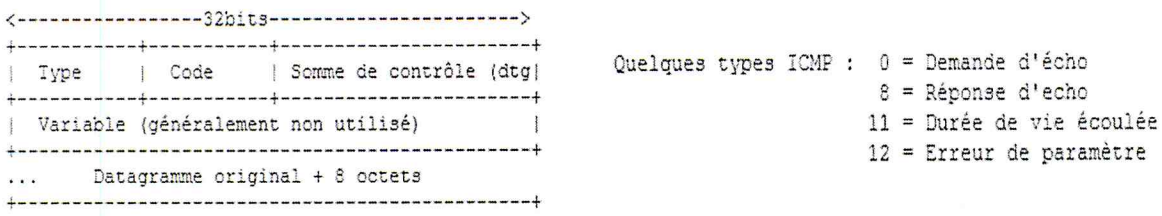


Fig. I.5 : Format d'un paquet ICMP

- **Structure de la trame Ethernet**

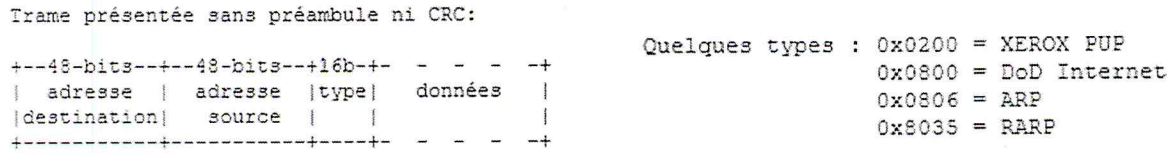


Fig. I.6 : Format d'une trame Ethernet

I.7 Les protocoles réseau

I.7.1 Qu'est-ce qu'un protocole de communication ?

Un protocole est une spécification standard qui permet la communication entre deux équipements. Ce sont des règles et des procédures qui définissent le type de codage et la vitesse utilisé pendant la communication, ainsi que la façon d'établir et de terminer la connexion.[ADN10].

I.7.2 Les 2 modes de communication

1) **Mode non connecté, non fiable**, avec lequel l'expéditeur envoie des paquets au destinataire sans établir de connexion et sans garantie que les paquets arrivent au destinataire. Utilisé essentiellement pour le DNS.[ADN10].

2) **Mode connecté, fiable**, avec lequel l'expéditeur et le destinataire établissent une connexion fiable avant tout transfert de données .Utilisé pour des commandes telles que net use, Net View, Net Start...

I.7.3 Liste des protocoles

ARP: Niveau 2 de la couche OSI, (Address Resolution Protocol) permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IPV4. Il se situe à l'interface entre la couche réseau 3 et la couche de liaison 2 du modèle OSI.[ADN10].

RARP: (Reverce Address Resolution Protocol). Inverse du protocole ARP, permet de connaître l'adresse IP correspondant à l'adresse physique d'une carte réseau.[ADN10].

CSMA/CA: (Carrier Sense Multiple Access with Collision Avoidance) Le protocole CSMA/CA tente d'éviter les collisions en imposant un accusé de réception systématique des paquets (ACK), ce qui signifie que pour chaque paquet de données arrivé intact, un paquet ACK est émis par la station de réception.[ADN10].

CSMA/CD: (Carrier Sense Multiple Access with Collision Detection).Signifie littéralement accès multiple par écoute de la porteuse avec détection de collisions. Cette méthode permet à une station d'écouter le support physique de liaison (câble ou fibre) pour déterminer si une autre station transmet des données. Si aucune transmission n'est détectée, la station qui écoute peut alors émettre. Néanmoins l'accès multiple fait que plusieurs stations peuvent émettre au même moment ce qui provoque une collision (donc une perte de données) Comme les stations écoutent aussi les collisions elles savent qu'elles doivent réémettre après avoir attendu pendant un délai aléatoire.[ADN10].

DHCP: Protocole qui permet à un ordinateur qui se connecte sur un réseau et d'obtenir dynamiquement une adresse IP. Le but principal étant la simplification de l'administration du réseau. (Dynamic Host Configuration Protocol).[ADN10].

On considère le protocole DHCP comment distribuant des adresses IP, mais il a été conçu à l'origine comme complément au protocole BOOTP(Boot strap Protocol) qui est utilisé lorsque l'on installe une machine(de type terminal) à travers un réseau. Les versions actuelles desserveurs DHCP fonctionnent pour IPv4. Une spécification pour IPv6 est encours de développement par l'IETF.[ADN10].

HTTP:Niveau 7 de la couche OSI, (HyperText Transfert Protocol) Protocole permettant le transfert de fichiers (essentiellement au format HTML) localisé grâce à une chaîne de caractères appelée URL.[ADN10].

HTTPS: HyperText Transfer Protocol Secure, protocole de transmission issu de Netscape lié à une connexion par socket sécurisée. C'est du http avec une pincée de SSL (Secure Socket Layer).[ADN10].

ICMP: Niveau 3 de la couche OSI, (Internet Control Message Protocol).Protocole qui permet de gérer les informations relatives aux erreurs des machines connectées. Il ne permet pas de corriger ces erreurs mais il en fait part aux protocoles des couches voisines. Les routeurs utilisent ICMP pour signaler les erreurs (Delivery Problem).[ADN10].

POP: Niveau 7 de la couche OSI, (Post office Protocole) Protocole qui permet de recevoir le courrier électronique (email).[ADN10].

IMAP (Internet Message Access Protocol) : est un protocole qui permet de récupérer les courriers électroniques sur des serveurs de messagerie. Son but est donc similaire à POP3, l'autre principal protocole de relève du courrier. Mais contrairement à ce dernier, il a été conçu pour permettre de laisser les messages sur le serveur. [ADN10].

SMTP: Niveau 5/6/7 de la couche OSI, (Simple Mail Transfert Protocol.)Protocole qui permet d'envoyer du courrier électronique (email).[ADN10].

SNMP: Niveau 3 de la couche OSI, (Simple Network Management Protocol) Protocole qui permet aux administrateurs réseau de gérer les équipements du réseau.[ADN10].

TCP/IP: Niveau 4 & 3 de la couche OSI, Il signifie (Transmission Control Protocol / Internet Protocol) Grâce à Internet, TCP/IP est le plus célèbre des protocoles, il est basé sur le repérage de chaque ordinateur par une adresse IP.[ADN10].

TCP: Niveau 4 de la couche OSI,(Transmission Control Protocol) Permet de remettre en ordre les data grammes en provenance du protocole IP, de vérifier le flot

de données afin d'éviter une saturation du réseau, de formater les données en segments de longueur variable afin de les remettre au protocole IP, de multiplexer les données, c'est-à-dire de faire circuler simultanément des informations provenant de sources distinctes sur une même ligne et il permet enfin l'initialisation et la fin d'une communication.[ADN10].

IP: Niveau 3 de la couche OSI, (Internet Protocol) C'est un des protocoles les plus importants d'Internet car il permet l'élaboration et le transport des datagrammes IP (les paquets de données).[ADN10].

Telnet: Niveau 5/6/7 de la couche OSI, (Cet utilitaire permet l'utilisation de programmes sur des machines distantes, via un réseau de type Internet) Protocole standard permettant l'interfaçage de terminaux et d'applications.[ADN10].

SSH (Secure Shell) : est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite toutes les trames sont chiffrées. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur. [ADN10].

UDP: Niveau 4 de la couche OSI, (User Datagram Protocol) Le User Datagram Protocol offre seulement un service de transport minimal. Protocoles non orientés connexion, il envoie des données sans prévenir la machine réceptrice, et la machine réceptrice reçoit les données sans envoyer d'avis de réception à la première. Les données sont ainsi envoyées sous forme de blocs (datagrammes). Ce protocole est utilisé pour les résolutions DNS et aussi pour FTP.[ADN10].

URL:*Niveau 7 de la couche OSI, (Uniform Resource Locatore) Adresse des pages Internet exploitée par les navigateurs (Explorer, Netscape...)[ADN10].

I.8 L'adressage IPV4

Chaque hôte TCP/IP est identifié par une adresse IP logique. Cette adresse est unique pour chaque hôte qui communique via TCP/IP. Chaque adresse IP de 32 bits identifie un emplacement d'un système hôte sur le réseau de la même façon qu'une adresse de rue identifie une maison dans une ville.

De la même façon qu'une adresse de rue à un format standard en deux parties "un nom de rue et un numéro de maison", chaque adresse IP est séparée en deux parties : un ID de réseau et un ID d'hôte : L'ID de réseau, également appelé adresse de réseau, identifie.

Un segment de réseau unique dans un réseau d'interconnexion TCP/IP plus grand. Tous les systèmes associés au même réseau et partageant l'accès à ce réseau ont un ID de réseau commun dans leur adresse IP complète Cet ID est également utilisé pour identifier de manière unique chaque réseau dans le réseau d'interconnexion le plus grand.

L'ID d'hôte, également appelé adresse d'hôte, identifie un nœud TCP/IP (une station de travail, un serveur, un routeur ou un autre périphérique TCP/IP) dans chaque réseau. L'ID d'hôte de chaque périphérique identifie un seul système dans son propre réseau.

Voici un exemple d'adresse IP de 32 bits : 10000100 01101011000010000011001001. Pour faciliter l'adressage IP, les adresses sont exprimées en notation décimale pointée. L'adresse IP de 32 bits est segmentée en quatre octets de 8 bits. Les octets sont convertis en décimales (système de numérotation base 10) et sont séparés par des points. C'est la raison pour laquelle, dans l'exemple précédent, l'adresse IP est 132.107.16.201une fois convertie en notation décimale pointée.

L'illustration suivante présente un exemple de vue d'une adresse IP(132.107.16.201) telle qu'elle est divisée dans les sections de réseau et d'ID d'hôte. La partie d'ID de réseau (132.107) est signalée par les deux premiers nombres de l'adresse IP. La partie d'ID d'hôte (16.201) est signalée par les deux derniers nombres de l'adresse IP. [ADN10].

I.8.1 Classes d'adresses IP

La communauté de l'Internet a défini cinq classes d'adresses. Les adresses Classe A, B et C sont utilisées pour une affectation aux nœudsTCP/IP.

La classe d'adresse définit quels bits sont utilisés pour le réseau ainsi que les parties d'ID d'hôte de chaque adresse. La classe d'adresse définit également le nombre de réseaux et d'hôtes qui peuvent être pris en charge par réseau. Le tableau suivant utilise w.x.y.z pour indiquer les quatre valeurs d'octet d'une adresse IP donnée.[ADN10].

Ce tableau est utilisé pour présenter les éléments suivants :

Comment la valeur du premier octet (w) d'une adresse IP donnée, indique la classe de l'adresse.

Comment les octets d'une adresse sont divisés en ID de réseau et en ID d'hôte.

Le nombre de réseaux et d'hôtes possibles par réseau disponible pour chaque classe.

Classe	Valeur de W	ID réseau	ID hôte	Nb réseaux	Nb hôtes réseau
A	1 – 126	w	x.y.z	$2^7 - 2/126$	$2^{24} - 2/16777214$
B	128 - 191	w.x	y.z	$2^{14}/16384$	$2^{16} - 2/65534$
C	192 - 223	w.x.y	z	$2^{21}/2097152$	$2^8 - 2/254$
D	224 - 239	Réservé pour un adressage multi destinataire			
E	240 - 254				

Tab I.2 : Tableau d'adressage IP

Adresses pour réseau privé uniquement:

Classe A: 10.0.0.1 / 10.255.255.255

Classe B: 172.16.0.1 / 172.31.255.255

Classe C: 192.168.0.1 / 192.168.255.255

I.8.2 Les Masques de sous réseau

Dans tous les cas, le masque de réseau sert à identifier la partie de l'adresse IP correspondant au réseau et la partie correspondant à l'hôte. En effet, l'adresse du réseau est calculée simplement en faisant un ET logique entre l'adresse IP et le masque de réseau.[ADN10].

Pour cela, il faut traduire l'adresse décimale en binaire, puis faire le ET logique en respectant la table suivante:

0 et 0 = 0/0 et 1 = 0 / 1 et 0 = 0 / 1 et 1 = 1.

Chaque classe d'adresses possède son masque par défaut :

A : 255.0.0.0

B : 255.255.0.0

C : 255.255.255.0

I.9 Les Ports

De nombreux programmes TCP/IP peuvent être exécutés simultanément sur Internet (vous pouvez par exemple ouvrir plusieurs navigateurs simultanément ou bien naviguer sur des pages HTML tout en téléchargeant un fichier par FTP). Chacun de ces programmes travaille avec un protocole, toute fois l'ordinateur doit pouvoir distinguer les différentes sources de données. Ainsi, pour faciliter ce processus, chacune de ces applications se voit attribuer une adresse unique sur la machine, codée sur 16 bits: un port (la combinaison *adresse IP* + *port* est alors une adresse unique au monde, elle est appelée socket).L'adresse IP sert à identifier de

façon unique un ordinateur sur le réseau tandis que le numéro de port indique l'application à laquelle les données sont destinées.

De cette manière, lorsque l'ordinateur reçoit des informations destinées à un port, les données sont envoyées vers l'application correspondante. S'il s'agit d'une requête à destination de l'application, l'application est appelée application serveur. S'il s'agit d'une réponse, on parle alors d'application cliente. [ADN10].

I.10 Le routage

I.10.1 Qu'est-ce qu'un routeur ?

Les hubs et switchs ne gèrent que les transferts entre équipements dans la même classe d'adresse IP d'un même sous-réseau. Chaque équipement du LAN reçoit une adresse unique de type X.X.X.X, par exemple 192.168.1.1. Les valeurs X varient de 0 à 255. L'adresse IPV4 est constituée de 32 bits et d'un masque également codé sur 32 bits. Un routeur analyse les trames pour récupérer l'entête (adresses de destination et de départ) et permet de transférer les données entre des réseaux de classes d'adresses différentes. Il détermine également des routes (le routage) pour communiquer avec d'autres routeurs qui ne sont pas directement connectés dessus.

Il travaille sur la couche réseau (couche 3 du modèle OSI) et dissocie deux réseaux entre deux en filtrant les informations pour ne transmettre que ce qui est effectivement destiner au réseau suivant. Les données transitant sur le réseau local (pas Internet) restent à l'intérieur du LAN.

Comme les adresses des sites INTERNET sont dans des classes différentes de votre ordinateur en réseau local, la connexion d'un réseau LAN à INTERNET utilise obligatoirement un routeur.

De plus, les routeurs permettent en partie de masquer les ordinateurs du réseau interne en ne reprenant pour l'extérieur d'un seul équipement. Pour cela, il utilise le NAT (Network adress translation). Ce mécanisme utilise une table mémoire interne qui mémorise l'adresse de départ (l'ordinateur) et l'adresse de destination

(typiquement, l'adresse d'un site Internet). Le site ne revoit le résultat de la recherche que vers l'adresse externe du routeur. Le NAT va retransmettre les données au véritable destinataire. Le PAT (Port Adresse Translation) permet de rediriger les données au niveau des ports UDP et TCP/IP.

Les routeurs intègrent parfois un firewall hardware paramétrable et permettent notamment de bloquer certaines connexions Ethernet au niveau des ports TCP ou UDP. Ils sont utilisés pour interfacer différents groupes de PC (par exemple les départements) en assurant un semblant de sécurité. Certains switchs manageables peuvent en partie être utilisé pour le blocage d'adresses IP dans une même classe d'adresse. La principale utilisation est le partage de connexion Internet. D'autres informations sur les méthodes de partage de connexion Internet sont reprises dans différents chapitres du cours INTERNET (par Windows, routeurs) mais aussi en utilisant des serveurs Windows 2003 - 2008 (cours sur les systèmes d'exploitation).

Les routeurs peuvent également servir de pont (Bridge en anglais) pour interconnecter deux réseaux locaux dans des classes d'adresses différentes.

Il n'est pas possible de relier directement 2 réseaux en branchant 2 cartes réseaux dans un PC central, sauf en utilisant un logiciel de liaison proxy (passerelle) de type Wingate ou les fonctions RRAS (Routing and Remote Access Services) implantées dans Windows serveur 2000 mais surtout en standard en Windows 2003 et 2008..

Un serveur DHCP (Dynamic Host Configuration Protocol) peut être implanté de manière software (serveurs Windows par exemple) ou dans un routeur.

Cette possibilité permet d'attribuer automatiquement les adresses IP à chaque station dans une plage d'adresse déterminée (dans la même classe d'adresse).

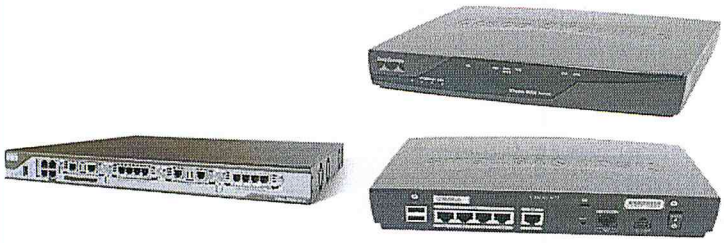


Fig. I.7 : Routeur

I.10.2 Qu'est-ce que le routage

Le routage est le processus de transmission de paquets entre des segments réseaux connectés. Chaque paquet entrant ou sortant est appelé paquet IP. Un paquet IP contient l'adresse source de l'hôte émetteur et l'adresse de destination de l'hôte destinataire. Les services de transport de l'hôte source transmettent les données sous la forme de segments TCP ou de messages UDP à la couche IP inférieure.

La couche IP crée des paquets IP à partir des informations d'adresses source et de destination permettant de router les données via le réseau. La couche IP transmet ensuite les paquets à la couche liaison inférieure, où les paquets IP sont convertis en trames en vue de leur transmission via un support de réseau physique. Ce processus se déroule en sens inverse sur l'hôte de destination.[ADN10].

I.10.3 Table de Routage (Routing Table)

Une table de routage est une liste contenant essentiellement trois types d'information : des adresses réseau avec le masque réseau associé et le moyen de les atteindre. Soit le réseau est directement connecté à l'appareil, dans ce cas le moyen de l'atteindre est le nom de l'interface, soit, il s'agit de l'adresse du prochain routeur situé sur la route vers ce réseau.[ADN10].

I.10.4 Structure de la table de routage

L'illustration suivante montre la structure de la table de routage.

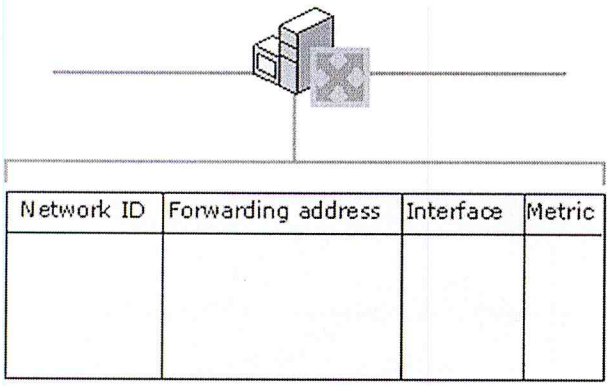


Fig. I.8 : Structure de la table de routage. [ADN10]

Chaque entrée de la table de routage comporte les champs d'information suivants :

- ID réseau ou adresse de réseau d'interconnexion pour un itinéraire hôte. Sur les routeurs IP, il existe un champ de masque de sous-réseau supplémentaire qui détermine l'ID du réseau IP à partir d'une adresse IP de destination.
- Adresse à laquelle le paquet est transmis. L'adresse de passerelle est une adresse matérielle ou une adresse de réseau d'interconnexion. Pour les réseaux auxquels l'hôte ou le routeur est directement rattaché, le champ adresse de passerelle peut correspondre à l'adresse de l'interface rattachée au réseau.
- Interface réseau utilisée lorsque des paquets sont transmis à l'ID réseau. Il peut s'agir d'un numéro de port ou de tout autre type d'identificateur logique.
- Métrique : Mesure relative au choix d'un itinéraire. En règle générale, la valeur métrique la plus faible correspond à l'itinéraire choisi. Si plusieurs itinéraires existent vers un réseau de destination donné, l'itinéraire dont la valeur métrique est la plus faible est utilisée. Certains algorithmes de routage ne stockent qu'un seul itinéraire vers un ID réseau dans la table de routage, même lorsqu'il existe plusieurs itinéraires. Dans ce cas, la valeur métrique est

utilisée par le routeur pour déterminer l'itinéraire à stocker dans la table de routage.[ADN10].

Exemple de table de routage :

Adresse réseau	Masque	Passerelle	Interface
200.50.62.0	255.255.255.0	200.50.62.2	200.50.62.2
200.50.63.0	255.255.255.0	200.50.63.2	200.50.63.2
200.50.64.1	255.255.255.255	200.50.64.2	200.50.64.2
0.0.0.0	0.0.0.0	200.50.64.1	200.50.64.2

Tab I.3 : Table de routage

I.10.5 Routage statique

La table routage est entrée manuellement par l'administrateur (pour de petits réseaux) Le routeur statique ne partage pas d'information avec les autres routeurs.[ADN10].

I.10.6 Routage dynamique

Le routeur construit lui-même sa table de routage en fonction des informations qu'il reçoit des protocoles de routage. Le routeur sélectionne la route la mieux adaptée à un paquet ou à un datagramme circulant sur le réseau. A la fin de chaque circuit, le routeur décide du chemin convenant le mieux en utilisant les informations d'état du réseau transmises d'un routeur à l'autre par des protocoles d'acheminement d'information.[ADN10].

I.10.7 Quelques commandes de routage

Route : Affiche et modifie les entrées dans la table de routage IP locale. Utilisée sans paramètres, la commande route permet d'afficher l'aide.[ADN10].

- **Syntaxe**

route [-f] [-p] [Commande [Destination] [mask Masque Sous Réseau][Passerelle][metric Métrique]] [if Interface]].

- **Paramètres**

/f

Supprime, dans la table de routage, toutes les entrées qui ne correspondent pas à des itinéraires hôtes (itinéraires avec le masque de sous réseau 255.255.255.255), à l'itinéraire réseau de bouclage (itinéraire avec la destination 127.0.0.0 et le masque de sous réseau255.0.0.0) ou une itinéraire multidiffusion (itinéraires avec la destination 224.0.0.0 et le masque de sous réseau 240.0.0.0). Lorsque cette commande est utilisée avec d'autres commandes (telles que add, change ou delete), le contenu de la table est supprimé avant l'exécution de la commande.[ADN10].

/p

Lorsque ce paramètre est utilisé avec la commande add, l'itinéraire spécifié est ajouté au Registre et permet d'initialiser la table de routage IP à chaque fois que le protocole TCP/IP est utilisé. Par défaut, les itinéraires ajoutés ne sont pas conservés lorsque le protocole TCP/IP est lancé. Associé à la commande print, ce paramètre affiche la liste des itinéraires persistants. Ce paramètre est ignoré pour toutes les autres commandes.[ADN10].

- **Commande** : Le tableau suivant présente la liste des commandes autorisées :

Commande	Action
route add	Ajoute un itinéraire.
route change	Modifie un itinéraire existant.
route delete	Supprime un ou plusieurs itinéraires.
route print	Imprime un ou plusieurs itinéraires.

Tab I.4 : commande routeur et leur action

- **Destination**

Spécifie la destination réseau de l'itinéraire. La destination peut être une adresse réseau IP dans laquelle les bits hôtes de l'adresse réseau sont définis à 0, une adresse IP pour un itinéraire hôte ou 0.0.0.0.pour l'itinéraire par défaut.[ADN10].

- **Masque**

Spécifie le masque de sous réseau associé à la destination réseau. Le masque de sous réseau peut être le masque de sous réseau approprié d'une adresse réseau IP, 255.255.255.255 pour un itinéraire hôte ou 0.0.0.0.pour l'itinéraire par défaut. Si ce paramètre est omis, le masque de sous réseau est 255.255.255.255. Étant donné la relation existant entre la destination et le masque de sous réseau dans la définition des itinéraires, la destination ne peut pas être plus spécifique que son masque de sous réseau correspondant. En d'autres termes, il est impossible de trouver un bit défini à 1 dans la destination si le bit correspondant dans le masque de sous réseau est défini à 0.[ADN10].

- **Passerelle**

Spécifie l'adresse de transmission ou le tronçon suivant de l'adresse IP par lequel il est possible d'atteindre les adresses définies par la destination réseau et le masque de sous réseau. Pour les itinéraires de sous réseaux liés localement, l'adresse de la passerelle correspond à l'adresse IP attribuée à l'interface liée au sous réseau. Pour les itinéraires distants, accessibles via un ou plusieurs routeurs, l'adresse de la passerelle est une adresse IP qu'il est possible d'atteindre directement et qui est attribuée à un routeur voisin.[ADN10].

- **Métrique**

Spécifie une métrique de coût exprimée par un nombre entier (compris entre 1 et 9999) pour l'itinéraire. Cette valeur est utilisée lorsqu'il est nécessaire de choisir parmi plusieurs itinéraires dans la table de routage qui correspondent le plus à l'adresse de destination d'un paquet en cours de transmission. C'est l'itinéraire dont la métrique est la plus faible qui est choisi. La métrique peut refléter le nombre de

tronçons, la vitesse permise par le chemin d'accès, la fiabilité et le débit du chemin d'accès ou les propriétés administratives.[ADN10].

- **If (Interface)**

Spécifie l'index d'interface permettant d'atteindre la destination. Pour obtenir la liste des interfaces et des index correspondants, utilisez la commande route <print>. Vous pouvez utiliser des valeurs décimales ou hexadécimales pour l'index d'interface. Si vous utilisez des valeurs hexadécimales, faites précéder la valeur de 0x. Si le paramètre if est omis, l'interface est déterminée à partir de l'adresse de la passerelle.[ADN10].

Remarque : /? : Affiche l'aide à l'invite de commandes.

I.10.8 Liste des protocoles de Routages dynamique

RIP: Protocole de routage - (Routing Information Protocol). Le protocole RIP est incorporé dans de nombreux systèmes d'exploitation UNIX. Il s'agit d'un protocole Distance Vector très simple (les routeurs Distance Vector fonctionnent en envoyant à leurs voisins l'entièreté de leur table de routage).La table de routage est transmise dans des paquets RIP, encapsulés dans des datagrammes UDP. Le numéro de port utilisé est le 520. Les paquets RIP ont une taille maximale de 512 octets. Si la table de routage à transmettre est plus grande, elle est envoyée en plusieurs paquets. Les paquets RIP sont envoyés en diffusion (broadcast) sauf dans le cas de réseaux point-à-point ou ne supportant pas la diffusion.[ADN10].

OSPF: Protocole de routage - (Open Short test Path First). La technique Link State (Etat des liens) a été développée pour pallier aux inconvénients de la technique Distance Vector : Au lieu d'envoyer à leurs voisins l'ensemble des destinations possibles, les routeurs leurs envoient des paquets décrivant la liste des liens auxquels ils sont raccordés, ainsi que le coût associé à ces liaisons. Ces paquets sont appelés Link State Packets (LSP) ou Link State Avertissements (LSA).[ADN10].

Les voisins qui reçoivent ces paquets les transmettent à leur tour à leurs voisins (sauf à celui qui a émis le paquet). Ces paquets sont envoyés lors de certains

évènements, comme un changement d'état d'un lien, un changement de coût ou l'arrivée d'un nouveau routeur. Les routeurs constituent une base de données au moyen de ces paquets, et calculent ensuite une "carte" complète du réseau à partir de laquelle ils peuvent déterminer la meilleure route vers une destination donnée (celle dont la somme des coûts est la plus faible). Il faut un mécanisme qui assure la bonne arrivée des paquets LSA, sinon des routeurs risquent de calculer une fausse carte du réseau. Les routeurs découvrent eux-mêmes leurs voisins en envoyant des paquets "Hello" auxquels les voisins répondent.[ADN10].

IGP: (protocole défini par la compagnie CISCO –Interior gateway protocol). Basé sur le distance-vector. Il demande à chaque routeur voisin de lui envoyer toute ou une portion de sa table de routage dans un message que l'on appelle routing-update à un intervalle donné.[ADN10].

CHAPITRE II

Sniffer

CHAPITRE II : SNIFFER

INTRODUCTION

Les administrateurs réseau utilisent les sniffers pour analyser le trafic réseau et ainsi pouvoir déterminer d'éventuels problèmes sur le réseau. Un responsable de la sécurité peut utiliser plusieurs sniffers, stratégiquement placé à travers le réseau comme un system de détection d'intrusion. Les sniffers sont très important car quand ils sont installés, ils permettent d' obtenir : noms d'utilisateurs (user names), mots de passe, numéros de carte de crédits, informations personnelles et d'autres informations –la liste est longue- ce qui peut porter une atteinte grave à la confidentialité du système s'ils sont utilisés par une personne malveillante.

II.1 La gestion des réseaux

La gestion d'un réseau requiert une capacité technique de recouvrement de tous les processus permettant d'administrer des stations de travail, d'identifier et de maîtriser le fonctionnement du parc informatique, de gérer des serveurs et de mettre en place des infrastructures de communication fiables et efficaces. Cette gestion a pour objectifs d'améliorer la productivité de l'entreprise, de procéder au suivi systématique du cycle de vie et le renouvellement des postes de travail, de définir les axes d'action prioritaires en cas de panne ou de dysfonctionnement pour minimiser la durée d'indisponibilité de l'outil de travail.

Une bonne pratique de l'outil de gestion d'un réseau informatique, associée à la maîtrise de l'évolution rapide des technologies de communication et à la connaissance du rôle et la domination d'Internet favorise la nécessité d'une conception de réseau dynamique, le choix et le respect des standards en matière de protocoles, la mise en place de moyens d'évaluation de l'activité du réseau, la présence de mesures de sécurité adaptées aux enjeux, la facilité d'analyse et d'identification des risques associés.[CheNeg2004]

II.1.1 Contrôler son réseau, c'est important!

La continuité des activités d'une entreprise dépend essentiellement de la qualité de son système d'information, qui repose en grande partie sur l'efficacité avec laquelle est géré son réseau.

À cet égard, l'administrateur de réseau doit gérer les fonctions suivantes :

- Les droits d'accès durant et après les heures de travail.
- Le trafic des données qui circulent sur le réseau.
- La sauvegarde des données.
- la politique de sécurité régissant tous les types d'accès au réseau (accès interne, accès à distance et interconnexion avec des tierces parties).
- la surveillance et l'assurance de la fiabilité générale du réseau.

II.2 Définition d'un sniffer

Un sniffer est un logiciel qui permet d'intercepter des données transitant sur un réseau. Les pirates utilisent ce type d'outils afin de récupérer à l'insu des utilisateurs et des administrateurs réseaux des informations sensibles et confidentielles qui traversent les réseaux telles que les couples identifiants/mots de passe. Le sniffing est un processus de collecte d'information dit passif puisque le pirate n'entre pas en communication directe avec les machines dont il renifle et voit passer les données.[BenOul2006]

II.3 Architecture d'un sniffer

La plupart des sniffers réalisé sous WINDOWS utilise le l'API (Application programming Interface) WinPcap afin qu'il leur offre les procédures qui aide à la capture des paquets circulant sur le réseau (sniffé).[BenOul 2006]

II.3.1 C'est quoi WinPcap ?

WinPcap est un API de filtrage. Intégré par de nombreuses applications (Windump, Ethereal), il permet d'accéder aux couches réseaux à bas niveau du système, d'en obtenir les statistiques ou de capturer à distance et de transmettre les paquets.Grâce à sa librairie et ses contrôleurs, les développeurs ont pu développer des programmes de surveillance réseau, de détection d'intrusions, d'analyse de protocole ou de trafic, et bien d'autres encore. [WinP 05]

II.3.2 Principe de capture des paquets avec Winpcap

Toutes les applications de capture de paquets (sniffeurs) se basent sur le même principe afin d'intercepter les paquets qui circulent sur le réseau, elles doivent interagir avec la partie physique du réseau (carte réseau) afin de donnerl'ordre à la carte réseau du hôte voulant faire la capture des paquets, qu`ils soient destinés ou pas à cet hôte.

Cette opération exige un certain nombre de procédures complexes faite en assembleur (niveau physique) afin qu'elle réussisse et c'est là qu` intervient le rôle de WinPcap qui joue le rôle d'une librairie de procédures de capture pour ces applications.

Après avoir capturé les paquets il suffit juste de les afficher ou de faire les traitements nécessaires qui permettent la bonne gestion du réseau.

La figure suivant décrit l'opération de la capture avec WinPcap :

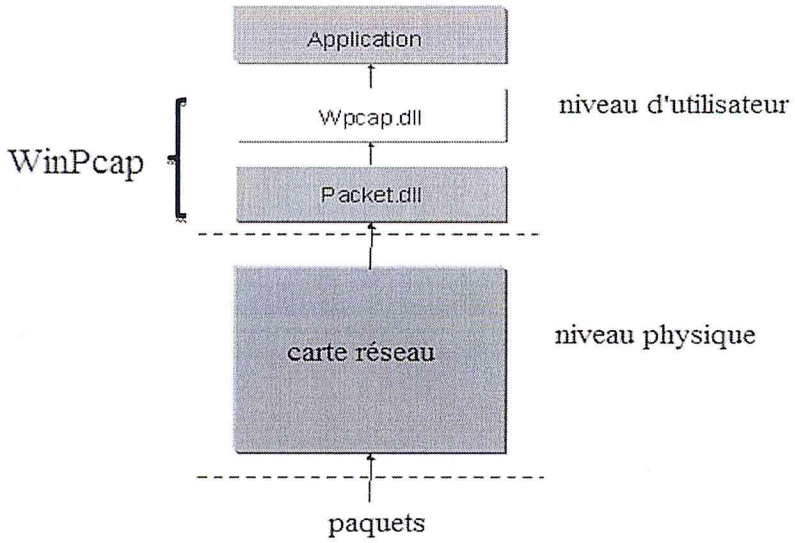


Fig. II.1 : La capture avec WinPcap. [WinP 05]

II.4 Exemples des sniffers

II.4.1 Wireshark (anciennement Ethereal)

Wireshark est un logiciel libre d'analyse de protocole, ou « packet sniffer », utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie, mais aussi le piratage. Wireshark est multiplate-forme, il fonctionne sous Windows, Mac OS X, Linux, Solaris, ainsi que sous FreeBSD.Wireshark reconnait 759 protocoles. [Wiki 10]

II.4.2 Tcp dump

Tcp dump est un Packet sniffer en ligne de commande. Il permet d'obtenir le détail du trafic visible depuis une interface réseau. C'est un outil de mise au point apprécié pour sa puissance ; les nombreuses informations qu'il faut trier conduisent à utiliser le filtre BPF. [Wiki 10]

II.4.3 IP Sniffer

IP Sniffer propose une suite d'outils IP construite autour d'un renifleur de paquets, plus communément "packet sniffers". Outre les traditionnels filtres, décodeurs et autres analyseur de trames, la suite propose une pléthore d'outils IP avec, entre autres, un moniteur de bande passante, des statistiques (IP et NDIS), un listing et la gestion des entrées ARP, des routes, des ports et des serveurs HTTP/FTP. IP Sniffer intègre également des outils de gestion de mot de passe, c'est la boîte à outil idéale pour tout administrateur.[Wiki 10]

II.4.4 Packet Sniffer SDK (PSSDK)

Est la suite de composants la plus puissante pour la capture d'ensemble d'un réseau dans l'environnement des systèmes d'exploitation Windows. Pas besoin de pilotes préinstallés car il contient un pilote interne pour l'ensemble, lequel est dynamiquement chargé/enlevé lorsque l'application qui utilise Packet Sniffer est lancée/clôturée. Packet Sniffer SDK (PSSDK) supporte les systèmes multiprocesseurs.

Packet Sniffer SDK est représenté pour le moment dans les exécutions suivantes : ActiveX, DLL, VCL et les librairies statiques compatibles avec Microsoft VC ainsi que les compilateurs Borland. Dès lors, la famille de composants/librairies du logiciel vous permet d'utiliser toute la puissance d'un environnement de développement visuel ou non afin de créer diverses applications de réseau. En utilisant ce logiciel le développeur n'a pas besoin de créer des pilotes de réseau spéciaux ou d'apprendre des exécutions internes des fonctionnalités du réseau dans la famille des systèmes d'exploitation Windows.

Les éléments de Packet Sniffer sont développés en tant qu'objets avec des propriétés, des méthodes et des évènements qui rendent le processus de développement d'applications plus simple et plus souple.[Wiki 10]

II.4.5 N top (Network TOP)

N top est un outil libre de supervision réseau. C'est une application qui produit des informations sur le trafic d'un réseau en temps réel (comme pourrait le faire la commande top avec les processus).

Il capture et analyse les trames d'une interface donnée, et permet d'observer une majeure partie des caractéristiques du trafic (entrant et sortant) et accepte pour cela, notamment deux modes de fonctionnement: Une interface web et un mode interactif. [Wiki 10]

II.5 Avantages et Inconvénients d'un sniffer

II.5.1 Avantages

1- Capture des paquets circulant sur le réseau.
2- Analyse du trafic réseau.
3- Réalisation des statistiques sur le réseau.
4- Analysedes impacts des applications sur le réseau.
5- Surveillancedes utilisateurs du réseau.
6- Aidedans la gestion et l'administration des réseaux.
7- Evitement des goulots d'étranglement de la bande passante.

II.5.2 Inconvénients

1- Saturation de la bande passante.
2- Fuite d'informations confidentielles.
3- Alourdissement du réseau.
4- Peut servir comme un moyen de piratage.

II.6 La technologie Netflow

Netflow est une technique mise au point par la société Cisco Systems pour réaliser de la métrologie réseau. Le concept majeur de Netflow est la notion de flux, un flux étant déterminé par les critères suivants :

- Adresses IP source et destination,
- Protocole(TCP, UDP, ICMP,...),
- ToS (Type Of Service)
- Ports applicatifs (http, smtp, dns,...),
- Interfaces d'entrée et de sortie du routeur.

Pour qu'un paquet IP appartienne à un flux, il doit correspondre à tous ces critères, simultanément.

Un routeur qui utilise Netflow garde en mémoire une table des flux actifs à un instant donné, et compte le nombre de paquets et d'octets reçus pour chaque flux. Cisco appelle cette table« cache Netflow » dans sa documentation.

A chaque paquet reçu, le routeur met à jour ce cache, soit en créant une nouvelle entrée si le flux n'est pas connu, soit en incrémentant les compteurs correspondant au flux déjà présent dans le cache.

Pour ne pas consommer toute la mémoire du routeur avec un ajout incessant de nouveaux flux, celui-ci efface au fur et à mesure les flux considérés comme terminés. Quand un flux a été inactif pendant un certain temps (« inactive timeout » est le terme utilisé par Cisco), le flux est retiré du cache. Un flux peut également être supprimé s'il a été actif trop longtemps (« active timeout »), afin que le cache ne garde pas indéfiniment des flux qui ne se terminent jamais. Enfin, lorsque le routeur voit les drapeaux TCP « RST » ou « FIN » qui signalent la fin d'une connexion TCP, le flux est également supprimé.

Pour connaître l' « inactivité » d'un flux, le routeur se sert de la date du dernier paquet reçu pour ce flux et la compare à la date actuelle.

L'intérêt de Netflow étant de pouvoir réaliser de la métrologie, il était donc nécessaire de fournir les informations sur les flux à un programme d'analyse. En fait, lorsqu'un flux a expiré et est supprimé du cache, il peut être exporté vers une machine de collecte, qui reçoit ainsi des paquets Netflow suivant un protocole bien défini par Cisco. Il en existe plusieurs versions, la dernière étant la version 9.

Pour des raisons d'efficacité et d'économie de bande passante, le routeur groupe l'envoi de plusieurs flux dans un même paquet (entre 20 et 30 flux par paquets).[Chr 2004]

II.6.1 Versions de Netflow

Cisco a créé plusieurs versions du protocole Netflow, au fur et à mesure de l'apparition de nouveaux besoins de ses clients. A ce jour, les versions 1, 5, 6, 7, 8 et 9 existent. La 9 devrait être en mesure de répondre aux problèmes d'évolutivité qui ont touché les versions précédentes et devrait donc être la dernière.

Pour rappel, la version 5 est la plus utilisée sur les routeurs. La version 7 est spécifique aux commutateurs Catalyst. La version 8 permet d'utiliser des schémas d'agrégation suivant certains critères.

Enfin, la version 9 supporte les « nouveaux protocoles », à savoir principalement IPv6 et MPLS (MultiProtocol Label Switching). [Chr 2004]

II.6.2 Paramétrage

Les paramètres à indiquer pour recevoir les datagrammes Netflow d'un routeur sont les suivants :

- L'adresse IP du routeur, avec laquelle sont envoyés les datagrammes. Il peut être nécessaire de fixer cette adresse sur le routeur au moyen de la commande IOS« IP flow-export source <adresse IP>|<interface> ».
- Une communauté SNMP avec privilège de lecture seule. Un accès SNMP est nécessaire sur le routeur pour déterminer les noms des interfaces associés à chaque index SNMP. Si aucune communauté n'est indiquée, le collecteur utilise la communauté « public » par défaut.
- Version de Netflow. Les versions supportées par le collecteur sont : 1, 5, 6, 7, 8 et 9. Si aucune version n'est spécifiée, v5 est la version utilisée par défaut.
- L'adresse IP et le port UDP de réception à utiliser pour recevoir les datagrammes.

Indiquer une adresse IP sert généralement dans le cas de machines disposant de plusieurs interfaces réseaux (*multi-homed*).

Fixer le port de réception permet de conserver la même configuration d'export du routeur (par défaut le port est attribué dynamiquement par le système). [Chr 2004]

Le format de configuration est le suivant(les commandes utilisés sont des commandes CISCO)

router<nom_de_routeur> {
ip-address<adresse_ip_routeur>;
snmp-community<communaute_snmp>;
netflow {
version 1|5|6|7|8|9;
receiver-address<adresse_ip_locale>;
receiver-port <port_de_reception>;
};};

Example

router 7500_UTC {
ip-address 193.51.1.105;
snmp-communitynetflow;

netflow {
version 5;
receiver-address 193.49.251.82;
receiver-port 8000;
};
};

Dans cet exemple, le routeur à superviser a pour adresse IP 193.51.1.105, et envoie des datagrammes Netflow v5. Le collecteur recevra les données sur l'interface de la machine ayant l'adresse IP 193.49.251.82, avec le port 8000/udp comme port de réception.

La configuration du routeur serait :

```
interface Loopback0
ip address 193.51.1.105 255.255.255.255;
!
ip flow-export version 5
ip flow-export source Loopback0
ip flow-export destination 193.49.251.82 8000
!
access-list 10 permit 193.49.251.82
snmp-communitynetflow RO 10
!
```

II.7 Le protocole SNMP (Les Sondes EMON)

II.7.1 Qu'est-ce que le protocole SNMP ?

Simple Network Management Protocol (abrégé **SNMP**), en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance

Il s'appuie sur 4 composantes principales :

- ✓ Des agents
- ✓ Un ou plusieurs managers
- ✓ Une MIB (Management Information Base)
- ✓ Des trames

II.7.2 Les différentes versions de SNMP

- ➢ SNMPv1 (ancien standard) : Première version apparue en 1989.
- ➢ SNMPsec (historique): Ajout de sécurité par rapport à la version 1
- ➢ SNMPv2p (historique) : Ajout de nouveau type de données.
- ➢ SNMPv2c (expérimental) : Amélioration des opérations du protocole
- ➢ SNMPv2u (expérimental) : Implémente la version 2c en ajoutant la sécurité utilisateurs.

- SNMPv2* (expérimental) : Combinaison des meilleures parties de v2u et v2p.
- SNMPv3 (nouveau standard) : La sécurité avant tout.

II.7.3 Le principe

Les systèmes de gestion de réseau sont basés sur trois éléments principaux : un superviseur, des nœuds (ou nodes) et des agents. Dans la terminologie SNMP, le synonyme *manager* est plus souvent employé que superviseur. Le superviseur est la console qui permet à l'administrateur réseau d'exécuter des requêtes de management. Les agents sont des entités qui se trouvent au niveau de chaque interface, connectant au réseau l'équipement géré (nœud) et permettant de récupérer des informations sur différents objets.

Switchs, hubs, routeurs et serveurs sont des exemples d'équipements contenant des objets gérables. Ces objets gérables peuvent être des informations matérielles, des paramètres de configuration, des statistiques de performance et autres objets qui sont directement liés au comportement en cours de l'équipement en question. Ces objets sont classés dans une sorte de base de données arborescente appelée MIB (« *Management Information Base* »). SNMP permet le dialogue entre le superviseur et les agents afin de recueillir les objets souhaités dans la MIB.

L'architecture de gestion du réseau proposée par le protocole SNMP est donc fondée sur trois principaux éléments :

- Les équipements gérés (*managed devices*) sont des éléments du réseau (ponts, switchs, hubs, routeurs ou serveurs), contenant des « objets de gestion » (*managed objects*) pouvant être des informations sur le matériel, des éléments de configuration ou des informations statistiques ;
- Les agents, c'est-à-dire les applications de gestion de réseau résidant dans un périphérique, sont chargées de transmettre les données locales de gestion du périphérique au format SNMP ;

- Les systèmes de gestion de réseau (network management systems notés NMS), c'est-à-dire les consoles à travers lesquelles les administrateurs peuvent réaliser des tâches d'administration.

II.8 Etude comparatif entre le SNMP et Netflow

	SNMP	NetFlow
Installation	Simple	Peut être compliqué
Filtrage du trafic	Non	Oui
Différencier la bande passante par protocole ou IPs	Non	Oui
PRTG peut affiché Top lists (Top Talker, Top Connections, Top Protocols, etc.)	Non	Oui
Filtrer par utilisation de bande passante IP	Non	Oui
Filtre la bande passante par adresse MAC	Non	non
Filtré La bande passante par le port réseau physique	Oui	non
Surveiller les autres paramètres du réseau que la bande passante	Oui	non
Chargement du processeur sur la machine qui exécute PRTG	Bas	haute
Consommation de la bande passante en excès de la surveillance	Petite	Dépond du trafic

TAB II.1 : Tableau comparatif entre le SNMP et Netflow. [BenOul 2006]

Cette étude comparative montre la différence entre le SNMP et le NetFlow et prouve que l'utilisation du NetFlow est plus utile que celle du SNMP et donc illustre pourquoi on a choisie l'utilisation de NetFlow.

CHAPITRE III

Conception

CHAPITRE III : CONCEPTION

INTRODUCTION

Pour le développement de notre application, nous avons adopté une approche orientéeobjet. Cette approche a prouvé, depuis plusieurs années, son efficacité lors de la construction des systèmes quel que soit leur complexité. La construction d'un système passe impérativement par une modélisation.

Un modèle est une simplification de la réalité. Nous utilisons des modelés afin de mieux comprendre le système que l'on développe.

Pour la modélisation de notre système, nous avons opté pour l'utilisation du langage UML (Unified Modeling Langage), car ce dernier permet la modélisation orienté objet.

III.1 Les notions UML

III.1.1 Définition d'UML

UML (Unified Modeling Langage) est un langage graphique conçu pour représenter, spécifier, construire et documenter les artefacts d'un système à dominante logicielle. Il permet d'écrire avec un langage standardisé les plans d'élaboration et de construction de logiciels.

UML est adapté à la modélisation des systèmes depuis les systèmes informatiques d'entreprises jusqu'aux applications distribuées basées sur le WEB en passant par les systèmes temps réel embarqués.

La modélisation d'un système peut faire appel à trois types de description :

- Model logique : des données, statistiques, … etc.
- Model fonctionnel : traitements applicatifs, dynamique, …
- Model physique.

Lorsque la description porte sur des spécifications externes, on parle généralement de modèles d'analyse. Et pour les spécifications internes, on parle de modèles de conception.[MEK 2005]

III.1.2 Les Diagrammes UML

Un diagramme est la représentation graphique d'un ensemble d'éléments qui constituent un système.

UML fournit neuf diagrammes pour spécifier les modèles :

1- Model logique :

- Diagrammes de classe : Ils représentent un ensemble de classes, d'interfaces et de collaborations, ainsi que leurs relations. C'est la vue de conception statique d'un système.
- Diagrammes d'objet : Ils représentent un ensemble d'objets et leurs relations

2- Model fonctionnel :

- Diagrammes de cas d'utilisation : Ils représentent un ensemble de cas d'utilisation et d'acteurs et leurs relations. Ils sont particulièrement importants dans l'organisation et la modélisation des comportements d'un système.
- Diagrammes de collaboration : Ce sont des diagrammes qui mettent l'accent sur l'interaction et l'organisation structurelle des objets qui envoient et reçoivent des messages.
- Diagrammes de séquence : Ces diagrammes mettent l'accent sur l'interaction et le classement chronologique des messages.
- Diagrammes d'états-transitions : Ce sont des automates à états finis, composés d'états, de transitions, d'événements et d'activités. Ils présentent la vue dynamique d'un système.
- Diagrammes d'activité : C'est un type particulier de diagramme d'états-transitions qui décrit la succession des activités au sein d'un système.

3- Model physique:

- Diagrammes de composant : Ils représentent l'organisation et les dépendances entre l'ensemble des composants au sein du système.
- diagrammes de déploiement : Ils représentent la vue de déploiement statique d'une architecture. [MEK 2005]

LA REALISATION

Dans notre projet il nous a était demandez de crée un outil informatique qui sert à la supervision et la gestion des réseaux. Pour commencer ont était obligé d'assimilé les notions réseaux telle que le matériels utilisé et ça configuration et pour cela on effectuer une étude théorique à l'aide d'un logiciel qui simule sur un ordinateur un réseau virtuel son nom est Packet Tracer ,après la maitrise des notions réseaux on est passé à la recherche d'une méthode qui nous permettra par la suite de détourner tous les paquets qui circule sur notre réseau vers un Hôte administrateur pour qu'il les analyse pour mieux supervisé et géré son réseau ;et c'est là qu'on a choisi la technologie Netflow qui a était créé par CISCO et intégré dans presque tous les nouveaux routeurs CISCO, cette technologie n'est d'autre qu'un ensemble de commandes CISCO qu'on va utiliser sur le routeur principale de notre réseau pour qu'il achemine tous le flux qui le travers vers une adresse IP qui sera celle de l'administrateur réseau. Suite à l'opération d'acheminement de flux on s'est trouvé dans l'obligation de changé le mode de la carte réseau de l'administrateur du mode normale au mode promiscuous c'est dire sauté du mode normal de la carte réseau qui dit que si un paquet arrive à la carte et qu'il porte comme adresse IP l'adresse la carte réseau donc il passe sinon il sera rejeté, vers un autre mode qui permet à la carte réseau de passé tous les paquets afin d'y accédé par la suite, et pour cela que durant la réalisation de notre application on a fait appel à des opérations qui se trouvé dans une librairie qu'on a fait intégrer dans notre application et qui s'appelle WinPcap. Après la capture des paquets on les enregistre sous une base de données (ACCESS)pour pouvoir y'accédé et effectuer des statistiques sur l'état du réseau afin de savoir sur qui et quand appliqué les opérations de gestion réseau telle que l'ajout des VLAN, Hôte, le blocage d'un Hôte malveillant à travers son adresse IP, contrôlé le flux, ...

III.2 Diagramme de cas d'utilisation

Un cas d'utilisation est une abstraction d'une partie du comportement du système. Après l'analyse des fonctionnalités que doit assurer notre système, il ressort qu'il interagit avec un ensemble d'acteurs.

Un Acteur représente un rôle qu'un homme, une machine ou même un autre système joue avec notre système.[MEK 2005]

Dans notre cas nous identifions trois acteurs :

- Administrateur : C'est la personne qui surveille, gère et assure le bon le fonctionnement du réseau.

Leurs représentations graphiques sont données dans la figure suivante :

Fig. III.1 : Représentation des acteurs

Les interactions fonctionnelles des acteurs, précédemment définies, avec le système sont données dans le tableau suivant :

Acteurs	Cas d'utilisation
Administrateur	• Authentification • Visualisation : Visualisation du flux réseau: ➢ Par interfaces. ➢ Par VLAN. ➢ Par port. ➢ Par Protocol. ➢ Par utilisateur. ➢ Les Top N. ➢ Visualisation de l'historique. ➢ Visualisation des statistiques. ➢ Visualisation la bande passante. • Gérer les VLANS et Hôtes. • Lancer la capture des paquets. • Analyser les paquets. • Enregistrer la capture. • Controle du Qos. • Controle du flux. • Controle des notifications.

TAB III.1 : Tableau des acteurs du use

Diagramme de cas d'utilisation du système

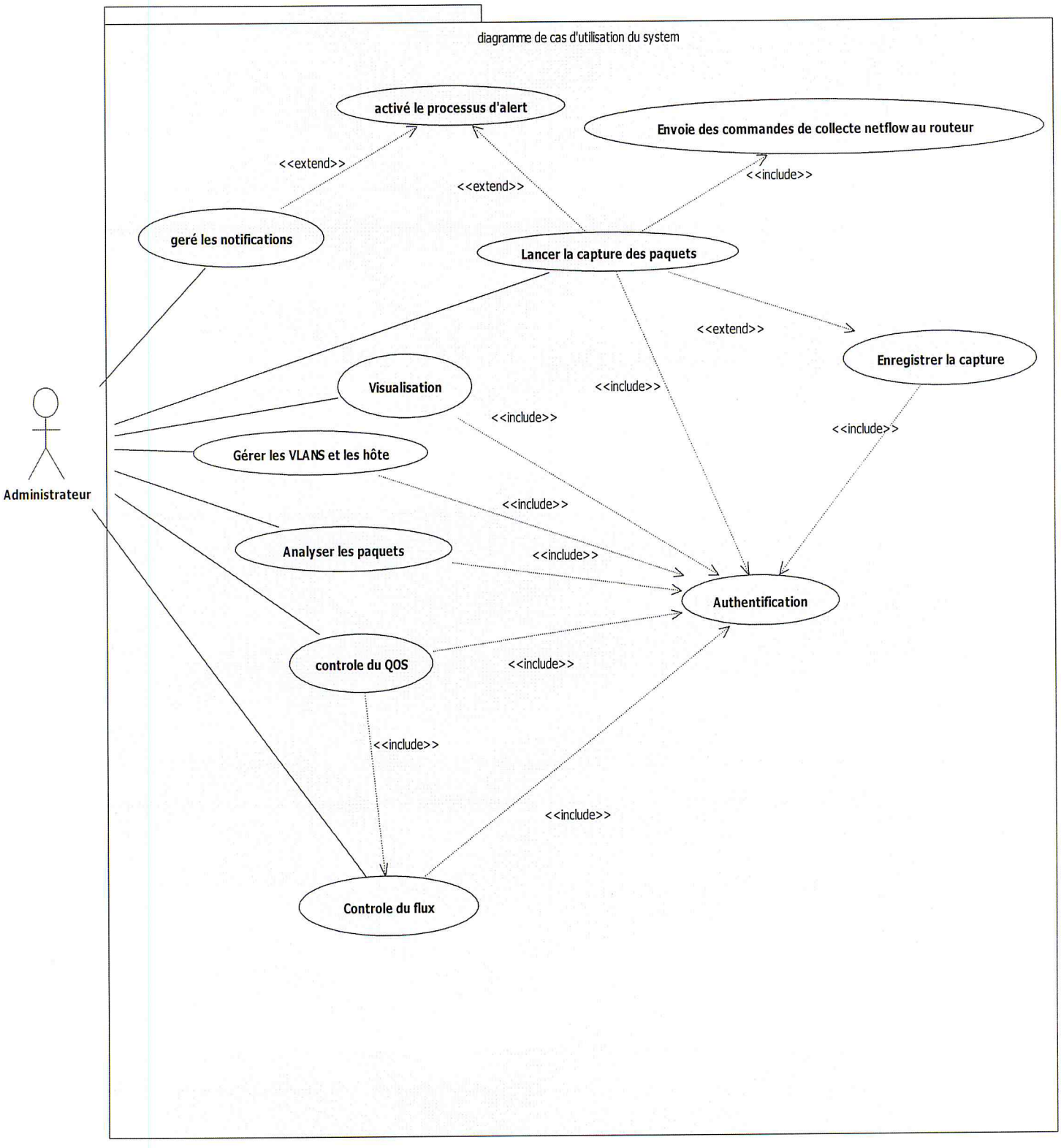


Fig. III.2 : Diagramme de cas d'utilisation du système

III.3 Diagramme de séquence

III.3.1 Diagramme de séquence de l'authentification

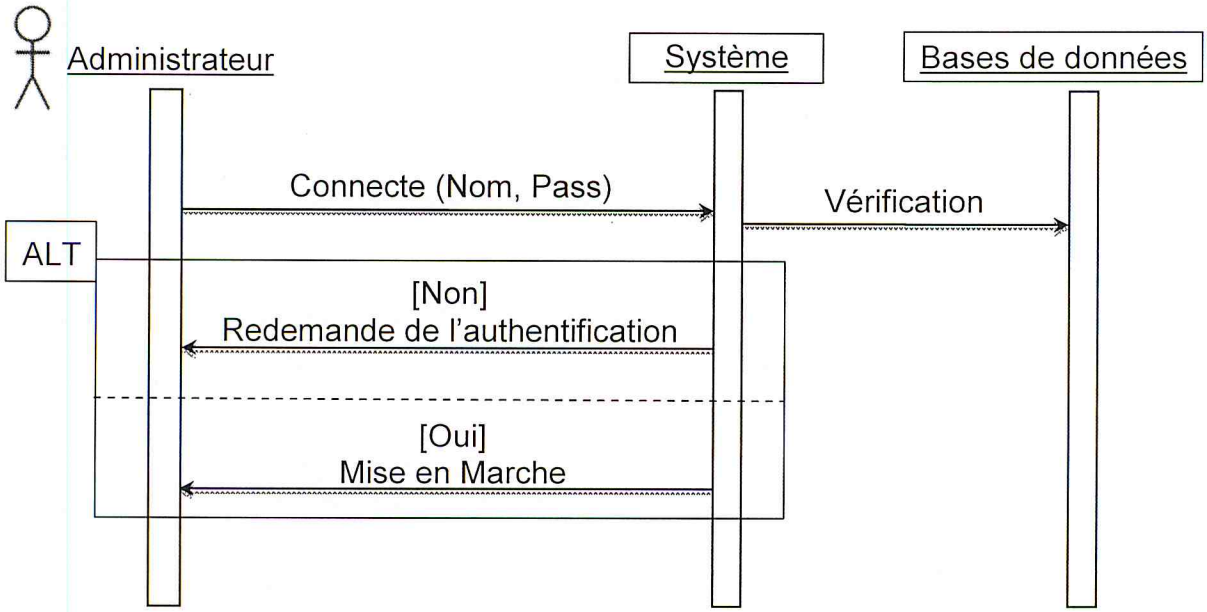


Fig. III.3 : Diagramme de séquence de l'authentification

Ce cas d'utilisation contient les étapes suivantes :

- L'administrateur accède à la fenêtre principale de l'application
- L'administrateur saisie son nom de session et mot de passe.
- Si l'existence du couple est confirmée, l'administrateur accède aux autres fonctionnalités du système
- Sinon, le système demande à l'administrateur de ressaisir le nom de session et son mot depasse.

Fig. III.2 : Diagramme de cas d'utilisation du système

III.3.2 Diagramme de séquence de lancement de la capture

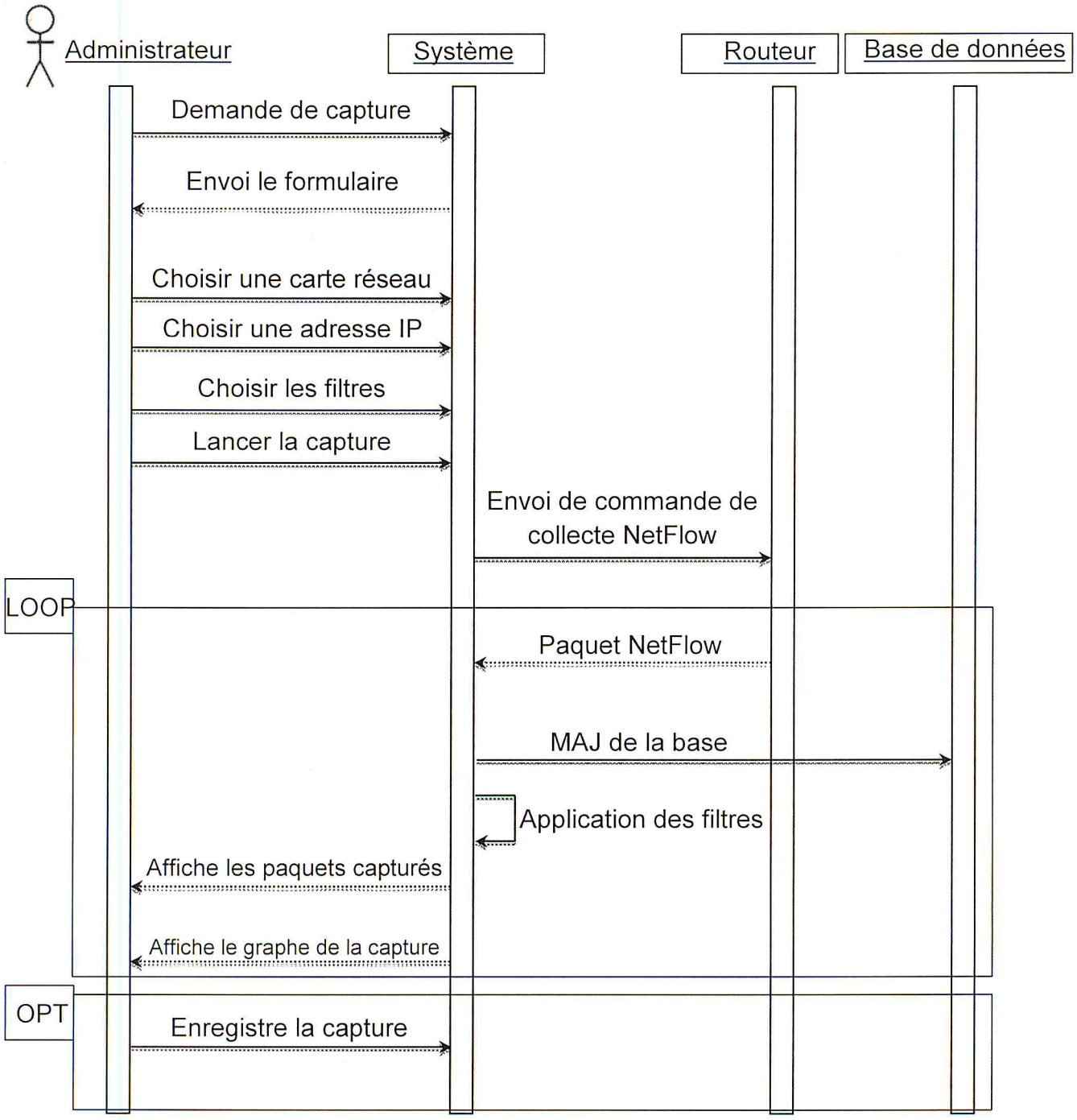


Fig. III.4 : Diagramme de séquence de lancement de la capture

Le lancement de la capture se produit comme suit :

- L'utilisateur lance l'opération de capture.
- Le système reçoit et traite les paquets NetFlow exportés par le routeur.
- Une fois les caractéristiques et flux des utilisateurs soit extraits, le système les sauvegardes dans la BASE.

III.3.3 Diagramme de séquence d'ajout d'un VLAN

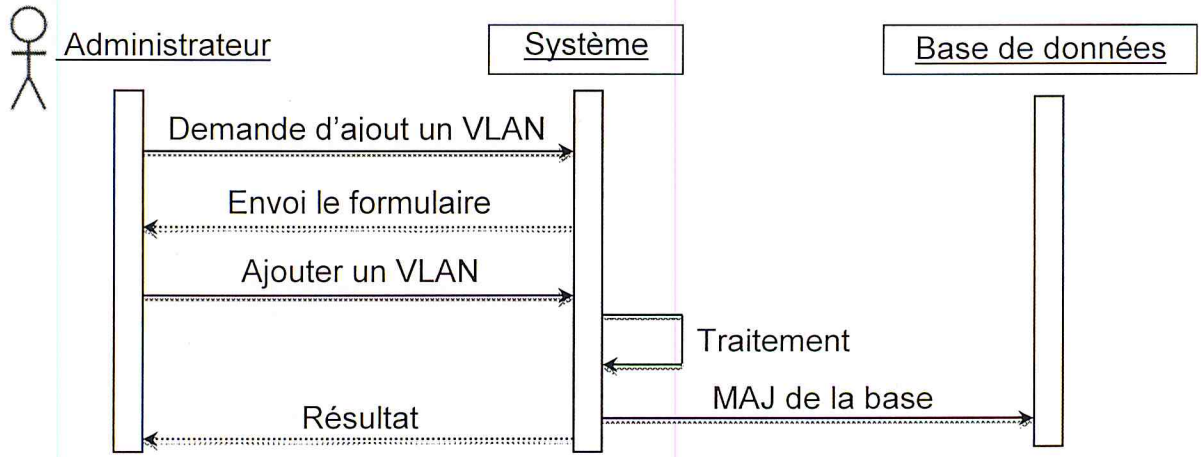


Fig. III.5 : Diagramme de séquence d'ajout d'un VLAN

L'ajout d'un VLAN se produit comme suit :

- L'utilisateur lance l'opération d'ajout.
- Le système reçoit et exécute l'opération.
- Le system renvoi le résultat d'ajout a l'utilisateur

III.3.4Diagramme de séquence de suppression d'un VLAN

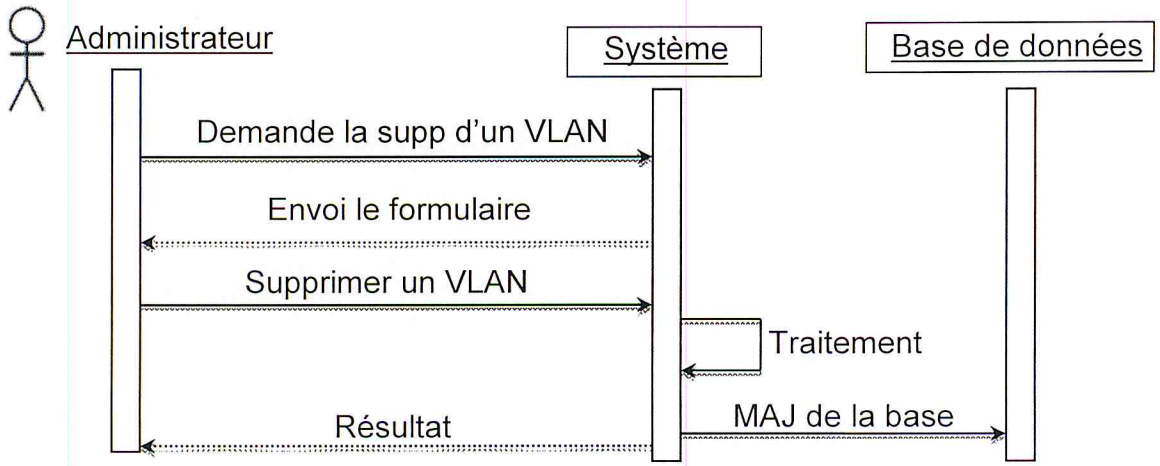


Fig. III.6 : Diagramme de séquence de suppression d'un VLAN

La suppression d'un VLAN se produit comme suit :

- L'utilisateur choisie un VLAN a supprimé et lance l'opération de la suppression.
- Le système reçoit et exécute l'opération.
- Le system renvoi le résultat de suppression a l'utilisateur.

III.3.5 Diagramme de séquence de modification d'un VLAN

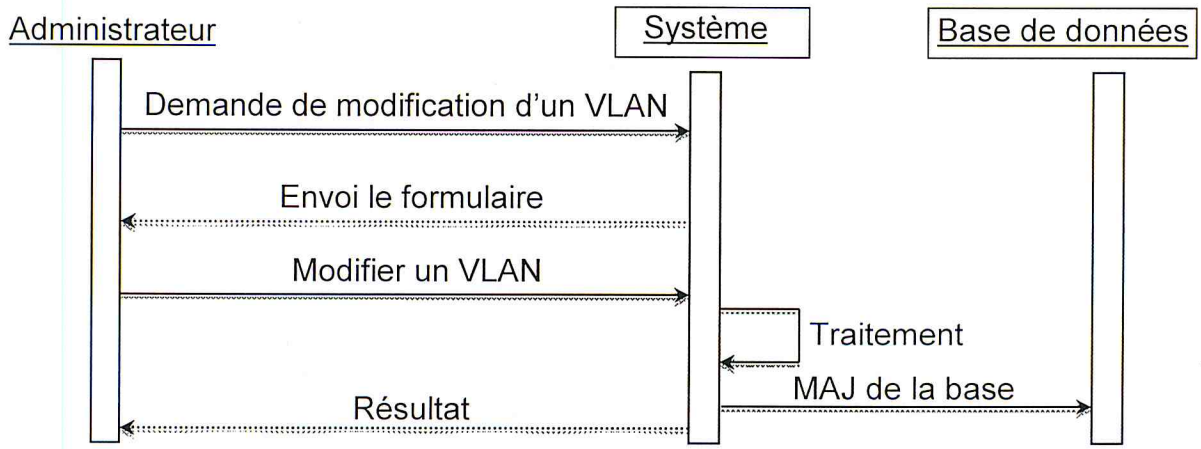


Fig. III.7 : Diagramme de séquence de modification d'un VLAN

La modification d'un VLAN se produit comme suit :

- L'utilisateur choisie un VLAN pour le modifié et lance l'opération de modification.
- Le système reçoit et exécute l'opération.
- Le system renvoi le résultat de modification à l'utilisateur.

III.3.6 Diagramme de séquence d'ajout d'un Hôte

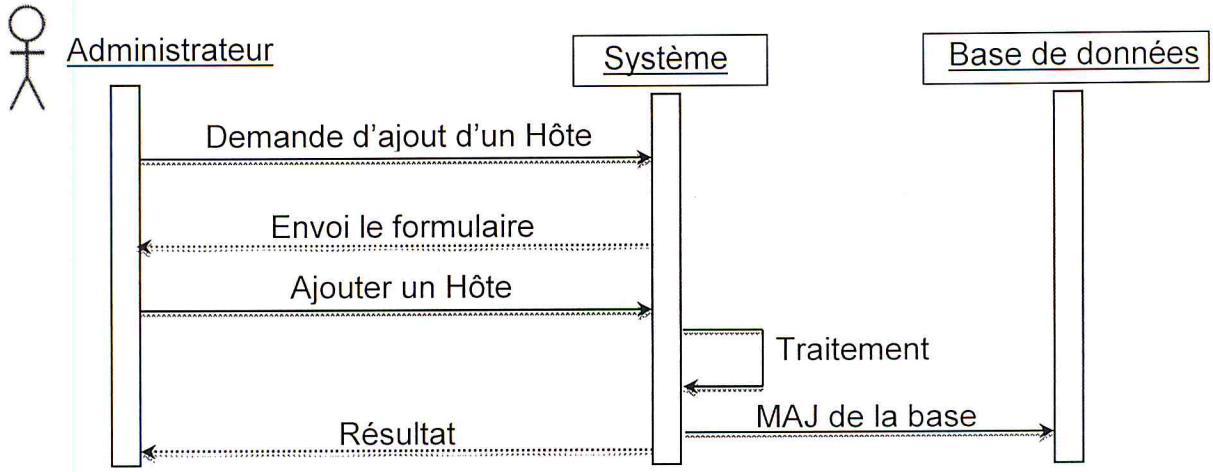


Fig. III.8 : Diagramme de séquence d'ajout d'un Hôte

L'ajout d'un Hôtese produit comme suit :

- L'utilisateur lance l'opération d'ajout.
- Le système reçoit et exécute l'opération.
- Le system renvoi le résultat d'ajout a l'utilisateur

III.3.7 Diagramme de séquence de suppression d'un Hôte

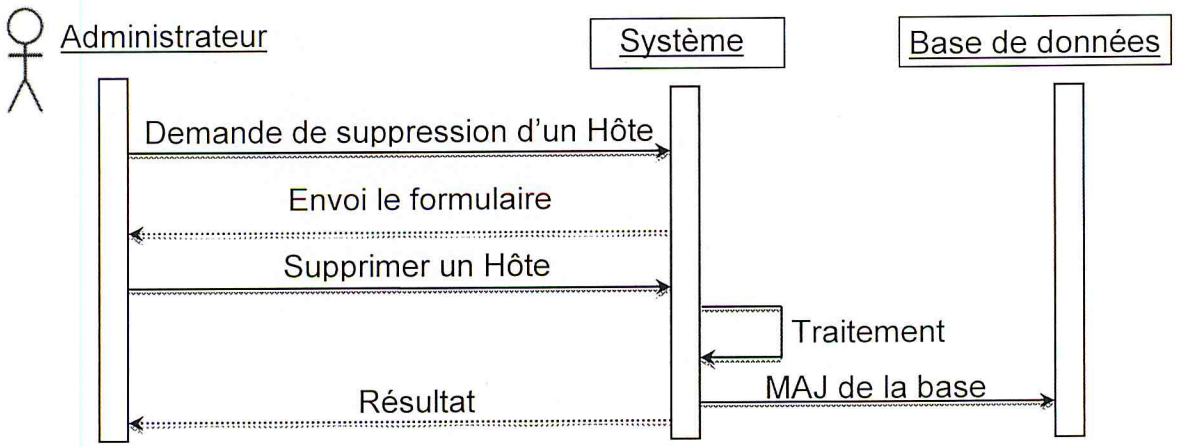


Fig. III.9 : Diagramme de séquence de suppression d'un Hôte

La suppression d'un Hôte se produit comme suit :

- L'utilisateur choisie l'hôte a supprimé et lance l'opération de suppression.
- Le système reçoit et exécute l'opération.
- Le system renvoi le résultat de suppression a l'utilisateur.

III.3.8 Diagramme de séquence de modification d'un Hôte

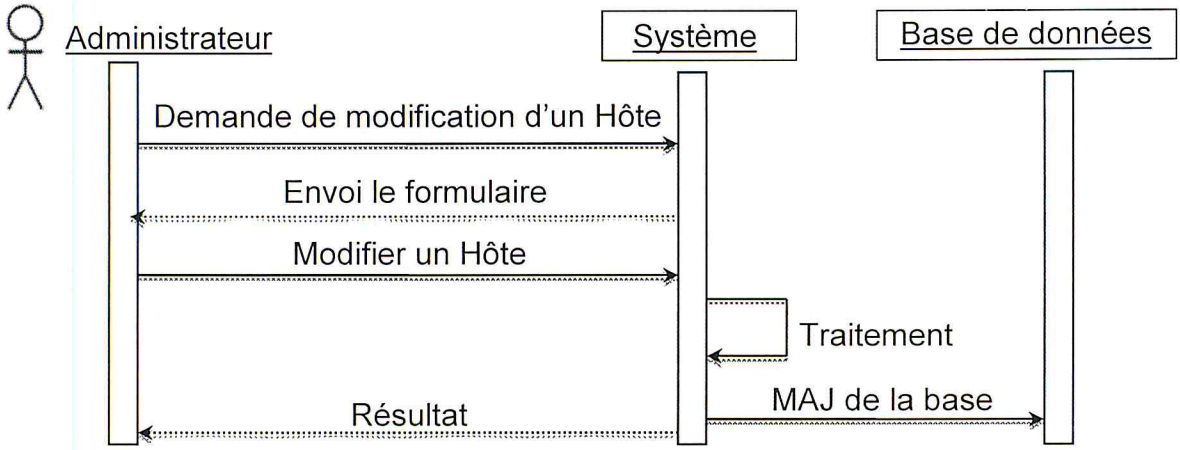


Fig. III.10 Diagramme de séquence de modification d'un Hôte

La modification d'un Hôte se produit comme suit :

- L'utilisateur choisie l'hôte a modifié et lance l'opération de modification.
- Le système reçoit et exécute l'opération.
- Le system renvoi le résultat de modification à l'utilisateur.

III.3.9 Diagramme de séquence pour trouver l'adresse MAC d'un Hôte

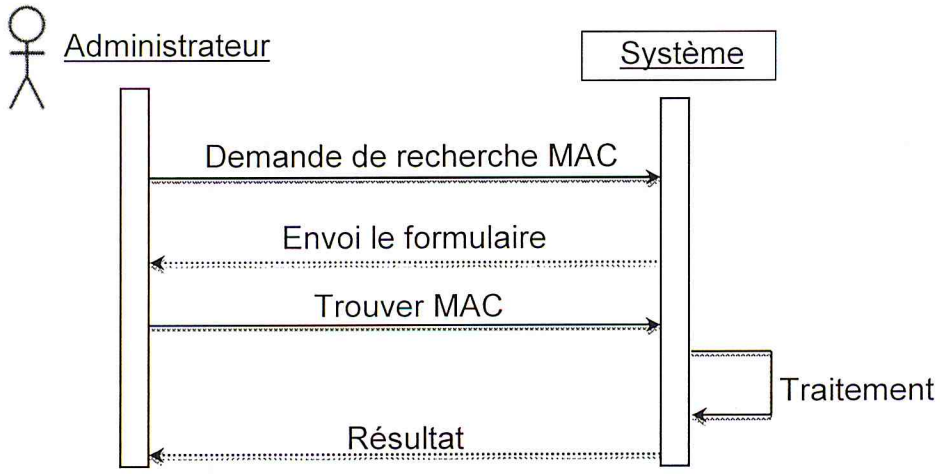


Fig. III.11 Diagramme de séquence pour trouver l'adresse MAC d'un Hôte

La recherche d'adresse MAC se produit comme suit :

- L'utilisateur lance l'opération de recherche.
- Le système reçoit et exécute l'opération.
- Le system renvoi le résultat de la recherche qui contient les adresses MAC des hôtes.

III.3.10 Diagramme de séquence pour trouver statut d'un Hôte

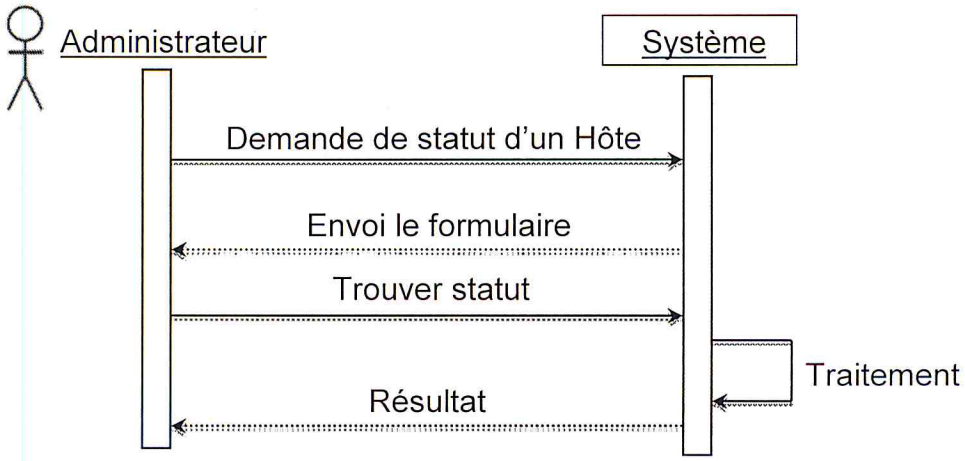


Fig. III.12 Diagramme de séquence pour trouver statut d'un Hôte

La recherche de statut d'un Hôte se produit comme suit :

- L'utilisateur choisie un hôte et lance l'opération de recherche.
- Le système reçoit et exécute
- Le système renvoi le résultat de la recherche (statut).

III.3.11 Diagramme de séquence de visualisation

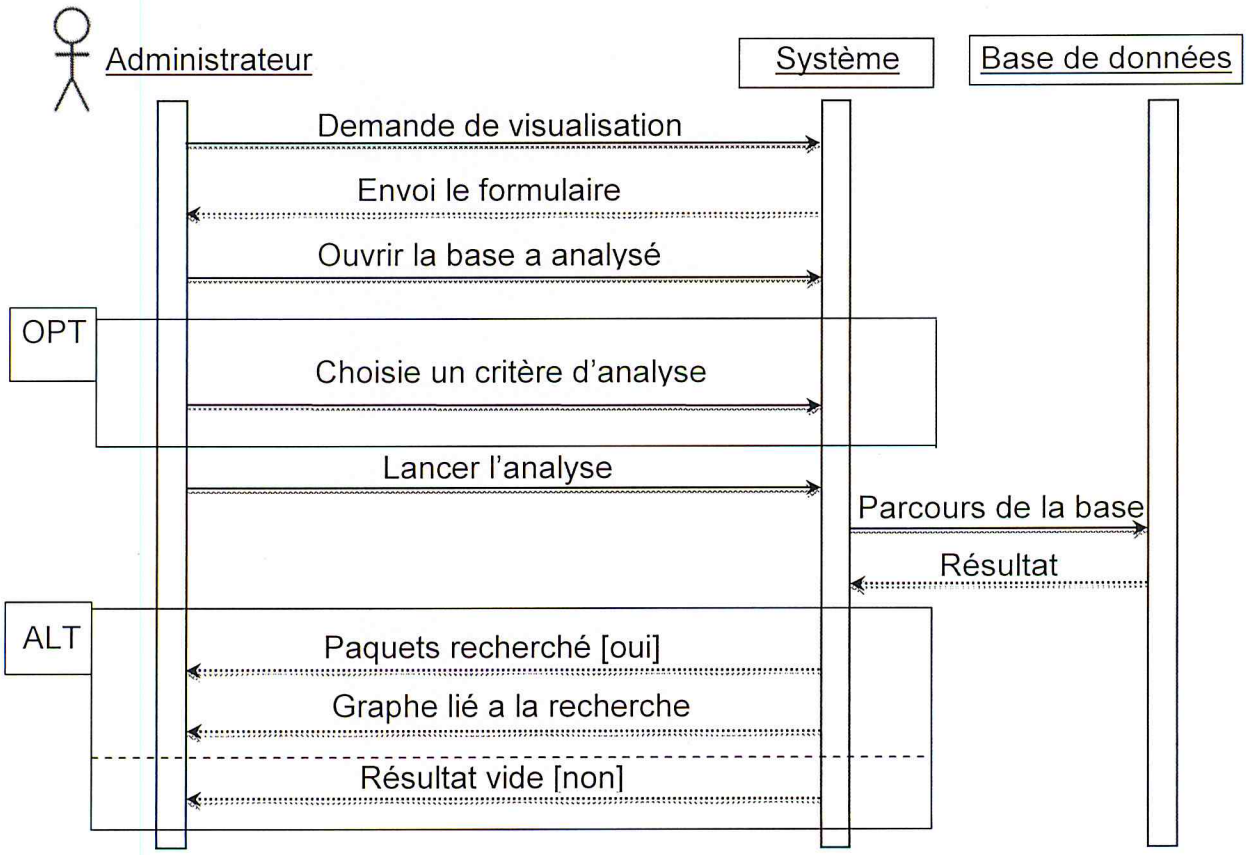


Fig. III.13 Diagramme de séquence de visualisation

La visualisation se produit comme suit :

- L'administrateur choisie le critère de visualisation.
- L'administrateur lance la visualisation.
- Le système faire un traitement.
- Le système renvoi le résultat

III.3.12 Diagramme de séquence de contrôle de flux

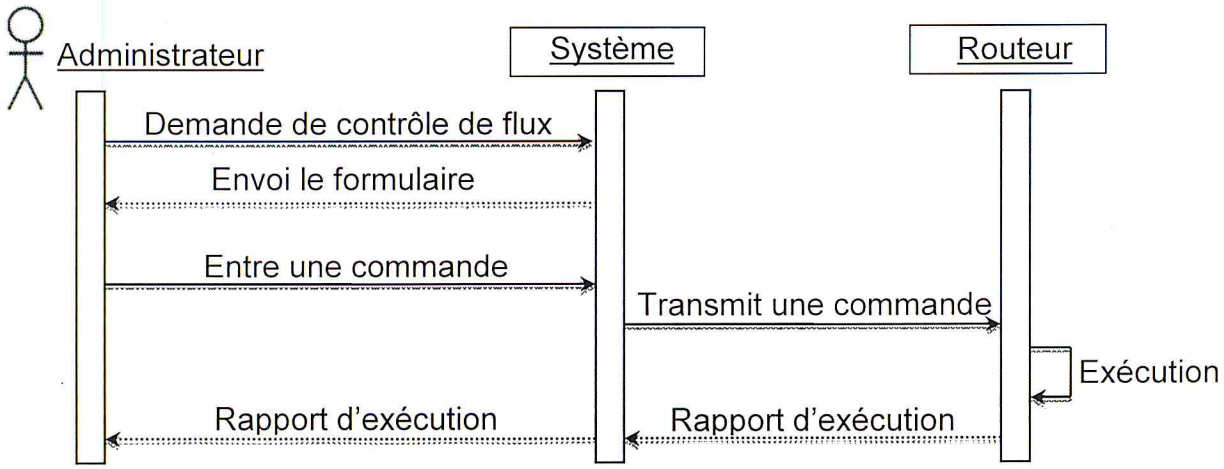


Fig. III.14 Diagramme de séquence de contrôle de flux

Le contrôle de flux se produit comme suite :

- l'administrateur s'authentifier en premier.
- l'administrateur entre une commande de contrôle de flux (commande CISCO).
- le system transmit la commande au routeur.
- le routeur exécute le commande et envoi un rapport sur l'exécution au system.
- le system transmit le rapport d'exécution du routeur à l'utilisateur.

III.4 Diagramme de classe

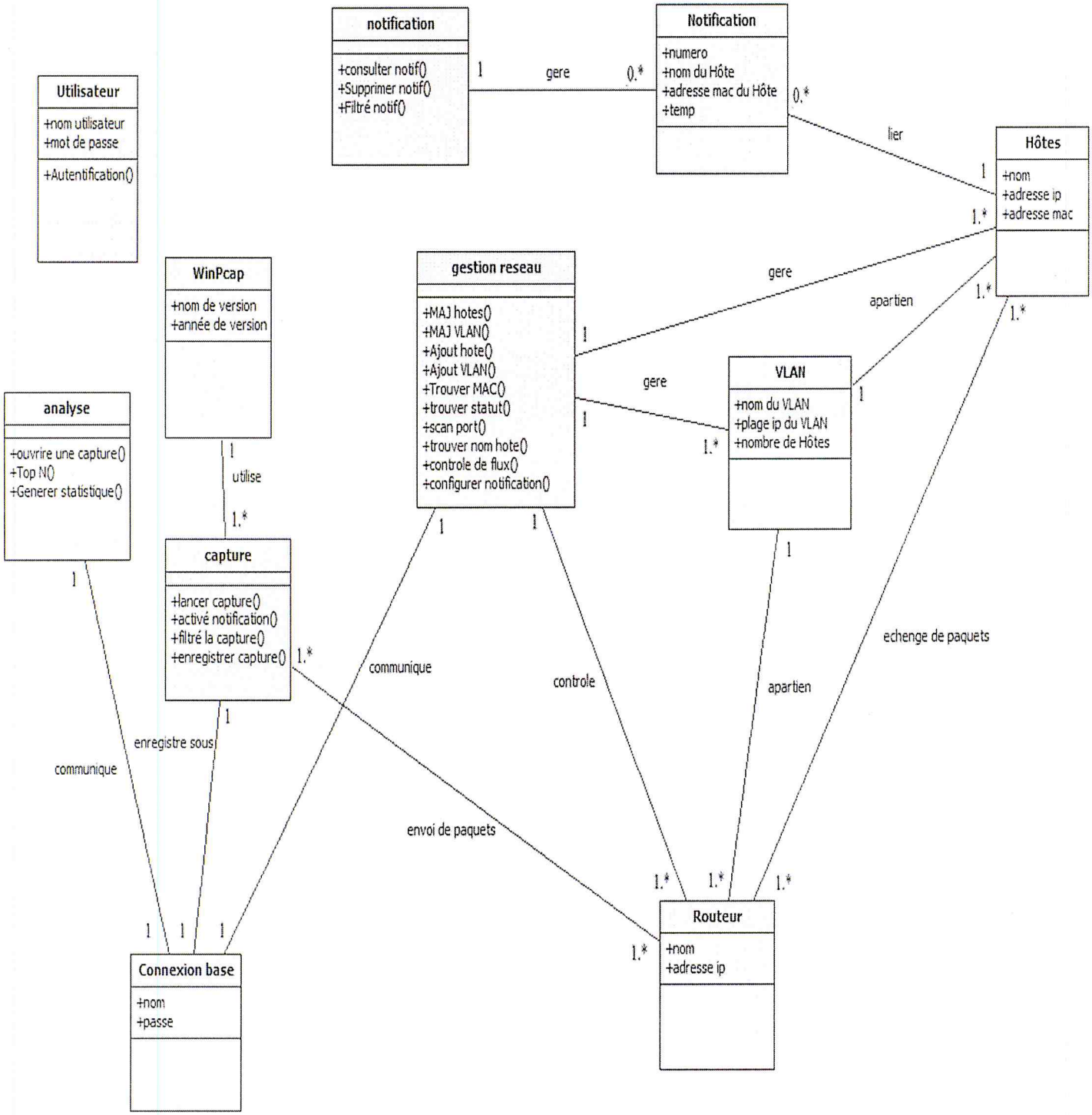


Fig. III.15 Diagramme de classe

III.5 Diagramme d'activité

III.5.1 Génération de notification

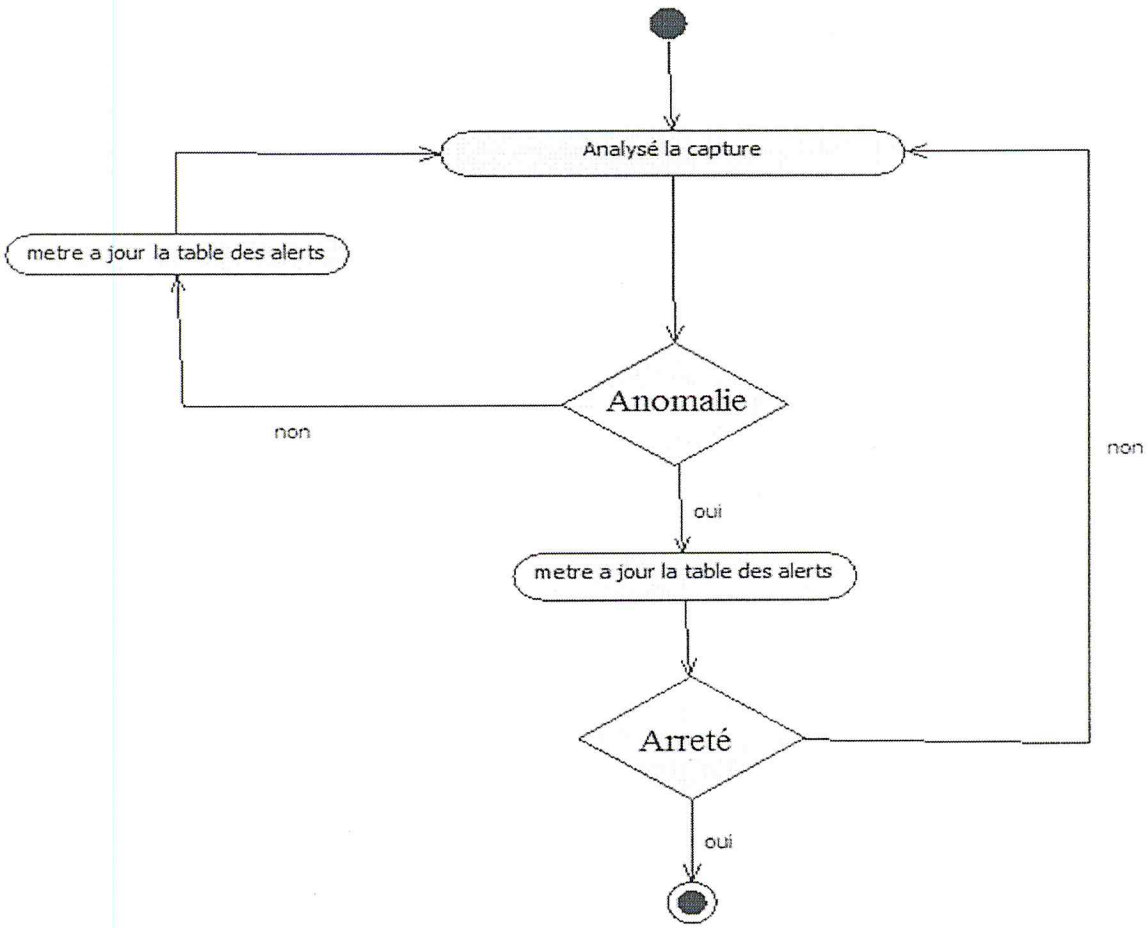


Fig. III.16 Diagramme d'activité de génération de notification

La génération des notifications se fait en analysant les données de la capture. Une temporisation est introduite de l'ordre de centaine de millisecondes pour ne pas avoir des itérations inutiles en analysant les mêmes données qui n'ont pas encore été mises à jour.

III.5.2 Détection d'une adresse IP non autorisé

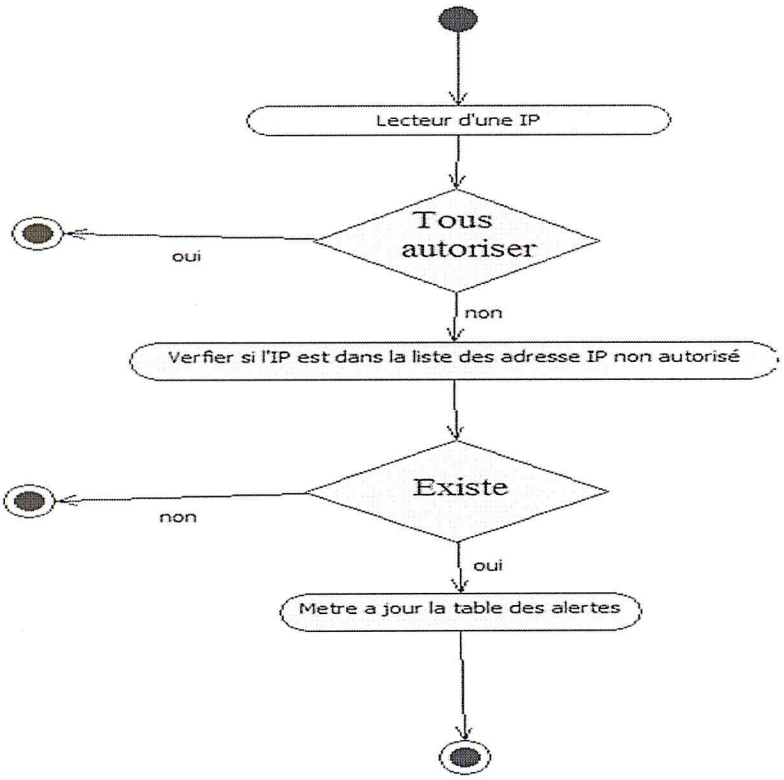


Fig. III.17 Diagramme d'activité de Détection d'une adresse IP non

Vu que ce traitement s'effectue au même temps que la réception des adresses IP, il doit être le plus rapide possible. Pour cette raison, la liste des adresses non autorisées est chargée en mémoire.

III.5.3 Détection des accès aux ports interdits

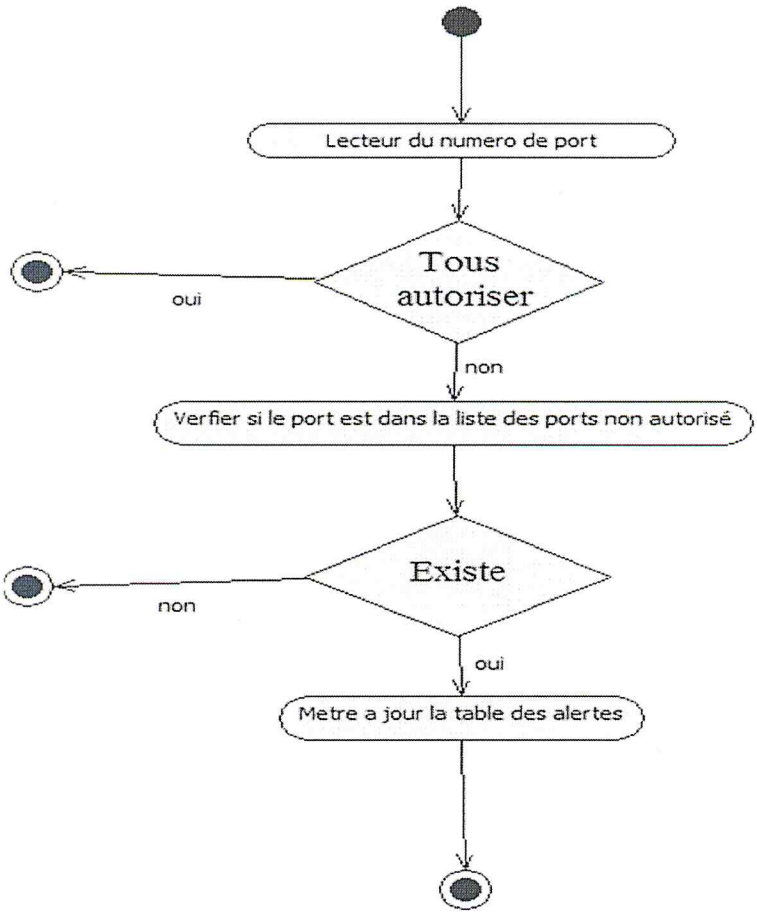


Fig. III.17 Diagramme d'activité de détection des accès aux ports

Vu que ce traitement s'effectue au même temps que la réception des ports, il doit être le plus rapide possible. Pour cette raison, la liste des ports non autorisées est chargée en mémoire.

III.6 DIAGRAMME DE COMPOSANTS

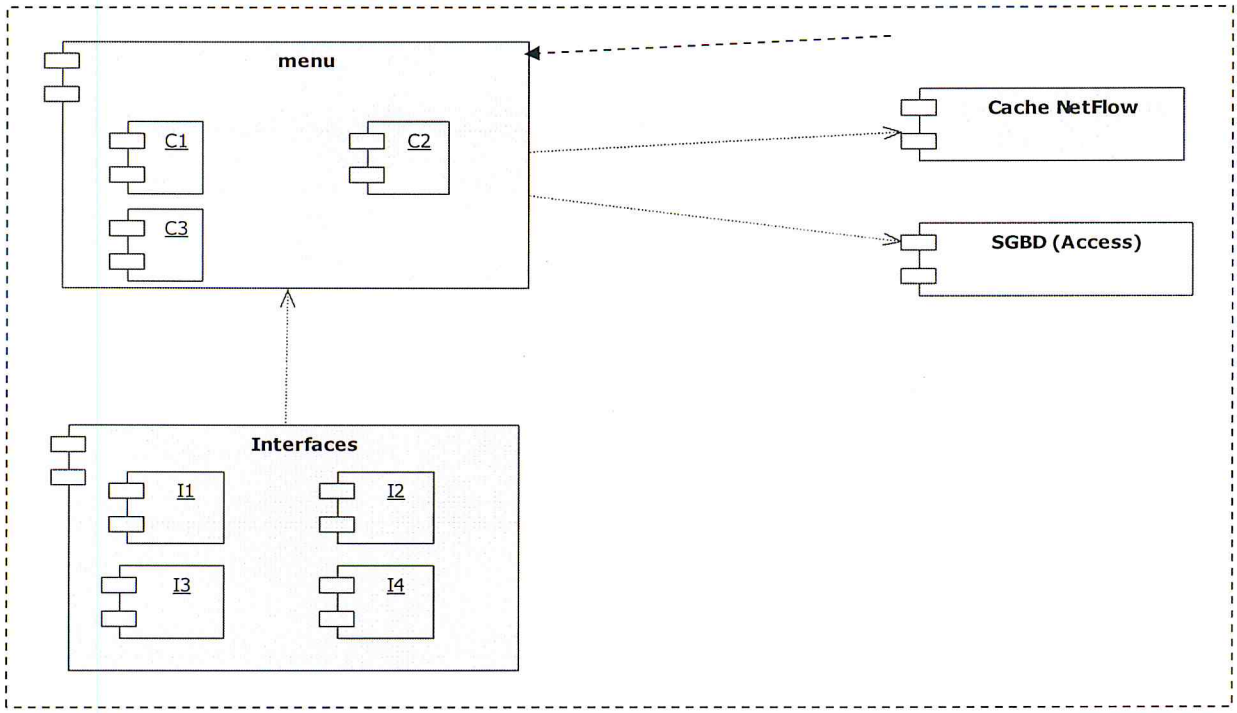


Fig. III.18 Diagramme de composants du système

Avec :

C1 : Collecteur NetFlow. **C2** : Gestion réseau.

C3 : Générateur de notification. **I1** : Interface capture.

I2 : Interface gestion réseau. **I3** : Interface gestion de notification.

I4 : Interface d'analyse.

III.7 DIAGRAMME DE DEPLOIEMENT

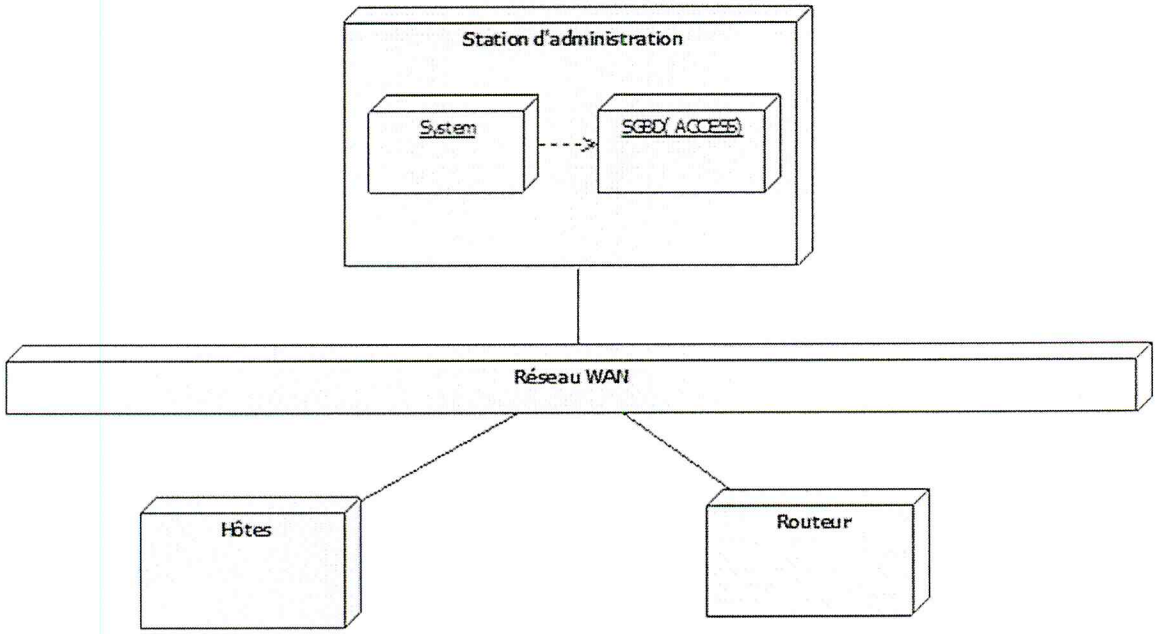


Fig. III.19 Diagramme de déploiement du système

Ce diagramme montre le déploiement de notre application sur les différents nœuds(Station d'administration, machine hôte) ainsi que les composants qui s'y trouvent sur ces nœuds:

La station d'administration qui gère les différents équipements du réseau contiendra un SGBD (MS Access) pour le stockage.

Cette station collectera les paquets NetFlow expédiés par le routeur. Elle communiquera à ce dernier les commandes CISCO pour le contrôle du flux.

III.8 LA BASE DE DONNEES

La figure suivante montre le schéma conceptuel de la base de donné de l'analyseur Netflow.

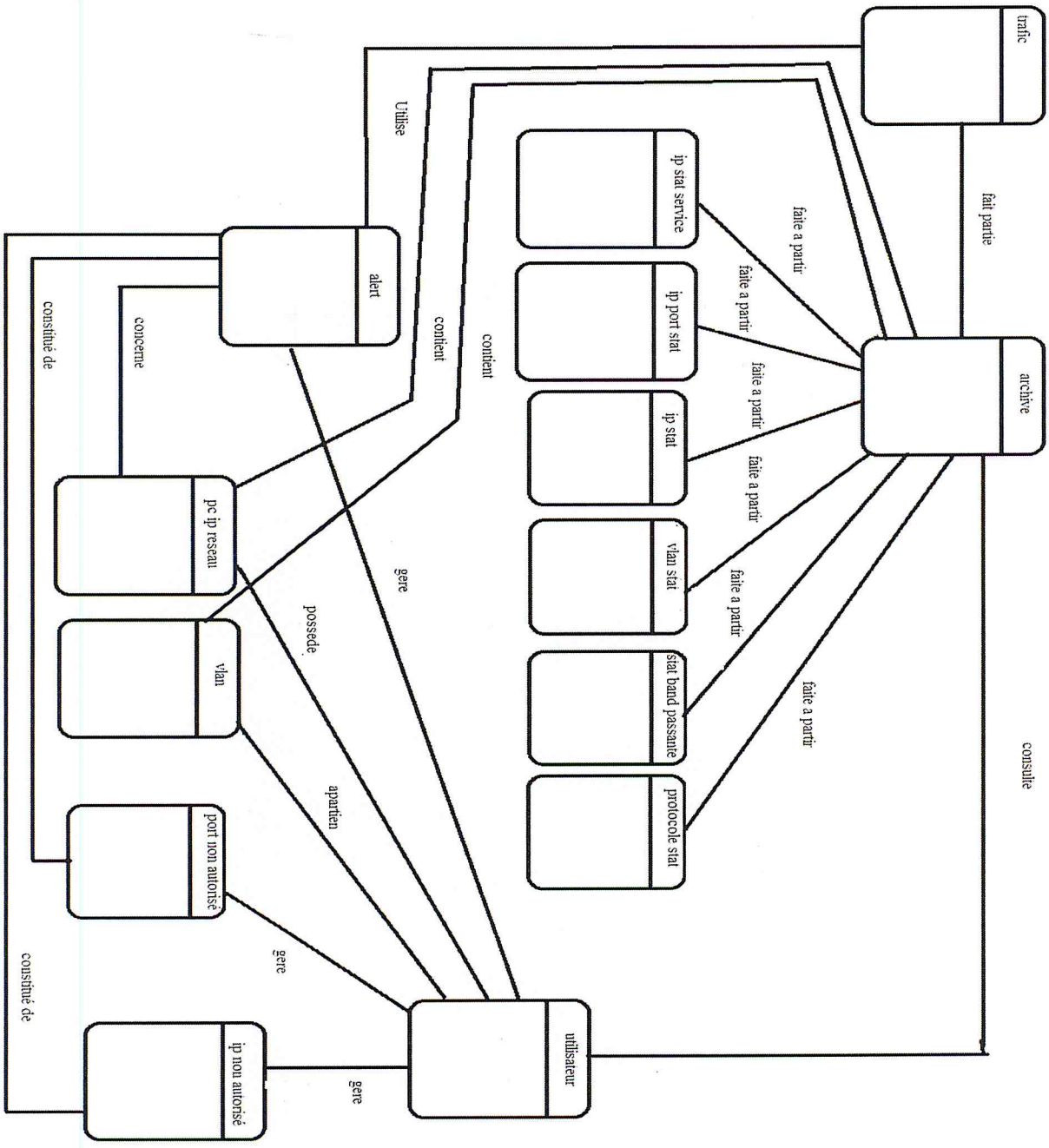


Fig. III.20 Schéma conceptuel de la base de données

CHAPITRE VI

Réalisation

CHAPITRE VI : REALISATION

INTRODUCTION

Nous avons réalisé une application qui donne accès, via une interface, à un large éventail d'informations obtenues par la collecte et l'analyse des données NetFlow. Notre application présente à l'administrateur le résultat d'une analyse et une synthèse faite sur les données sous forme de tables, graphiques ou alertes. De plus, elle donne à l'administrateur la possibilité de contrôler les flux.

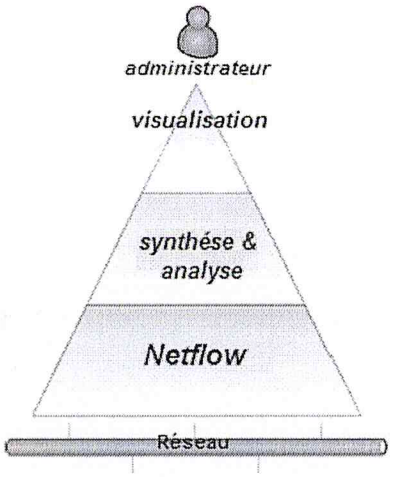


Fig. VI.1 : Architecture fonctionnelle de l'application

IV.1 Environnement matériel

Pour la réalisation de notre application, nous avons utilisé une station reliée à un réseau local. Ce réseau comporte un Switch de niveau trois : Cisco 3550 avec un IOS 12.1(22) EA1a. Ce dernier assure la fonction de routage et intègre la technologie Netflow.

IV.2 Environnement logiciel

Pour développer notre application nous avons opté pour l'utilisation du langage de programmation Delphi 7. Qui est un environnement de développement crée par Borland. Delphi permet de développer facilement et rapidement des applications visuelles pour Windows. La prise en main de Delphi est assez facile à

adopter. Delphi permet de développer des programmes Win32 et .NET à partir du même langage.

Pour la base de données nous avons utilisé le SGBD (Système de Gestion de Base de Données) Microsoft Access.

IV.4 PRESENTATION DE L'APPLICATION

Nous allons présenter dans cette dernière partie l'interface utilisateur de notre application. Nous commencerons par la console de contrôle locale qui permet de lancer les différents processus : collecte, visualisation et alerte. Elle permet aussi d'entrer les différents paramètres de configuration de la gestion réseau. Nous passerons en suite à une présentation générale des différents éléments du menu, nous verrons les différents interfaces regroupées par rubriques du menu.

IV.4.1 FENETRE D'AUTENTIFICATION:

Cette fenêtre va jouer le rôle d'un portail ou l'utilisateur va s'authentifier pour pouvoir accédé au menu et ces sous interfaces.

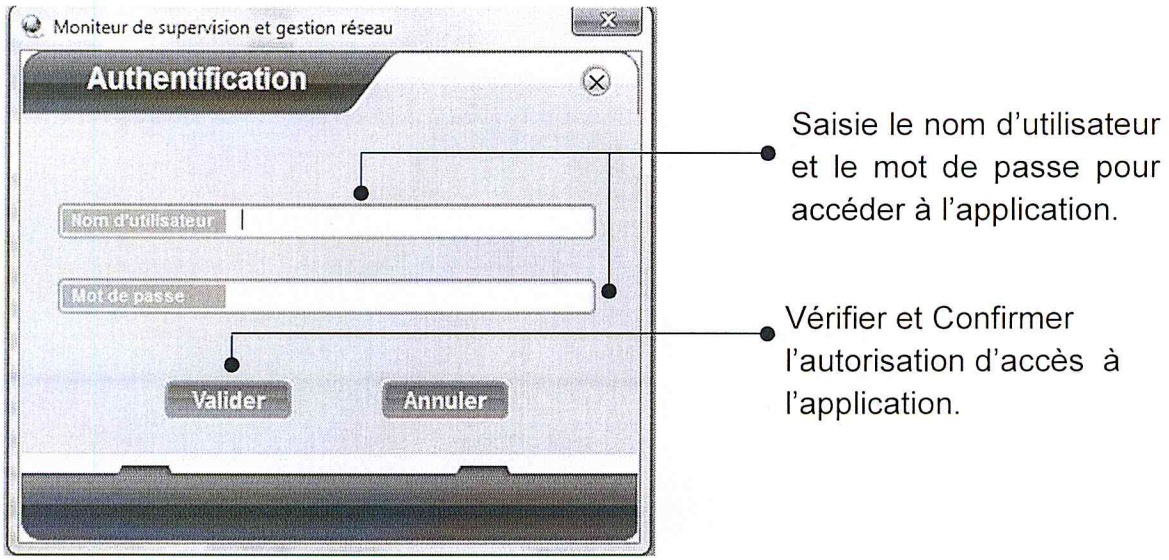


Fig. VI.2 : Fenêtre d'authentification

IV.4.2 L'ONGLET DE CAPTURE

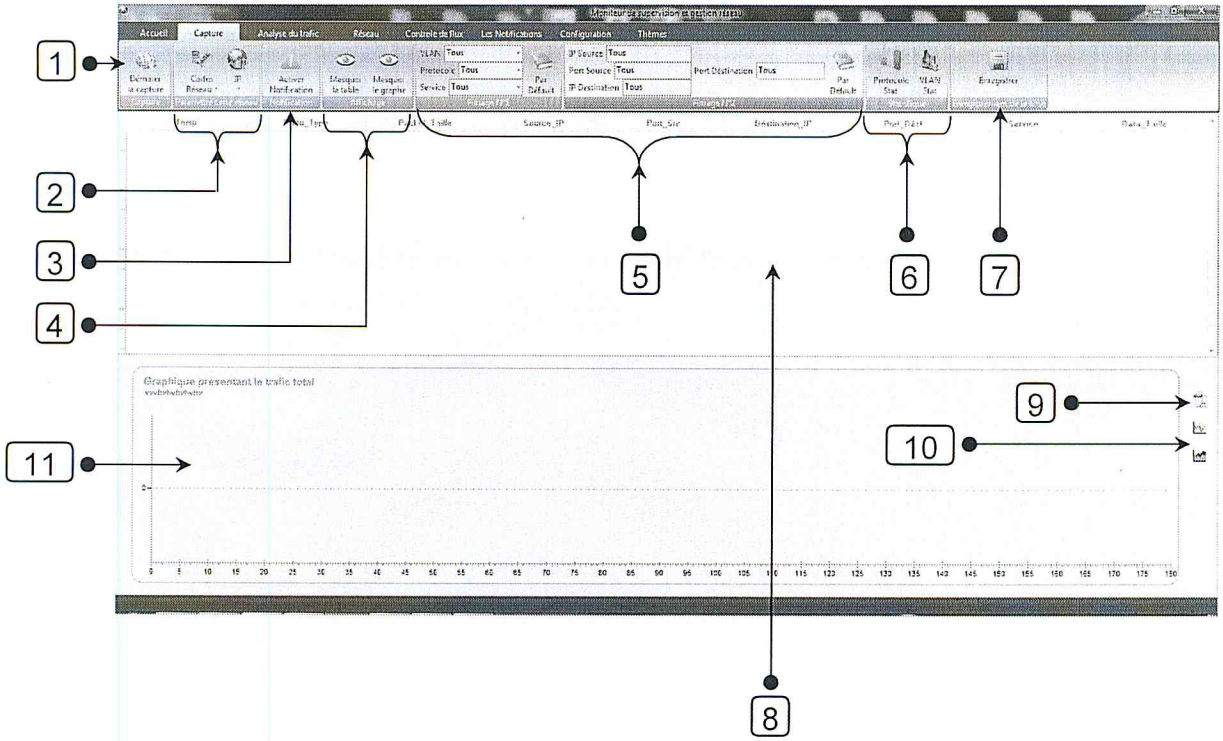


Fig. VI.3 : L'onglet de capture

1- Lancement de la capture et arrêt.
2- Choi de la carte réseau et l'adresse IP.
3- Activer ou désactiver les notifications.
4- Masqué ou afficher la table de la capture et le graphe.
5- Le filtrage de la capture.
6- Afficher les statistiques des protocoles et les VLANS.
7- Enregistrer la capture.
8- Zone d'affichage de la capture.
9- Enregistrer le graphe sous format PDF.
10- Choisir type de graphe a affiché.
11- Zone D'affichage des graphes.

IV.4.3 L'ONGLET D'ANALYSE RESEAU

Cet onglet permet à l'utilisateur de faire de différentes statistiques afin de mieux géré sont réseau.

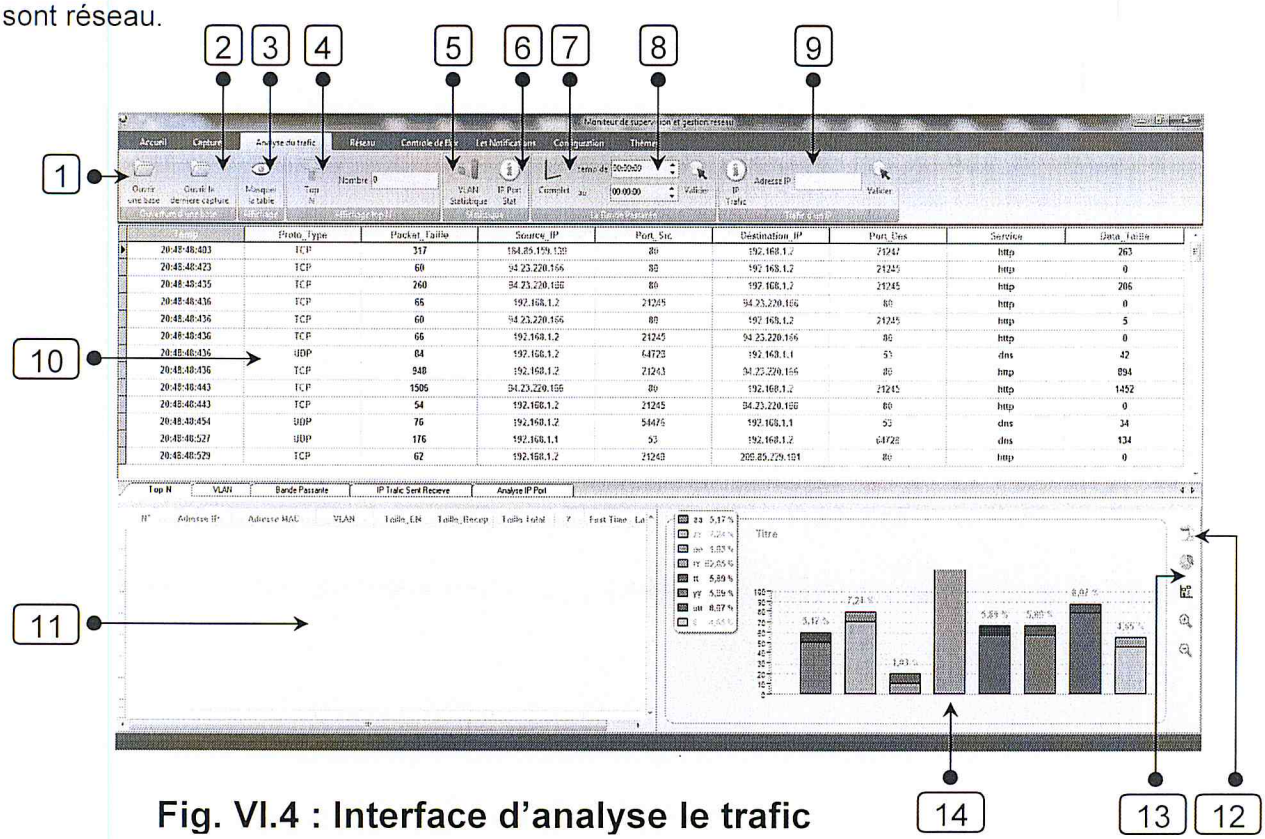


Fig. VI.4 : Interface d'analyse le trafic

1- Ouvrir une base de données.
2- Ouvrir la base de données de la dernière capture.
3- Masquer ou affiché la table d'analyse des paquets.
4- Afficher les tops N (les N premier Hôte qui consomme le plus de bande passante).
5- Statistiques sur les VLANS.
6- Statistiques sur les ports selon l'adresse IP.
7- Afficher le graphe de la bande passante au complet.
8- Choisir une période de temps où effectuer l'analyse.
9- Statistiques d'un hôte avec le reste du réseau.
10- Zone d'affichage de la capture.
11- Zone d'affichage le résultat de l'analyse.
12- Enregistrer le graphe sous format PDF.
13- Choisir type de graphe a affiché.
14- Le graphe.

VI.4.4 L'ONGLET GESTION RESEAU

Cet onglet permet les opérations de la gestion réseau telle que la gestion des Hôtes, VLAN, les adresses IP, les adresses MAC …

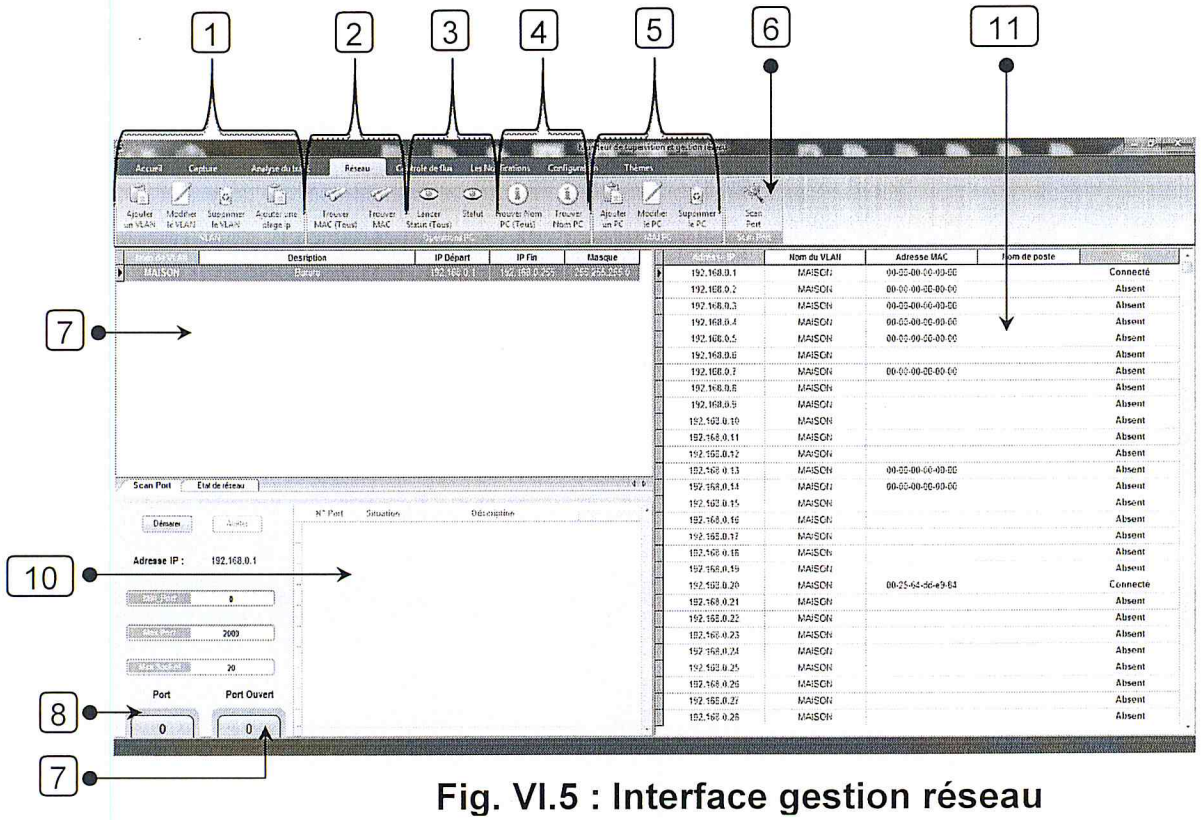


Fig. VI.5 : Interface gestion réseau

1- Gestion des VLANS.
2- Recherche d'adresse MAC.
3- Statut des Hôtes.
4- Trouver les noms des Hôtes.
5- Gestion des Hôtes.
6- Scanner les ports ouverts d'un Hôte (vulnérabilité).
7- Tables d'affichage des VLANS.
8- Nombre de ports parcouru pendant le scan des ports.
9- Nombre de ports ouvert trouvé.
10- Liste des ports ouverts avec leur information.
11- Liste des Hôtes d'un VLAN sélectionné.

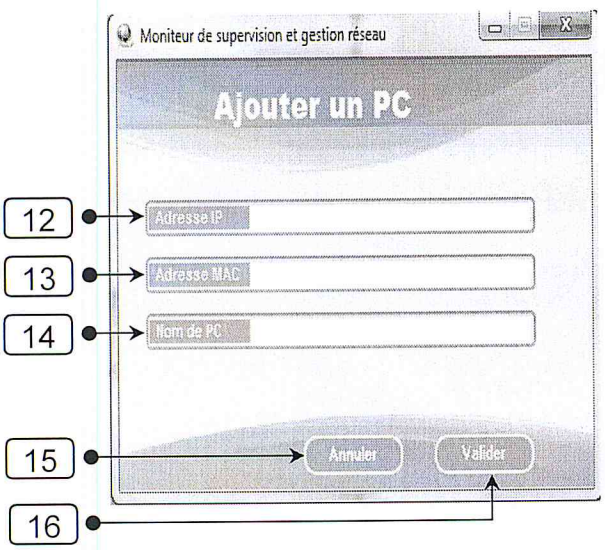


Fig. VI.6 : Interface d'ajout pc

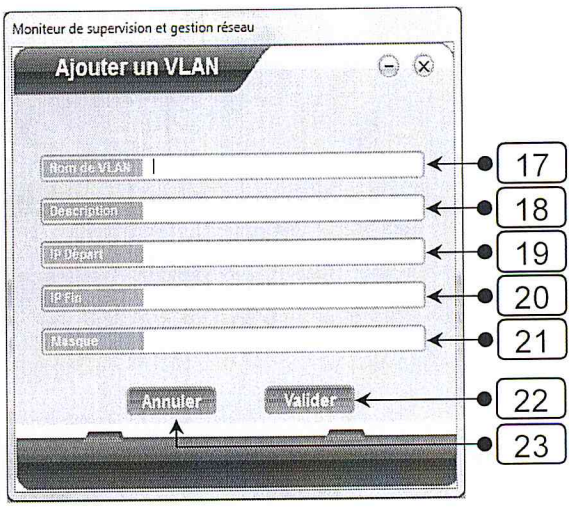


Fig. VI.7 : Interface d'ajout VLAN

12- Adresse IP du nouvel Hôte.
13- Adresse MAC du nouvel Hôte.
14- Nom du nouvel Hôte.
15- Annuler l'ajout d'un Hôte.
16- Valider l'ajout d'un Hôte.
17- Nom du nouveau VLAN.
18- Description du nouveau VLAN.
19- IP départ du nouveau VLAN.
20- IP fin du nouveau VLAN.
21- Masque sous réseau du nouveau VLAN.
22- Valider l'ajout d'un VLAN.
23-Annuler l'ajout d'un VLAN.

IV.4.5 L'ONGLET DE CONTROLE DE FLUX

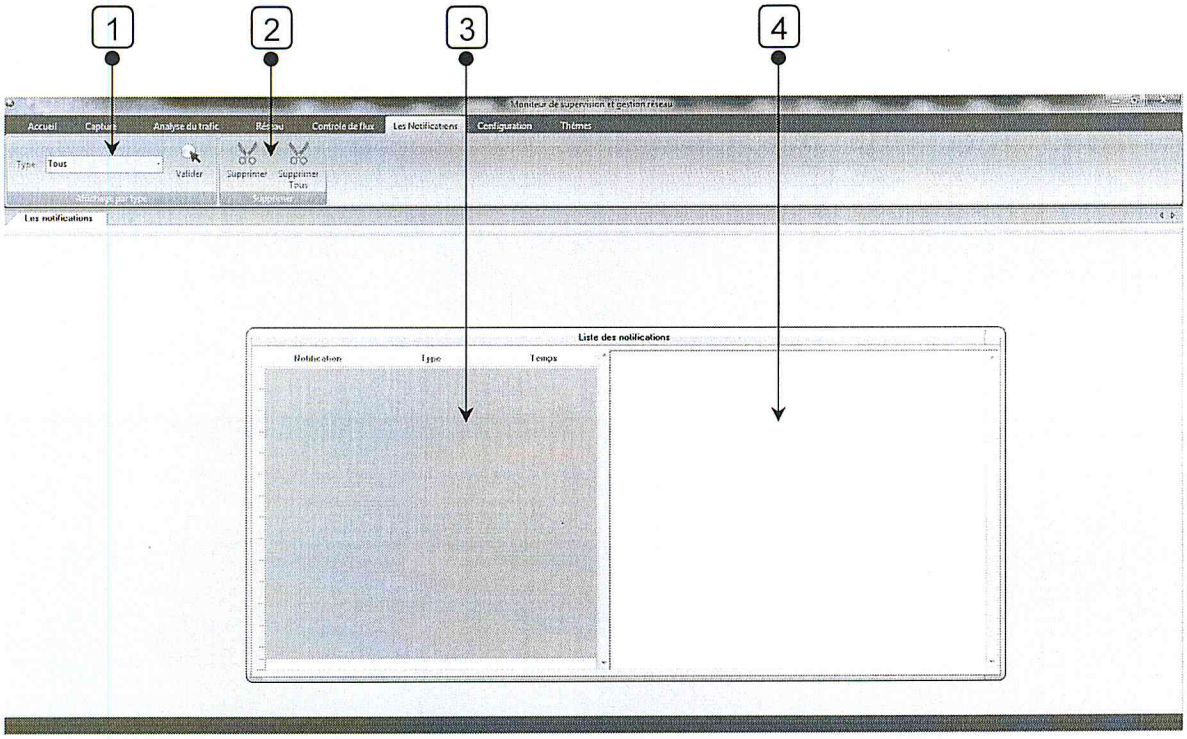


Fig. VI.8 : Interface d'affichage les notifications

1- Sélectionné le type de notification a affiché.
2- Supprimer une ou plusieurs notifications.
3- Table d'affichage de la liste de toutes les notifications.
4- Détails d'une notification sélectionnée.

IV.4.6 L'ONGLET DE CONFIGURATION

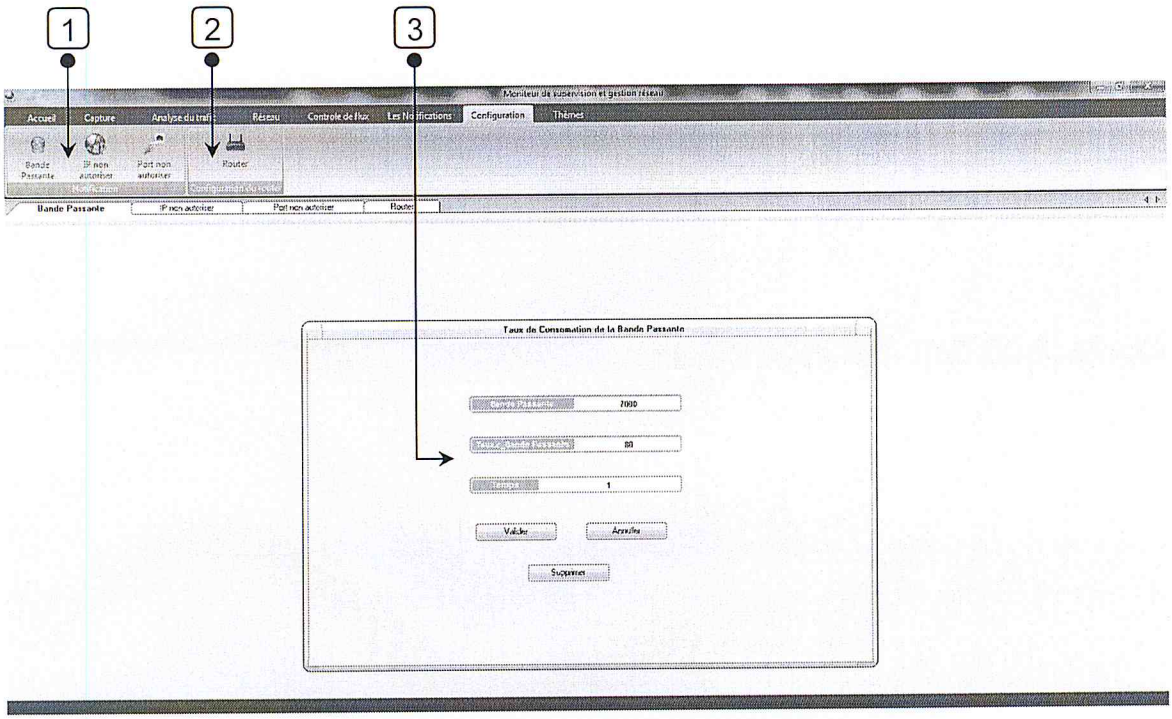


Fig. VI.9 : Interface configuration

1- Configuration des types de notification.
2- Configuration du router.
3- Configuration de notification de la bande passante, contient :
    - Débit maximum de la bande passante.
    - Taux de la consommation de la bande passante en pourcentage.
    - Période de vérification de la consommation.

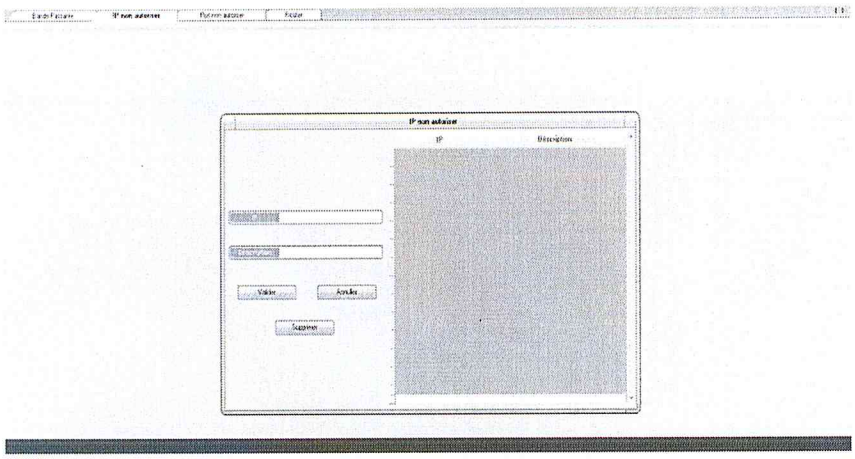


Fig. VI.10 : Interface configuration IP on autoriser (Notification)

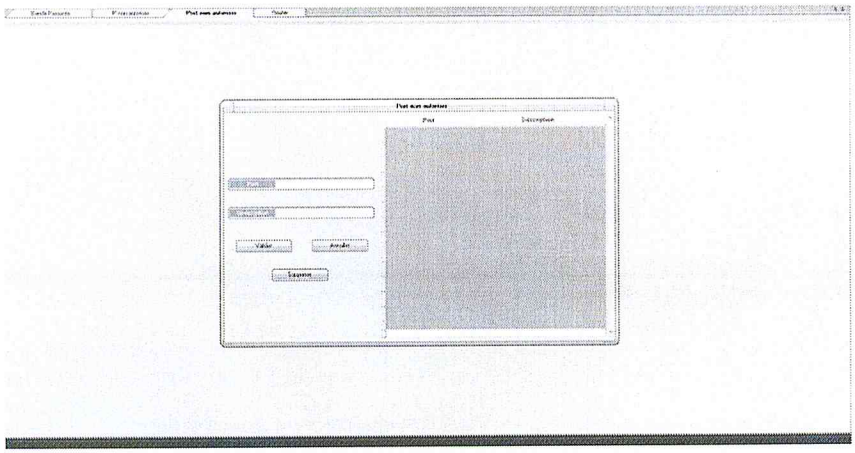


Fig. VI.11 : Interface configuration port on autoriser (Notification)

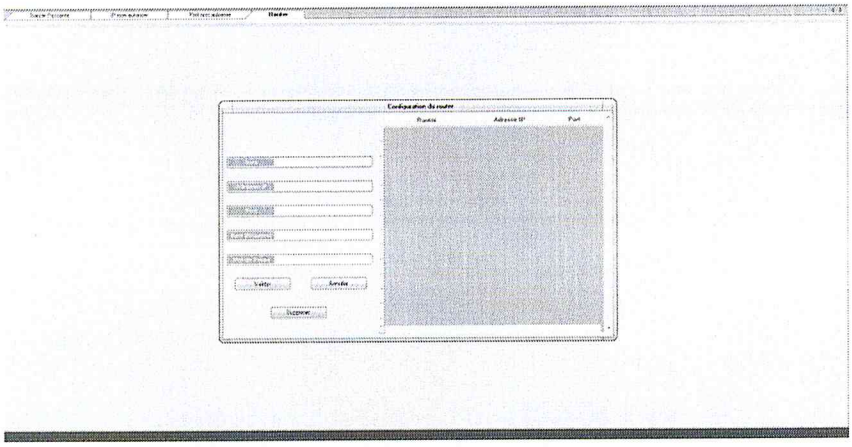


Fig. VI.12 : Interface configuration du routeur

IV.5 Test démonstratif du déroulement de l'application

Dans cette partie on va déroulé un exemple sur la mise en marche de notre application, on va commencer par lancer la capture sur un petite réseau Lan pendant un intervalle de temps puis trouver les 5 premiers hôte qui consomme le plus de bande passante (Top N) . Ensuite on fait des statistiques de chaque VLAN on se basant sur son taux d'échange de données. Par la suite on visualise le changement de consommation de bande passante durant un intervalle de temps pour détecter les pics de bande passante, ensuite on visualise les vulnérabilités de chaque hôte (port ouvert).

IV.5.1 la fenêtre principale de la capture

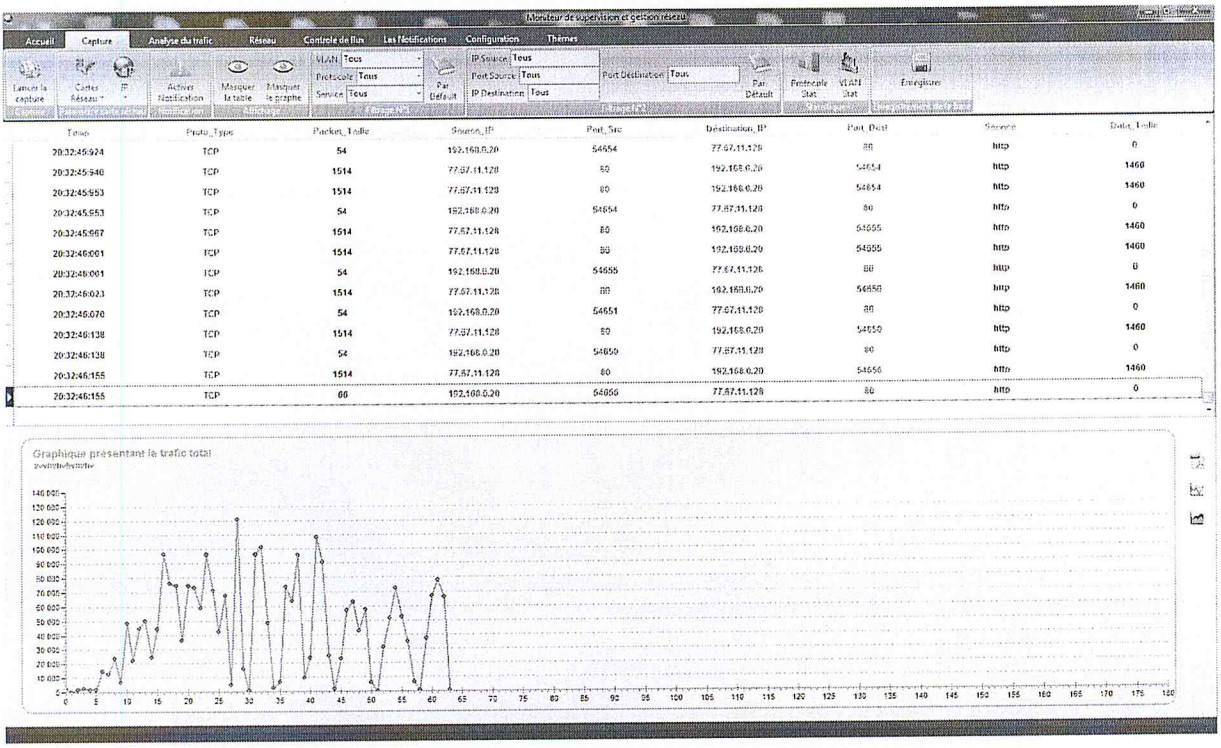


Fig. VI.13 : La fenêtre principale de la capture (Test)

IV.5.2 Top N

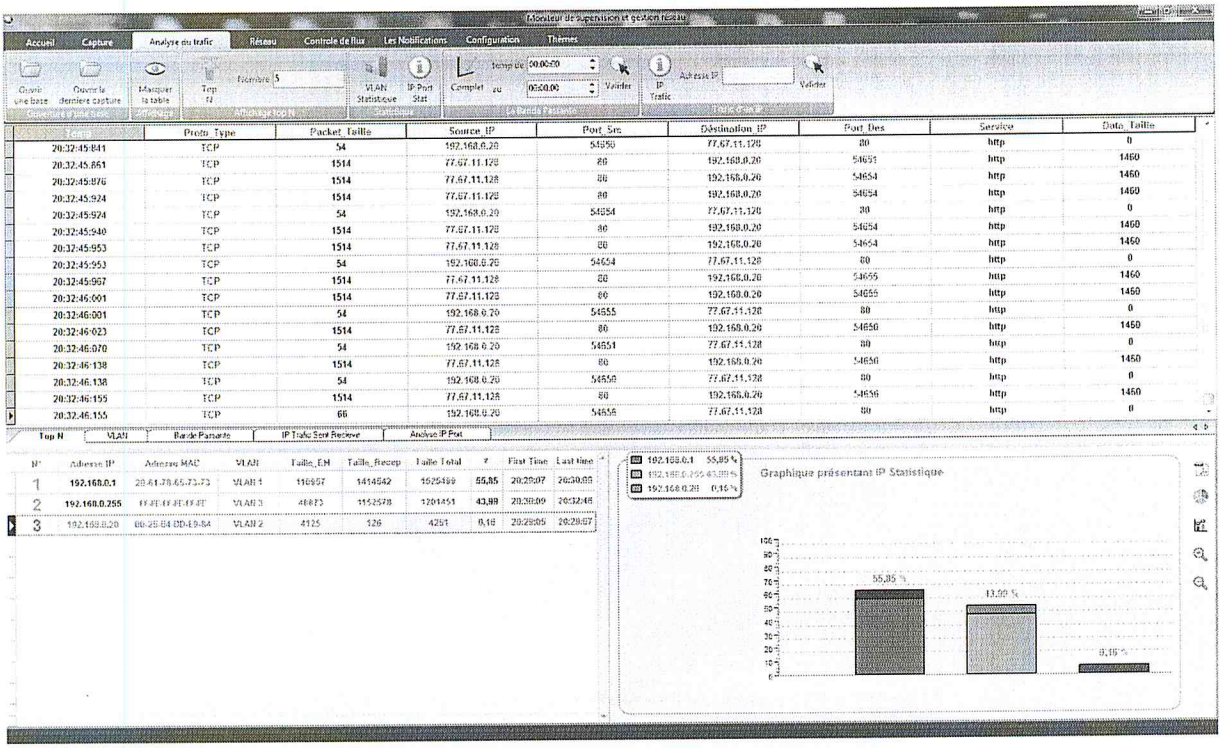


Fig. VI.14 : Top N (Test)

IV.5.3 VLAN Statistiques

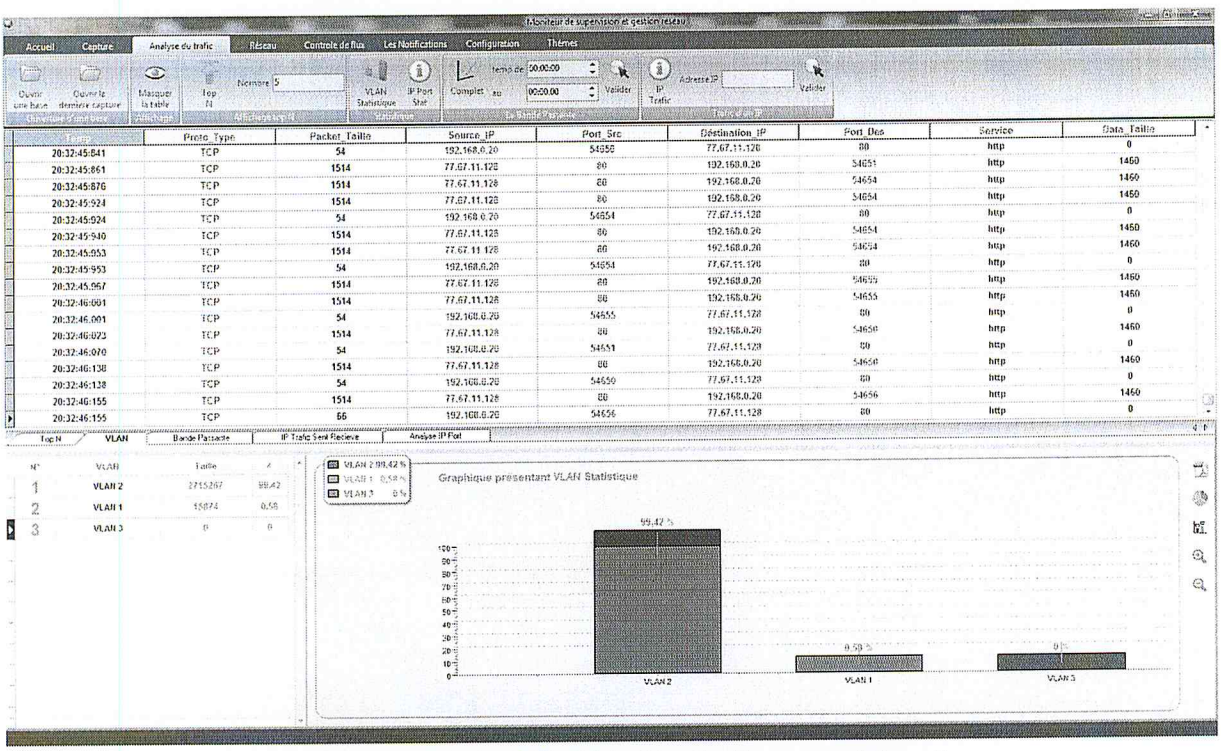


Fig. VI.15 : VLAN Statistiques (Test)

IV.5.4 Visualisation de la bande passante

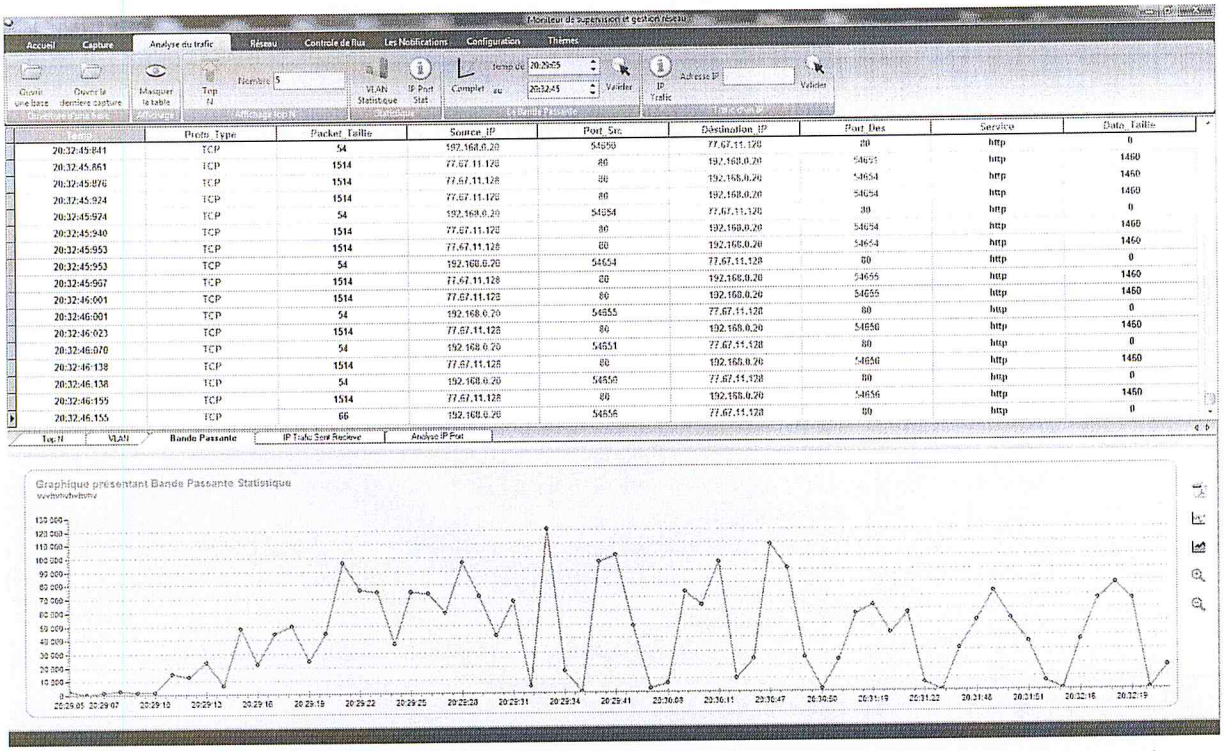


Fig. VI.16 : Interface de visualisation de la bande passante

IV.5.5 Visualisation les ports ouverts d'un hôte

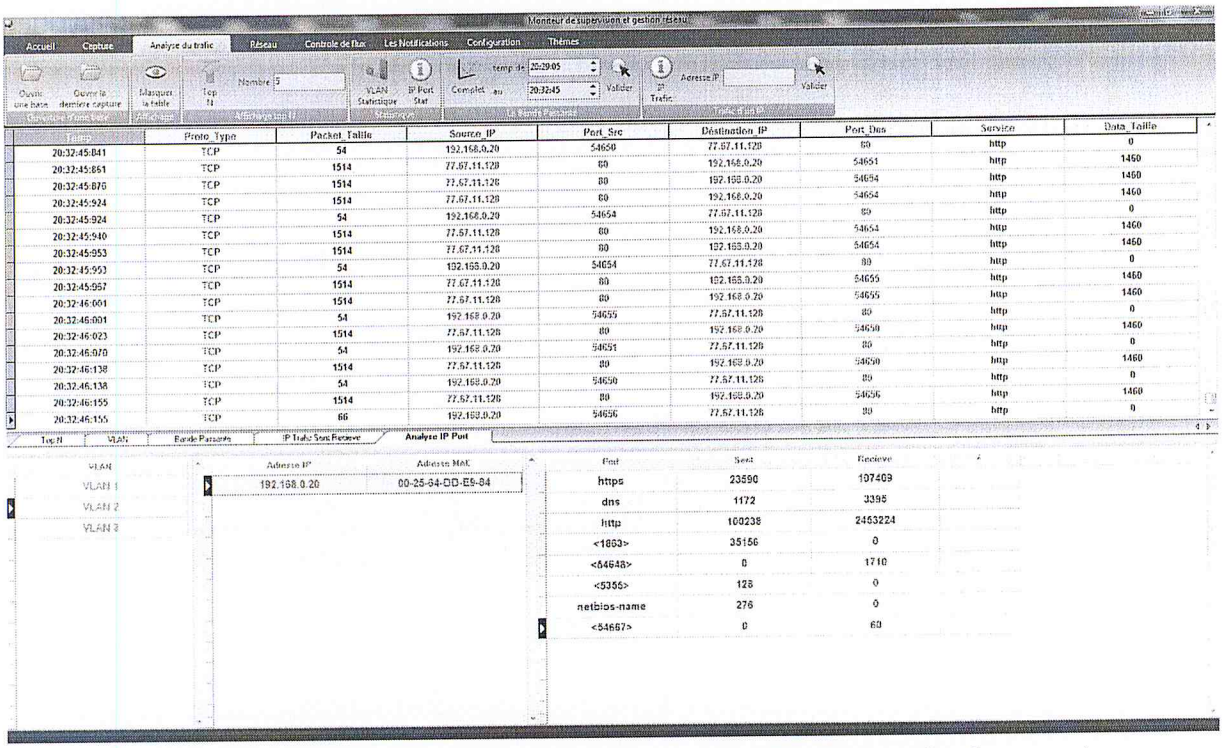


Fig. VI.17 : Les ports ouverts d'un hôte après la capture

CONCLUSION GENERALE ET PERSPECTIVES

CONCLUSION GENERALE ET PERSPECTIVES

La gestion des réseaux informatiques constitue, de nos jours, une des priorités pour le développement des entreprises. L'analyse du trafic est la condition primordiale pour une gestion efficace de ces réseaux. Elle permet d'obtenir des informations précises sur l'état du réseau, les applications en cours de fonctionnement et le comportement des utilisateurs. Ces informations permettent la planification et une meilleure gestion des ressources, des performances et de la sécurité du réseau.

Dans ce présent mémoire, nous avons donné un aperçu général sur l'administration des réseaux selon la normalisation OSI tout en s'intéressant à l'aspect fonctionnel de la gestion et ses enjeux. En suite, nous avons étudié la technologie Netflow de Cisco.

L'étude théorique que nous avons fait sur Netflow et ses différentes versions nous a permis d'extraire certaines informations qui peuvent être utilisées dans des processus d'analyse du flux afin d'améliorer la sécurité et la performance du réseau. Cette étude nous a servi de support pour réaliser une application de gestion de réseau.

Cette dernière permettant

- La visualisation du trafic et l'activité réseau.
- La génération des alertes en cas de comportement suspect des utilisateurs.
- Le contrôle le flux.
- La gestion des réseaux.

Finalement, et afin d'enrichir cette application, nous proposons comme perspectives:

- Validation des paramètres de QoS (qualité de service).
- Génération automatique des commandes CISCO selon le cas signalé.

Références bibliographiques :

[MEK 2005] :Mekfouldji Abderezak « Analyseur du trafic réseau Ethernet » projet fin d'étude ingénieur d'état en informatique Université Saad Dahleb Blida USDB 2005.

[CheNeg2004] : CHELLAL Abd El Hamid - NEGGAZI Brahim « Conception et réalisation d'un superviseur réseau Ethernet » projet de fin d'étude génie informatique
Ecole Militaire Polytechnique 2004.

[BenOul 2006] :Tayeb BENHADDAD - Youcef OULD YAHIA «APPLICATION D'ANALYSE DU FLUX RESEAU EN UTILISANT NETFLOW» projet de fin d'étude génie informatique 2006

[Chr 2004] : Christophe Fillot «Administration et métrologie pour un réseau IPv6» Service Informatique Université de Technologie de Compiègne 2004

Internet :

[Son10] : Site officiel de Sonatrach www.sonatrach-dz.com 2010 visité le 22/02/2011
[ADN 10]: ADNAVIGO IRS www.locoche.net 2010 visité le 10/03/2011
[WinP 05]: Site officiel du WinPcap www.winpcap.org 2005 visité 10/03/2011
[Wiki 10]: Wikipedia http://fr.wikipedia.org 2010 visité le 15/02/2011
[Cisc 10] :Cisco Systems, Inc www.cisco.com 2010 visité le 15/12/2010

Annexe

ANNEXE A

Transmission Control Protocol

TCP, acronyme de **Transmission Control Protocol**, est un protocole de transport fiable, en mode connecté, documenté dans la RFC 793 de l'IETF. Dans le modèle TCP/IP, TCP est situé entre la couche de réseau (généralement le protocole IP), et la couche application. Les applications transmettent des flux d'octets sur le réseau. TCP découpe le flux d'octets en segments, dont la taille dépend de la MTU du réseau sous-jacent (couche liaison de données).

Fonctionnement

Une session TCP fonctionne en trois phases :

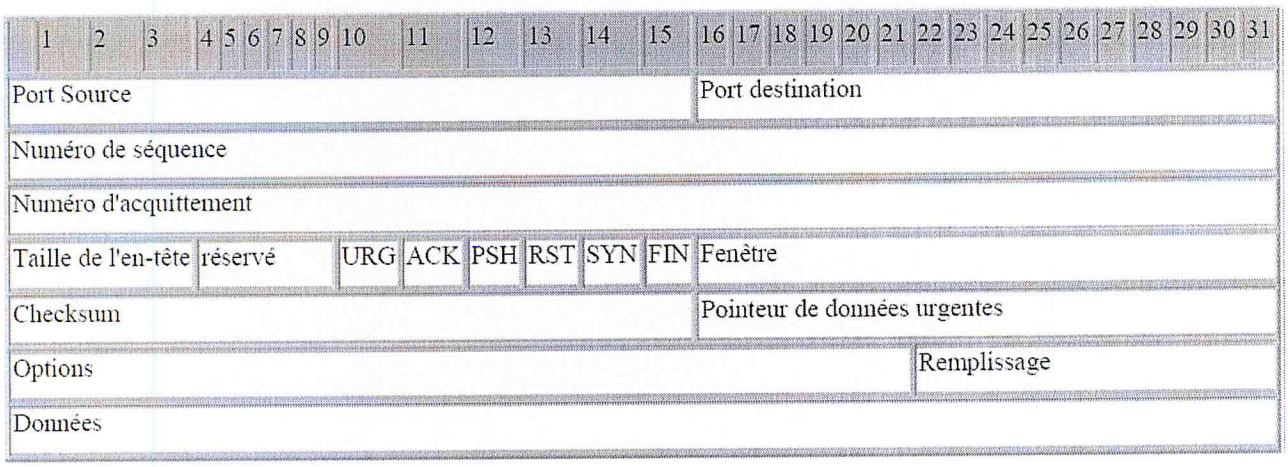
L'établissement de la connexion ;

Les transferts de données ;

La fin de la connexion.

L'établissement de la connexion se fait par une poignée de main en trois temps. La rupture de connexion, elle, utilise une poignée de main en quatre temps. Pendant la phase d'établissement de la connexion, des paramètres comme le numéro de séquence sont initialisés afin d'assurer la transmission fiable (sans perte et dans l'ordre) des données.

Structure d'un segment TCP



Signification des champs :

Port source : Numéro du port source

Port destination : Numéro du port destination

7Numéro de séquence : Numéro de séquence du premier octet de ce segment

Numéro d'acquittement : Numéro de séquence du prochain octet attendu

Taille de l'en-tête : Longueur de l'en-tête en mots de 32 bits (les options font partie de l'en-tête)

Réservé : Réservé pour un usage futur Drapeaux

- o URG : Signale la présence de données UR Gentes
- o ACK : Signale que le paquet est un accusé de réception (ACK nowledgement)
- o PSH : Données à envoyer tout de suite (PuSH)
- o RST : Rupture anormale de la connexion (ReSeT)
- o SYN : Demande de SYNchronisation ou établissement de connexion
- o FIN : Demande la fin de la connexion

Fenêtre : Taille de fenêtre demandée, c'est-à-dire le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception

Checksum : Somme de contrôle (CRC, Cyclic Redundancy Check) calculé sur l'ensemble de l'en-tête TCP et des données, mais aussi sur un pseudo en-tête (extrait de l'en-tête IP)

Pointeur de données urgentes : Position relative des dernières données urgentes

Options : Facultatives

Remplissage : Zéros ajoutés pour aligner les champs suivants du paquet sur 32 bits, si nécessaire

Données : Séquences d'octets transmis par l'application (par exemple: +OK POP3 server ready, ...)

Établissement d'une connexion

Même s'il est possible, pour deux systèmes, d'établir une connexion entre eux simultanément, dans le cas général, un système ouvre un 'socket' (point d'accès à une connexion TCP) et se met en attente passive de demandes de connexion d'un autre système. Ce fonctionnement est communément appelé *ouverture passive*, et est utilisé par le côté *serveur* de la connexion. Le côté *client* de la connexion effectue une *ouverture active* en envoyant un segment SYN au serveur, ce qui constitue la première étape de la poignée de mains en trois temps. Le serveur doit répondre à un segment SYN valide par un segment SYN/ACK. Enfin, le client répond au serveur avec un segment ACK, complétant la poignée de main en trois temps, et donc la phase d'établissement de la connexion

Transferts de données

Pendant la phase de transferts de données, certains mécanismes clefs permettent d'assurer la robustesse et la fiabilité de TCP. En particulier, les numéros de séquence sont

utilisés afin d'ordonner les segments TCP reçus et de détecter les données perdues, les checksums permettent la détection d'erreurs, et les acquittements ainsi que les temporisations permettent la détection des segments perdus ou retardés. Pendant la phase d'établissement de la connexion, les numéros de séquence initiaux sont échangés par les deux interlocuteurs. Ces numéros de séquence sont utilisés pour décompter les données dans le flux d'octets. On trouve toujours deux de ces nombres dans chaque segment TCP, qui sont le numéro de séquence et le numéro d'acquittement. Le numéro de séquence représente le propre numéro de séquence de l'émetteur TCP, tandis que le numéro d'acquittement représente le numéro de séquence du destinataire. Afin d'assurer la fiabilité de TCP, le destinataire doit acquitter les segments reçus en indiquant qu'il a reçu toutes les données du flux d'octets jusqu'à un certain numéro de séquence. Une amélioration de TCP, nommée acquittement sélectif (selective ackn owlegement ou SACK), autorise le destinataire TCP à acquitter des blocs de données reçus dans le désordre.

Terminaison d'une connexion

La phase de terminaison d'une connexion utilise une poignée de main en quatre temps, chaque extrémité de la connexion effectuant sa terminaison de manière indépendante. Ainsi, la fin d'une connexion nécessite une paire de segments FIN et ACK pour chaque extrémité.

ANNEXE B

Configuration de NetFlow :

Pour configurer NetFlow, il faut d'abord que le routage soit correctement configuré. Apres cela entrez les commandes suivantes en mode configuration de l'IOS.

	Actions	commande
Etape1	Indiquez l'interface, et entrez dans l'interface en mode configuration.	**interface** *vlan/port*
Etape2	Activer le NetFlow	**ip route-cache flow**

Ces commandes activent le cache flow, ce qui permet d'enregistrer les statistiques concernant le trafic IP, la taille par défaut du cache est de 65536 entrées, cette taille peut être configurée entre 1024 et 524228 entrées avec la commande suivante :
Pour désactiver le cache flow utilisez la commande **no ip route-cache flow**

Configurer le nombre d'entrées du cache flow **ip flow-cache entries** *number*	`ip flow-cache entries 1024`

Après que le cache soit activé, nous pouvons configurer l'export de NetFlow :

Indiquez l'adresse de destination, le port de destination. **ip flow-export** *ip-address* *udp-port* [**version 1**]	`Ip flow-export 1.1.15.1 0 version 5`

La version de NetFlow par défaut est la version 1.

On peut aussi configurer le Timeout active et le Timeout inactive qui sont respectivement le nombre de minutes pondant lesquelles le flux peut resté active avant d'êtres exporté, et le nombre de seconde pondant lesquelles le flux est resté inactive avant d'être exporté.

Timeout inactive	**ip flow-cache timeout inactive** *<seconds>*
Timeout inactive	**ip flow-cache active inactive** *<minutes>*

Les valeurs par défaut sont 15 secondes pour le Timeout inactive et de 30 minutes pour le Timeout active.

Visualiser les statistiques sur l'export et le contenue du cache et éventuellement

Statistique sur le cache	**show ip route flow**
Effacer le contenue du cache	**clear ip flow stats**
Statistique sur l'export	**show ip flow export**

l'effacer :

Voici un exemple de configuration :

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config) #int vlan1

Router(config-if)#ip route-cache flow

Router(config-if)#exit

Router(config) #int fastethernet0/1

Router(config-if)#ip route-cache flow

Router(config-if)#exit

Router(config)#ip flow-export 192.100.21.34 60 version 5

Router(config)#ip flow-cache timeout inactive 15

Router(config)#ip flow-cache timeout active 30

Router(config)#ip flow-cache entries 65536

Annexe D

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version																Count															
System Uptime																															
UNIX Seconds																															
Package Sequence																															
Source ID																															

Netflow Version9 :En-tête

Description des champs

NetFlow Version 9 :le format de la TempateFlowSet

Champ	Description
Version	Le numéro de la version NetFlow (ici c'est 9)
Count	Le nombre de FlowSet (template et data) contenue dans le paquet
System Uptime	Temps en millisecondes depuis le démarrage de l'équipement qui a exporté le NetFlow.
UNIX Seconds	Nombre de secondes écoulés depuis le 1 janvier 1970 :Timestamp Unix
Sequence Number	Compteur de paquets exportés par l'équipement; cette valeur est cumulative, elle peut être employée pour identifier si des paquets ont été perdus au cours de l'exportation. NB: Dans les version 5 et 8,ce champs représente "total flows."
Source ID	La valeur de sourceID est sur 32 bits. Elle permet d'identifier la source des paquets NetFlow.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
FlowSet ID = 0															
Length															
Template ID															
Field Count															
Field 1 Type															
Field 1 Length															
Field 2 Type															
Field 2 Length															
-															
Field N Type															
Field N Length															
Template ID															
Field Count															
Field 1 Type															
Field 1 Length															
Field 2 Type															
Field 2 Length															
-															
Field N Type															
Field N Length															

Description des champs:

Champ	Description
FlowSetID	Ce champ est utilisé pour distinguer les templates des données (Data).Les templates ont toujours un FlowSetID entre 0 et 255. La template qui décrit les champs qui la succèdent immédiatement porte un FlowSetID=0 et celle qui décrit les champs optionnels porte un FlowSetID=1. Un enregistrement de données porte toujours un FlowSetID > 255.
Length	La longueur totale du FlowSet. Cette valeur permet de déterminer le début du prochain FlowSet (qui peut être soit une template FlowSet soit un Data FlowSet).
Template ID	Un routeur génère des template FlowSet pour décrire les données qu'il va exporter. il alloue à chaque template un ID unique afin d'identifier les données qu'elle décrit.
Field Count	Indique le nombre de champs dans la template désignée juste au-dessus.
Field Type	C'est une valeur numérique qui représente le type du champ. Les valeurs possibles du type de champ sont détaillées dans la table (4).
Field Length	Donne la longueur du champ (en octe) définie au-dessus.

NetFlow Version 9 : Format de Data FlowSet

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
FlowSet ID = Template ID															

Length
Enregistrement 1 - Valeur du champ 1
Enregistrement 1 - Valeur du champ 2
Enregistrement 1 - Valeur du champ 3
Enregistrement 1 - Valeur du champ 4
-
Enregistrement 1 - Valeur du champ N
Enregistrement 2 - Valeur du champ 1
Enregistrement 2 - Valeur du champ 2
Enregistrement 2 - Valeur du champ 3
-
Enregistrement 2 - Valeur du champ N
-
Padding

Description des champs :

Champ	Description
FlowSet ID = Template ID	Le champ FlowSet ID réfère la template qui décrit le présent Data FlowSet
Length	Ce champ donne la longueur du Data FlowSet.
Enregistrement N – Valeur du champ N	Le reste des enregistrements FlowSet est une collection de valeurs de champs. Le type et la longueur de ces champs sont définis dans la template correspondante (désignée par FlowSet ID/template ID)
Padding	Les bits de remplissage sont ajoutés pour aligner la fin du FlowSet sur 32 bits. Il faut noter que ces bits sont inclus lors du calcule de la longueur du FlowSet.

Résumé

Ce projet rentre dans le cadre de développement des applications de gestion des réseaux.

Après une étude théorique sur les réseaux informatique et leur gestion nous avons abordé les différents aspects de la technologie Netflow.

Enfin, nous avons réalisé une application qui permet de superviser l'état du réseau, avoir des rapports d'activités ainsi qu'un mécanisme d'alertes se basant sur les tendances et le comportement des utilisateurs du réseau, le contrôle de circulation des paquets et le flux sur le réseau et quelques méthodes d'analyse des paquets Netflow.

Mots clefs

Netflow, analyse du trafic réseau, Supervision, gestion des réseaux, Notification, Paquets.

Abstract

This project falls within the application development of network management. After a theoretical study of computer networks and their management we discussed the various aspects of Netflow technology.

Finally, we realized an application thatallows the user to monitornetwork status, haveactivity reportsand analertmechanismbased on thetrendsand behavior ofnetwork users, control of movement ofpacketsand the flowon the networkand somemethods of analysis ofNetflowpackets.

Keywords

Netflow, network traffic analysis, Supervision, network management, notification, Packages.

ملخص :

هذا المشروع يندرج في تطوير التطبيقات لإدارة الشبكة. بعد دراسة نظرية لشبكات الكمبيوتر وإدارتها ناقشنا مختلف جوانب التكنولوجياNetflow .

أخيرا، طورنا برنامجا يتيح للمستعمل مراقبة حالة الشبكة، انشاء تقارير عن الأنشطة وآلية التنبيهات مبنية على اتجاهات و سلوك مستخدمي الشبكة، ومراقبة التدفق على الشبكة و بعض طرق التحليلNetflow.

مفاتيح :

تسيير شبكات المعلوماتية

Netflow,.