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

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention

Du Diplôme de Master II en Electronique

Option : Réseaux et télécommunication

Thème :

Implémentation d'une politique de sécurité au réseau informatique de l'entreprise ENIEM de Tizi-Ouzou

Proposé et dirigé par :

Mr. BOUTALEB Salim
Mr. LAHDIR Mourad

Présenté par :

Mlle .ALICHE Sonia
Mr. HADDAD Abbas

Année universitaire 2010/2011

Remerciements

Nous remercions tout d'abord, Allah qui nous a donné la force et le courage pour terminer nos études et élaborer ce modeste travail.

Nous tenons à exprimer nos plus sincères remerciements à notre promoteur Mr.Lahdir, qui nous a aidés tout au long du travail.

Un grand merci à notre Co-promoteur Mr.Boutaleb(ENIEM) pour ses encouragements et ses orientations qui nous ont beaucoup aidés au cours de notre projet.

Nous sommes aussi reconnaissants à Mr.Khaldi(ENIEM) qui nous a aussi soutenus et un grand merci à Mr.Mamou pour ses informations qui nous a beaucoup servis.

Nous tenons à remercier également nos amis (es) etnos familles pour leurs aides considérables.

Dédicaces

« Louange à Dieu, le seul et unique »

Je dédie ce modeste travail a mes chers parents, ma chère grand-mère pour tous leur sacrifices et soutiens durant la préparation

merci infiniment,

A mes plus chers frères surtout Samir et a mes chères sœurs

A ma petite sœur Thilleli

A mon neveu Momoh

A tous mes ami(es) avec lesquels j'ai partagé les bons et les mauvais moments :Yacine, Amar, Abbas, Samia, Dihia, Lila, Zazi, Sonia

A tout ceux qui mon aidé de prés ou de loin.

(Sonia)

Dédicaces

« Louange à Dieu, le seul et unique »

Je dédie ce modeste travail à tous ceux que j'aime ainsi que ceux qui m'aiment.

(Abbas)

Sommaire

Chapitre I : Presentation du l'organisme d'acceuil

Chapitre II : Généralités sur les réseaux informatiques

Chapitre III : Sécurité des réseaux informatiques

Chapitre IV :Mise en place d'un plan de sécurité pour le réseau informatiquede l'ENIEM

Introduction générale

Si les premiers réseaux de données se limitaient à échanger des informations reposant sur des caractères entre des systèmes informatiques connectés, aujourd'hui les découvertes en matière de supports étendent sans cesse la portée de nos communications. Parconséquent, les réseaux modernes ont évolué pour prendre en charge le transfert audio, des flux vidéo, du texte et des graphismes entre des périphériques de types très différents. Des moyens de communication autrefois séparés et bien distincts convergent maintenant sur une plateforme commune. À l'image de tous les progrès dans le domaine des technologies de la communication, la création et l'interconnexion de réseaux de données solides ont un profond impact, la technologie constitue peut-être aujourd'hui le principal vecteur de changement au monde car elle contribue à créer un univers dans lequel les frontières nationales, les distances et les limites physiques perdent de leur importance et représentent de moins en moins des obstacles. Comme Internet connecte les individus et favorise des communications informelles, il constitue la plateforme permettant de travailler, de résoudre des urgences et d'informer. Il prend également en charge l'enseignement, les sciences et le gouvernement.

Ainsi pour bénéficier des grands avantages que l'interconnexion des réseaux apportent, de plus en plus d'entreprises ouvrent leurs systèmes d'informations a leurs partenaires ou leurs fournisseurs afin de satisfaireleurs besoins commerciaux et faire face aux insuffisances de l'utilisation des réseaux locaux en terme de communication, et dans ce cas, lorsque la sécurité d'un réseau est compromise, de très graves conséquences peuvent en résulter, comme l'atteinte à la vie privée, le vol d'informations et même l'engagement de la responsabilité civile et pour rendre cette situation encore plus difficile, les types de menaces potentielles sont en évolution constante. De plus, la difficulté que représente la sécurité dans son ensemble est de trouver un compromis entre deux besoins essentiels : le besoin d'ouvrir des réseaux pour profiter de nouvelles opportunités commerciales et le besoin de protéger des informations privées ou publiques et des informations commerciales stratégiques. Pour cela la sécurité se place actuellement au premier plan de la mise en œuvre et de l'administration réseau. Donc, L'application d'une stratégie de sécurité efficace est l'étape la plus importante qu'une entreprise doit franchir pour protéger son réseau. Cette stratégie définit les directives concernant les activités et les ressources nécessaires à la sécurisation d'un réseau d'entreprise.

En effet, la sécurité des réseaux ne peut pas être garantie a cent pour cent, néanmoins plusieurs techniques sont utilisées pour diminuer le risque des menaces et d'attaques qui peuvent être soit intentionnel ou accidentel. Et à cet effet, l'objectif visé dans notre travail de mémoire est d'implémenter une politique de sécurité basée sur le principe de

filtrage,del'organisation et de l'administration du réseau informatique de l'entreprise nationale ENIEM. Et comme le matériel réseau utilisé au sein de cette entreprise est pratiquement le matériel CISCO, donc la mise en œuvre de la politique de sécurité est inspirée de différentes techniques, méthodes et stratégies qui caractérisent ce matériel.

Notre mémoire est structuré en quatre chapitre, le premier consiste à présenter l'organisme d'accueil de l'entreprise ENIEM ou nous avons effectué notre stage pratique, le deuxième chapitre intitulé « généralités sur les réseaux informatiques», a pour but de donner des informations sur les réseaux et les différents éléments constituant un réseau ,le troisième chapitre présente le rôle de la sécurité contre les différentes attaques et menaces qui peuvent endommager le bon fonctionnement d'un réseau et en suite expose des méthodes et astuces pour protéger son réseau, et dans le quatrième chapitre après avoir étudier les failles et anomalies du réseau existant de l'entreprise ENIEM ce chapitre propose une politique de sécurité qui portera une bonne administration du réseau et qui propose une configuration basé sur un système de filtrage des différentes entités.

I.1.Introduction

Suite à la phase difficile que traverse notre économi,.Les entreprises publiques économiques doivent faire des efforts pour conformer aux nouvelles exigences technologiques et aux normes internationales de leurs produits ; ce qui oblige la certification à l ' I S O 9002 à fin de permettre une bonne compétitive à l'entreprise.

I.2. Situation géographique

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

I.3. Historique de l'organisme ENIEM

ENIEM résulte d'un contrat "produit en main" établi dans le cadre du premier plan quadriennal, et signé le 21 Août 1971 avec un groupe d'Entreprises allemandes représentées par le chef de file D.I.A.G (Société allemande) pour une valeur de 400 millions de dinars les travaux de Génie Civil ont été entamés en 1972 et la réception des bâtiments avec tous les équipements nécessaires a eu lieu en juin 1977.

En 1983, l'ENIEM issue la restructuration de SONELEC en 1983, elle est donc une entreprise au statut de la société nationale.

En 1989, l'ENIEM est passée à l'autonomie, les premières réformes ont été engagées et dans ce cadre l'ENIEM fut dotée de tous les organes de gestion légaux:

- Une assemblée Générale.
- Un Conseil d'Administration
- Un Capital Social.

Ainsi que le redéploiement des activités à l'intérieur de l'unité ces plans d'extension et de redéploiement de l'ENIEM se conjuguent directement avec ses autres programmes relatifs à la formation et à l'amélioration de la gestion, de la maintenance et de la qualité.

I.4. La gamme de production

- Réfrigérateurs 1601, 200 1, 2401 – 1 porte (2 étoiles)
- Réfrigérateurs 300 D, 290 C - 2 porte (3 étoiles)
- Congélateur vertical 220F - 1 porte, (4 étoiles)
- Réfrigérateur vertical 350 S - 1 porte, 2 étoiles.
- Congélateurs Bahut 350I, 480l (4 étoiles)
- Réfrigérateurs 520l - 2 portes, (3 étoiles)
- Cuisinières tout Gaz 6400, 6000, 6100 (4 feux)
- Cuisinières tout gaz 8200 (5 feux)
- Climatiseurs Type fenêtre - 9000, 12000, et 15000 BTU/h
- Climatiseurs Split système S320 - 11250 BTU/h
- Climatiseurs Split système S430 - 14950 BTU/hs
- Climatiseurs Split système S530 - 18000 BTU/h

I.5. Activités de l'entreprise

L'activité de l'ENIEM sera concentrée sur la fabrication de réfrigérateurs, cuisinières, et climatiseurs. Cette activité sera assurée par plusieurs unités de production :

I.5. a. Unité Froid

Elle est composée de 3 lignes de production.

I.5. a.1.Une Ligne de réfrigérateurs petits modèles

Les capacités installées sont de 110.000 réfrigérateurs / an, dont les modèles fabriqués sous licence BOSCH –Allemagne - 1977. Sont :

- 160 l - 1 porte 2 étoiles
- 200 l - 1 porte 2 étoiles

- 240 l - 1 porte 2 étoiles

I.5. a.2.Une Ligne de réfrigérateurs grands modèles

Les capacités installées sont de 390.000 Réfrigérateurs par an dont les modèles fabriqués sous licence TOSHIBA - JAPON - 1987. Sont :

- Réfrigérateurs 300 D 2 portes, 3 étoiles
- Réfrigérateurs congélateurs 290C 2 portes, 3 étoiles
- Congélateur vertical 220 F 1 porte.
- Réfrigérateur vertical 350 S 1 porte.

I.5. a.3.Une Ligne de congélateurs bahut et réfrigérateurs de 520 L

Les capacités installées sont de 520L de 60.000 appareils par an. Dont les modèles sous licence LEMATIC-Liban- 1993 sont:

- Congélateurs bahut 350L, 4 étoiles
- Congélateurs bahut 480L, 4 étoiles
- Réfrigérateurs 520Ll 2 portes, 3 étoiles.

I.5.b. Unité Cuisson

Elle assure la production des cuisinières, et les capacités installées sont de 150000 cuisinières par an fabriquées sous licence TECHNO GAZ- Italie – 1991 dont les modèles sont :

- Cuisinières tout Gaz 6400 4 feux
- Cuisinières tout gaz 6000 4 feux
- Cuisinières tout gaz 6100 4 feux
- Cuisinières tout gaz 8200 5 feux

I.5.c. Unité Climatisation

Les capacités existantes sont de 60.000 climatiseurs sous Licence AIWELL - France 1977 dont les modèles sont :

- Climatiseurs Type fenêtre - 9000, 12000, et 15000 BTU/h
- Climatiseurs Split système S320 - 11250 Bh
- Climatiseurs Split système S430 - 14950 BTU/h
- Climatiseurs Split système S530 - 18000 BTU/h
- Machine à laver 07 Kg
- Chauffe eau 10 litre à GN et GB

I.5.d. Unité Commerciale

Ses activités sont :

la distribution et l'exportation des produits ENIEM,

Le service après-vente (à travers ses moyens propres et un réseau d'agents agréés).

I.5.e Unité Prestations Techniques

Cette unité assure les fonctions de soutien aux unités de production dans les domaines de :

- Réparation des outils et moules.
- Fabrication de pièces de rechange mécanique.
- Conception et réalisation d'outillages.
- Gestion des énergies et fluides.
- Gardiennage et sécurité.
- Travaux d'imprimerie.

I.6. Missions et objectifs

- **Missions**

La mission de L'ENIEM est d'assurer la production, le montage, la commercialisation, le développement et la recherche dans les différentes branches de l'électroménager notamment :

-Les appareils de cuisson par unité cuisson.

-Les appareils de climatisation par l'unité climatisation.

-Les produits sanitaires par unité d'AIN DEFLA.

- **Objectifs**

L'amélioration de la qualité des produits.

La maîtrise des coûts de production.

L'augmentation des capacités d'études et de développement.

L'amélioration de la maintenance de l'outil de production des installations.

La valorisation des ressources humaines.

L'augmentation des taux d'intégration (Interne et Externe).

L'augmentation du volume de production.

- **Le règlement intérieur qui englobe :**

L'organisation générale de travail (horaires de travail, et de sortie, la tenue de travail, le contrôle de présence, etc.……) l'hygiène, sécurité et médecine du travail.

Ce présent règlement intérieur a pour but :

De contribuer à l'amélioration de la production et de la productivité.

De fixer les principes et les règles relatifs à l'organisation technique de travail, ainsi que celles relatives à l'hygiène, la sécurité, la discipline et la médecine du travail.

I.7.Organigramme de l'entreprise

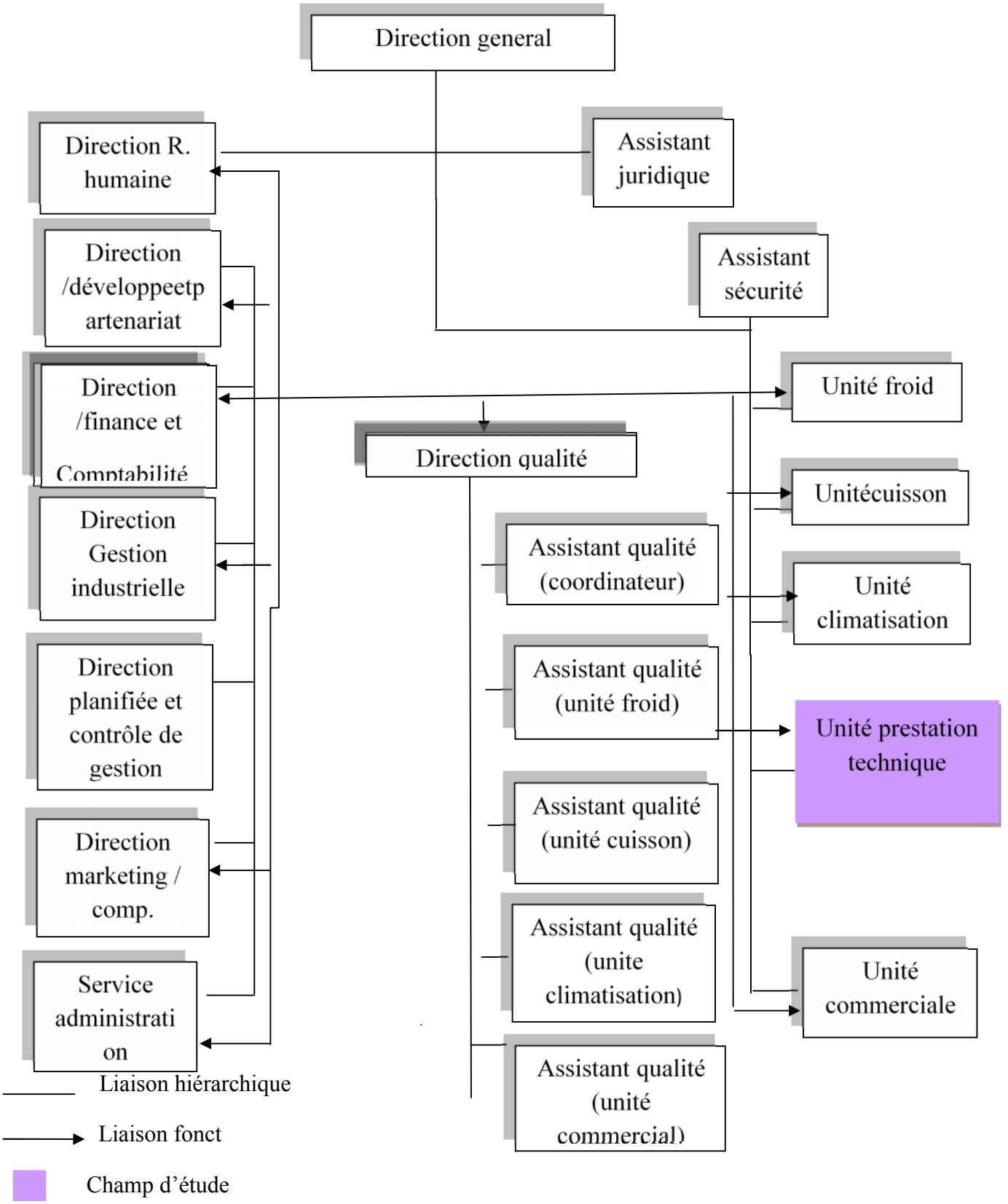


Figure I.1 : Organigramme de l'entreprise

I.8. Présentation du champ d'études

Cette partie nous permettra de mieux définir le domaine d'étude et de mieux apercevoir ses objectifs, elle nous aidera aussi à relever les éventuels manques et anomalies dans le système existant dans notre champ d'étude qui est l'unité de prestation technique.

I.8.1. Présentation de l'unité de prestation technique

Elle a pour rôle d'assurer les fonctions de soutiens aux unités de production dans les domaines de :

- Réparation des outils et moules
- Fabrication de pièces de rechanges mécaniques
- Conception et réalisation d'outillages
- Gestion des énergies et fluides
- Gardiennage et sécurité
- Travaux de menuiserie
- Travaux de nettoyage

I.8.2. Organigramme de l'unité de prestation technique

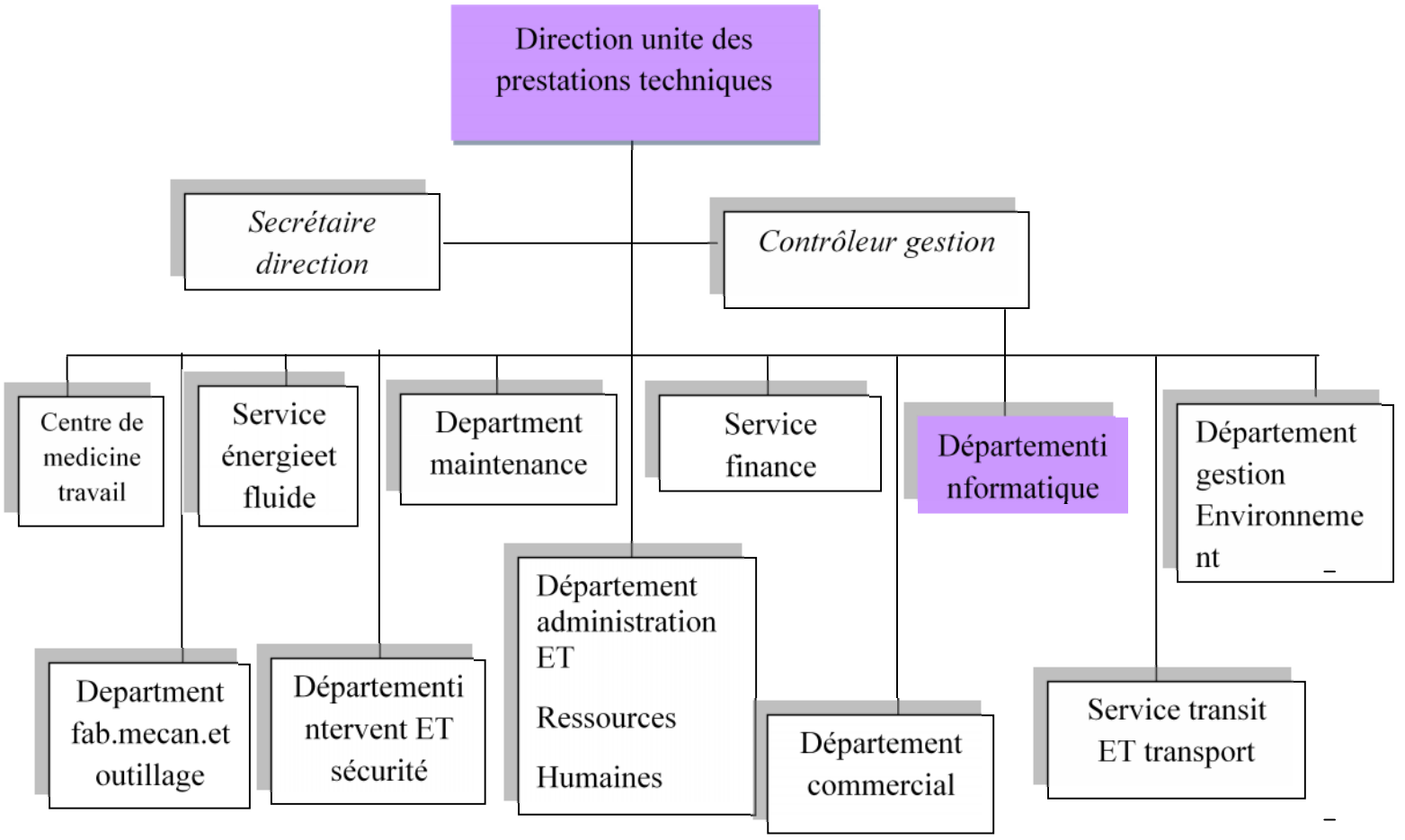


Figure I.2 : Organigramme de l'unité de prestation technique

I.8.3. Situation informatique

I.8.3.1. sétuation matériels

- **Le Matériel affectés pour chaque unité**

Ce tableau montre le matériel existant dans chaque unité :

Unités	Matériel	type
Unité froid	24 pc 13 terminaux 04 pairs modems 03pairs multiplexeurs	PIV et PIII HP D 330 et 700/92A TRT 2334 A 2934 A et 2563 B
Unité climatisation	06 PC 02 Terminaux 02 Imprimantes	PIV 700/92 A 2934A
Unité commerciale	02 PC 02 Pairs modems	PIII TRT
Unité prestation technique	27PC 05 Terminaux 01 Pair modem	PIII et PIV 700/92 A TRT
Unité cuisson	09PC 05 Terminaux 03 Pairs modems 04 multiplexeurs 03 Imprimantes	PIV 700/92A TRT 2334A 2934A

Tableau I.1 : Le Matériel affectés pour chaque unité

- **Le réseau informatique de l'entreprise l'ENIEM**

Elle utilise un réseau intranet qui est un réseau informatique utilisé à l'intérieur d'une entreprise ou de toute autre entité organisationnelle utilisant les techniques de communication d'Internet (IP, serveurs HTTP), ce réseau est constitué d'un :

- **Réseau client_serveur**

Ce réseau est composé de 39 terminaux dont 27 écrans HP (modèle 700/92 A, 2392A) et 12 imprimantes HP (modèle 2563B, 2934 A, Rugged Writer 480) reliés au serveur (HP3000/A500) par des liaisons directes (distances inférieures ou égales à **120** mètres), modem (pour les distances supérieures à 120 mètres), et multiplexeur modem (pour les installations de plusieurs terminaux distants).

- **Caractéristiques de ce réseau**

Parmi ces caractéristiques, la topologie choisie est celle dite étoile, vue la configuration du site, à savoir : deux bâtiments en formes de T.

Le schéma général du câblage est défini selon le nombre de bureaux et le nombre d'utilisateurs par bureau.

Tous les bureaux sont dotés d'au moins une prise. Il en existe en tous 170 prises (actuellement il n'y a que 65 micro- ordinateurs connectés). Toutes les prises d'un même étage ou tout les ordinateurs d'un même étage avec ses différentes unité et fonctions sont reliés a un switch contenu dans une armoire, cette dernière est reliée par un câble fibre optique à un Switch dit fédérateur contenu dans l'armoire centrale installée au niveau de la salle machine au sous sol du bâtiment B.

Le réseau est composé de 06 armoires départagées dans 03 bâtiments, une à chaque étage. L'emplacement est dicté par la distance maximale entre un Switch et un poste de travail, qui ne doit pas dépasser 100 mètres.

➢ **Les armoires de brassage existantes**

- **L'armoire d'étage centrale**

C'est l'armoire qui regroupe toutes les armoires de brassages (qui se trouvent dans chaque étage) par son Switch fédérateur ; elle est constituée des éléments suivants :

02 panneaux de brassage à 16 ports : contient des connecteurs RJ45 (câble torsadé).

01 Switch d'étage Cisco : contient des ports RJ45 et des ports GBIC (pour câble fibre optique).

01 onduleur : pour avoir le temps à sauvegarder les données.

01 Switch fédérateur : contient 7 ports GBIC.

03 tiroirs optiques : qui relient les armoires des blocs.

01 Panneau électrique à 06 prises sous onduleur : pour alimenter les périphériques actifs.

Cette figue nous présente l'armoire centrale

Figure I.3 : L'armoire d'étage

- **L'armoire de brassage**

Elle est constituée des éléments suivants :

01 Switch Cisco.

01 panneau de brassage le grand à 16 ports.

01 tiroir optique.

01 panneau d'alimentation

Figure.1.4 : L'armoire de brassage

➢ **Description du système du serveur HP3000/A500**

- **La face arrière**

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

Les ports sur le DDP sont du type RJ45 (norme RS423) et numérotés de 100 à 115, 200 à215 pour les ports écrans et de 300 à 315 pour les ports imprimantes.

Les ports sur le MDP sont du type DB25 (norme RS232) et numérotés de 400 à 415,500 à 515 pour les ports écrans et de 600 à 615 pour les ports imprimantes.

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

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

Console UPS port qui peut être connecté à 3 consoles sorties DB9 avec des câbles HP24252 :

UPS : pour brancher l'onduleur

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

Console principale.

Une console LAN10 base T (console réseau).

Le dérouleur : pour lire les cartes de l'ancien système.

- **La face avant**

Elle est composée des éléments suivants :

Lecteur de cassettes DLT.

Lecteur DVD.

Lecteur DDS.

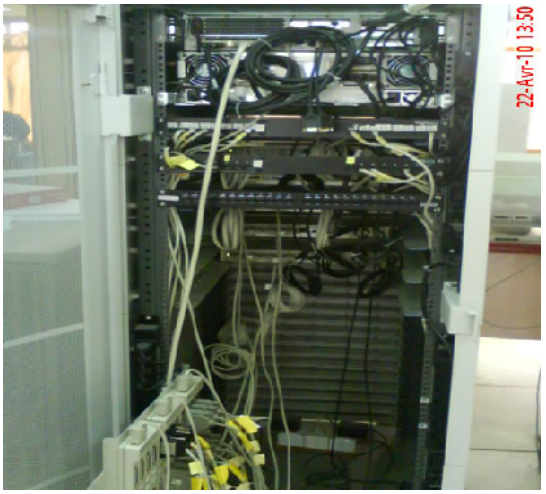


Figure I.5 : La face arrière

Figure I.6 : La face avant

I.8.3.2.Aspect logiciels

Les différents logiciels utilisés sont :

- **Réflexion x :** est un émulateur d'accès au serveur depuis les différents fonction.
- **EASY** : est une application installée dans le serveur pour gérer la comptabilité des différentes unités.
- **COBOL :** L'engage de programmation avec lequel toutes les applications opérationnelles sont développées.
- **ACPAE** : Gestion de la paie (calcul de la paie).
- **Système MM0909 :** pour la pièce de recharge.
- **Système MM ref :** gestion de la production pour l'unité froid.
- **Système MM cuis** : gestion de la production pour l'unité cuisson.
- **Système achat :** tout ce qui est relatif a la fonction achat.
- **Système MM3000 pour la gestion de production :** il se charge de la production et tenue du stock des matières premières et pièce de recharges.
- **Gestion de la comptabilité** : on trouve la comptabilité clients, fournisseurs, générale, analytique, budget et d'autres.

I.8..3.3.Aspect humain

- **Organigramme de département informatique**

Le département informatique se décompose en deux services :

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

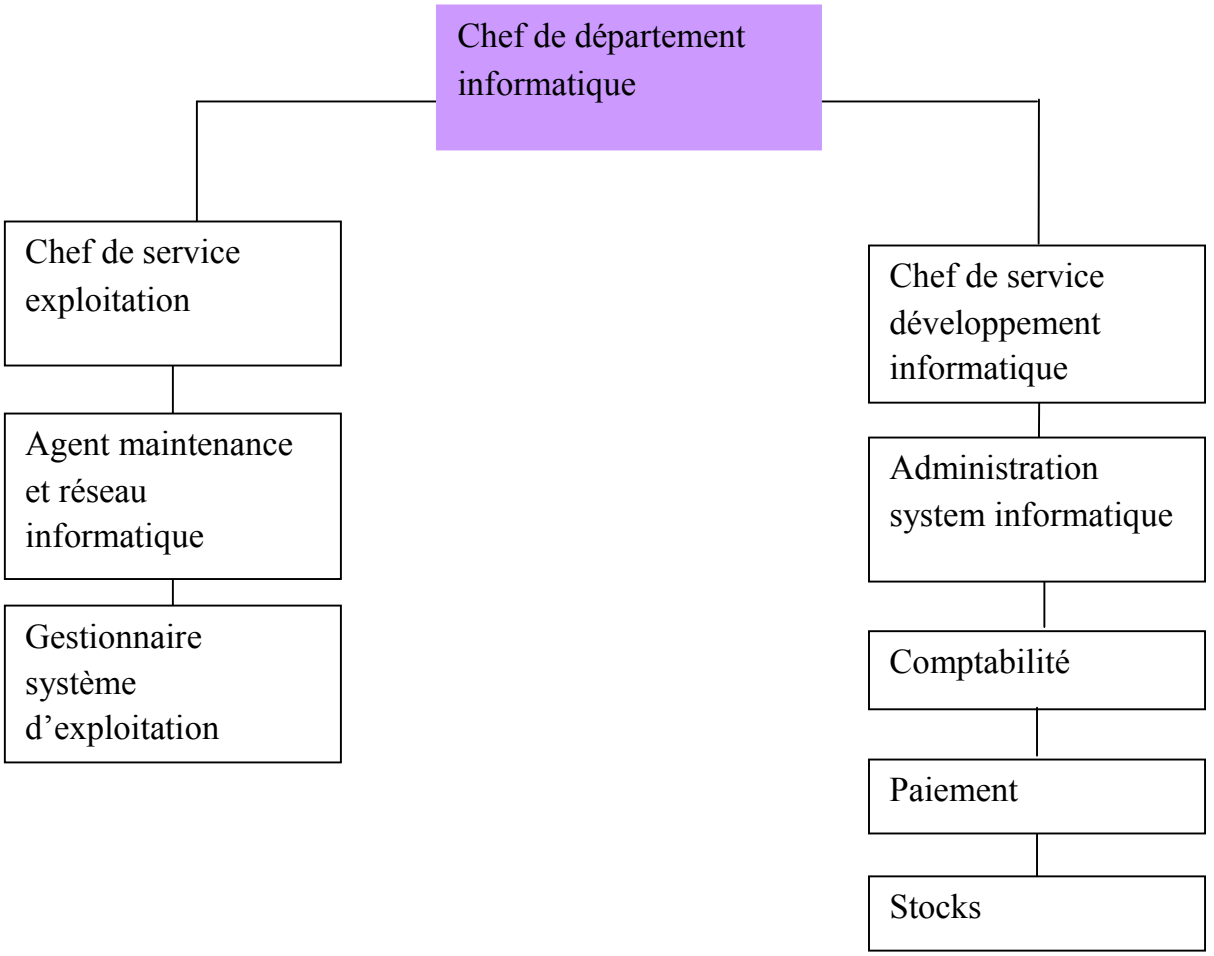


Figure I.6 : Organigramme de département informatique

- **Chef de département**

Anime et contrôle tous les travaux de conception, de mise en place , maintenance et de développement des systèmes de gestion informatique des unités.

- **Chef de service exploitation**

Il veille sur la gestion d'ensemble de moyens informatique de saisie, de traitement de transmission et de restitutions de l'informatique assiste les utilisateurs et interviens sur les incidents.

- **Agent maintenance et réseau informatique**

Surveille le réseau et maintient la machine dans un état propre même à contourner certains obstacles (indispensabilité, espace disque , sécurité ….). Établit de bonne relations avec les utilisateurs et bien métriser les respects systèmes et télé communication.

- **Gestionnaire système d'exploitation**

Procède au chargement des énergies (air conditionné ,électricité via onduleur …)des ordinateurs et du système d'exploitation .

Contrôle l'utilisation des diverses unités périphériques.

- **Chef de service développement systèmes informatique**

la tache de ce poste consiste à assurer la maintenance des différents systèmes et leurs adaptations aux exigences nouvelles. Elle assure également le développement de nouveaux systèmes conformément au plan informatique

- **Administrateur système informatique (comptable)**

Sont role est de réaliser les différents programmes de l'application et ce par :

- Un découpage des unités de traitement en programme .
- Une écriture de programme dans la longue choisie.
- La mise au point des teste de contrôle , la correction et la finalisation de programme.
- Rédiger un dossier d'exploitation pour le compte de la structure concernée.
- Assiste les utilisateurs et suit le déroulement des phases de lancement.
- Assiste les utilisateurs dans l'application dont il a la charge.
- Assiste sa hiérarchie dans l'élaboration et la maintient de la documentation.

- **Administrateur système informatique (stock, piece de rechange, gestion personnelle, … etc)**

- Assurer l'analyse organique de l'étude , a savoir l'élaboration de la solution qui a été retenue et ce par :
- Une reprise de la chaine fonctionnelle pour la découper en unité de traitement qui correspondent a des programmes définissants pour chacune d'elles ,un mode de stockage des programmes, fichiers, etc…et de l'enchainement des opérations a effectuer (chaine organique).

- La confection de dossier d'exploitation définissant les conditions.
- La maintenance des chines de traitement.

- **Administrateur système informatique (paie)**

Assure l'étude de l'application et rend compte a sa hiérarchie.

Assure l'analyse fonctionnelle du projet conformément au planning de réalisation préétabli par hiérarchie et ce par :

- Une etude approfondit du cahier des charges (choix de méthode d'analyse, flux, et diagramme d'information, production de données et élaboration d'un dictionnaire de données, élaboration de la base de données, et élaboration de procédure .
- Un découpage de l'application en module simple de manière a facilité la compréhension l'écriture ,l'exploitation et la maintenance des programmes.
- L'établissement d'un dossier d'analyse qui comporte l'objet de l'application et la solution technique.

II.1.Introduction

L'installation d'un réseau est d'un point de vue matériel un processus assez linéaire ; il est impératif de faire les choses dans un certain ordre, afin de s'assurer du bon fonctionnement futur de l'ensemble.

Dans ce chapitre, nous allons se familiarisé avec les différents éléments qu'un réseau doit constituer pour qu'une information émise d'un ordinateur puisse être acheminée et routée vers son ordinateur réceptif voulu.

II.2. Définition d'un réseau

Un réseau informatique est une collection de PC et d'autres dispositifs interconnectés par câbles pour pouvoir communiquer entre eux et partager les ressources et informations.

II.3.classification des réseaux

On distingue quatre niveaux de classification : suivant la taille, suivant l'organisation, suivant la méthode d'accès et selon le type de machine.

II3.1.classification selon la taille

La figure II.1 nous montre les différents types des réseaux selon la taille, et on distingue :

- Les ***LAN***(*Local Area Network*) : Réseaux locaux pour de courtes distances avec des débits de quelques dizaines de Mbits / seconde jusqu'à quelques centaines.
- ***Les MAN***(*Metropolitan Area Network*) : Destinés à courir de très grands périmètres qui sont fédérateurs de réseaux locaux.
- ***WAN***(*Wide Area Netwok*) : qui signifie réseau étendu, permettent de connecter plusieurs LAN éloignées entre elles. Le débit devient de plus en plus faible en fonction de la distance. « Internet est un regroupement de WAN »

II.3.2.Classification selon l'organisation

- **Égal à égal**

  Dans un réseau d'architecture égal à égal (Peer-to-Peer) tous les ordinateurs connectés ont le même statut et se partagent toute l'information et tous les services sans l'aide d'un serveur.

- **Client/serveur**

  Un réseau d'architecture client/serveur est celui où des ordinateurs (clients) sont reliésà un serveur dédié qu'est un ordinateur central fournit des services réseau aux clients.

II.3.3.Classification selon la méthode d'accès

Cette méthode dépend étroitement de la topologie et donc de l'organisation spatiale des stations les unes par rapport aux autres.

- **Topologie en bus**

Raccorder sur un même support physique des ordinateurs, et permettre de communiquer avec un ensemble d'ordinateurs sur ce support. Un seul message sur le support peut être lu par plusieurs ordinateurs.

Figure II.2: Topologie en bus

- **Topologie en anneau**

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

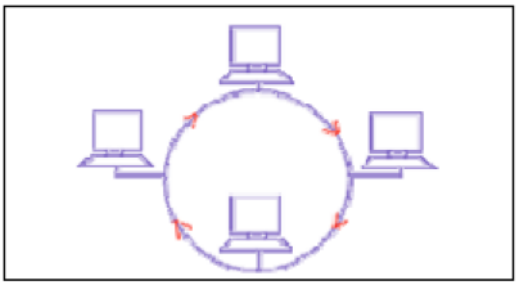


Figure 1I.3: **Topologie en anneau**

Dans cette topologie, les machines ont un rôle actif qui est la ré-amplification du signal.

- **Topologie en étoile**

C'est la topologie réseau la plus courante, notamment avec les réseaux Ethernet, les ordinateurs du réseau sont relies a un système matériel central appelé concentrateur, il comprend un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Donc il assure la communication entre les différentes jonctions.

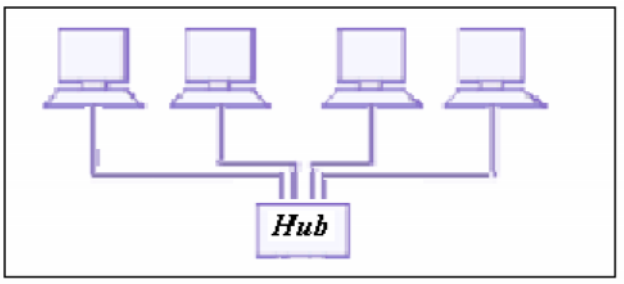


Figure 1I.4: Topologie en étoile

Ce type de réseaux est facile à maintenir mais la défectuosité du nœud centrale provoque un arrêt de tout le réseau.

II.3.4.Classification suivant le type de machine:

- Homogène : tous les ordinateurs sont du même constructeur (Appele-talk).
- Hétérogène : les ordinateurs reliés au réseau sont de constructeurs divers. (Ethernet).

II.4.Support de transmission

lors de la conception d'un réseau, le choit du support de transmission dépendra d'un certain nombres de critère parmi lesquels on distingue :

- Le coût.
- Bande passante : La bande passante d'une voie est la plage de fréquence sur laquelle la voie est capable de transmettre des signaux sans que leur affaiblissement soit trop important.
- Vitesse de transmission.
- Distance du câble.
- Insensibilité au bruit.
- Type du signale véhiculé (analogique ou numérique).

II.4.1.Câble coaxial

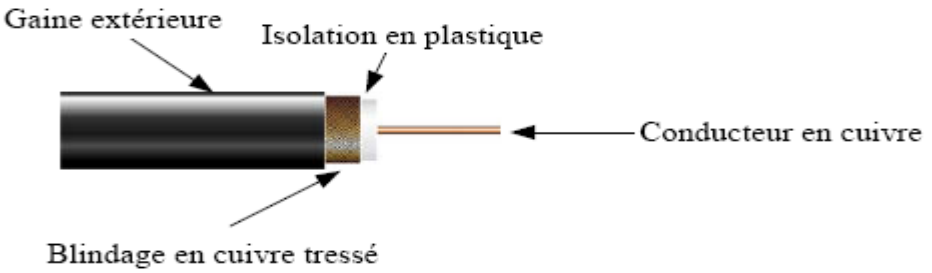


Figure I.5 : Câble coaxial

- La gaine permet de protéger le câble de l'environnement extérieur. Elle est habituellement en caoutchouc (parfois en Chlorure de polyvinyle (PVC), éventuellement en téflon)
- Le blindage (enveloppe métallique) entourant les câbles permet de protéger les données transmises sur le support des parasites (autrement appelé bruit) pouvant causer une distorsion des données.
- L'isolant entourant la partie centrale est constitué d'un matériau diélectrique permettant d'éviter tout contact avec le blindage, provoquant des interactions électriques (court-circuit).

On distingue habituellement deux types de câble coaxial utilisé pour des transmissions en bande de base :

• **Thicknet**: Epais et raide (diamètre environ 12mm) à cause de son blindage, il est recommandé pour l'installation de câble fédérateur. Sa gaine est jaune. Utilisée pour 10base 5.

• **Thinnet**: D'un diamètre plus réduit, il est plus pratique dans des installations comprenant des courbes. De plus, il est plus économique, mais dispose d'un blindage moins conséquent utilisée pour 10 base 2.

Le câble coaxial offre de nombreux avantages du fait de sa capacité à s'étendre sur une plus grande distance et de son coût parmi les plus faibles. C'est une technologie utilisée depuis de nombreuses années pour tous les types de communications de données.

- **Connecteurs du câble coaxial**


Figure II.6 : Connecteur BNC femelleFigureII.7 : Connecteur BNC mâle

II.4.2.La paire torsadée

Une paire torsadéeest uneligne de transmission formée de deux fils conducteurs enroulés en hélice l'un autour de l'autre. Cette configuration a pour but de maintenir précisément la distance entre les fils et de diminuer ladiaphonie.

Le maintien de la distance entre fils de pair permet de définir une impédance caractéristique de la paire, afin de supprimer les réflexions de signaux aux raccords et en bout de ligne. Les contraintes géométriques (épaisseur de l'isolant/diamètre du fil) maintiennent cette impédance autour de 100 ohms.

- **Les connecteurs utilisés**

Figure II.8 : Prise murale Figure II.9 :RJ45 câble réseau 8 fils

- **Les types de blindages**

Les paires torsadées sont souvent blindées afin de limiter les interférences. Comme le blindage est fait de métal, celui-ci constitue également un référentiel de masse. Le blindage peut être appliqué individuellement aux paires ou à l'ensemble formé par celles-ci. Lorsque le blindage est appliqué à l'ensemble des paires, on parle d'écrantage.

- **Paire torsadée non blindée Unshielded twisted pair (UTP)**

Le câble UTP obéit à la spécification 10base t .c'est le type de paire torsadée le plus utilisé.
Voici quelques caractéristiques :

- Longueur maximale d'un segment : 100métre.
- Composition : 2 fils décuivre recouverts d'isolant.
- Normes UTP : conditionnent le nombre de torsions par pied (33cm) de câble en fonction de l'utilisation prévue.

- **Paire torsadée écrantée**

Foiled twisted pair (FTP) ouscreened unshielded twisted pair - denomination officielle (F/UTP). Les paires torsadées ont un blindage général assuré par une feuille d'aluminium. L'écran est disposé entre la gaine extérieure et les 4 paires torsadées. Elle est utilisée pour le téléphoneet lesréseaux informatiques.

- **Paire torsadée blindée**

Shielded twisted pair (ST*P*) - nouvelle dénomination U/FTP. Chaque paire torsadéeblindée (ou STP pour shielded twisted pairs) est entourée d'une couche conductrice de blindage, de façon

similaire à un câble coaxial. Cela permet une meilleure protection contre lesinterférences. Elle est communément utilisée dans les réseaux token ring.

II.4.3. Fibre optique

La fibre optique représente une technologie relativement récente puisqu'il a fallu attendre la fin desannées 60 et l'invention du laser pour voir émerger cette technologie. Cette technique est basée sur latransmission de signaux lumineux (un 1 étant codé par une impulsion lumineuse et un 0 par une absence).Cette lumière est transmise avec une onde de 108 Hz.

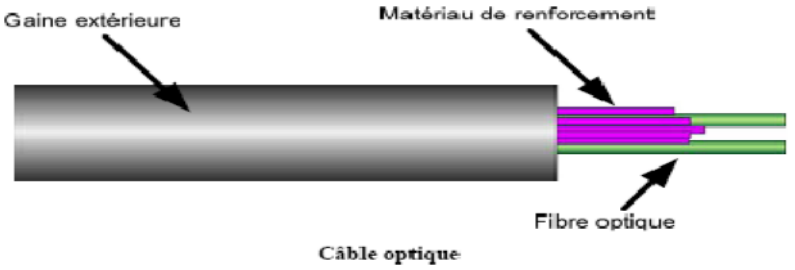


Figure II.10 : La fibre optique

II.5. Equipements d'interconnexion

Les réseaux hétérogènes formant Internet sont reliés entre eux grâce à desdispositifs d'interconnexion (Passerelles, Routeurs, Ponts …) qui assurent le transfert des données

II.5.1. Carte réseau

Son rôle est d'envoyer et de contrôler les données sur le réseau ; actuellement elle peut être doté d'un transcrive et d'une adresse unique (MAC medium Access contrôle) : une partie représente la dénomination du constructeur et la deuxième partie représente le numéro de série de cette carte. Généralement sur 6 octets.

II.5.2.Les Hubs (concentrateurs)

Le Hub est également appelé concentrateur ou répétiteur. C'est un boîtierélectronique assurant la liaison des postes et des périphériques du réseau.
Le répétiteurse contente de transférer les ressources qui lui arrivent vers tous les autres éléments duréseau (dont le destinataire).

II.5.3.Les Switchs

Egalement appelés Commutateurs, Boîtier électronique assurant la liaison et l'optimisation des échanges entre les éléments du réseau. Contrairement au Hub, leSwitch est capable d'orienter les ressources vers leur unique destinataire sur le réseau.

Le Switch permet ainsi de libérer la bande passante en évitant ainsi le transfert de Données inutiles sur le réseau.

II.5.4. Les Ponts

Ce sont des dispositifs permettant de relier des réseaux travaillant avec les mêmes protocoles .ils permettent de filtrer les trames de données et ne laissent passer que celle dont corresponde à une machine situe à l'oppose du pont. Cela permet de réduire le trafic entre les sous réseaux notamment le nombre de collision.

II.5.5.Les Routeurs

Leurs rôles et d'acheminer le différent segment des paquets en fonction de la couche trois les routeurs prennent des discision logique d'optimisation pour choisir la meilleur voie des données d'un réseau a un autre et de diriger ensuite les paquets vers le pont de sortie qui correspond au port de sortie suivant.

II.5.6.Les Passerelles

Ce sont des systèmes matériels et/ou logiciels permettant de faire des liaisonsentre plusieurs réseaux de protocoles différents, l'information est codée et transportéedifféremment sur chacun des réseaux.

Elles permettent aussi de manipuler les données afin de pouvoir assurer lepassage d'un type de réseau à un autre. Les réseaux ne peuvent pas faire circuler lamême quantité de données simultanément en termes de taille de paquet de données,mais la passerelle réalise cette transition en convertissant les protocoles decommunication de l'un vers l'autre.

II.6. Description du modèle OSI :

L'échange d'information nécessite une normalisation entre systèmes communicants de nature différente. La modélisation **OSI** est la référence en architecture de réseau, Utilisée depuis 1982, elle permet la communication entre supports variés, dans un environnement hétérogène, et sur de longues distances.

Le modèle OSI (**O**pen **S**ystème **I**nterconnections) est une architecture de réseau comprenant sept couches complémentaireset il s'agitd'assurer :

- La transmission des données au départ.
- La gestion du transport de bout en bout.
- Le traitement des donnés à l'arrivées.

Le modèle OSI permet de décomposer les fonctionnalités des réseaux en 7 sous-ensembles homogènes et ordonnés.

Le tableau ci-dessous décrit le rôle de chaque couche :

Couches	Fonctions
7. application	Services d'applications : gère les différentes utilisations des autres couches et fournit un service à l'utilisateur.
6. présentation	Permet le transcodage du format : pour permettre à des entités de nature différentes de dialoguer.
5. session	Organise et synchronise les échanges entre utilisateurs.
4. transport	Assure le contrôle de l'acheminement.
3. réseau	Gère le routage des données et la commutation.
2. liaison de données	Assure l'acheminement point à point des trames.
1. physique	Gère le signale en l'adaptant au support physique.

Tableau II.1 : Rôle des couches du modèle OSI

II.7.Architecture de TCP/IP

TCP/IP fournit un protocole standard pour résoudre le problème de connexion entre différents réseaux, TCP (Transfert Contrôle Protocole) se charge du transport de bout en bout pour toute application alors que IP (Internet Protocole) est responsable du routage à travers le réseau.

TCP/IP est structuré en quatre niveaux :

- ✓ L'interface réseau (1 et 2 du modèle OSI).
- ✓ Le routage (3 du modèle OSI).
- ✓ Le transport (4 et 5 du modèle OSI).
- ✓ L'application (5,6et7 du modèle OSI).

II.8.Encapsulation des données

Lors d'une transmission, les données traversent chacune des couches au niveaude la machine émettrice. A chaque couche, une information est ajoutée au paquet dedonnées, il s'agit d'un en-tête, ensemble d'informations qui garantissent latransmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche,l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son étatoriginal.

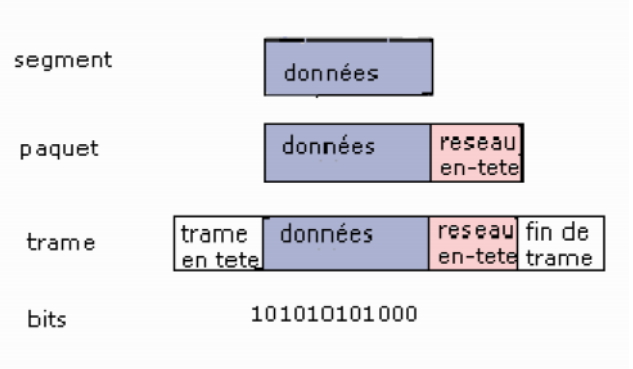


Figure II.11 :principe d'encapsulation

II.9.Les protocoles réseaux

II.9.1.Définition d'un protocole

Un protocole est une méthode standard qui permet la communication entre deux machines c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

II.9.2.Les types de protocoles

- **Protocole TCP**

TCP est un protocole de transport qui pourrait être indépendant de IP et même s'appuyer directement sur des réseaux physiques comme ETHERNET. Cependant on le trouve toujours en relation avec IP d'ou le terme **TCP/IP**.

TCP est un protocole connecté. C'est à dire qu'il existe une phase de création d'une connexion où les deux machines négocient leurs options et réservent des ressources.

- **Protocole UDP**

UDP s'inscrit dans la couche 4. Il s'agit d'un transport en mode non connecté. UDP envoie des datagrammes et utilise une information complémentaire, le numéro de PORT., La trame UDP est constituée d'un numéro de port source et d'un numéro de port destination, Ce transport est en fait une succession de messages sans liens.

UDP est utilisé par des applications qui ne transfèrent que des petitsmessages, TCP étant trop coûteux pour ce genre d'opérations.

- **Protocole IP**

C'est lui qui gère la fragmentation des données lorsque par exemple une section du réseau admet une taille différente des paquets, Mais le rôle le plus important de ce protocole est d'acheminer les données à travers un ensemble de réseaux interconnectés grâce à la gestion des adresses IP.

- **ARP ET RARP**

Ces protocoles permettent de convertir l'adresse logique en adresse physique etvice versa.

Le protocole **ARP** a un rôle phare parmi les protocoles de la couche Internet dela suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseaucorrespondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolutiond'adresse.

Chaque machine connectée au réseau possède un numéro d'identificationsur 48 bits. Ce numéro est un numéro unique qui est fixé dès la fabrication de la carteréseau en usine.

Le protocole **RARP** est dans le réseau Internet. Permet à une machine d'utiliser son adresse physique pour déterminer son adresse logique.

- **RIP**

L'un des protocoles de routage les plus populaires est RIP (Routing Information Protocol) qui est un protocole de type vecteur de distance, C'est-à-dire que lesmessages échangés par des routeurs voisins contiennent un ensemble de distancesentre routeur et destinations qui permet de réactualiser les tables de routage.

Ce protocole utilise une métrique simple : la distance entre une source et une destination

est égale au nombre de sauts qui les séparent. Elle est comprise entre 1 et 15, la valeur16 représentant l'«infini». Ceci implique que RIP ne peut être utilisé qu'à l'intérieur deréseaux qui ne sont pas trop étendus.

- **OSPF**

Est un nouveau type de protocole de routage dynamique qui élimine leslimitations de RIP.

C'est un protocole d'état de liens, c'est-à-dire qu'ici un routeurn'envoie pas des distances à ses voisins, mais il teste l'état de la connectivité qui lerelie à chacun de ses voisins. Il envoie cette information à tous ses voisins, qui ensuitele propagent dans le réseau. Ainsi, chaque routeur peut posséder une carte de latopologie du réseau qui se met à jour très rapidement lui permettant de calculer desroutes aussi précises qu'avec un algorithme centralisé. En fait, RIP et OSPF, sont desprotocoles de type IGP (Interior Gateway Protocol) permettant d'établir les tables desrouteurs internes des systèmes autonomes. Un système autonome peut être défini par un ensemble de routeurs et de réseaux sous une administration unique.

Cela peut doncaller d'un seul routeur connectant un réseau local à Internet, jusqu'à l'ensemble desréseaux locaux d'une multinationale. La règle de base étant qu'un système autonomeassure la connexité totale de tous les points qui le composent en utilisant notamment un protocole de routage unique.

- **ICMP**

Le protocole ICMP (Internet Control Message Protocol) permet d'envoyer desmessages de contrôle ou d'erreur vers d'autres machines ou passerelles.

ICMPrapporte les messages d'erreur à l'émetteur initial. Beaucoup d'erreurs sont causées par l'émetteur, mais d'autres sont dues à des problèmes d'interconnexions rencontréessur l'Internet : machine destination déconnectée, durée de vie du datagrammes expirée,congestion de passerelles intermédiaires.

Si une passerelle détecte un problème sur un datagrammes IP, elle le détruit etémet un message ICMP pour informer l'émetteur initial. Les messages ICMP sont véhiculés à l'intérieur de datagrammes IP et sont routés comme n'importe queldatagramme IP sur l'Internet. Une erreur engendrée par un message ICMP ne peutdonner naissance à un autre message ICMP.

- **IGMP**

Ce protocole permet au groupe de machines d'utiliser les ressources de réseau defaçon efficace et optimale. L'adressage multipoint Permet l'envoi de datagrammesvers plusieurs destinataires, l'envoi du réponse pour chaque machine d'un sous réseauest unique.

- **DNS**

Le DNS est le mécanisme qui permet de convertir le symbolique en adresse IP, lorsque les machines communiquent sur un réseau informatique, c'est toujours parl'utilisation d'une adresse (IP ou autre) source ou destination. Mais ces adresses bienque nécessaires, sont difficiles à mémoriser et ne permettent pas de souplesse dans lesconfigurations des stations.

Le service DNS est donc utilisé pour la « résolution de noms », Cette opérationconsiste à fournir aux clients DNS qui en font la demande une association adresse IP,un nom symbolique et vice-versa.

- **DHCP**

Le protocole DHCP (Dynamic Host Configuration Protocol) attribueautomatiquement des adresses IP aux équipements branchés au réseau.

Lorsqu'unclient essaie de se brancher au réseau, une demande de paramètres de configuration estenvoyée au serveur DHCP. Une fois que le serveur a reçu le message, le serveurDHCP envoie une réponse au client, qui comprend les informations de configuration,puis enregistre en mémoire les adresses qui ont été attribuées. DHCP utilise leprotocole *BOOTP* pour communiquer avec les clients.

Les clients doivent renouvelerleur adresse IP à 50 % de la période d'utilisation, puis de nouveau à 87,5 %, enenvoyant un message *DHCPREQUEST*. Les hôtes clients conservent leur adresse IPjusqu'à l'expiration de leur période d'utilisation, ou lorsqu'ils envoient une commande*DHCPRELEASE. IPCONFIG* et *WINIPCFG* sont des utilitaires exécutés à partir de laligne de commande et qui permettent de vérifier les informations de l'adresse IP qui aété attribuée à l'hôte client.

- **Frame Relay**

Frame Relay est un protocole de réseau étendu qui intervient dans les couches physique et liaison de données du modèle de référence OSI.

Inventé par Eric Scace, ingénieur chez Sprint International, ce protocole était destiné aux interfaces RNIS (Réseaux Numériques à Intégration de Services), en tant que version simplifiée du protocole X.25. De nos jours, bien d'autres interfaces réseau l'utilisent également dans la première mise en œuvre du protocole Frame Relay dans son réseau public.

II.10.Le routage dans les réseaux

Les routeurs sont les responsables de la transmission des paquets à travers différents réseaux.

II.10.1.Fonctionnement d'un routeur

Au centre du réseau se trouve le routeur. Globalementun routeur relie plusieurs réseaux. Pour ce faire, il dispose de plusieurs interfaces, chacune appartenant à un réseau IP différent. Lorsqu'un routeur reçoit un paquet IP sur une interface, il détermine quelle interface utiliser pour transférer le paquet vers sa destination. Le routeur utilise sa table de routage pour déterminer le meilleur chemin pour le transfert du paquet. Il prend sa décision principale de transfert au niveau de la couche 3 mais il participe également aux processus des couches 1 et 2. Une fois qu'un routeur a examiné l'adresse IP de destination d'un paquet et consulté sa table de routage pour prendre sa décision de transfert, il peut transférer ce paquet à l'interface appropriée pour que celui-ci puisse atteindre sa destination. Le routeur encapsule le paquet IP de couche 3 dans la partie données d'une trame liaison de données de couche 2 appropriée à l'interface de sortie. La trame peut être de type Ethernet ou HDLC, ou relever d'une autre encapsulation de couche 2, quelle que soit l'encapsulation utilisée sur cette interface. La trame de couche 2 est encodée dans les signaux physiques de couche 1 utilisés pour représenter les bits sur la liaison physique.

Les interfaces de routeur peuvent être classées en deux groupes principaux :

- ✓ Interfaces LAN - telles qu'Ethernet et FastEthernet : sont utilisées pour connecter le routeur au réseau local,elles utilisent généralement une prise RJ-45 prenant en charge des câbles à paires torsadées non blindées
- ✓ Interfaces WAN - telles que les interfaces série, RNIS et Frame Relay :elles permettent de connecter des routeurs à des réseaux externes, généralement sur une distance géographique

importante. Chaque interface WAN a sa propre adresse IP et son propre masque de sous-réseau, lui permettant d'être identifiée comme faisant partie d'un réseau donné

II.10.2.Routes statiques et routes dynamiques

Les réseaux distants sont ajoutés à la table de routage grâce à la configuration de routes statiques ou à l'activation d'un protocole de routage dynamique. Lorsque l'IOS doit atteindre un réseau distant et qu'il est informé de l'interface à utiliser, il ajoute cette route à la table de routage tant que l'interface de sortie est activée.

- **Routage statique**

Une route statique inclut l'adresse réseau et le masque de sous-réseau du réseau distant, ainsi que l'adresse IP du routeur du tronçon suivant ou de l'interface de sortie. Le routage statique est utilisé dans les cas suivants :

- ✓ Un réseau ne comporte que quelques routeurs. Dans ce cas, l'utilisation d'un protocole de routage dynamique ne présente aucun bénéfice substantiel. Par contre, le routage dynamique peut accroître la charge administrative.
- ✓ Un réseau est connecté à Internet via un seul FAI. Il n'est pas nécessaire d'utiliser un protocole de routage dynamique sur cette liaison car le FAI représente le seul point de sortie vers Internet.

- **Routage dynamique**

Les protocoles de routage dynamique effectuent plusieurs tâches, notamment :

- ✓ pour partager des informations sur l'accessibilité et l'état des réseaux distants.
- ✓ la détection de réseaux : au lieu de configurer des routes statiques vers des réseaux distants sur chaque routeur, un protocole de routage dynamique permet aux routeurs de recevoir automatiquement, par le biais d'autres routeurs, les informations nécessaires concernant ces réseaux. Ces réseaux (et le meilleur chemin d'accès à chacun d'eux) sont ajoutés dans la table de routage du routeur et désignés comme acquis par un protocole de routage dynamique spécifique.
- ✓ la mise à jour des tables de routage :Après la découverte initiale du réseau, les protocoles de routage dynamique mettent à jour et gèrent les réseaux dans leurs tables de routage.

II.11.Adressage

Chaque ordinateur du réseau Internet dispose d'une adresse IP unique codée sur32 bits. Plus précisément, chaque interface dispose d'une adresse IP particulière.

En effet, un même routeur interconnectant 2 réseaux différents possède uneadresse IP pour chaque interface de réseau. Une adresse IP est toujours représentéedans une notation décimale pointée constituée de 4 nombres (1 par octet) comprischacun entre 0 et 255 et séparés par un point.

Plus précisément, une adresse IP est constituée d'une paire *(*id. de réseau, id demachine*)* et appartient à une certaine classe (A, B, C, D ou E) selon la valeur de sonpremier octet, comme détaillé dans la figure II.12

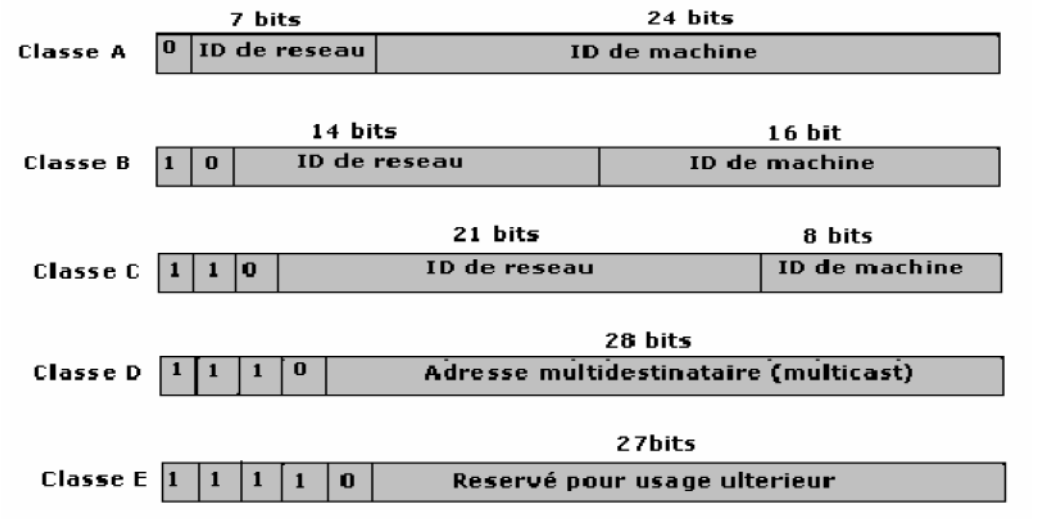


Figure II.12: Les cinq classes d'adresses IP

Le tableau ci-après donne l'espace d'adresses possibles pour chaque classe :

Classe	adresses
A	0. 0. 0. 0 à 127. 255. 255. 255
B	128. 0. 0. 0 à 191. 255. 255. 255
C D E	192. 0. 0. 0 à 223. 255. 255. 255 224. 0. 0. 0 à 239. 255. 255. 255 240. 0. 0 .0 à 247. 255. 255. 255

Tableau II.2 :L'espace d'adresse

- **Adresses particulières :** sont des adresses a ne pas utiliser comme :

La partie machine toute a zéro

La partie machine toute a un (1)

Adresse locale hôte : 127.0.0.1

Les plages d'adresses suivantes sont réservées à l'usage privé et il ne faut pas qu'elles soient défaussées sur internet :

10.0.0.0 ⟶ 10.255.255.255
172.16.0.0 ⟶ 172.31.0.0
192.168.0.0 ⟶ 192.168.255.255

II.12.VLAN (Virtuel Local Area Network**):**

La notion de VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de système de câblage. Ces réseaux permettent de définir des domaines de diffusion restreinte, cela signifie qu'un message émis par une station du VLAN ne pourras être reçu que par les stations de ce même VLAN.

Un VLAN, est donc, un regroupement logique, et non physique, de plusieurs stations. Pour réaliser ce regroupement, on intervient directement, par voie logicielle, sur le ou les éléments actifs que sont les commutateurs VLAN.

III.1. Introduction

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs dites machines possèdent uniquement les droits qui leur ont été octroyéainsi la mise en œuvre de la sécurité est indispensable au sein d'un réseau afin de le protéger de toute sorte d'intrusion malveillante, ce qui implique la réalisation des fonctions essentielles suivantes :

- ✓ Intégrité : pour garantir que les données sont bien celles que l'on croit être.
- ✓ Confidentialité : consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction c'est-à-dire consistent à assurer que seules les personnes autorisées aient accès aux ressources échangées.
- ✓ Disponibilité: permettant de maintenir le bon fonctionnement du système d'information quand les informations sont accessibles au moment voulu.
- ✓ Non-répudiation : permettant de garantir qu'une transaction ne peut être niée
- ✓ Authentification : garantit l'identité des correspondants ou des partenaires qui communiquent.

III.2.Politique de sécurité :

Une politique de sécurité ou stratégie de sécurité est une déclaration formelle des règles qui doivent être respectées par les personnes qui ont accès aux ressources technologiques et aux données vitales de l'entrepriseen vue de protéger son réseau contre les attaques menées soit de l'intérieur, soit de l'extérieur .Une stratégie de sécurité comprend les objectifs suivants :

- identifier les objectifs de sécurité de l'entreprise
- documenter les ressources à protéger
- identifier l'infrastructure réseau par des schémas et des inventaires à jour
- identifier les ressources vitales qui doivent être protégées, telles que les données de recherche et développement, les données financières et les données relatives aux ressources humaines. Il s'agit d'une analyse des risques

III.3. Les menaces contre la sécurité

III.3.1.Les types de menaces

Les menaces sont considérées comme une violation potentielle du système de sécurité elles viennent d'individus compétents intéressés par l'exploitation des vulnérabilités (faiblesses) de sécurité.Il existe deux types fondamentaux de menaces :

- **Les menaces accidentelles (les risques)**

Les menaces accidentelles peuvent se manifester ou résulter de l'exposition ou de la modification d'un objet. L'exposition peut émerger des pannes hardware, software ou bien de l'utilisateur et le résultat pourra être une violation de la confidentialité des objets. Par exemple, une exposition se produit quand un utilisateur envoie un e-mail confidentiel à la mauvaise personne. Les menaces accidentelles peuvent se réaliser par elle-même durant les modifications des objets (informations et/ou des ressources). La modification d'une ressource se présente quand une ressource entre dans un état illégal résultant d'un événement accidentel.

- **Les menaces intentionnelles (les attaques) :**

L'attaque est une menace intentionnelle. C'est une action exécutée par une entité pour violer la sécurité,la modification et la violation de l'information, l'utilisation non autorisée des ressources, l'envoi de messages anonymes sont quelques exemples d'attaques.

III.3.2.L'augmentation des menaces

Au fil des ans, les outils et les méthodes permettant d'attaquer les réseaux ont constamment évolués .Comme la figure suivante le montre en 1985, un pirate devait posséder un ordinateur de pointe, des connaissances en programmation et en réseaux pour réaliser des attaques élémentaires avec des outils rudimentaires. Au fil du temps, les méthodes et les outils d'attaque se sont améliorés et les pirates n'ont plus eu besoin de posséder le même niveau de connaissances. Les exigences pour devenir pirate débutant ont effectivement diminué. Des personnes qui auparavant n'auraient pas commis de délits informatiques sont à présent à même de le faire.

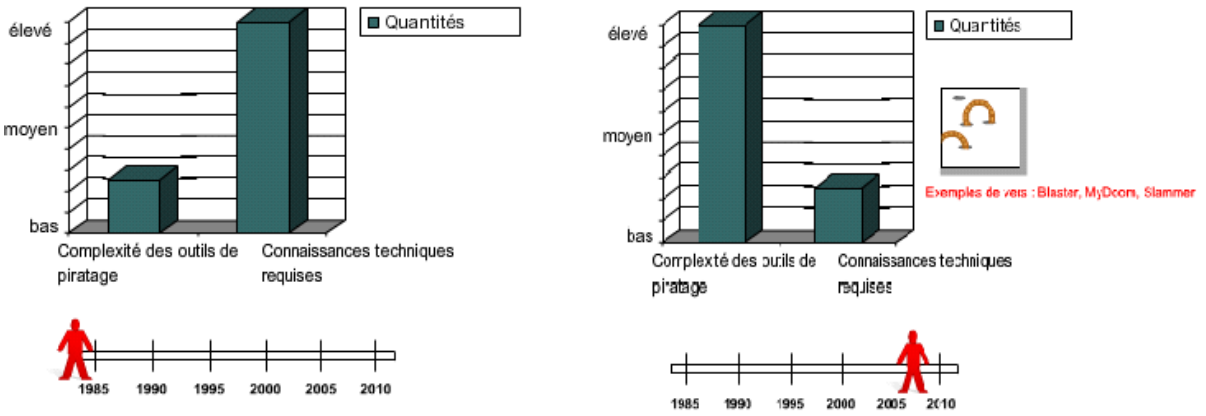


Figure III.1: l'augmentation des menaces

À mesure que les types de menaces, d'attaques et d'exploits évoluaient, différents termes ont été inventés pour désigner les individus impliqués dans ces malveillances. Voici quelques exemples des termes les plus courants :

- **Fouineur** (white hat en anglais) :

Individu qui recherche des vulnérabilités dans des systèmes ou réseaux et qui signale ces vulnérabilités à leurs propriétaires de manière à ce qu'ils puissent les éliminer. Ils ont une éthique qui les oppose à tout usage abusif des systèmes informatiques. Les fouineurs tendent généralement à sécuriser les systèmes informatiques, tandis qu'à l'opposé, les pirates (black hat, en anglais) veulent y pénétrer par intrusion.

- **Bidouilleur** (hacker en anglais) :

Terme général utilisé dans le passé pour désigner un expert en programmation.

Actuellement, ce terme est souvent utilisé de manière péjorative pour désigner un individu qui tente d'accéder de manière non autorisée aux ressources des réseaux avec une intention malveillante.

- **Pirate** (black hat en anglais) :

Autre terme désignant les personnes qui utilisent leurs connaissances des systèmes informatiques pour accéder de manière non autorisée à ces systèmes ou réseaux, habituellement dans un but personnel ou lucratif. Le terme anglais « cracker » est synonyme de « black hat ».

- **Spammeur** :

Individu qui envoie une grande quantité de courriels non sollicités. Les spammeurs utilisent souvent des virus pour prendre possession d'ordinateurs familiaux et utiliser ces derniers pour leurs envois massifs.

- **Hameçonner** (phisher en anglais) :

Individu qui utilise le courriel ou d'autres moyens pour amener par la ruse d'autres utilisateurs à leur fournir des données sensibles, comme des numéros de carte de crédit ou de passeport. L'hameçonner se fait passer pour une institution de confiance qui aurait un besoin légitime de ces données sensibles.

III.4. Les faiblesses de sécurité

III.4. 1.Faiblesses technologiques

Les technologies informatiques et de réseau ont des faiblesses de sécurité intrinsèques. Celles-ci comprennent :

- les faiblesses du protocole TCP/IP : par exemple les protocoles HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol) et ICMP (Internet Control Message Protocol) sont intrinsèquement non sécurisés

- les faiblesses du système d'exploitation : Tous les systèmes d'exploitation (UNIX, Linux, Windows NT, XP et Vista) présentent des problèmes de sécurité qui doivent être résolus.
- Les faiblesses de l'équipement réseau : tels que les routeurs, et les commutateurs, ont des faiblesses de sécurité qui doivent faire l'objet d'une détection et d'une protection. Ces faiblesses concernent la protection des mots de passe, le manque d'authentification, les protocoles de routage et les ouvertures dans les pare-feu.

III.4.2.Faiblesses de configuration

Les administrateurs réseau et les ingénieurs système doivent apprendre ce que sont les faiblesses de configuration et les compensées en configurant convenablement leurséquipements informatiques et réseau. Les exemples fréquents qu'on peut citer sont les suivants :

- Paramètres par défaut non sécurisés dans les produits logiciels
- Équipement réseau mal configuré : par exemple, des listes d'accès, des protocoles de routage ou des chaînes de communauté SNMP mal configurées peuvent ouvrir de larges failles dans la sécurité.

III.4.3.Faiblesses dans la stratégie de sécurité

Il existe des risques de sécurité pour le réseau si les utilisateurs ne respectent pas la stratégie de sécurité.

III.5. Les principales attaques

III.5.1.Les différentes étapes d'une attaque

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant lemême schéma :

- **Identification de la cible**

Cette étape est indispensable à toutes attaques organisées, elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'interrogation des serveurs DNS,….

- **Le scanning**

L'objectif est de compléter les informations réunies sur une cible visées.Il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée (OS, versions des services, subnet, règles de firewall….). Il faut noter que certaines techniques de scans particulièrement agressives sont susceptibles de mettre à mal un réseau et entraîner la défaillance de certains systèmes.

- **L'exploitation**

Cette étape permet à partir des informations recueillies d'exploiter lesfailles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau.

- **La progression**

Il est temps pour l'attaquant de réaliser ce pourquoi il a franchit les précédentes étapes. Le but ultime étant d'élever ses droits vers un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations, installation de backdoors, nettoyage des traces,…).

III.5.2. Les différents types d'attaque

Il existe un grand nombre d'attaques permettant à une personne mal intentionnée de s'approprier des ressources, de les bloquer ou de les modifier. Certaines requièrent plus de compétences que d'autres, le diagramme suivant résume d'une façon générale les déférents types d'attaque:

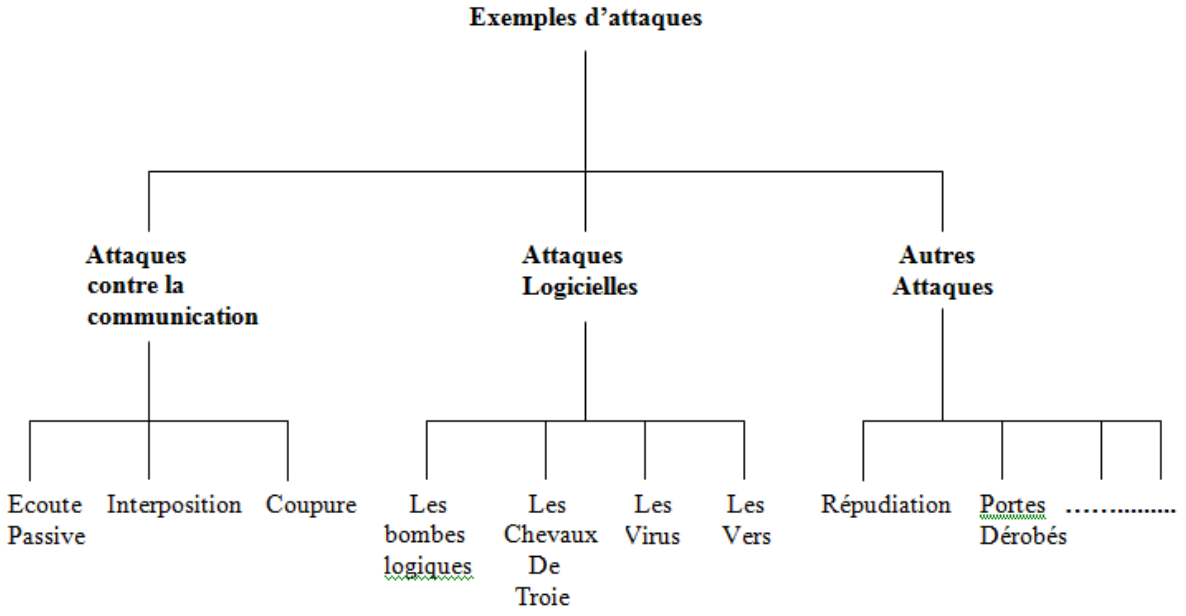


Figure III.2 : Les types d'attaques

III.5.2.1. Attaques contre la communication

- **Ecoute passive :**

Est un type d'attaque contre la confidentialité, qui consiste à accéder sans modification aux informations transmises ou stockées, l'information n'est pas altérée par celui qui en prélève une copie. Ces attaques sont donc indétectables par le système et peuvent seulement être parées par des mesures préventives.

- **Interposition :**

Il s'agit d'un « déguisement » en émission ou en réception, il consiste à tromper les mécanismes d'authentification pour se faire passer pour un utilisateur (personne ou service disposant des droits dont on a besoin) pour compromettre la confidentialité, l'intégrité ou la disponibilité.

Exemple : Le vol d'adresse (IP spoofing)

Ce type d'attaque n'implique rien de plus que l'usurpation d'une adresse source. Cela consiste à utiliser une machine en se faisant passer pour une autre.

- **Coupure (message interception) :**

Est un accès avec modification à des informations transmises sur des voies de communication, il s'agit donc d'une attaque contre l'intégrité.

III.5.2.2.Attaques logicielles

- **Les virus**

Un "virus" est un bout de programme glissé volontairement dans une application dans le but de nuire. Il est possible d'attraper un virus avec n'importe quelle application que l'on a installée et que l'on exécute, ce n'est pas un problème typique d'une connexion permanente. Un virus ne peut être introduit dans sa machine que si l'on exécute une application infectée, application récupérée sur l'Internet ou sur n'importe quel autre support informatique: Disquette, CD ROM etc.

Sur Internet, les virus peuvent contaminer une machine de plusieurs manières :
• Téléchargement de logiciel puis exécution de celui-ci sans précautions,
• Ouverture sans précautions de documents contenant des macros,
• Pièce jointe de courrier électronique (exécutable, script type VBs…),
• Ouverture d'un courrier au format HTML contenant du JavaScript exploitant une faille de sécurité du logiciel de courrier (normalement JavaScript est sans danger).

- **Le Cheval de Troie**

Un cheval de Troie ou troyen (Trojan Horse ou Trojan) n'est ni un virus ni un ver, parce qu'il ne se reproduit pas. Un cheval de Troie introduit sur une machine a pour but de détruire ou de récupérer des informations confidentielles sur celle-ci. Généralement il est utilisé pour créer une porte dérobée sur l'hôte infecté afin de mettre à disposition d'un pirate un accès à la machine depuis internet. Les opérations suivantes peuvent être effectuées par l'intermédiaire d'un cheval de Troie :

- récupération des mots de passe grâce à un keylogger.
- administration illégale à distance d'un ordinateur.
- relais utilisé par les pirates pour effectuer des attaques.
- serveur de spam (envoi en masse des e-mails).

- **Les vers**

Un ver est un programme indépendant, qui se copie d'ordinateur en ordinateur. La différence entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme et donc l'infecter. Il va simplement se copier via un réseau ou Internet, d'ordinateur en ordinateur. Ce type de réplication peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances du réseau dans une entreprise. Comme un virus, un ver peut

contenir une action nuisible du type destruction de données ou envoi d'informations confidentielles.

- **Le sniffing (l'écoute du réseau**)

Grâce à un logiciel appelé "sniffer", il est possible d'intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées. Si quelqu'un se connecte par Telnet par exemple à ce moment-là, son mot de passe transitant en clair sur le net, il sera aisé de le lire. De même, il est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception.

III.5.2.3.Autres attaques

- **Le DoS (Denial of Service)**

Le DoS est une attaque visant à générer des arrêts de service et donc à empêcher le bon fonctionnement d'un système. Cette attaque ne permet pas en elle-même d'avoir accès à des données. En général, le déni de service va exploiter les faiblesses de l'architecture d'un réseau ou d'un protocole. Il en existe de plusieurs types comme le flooding, le TCP-SYN flooding, le smurf ou le débordement de tampon (buffer-overflow)

- **Intrusion**

L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace et est donc une attaque. Les conséquences peuvent être catastrophiques : vol, fraude, incident diplomatique, chantage… Le principal moyen pour prévenir les intrusions est le coupe-feu ("firewall"). Il est efficace contre les fréquentes attaques de pirates amateurs, mais d'une efficacité toute relative contre des pirates expérimentés et bien informés. Une politique de gestion efficace des accès, des mots de passe et l'étude des fichiers « log » (traces) est complémentaire

- **Le craquage de mots de passe**

Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon.Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants (etde leur variantes), ou par la méthode de brute force (toutes les combinaisons sontessayées jusqu'à trouver la bonne). Cette technique longue et fastidieuse, souventpeu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machines.

III.6. Mécanismes de protection

Pour garantir la conformité aux règles de la stratégie de sécurité, la roue de la sécurité s'est révélé une méthode efficace en tant que processus continu. La roue de la sécurité incite à tester et à appliquer de manière continue des mesures de sécurité mises à jour (Figure III.3).

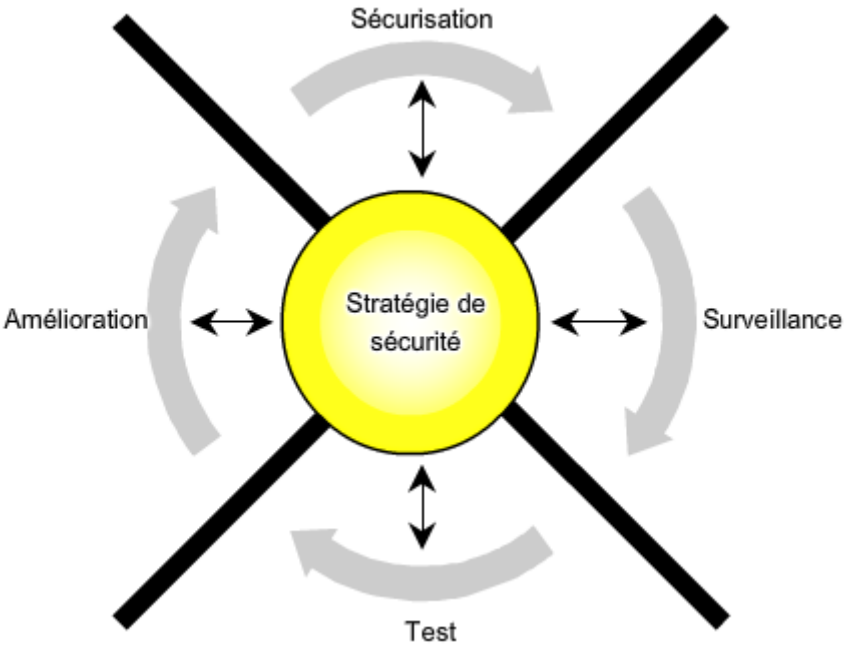


Figure III.3: la roue de sécurité

La figure III.2 nous illustre que la stratégie de sécurité est un moyeu auquel se rattachent les quatre rayons ou étapes de la roue de la sécurité. Ces étapes sont la sécurisation, la surveillance, le test et l'amélioration. Comme c'est expliqué c'est dessous, chacune de ces étapes nécessite des moyens et des astuces pour bien mettre en œuvre son principe.

III.6.1. Etape 1 :sécurisation

Sécurisez le réseau en appliquant la stratégie de sécurité et en mettant en œuvre les solutions de sécurisation suivantes :

- **Antivirus :**

Protection contre les menaces comme les virus, les vers en utilisant des antivirus. La plupart des antivirus sont basés sur l'analyse de signature des fichiers, la base des signatures doit donc être très régulièrement mise à jour sur le site de l'éditeur.

- **Inspection dynamique et filtrage des paquets : firewall**

Pour filtrer le trafic du réseau et ne permettre que le trafic et les services valides, l'inspection dynamique se rapporte à un firewall (pare-feu)qui est une machine dédiée au routage entre LAN et Internet. Le trafic est analysé au niveau des datagrammes IP (adresse, utilisateur, contenu...). Un datagramme non autorisé sera simplement détruit, IP sachant gérer la perte d'information. Une translation d'adresse pourra éventuellement être effectuée pour plus de sécurité (protocole NAT Network Address Translation).

- **Désactivation des services inutiles** :

Pour rendre l'accès plus difficile aux employés mécontent (pirate, hacker) en limitant le nombre de services activés.

- **Utilisation des protocoles de sécurité**

SSH (Secure Shell) : qui permet de chiffrer la communication et l'authentification des participants.

SSL (Security Sovkets Layers) : le but de SSL est de mettre un canal de communication sécurisé afin d'assurer la sécurité des transferts sur réseau .un grand avantage de SSL est que celui-ci est indépendant des protocoles utilisés dans la couche application, la mise en place de la sécurité avec ce protocole est basée sur l'échange des clés entre le client et le serveur.

IPSEC : est un Protocol de couche 3 dans le but est d'apporter de la sécurité sur Internet.

- **Authentification et cryptage :**

Le chiffrement ou le cryptage du trafic réseau permet d'empêcher une divulgation indésirable à des personnes non autorisées ou à des individus malveillants. Par le cryptage on peut identifier de manière sûre l'utilisateur connecté pour éviter l'espionnage, la modification du contenu, l'ajout de message.

Un service d'authentification repose sur deux composantes :

L'identification : dont le rôle est de définir les identités des utilisateurs.

L'authentification : permettant de vérifier les identités présumées des utilisateurs .lorsqu'il existe une seule preuve de l'identité (mot de passe par exemple) on parle d'authentification simple. Lorsque l'authentification nécessite plusieurs facteurs, on parle alors d'authentification forte.

- **Application de la stratégie de sécurité**

Il convient de s'assurer que les utilisateurs finaux et les périphériques d'extrémité respectent la stratégie de sécurité. Pour y arriver la sensibilisation et la formation des utilisateurs s'avèrent une étape très importante car on considère généralement que la majorité des problèmes de sécurité sont situés entre la chaise et le clavier

Pour cela la sensibilisation des utilisateurs à la faible sécurité des outils de communication et à l'importance du non divulgation d'informations par ces moyens est indispensable.

III.5.2. Etape 2 : surveillance

- **Système de détection d'intrusion**

La surveillance de la sécurité fait intervenir l'utilisation des périphériques de détection d'intrusion (Intrusion Système Détection ISD) baptisés sondes ou encore sniffer, ce sont des outils qui s'installent à un point stratégique du réseau. Ils analysent en permanence le trafic à la recherche d'une signature connue de piratage dans les trames. Ces systèmes ne repèrent que les attaques qui figurent déjà dans leur base de signatures. Ces sondes doivent être :

- Puissantes (débits des réseaux élevés) pour analyser toutes les trames.
- Capables de conserver un historique (actes de malveillance divisés sur plusieurs Trames).
- Fiable, c'est à dire tolérante aux pannes (retour à l'état initial après une interruption).

La surveillance de la sécurité fait intervenir aussi analyse du comportement de l'utilisateur qu'est installée sur les systèmes d'exploitation (OS) ou sur les applications, l'analyse du comportement scrute les fichiers d'événements et non plus le trafic pour cela des administrateurs réseau compétant sont placés sur le système ou l'application supervisés. Leur mission consiste à repérer tout abus ou comportement suspect (visent à vérifier et d'interpréter les données du fichier journal)

III.6.3. Etape 3 : test

La phase de test de la roue de la sécurité consiste à tester de manière proactive les mesures de sécurité. La vérification concerne en particulier le fonctionnement des solutions de sécurité de l'étape 1 et 2 pour cela on utilise :

- **Des Tests de maintenance** : en utilisant les commandes de tests suivantes :

Ping : commande pour tester la présence d'une machine sur le réseau. Elle Compte le temps nécessaire pour aller de la machine où l'on se trouve à la machine appelée ; cette commande vérifie la connectivité IP d'un ordinateur utilisant les protocoles TCP/IP en envoyant des messages(Requête) dans le but d'avoir des réponses d'une machine.

Traceroute : permet de déterminer le chemin d'un point à un autre avec des délais

Finger : permet de connaitre les caractéristiques d'un utilisateur connecté.

- **Logiciels de test de la sécurité d'une installation** :

En utilisantsoit des systèmes de détection d'intrusions comme :NIDS, HIDS ; et d'autres logiciels comme :

Crack : test les mots de passes Unix

Satan : permet le test de machines UNIX sur un réseau

III.6.4. Etape 4: amélioration

Le maintien d'un réseau dans un état aussi sécurisé que possible impose de répéter continuellement le cycle de la roue de la sécurité, car de nouvelles vulnérabilités et de nouveaux risques apparaissent tous les jours. La stratégie de sécurité doit subir un réajustement dès que de nouvelles vulnérabilités ou de nouveaux risques sont découverts.

III.7.La sécurité dans lés réseau en utilisant des firewalls et routeurs

III.7.1.Notions de base sur les firewalls

III.7.1.1 .L'utilité d'un firewall

Un pare-feu (appelé aussi *coupe-feu*, *garde-barrière* ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Il est utilisé pour :

Contrôlerle trafic sortant d'un réseau, et notamment éviter que les utilisateurs accèdent à certains nœuds du réseau.

Sécuriserle trafic entrant d'un réseau, et empêcher certains nœuds extérieurs de se connecter un réseau local.

Enfin, pour une question de**vigilance**, et éviter que certaines machines mal configurées du réseau local n'envoient des données vers l'extérieur.

Le firewall ainsi défini permet de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'unepasserelle filtrante comportant au minimum les interfaces réseau suivante :

- Une interface pour le réseau à protéger (réseau interne).
- Une interface pour le réseau externe.

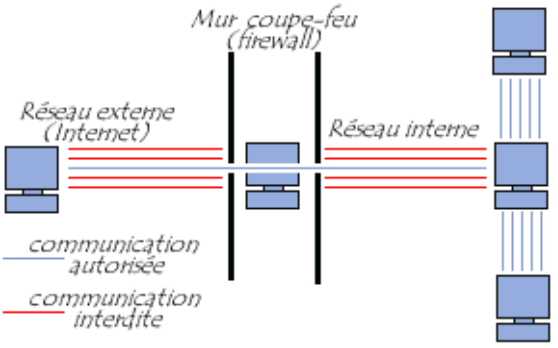


Figure III.4 : Fonctionnement d'un firewall

III.7.1.2.Fonctionnement générale

Un système pare-feu contient un ensemble de règles prédéfinies permettant soit d'autoriser la connexion (permit),soit de la bloquer (deny) ou bien de rejeter la demande de connexion sans avertir l'émetteur (drop).Le but ultime est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège. En effet ces zones sont souvent de trois passages qui sont les suivants :

- Entre le réseau privé et le Net : ce passage concerne la connexion entre le réseau local et l'extérieur
- Entre la DMZ et le Net : Appliqué à une infrastructure réseau, la DMZ, qu'est une zone démilitarisée, permet de déporter certains serveurs nécessitant un accès extérieur (par exemple un serveur Web), afin que ceux-ci ne mettent plus en péril la sécurité du réseau interne sécurisé ainsi un passage entre la DMZ et l'internet doit se faire du moment que nous avons des serveurs qui doivent être accessibles depuis le Net.

- Entre le réseau privé et la DMZ dans le but de :

Mettre à jour les serveurs web

Envoyer et recevoir les messages, puisque le SMTP est dedans

Mettre à jour le contenu du FTP (droits en écriture).

En revanche, depuis la DMZ, il ne devrait y avoir aucune raison pour qu'une connexion soit initiée vers la zone privée.

III.7.1.3.Les Types de filtrage

- **Le filtrage simple des paquets** :stateless packet filtering

Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure. Ainsi, les paquets de données échangées entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- adresse IP de la machine émettrice
- adresse IP de la machine réceptrice
- type de paquet (TCP, UDP, etc.)
- numéro de port (rappel: un port est un numéro associé à un service ou une application réseau).

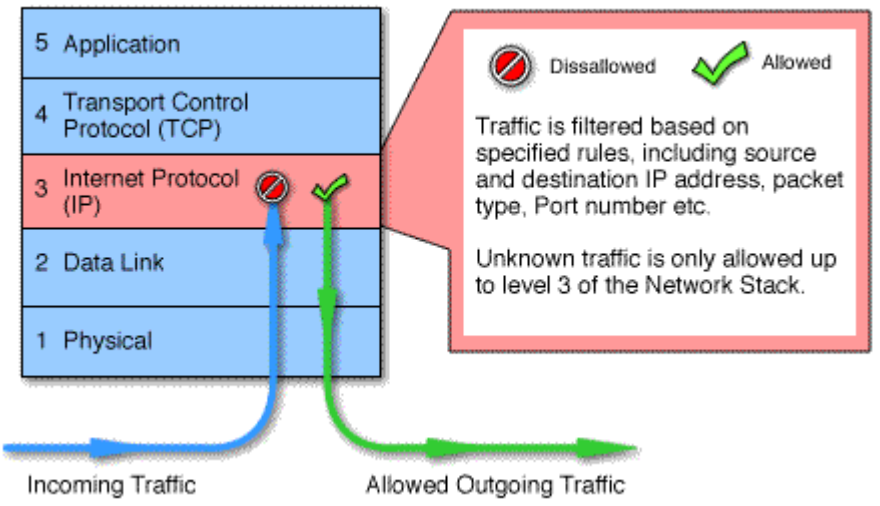


Figure III.5 : Filtrage des paquets IP

- **Filtrage dynamique** : stateful packet filtering

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services (le FTP par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire) un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente.

Ainsi, il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de filtrage dynamique de paquets est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur. Un dispositif pare-feu de type « stateful inspection » est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu; l'ensemble des paquets transitant dans le cadre de cette Connexion seront implicitement acceptés par le pare feu. Si le filtrage dynamique est plus performant que le filtrage de paquets basique, il ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications. Or ces vulnérabilités représentent la part la plus importante des risques en termes de sécurité.

- **Filtrage applicatif**

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI . De plus, il permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire. Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application.

Un firewall effectuant un filtrage applicatif est appelé généralement « passerelle applicative » (ou proxy).

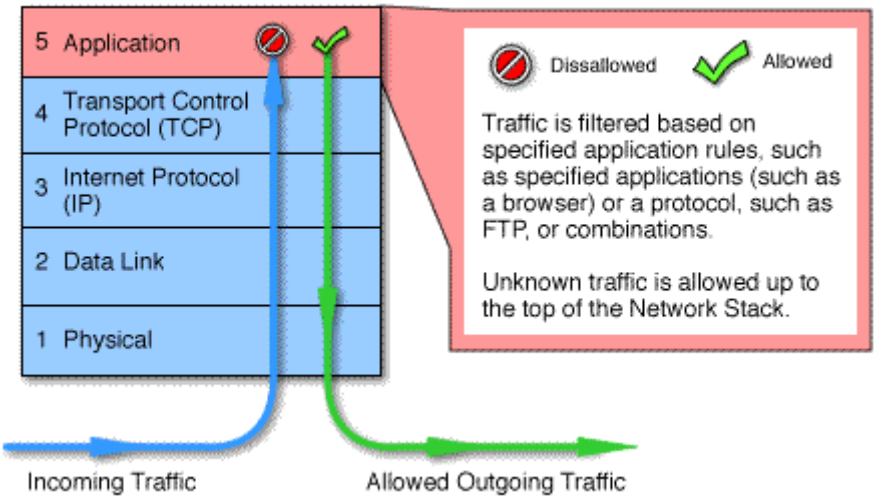


Figure III.6 : Filtrage des protocoles applicatifs (FTP, HTTP, ...)

III.7.1.4.Les Limites des firewalls

Les firewalls n'offrent une protection que dans la mesure où l'ensemble des communications vers l'extérieur passe systématiquement par leur intermédiaire et qu'ils sont correctement configurés. Ainsi, les accès au réseau extérieur par contournement du firewall sont autant de failles de sécurité. C'est notamment le cas des connexions effectuées à partir du réseau interne à l'aide d'un modem ou de tout moyen de connexion échappant au contrôle du pare-feu

III.7.2.Mise en œuvre de la sécurité dans les firewalls et dans les routeurs

La technologie de sécurité basée sur la configuration des listes de contrôle d'accès (ACL) et la translation d'adresses (NAT ,PAT) s'avère la plus largement utilisée dans le monde et c'est grâce a cette technologie que les firewalls dédiés de la gamme CISCO PIX occupent aujourd'hui la première place du marché.

III.7.2.1. Les listes de contrôle d'accès(ACL)

Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus,appelé respectivement **permit** et **deny**, qui s'appliquent aux adresses ou aux protocoles de couche supérieure.

III.7.2.1.1.le fonctionnement des ACL

Les listes de contrôle d'accès représentent un outil puissant pour contrôler le trafic entrant ou sortant d'un réseau ;

✓ **Listes de contrôle d'accès entrantes** : les paquets entrants sont traités avant d'être routés vers l'interface de sortie. Une liste de contrôle d'accès entrante est efficace car elle réduit la charge des recherches de routage en cas d'abandon du paquet. Si le paquet est autorisé à l'issue des tests, il est soumis au routage.

✓ **Listes de contrôle d'accès sortantes** : les paquets entrants sont routés vers l'interface de sortie puis traités par le biais de la liste de contrôle d'accès sortante.

Les instructions d'une liste de contrôle d'accès fonctionnent dans un ordre séquentiel. Elles évaluent les paquets en les validant par rapport à la liste de contrôle d'accès, de haut en bas, une instruction après l'autre. La figure III.7 illustre la logique de fonctionnement des ACLs :

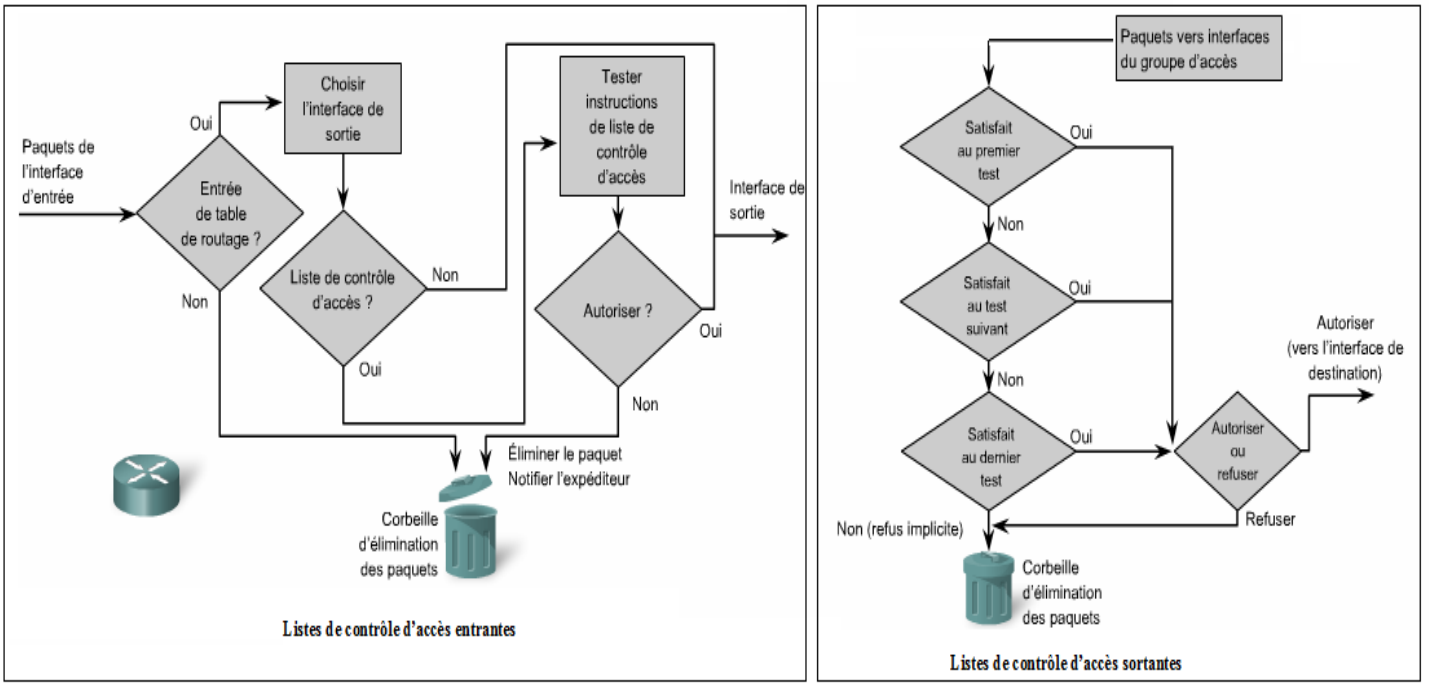


Figure III.7 :Fonctionnement des listes de contrôle d'accès (ACL)

III.7.2.1.2.Types de liste de contrôle d'accès:

Il existe deux types de liste de contrôle d'accès Cisco : standard et étendue.

➢ **Listes de contrôle d'accès standard** :

Les listes de contrôle d'accès standard permettent d'autoriser et de refuser le trafic en provenance d'adresses IP source. La destination du paquet et les ports concernés n'ont aucune incidence.

- **Listes de contrôle d'accès étendues** :

Les listes de contrôle d'accès étendues filtrent les paquets IP en fonction de plusieurs attributs, dont le type de protocole, l'adresse IP source, l'adresse IP de destination, les ports TCP ou UDP source, les ports TCP ou UDP de destination, et les informations facultatives sur le type de protocole pour une meilleure précision du contrôle.

Au moment de configurer les listes de contrôle d'accès (standard ou étendue) on doit identifier chaque liste en lui attribuant un numéro unique. Cenuméro identifie le type de liste d'accès créé et doit être compris dans la plage de numéros telque :

la plage 1-99,et 1300-1999 : pour les ACLs standard

la plage 100-199,et 2000-2699 :pour les ACLs étendu

III.7.2.1.3.positionnement des listes de contrôle d'accès

Chaque liste de contrôle d'accès doit être placée là où elle aura le plus grand impact sur les performances. Les règles de base sont les suivantes :

- ✓ Placez les listes de contrôle d'accès étendues le plus près possible de la source du trafic refusé. Ainsi, le trafic indésirable est filtré sans traverser l'infrastructure réseau.
- ✓ Étant donné que les listes de contrôle d'accès standard ne précisent pas les adresses de destination, donc on les places le plus près possible de la destination.

III.7.2.1.4.Configuration des listes de contrôle d'accès :

Les listes de contrôle d'accès (standard ou étendue) sont créées en mode de configuration globale.Les commandes qui configure les listes de control d'accès peuvent être de très longues chaines de caractères .ces commandes peuvent être réduites à deux éléments principaux :

- ✓ Création de la liste d'accès

Les ACLs sont crées au moyen de la commande « **acces-list** » sous la forme suivante :

Firewall (config)#**acces-list**numero-de-liste {**permit / deny**} {**condition à tester** }:cette instruction identifie la liste d'accès par :

Un numéro qui indique de quel type elle sera : standard ou étendue

Permit et deny qui indiquent la façon dont les paquetscorrespondant ou non aux conditions à tester seront traités par le logiciel IOS.

Le paramètre final de cette instruction spécifie les conditions que cette instruction testera.

- ✓ Association de la liste d'accès a une interface

Après avoir créer la liste de contrôle d'accès,il faut l'associée a une interface de routeur (ou d'un firewall) donnée dans l'invite **config-if .**L'instruction générale s'écrit comme suit :

Router(config-if)#{protocoles}acces-group numero-de-liste {in/out}

In ou out pour spécifier est ce que l'ACL crée est appliquée aux paquets entrants (in) ou sortants(out) .

Quand on applique une ACL à une interface,celle-ci oblige le firewall(ou routeur) à lire l'en-tête de couche 3, et de couche 4, d'un paquet transitant sur le réseau pour voir s'il remplit les conditions du test.

Pour filtrer les paquets TCP/IP,les listes d'accès IP vérifient dans les en-têtes de couches supérieures les éléments suivants :

Adresse IP source en utilisant des listes d'accès standard,celle-ci sont identifiée par un numéro entre 1et 99.

Adresse IP source et destination,protocoles spécifiques et numéro de port de TCP ou UDP en utilisant les ACLs étendues sui sont identifiées par un numéro compris entre 100 et 199.

- **Configuration d'une ACL standard**

Firewall(config)#access-list numero-de-list {permit/deny } source [IP address et wildcard mask]télque :

wildcardmask=masque générique

numerous de liste compris entre [1 99]

- **Configuration d'une ACL étendue :** la forme de l'instruction est la suivante :

Firewall(config)#access-list numero-de-list {permit/deny} {source protocol, source-adresse ,source-wildcard }{destination -adresse ,destination-wildcard } eq { numero-de-port }

III.7.2.1.5.Principe de masque générique

Un masque générique est une chaîne de chiffres binaires de 32 bits spécifiant au routeur quel numéro de sous-réseau vérifier.

Les deux types de masque :générique et masque de sous réseau utilisent les chiffres binaires 1 et 0. Les masques de sous-réseau utilisent les chiffres binaires 1 et 0 pour identifier

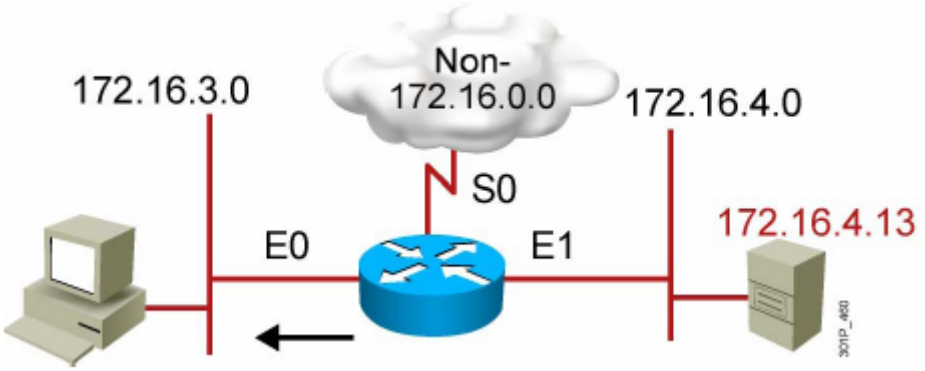
la partie réseau, la partie sous-réseau et la partie hôte d'une adresse IP.Les masques génériques utilisent les chiffres binaires 1 et 0 pour filtrer des adresses IP individuelles ou des groupes d'adresses IP, afin d'autoriser ou de refuser l'accès aux ressources en fonction d'une adresse IP telque :

Bit 0 de masque générique : permet de vérifier la valeur du bit correspondant dans l'adresse.

Bit 1 de masque générique : permet d'ignorer la valeur du bit correspondant dans l'adresse.

Pour le calcul du masque générique d'une adresse IP, on utilise 255.255.255.255 et le soustraire de masque de sous réseau correspondant a cette adresse IP.

III.7.2.1.6.Exemple de configuration des AClsdans un routeur



FigureIII.8: Exemple de configuration d'une ACL

- **Cas de configuration d'une ACL standard :**

Le but est d'appliquer les deux exemples suivants :

1- bloquer l'adresse hôte :172.16.4.13 d'accéderà l'adresse réseau 172.16.3.0
2- permettre toutes autres adresses

la configuration de ces deux exemples est la suivante:

Router (config)#access-list 4 deny 172.16.4.13 0.0.0.0

Router (config)#access-list 4 permit 0.0.0.0 255.255.255.255

Router(config)#interface Ethernet 0

Router(config-if)#IP access-group 4 out

- **Cas de configuration d'une ACL étendue :**

Le but est :

1- De bloquer le transfert de fichier TFTP(port 21) et le TELNET(23) provenant du réseau 172 .16.4.0 d'accéder au réseau 172.16.3.0
2- Permettre le Protocol TCP de tous les autres réseaux de passer au réseau 172.16.3.0

Ces deux étapes sont configurées respectivement ci-dessous :

router(config)#access-list 101 deny TCP 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21

Router(config)#access-list 101 deny TCP 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 23

Router(config)#access-list 101 permit TCP any any

Router(config)#interface Ethernet 0

Router(config-if)#ip access-group 101 out

II.7.2.2.Translation d'adresse :NAT

II.7.2.2.1.Principe de translation d'adresse

La principale fonction de NAT est d'enregistrer les adresses IP en autorisant les réseaux à utiliser des adresses IP privées. NAT traduit les adresses non routables, privées et internes en adresses routables publiques. NAT permet également d'ajouter un niveau de confidentialité et de sécurité à un réseau car il empêche les réseaux externes de voir les adresses IP internes.

Le principe du NAT consiste donc à utiliser une passerelle de connexion à internet, possédant au moins une interface réseau connectée sur le réseau interne et au moins une interface réseau connectée à Internet (possédant une adresse IP routable), pour connecter l'ensemble des machines du réseau.Il s'agit de réaliser, au niveau de la passerelle, une translation (littéralement une « traduction ») des paquets provenant du réseau interne vers le réseau externe.Ainsi, chaque machine du réseau nécessitant d'accéder à internet est configurée pour utiliser la passerelle NAT (en précisant l'adresse IP de la passerelle dans le champ « Gateway » de ses paramètres TCP/IP). Lorsqu'une machine du réseau effectue une requête vers Internet, la passerelle effectue la requête à sa place, reçoit la réponse, puis la transmet à la machine ayant fait la demande.

Étant donné que la passerelle camoufle complètement l'adressage interne d'un réseau, le mécanisme de translation d'adresses permet d'assurer une fonction de sécurisation. En effet,

pour un observateur externe au réseau, toutes les requêtes semblent provenir de l'adresse IP de la passerelle.

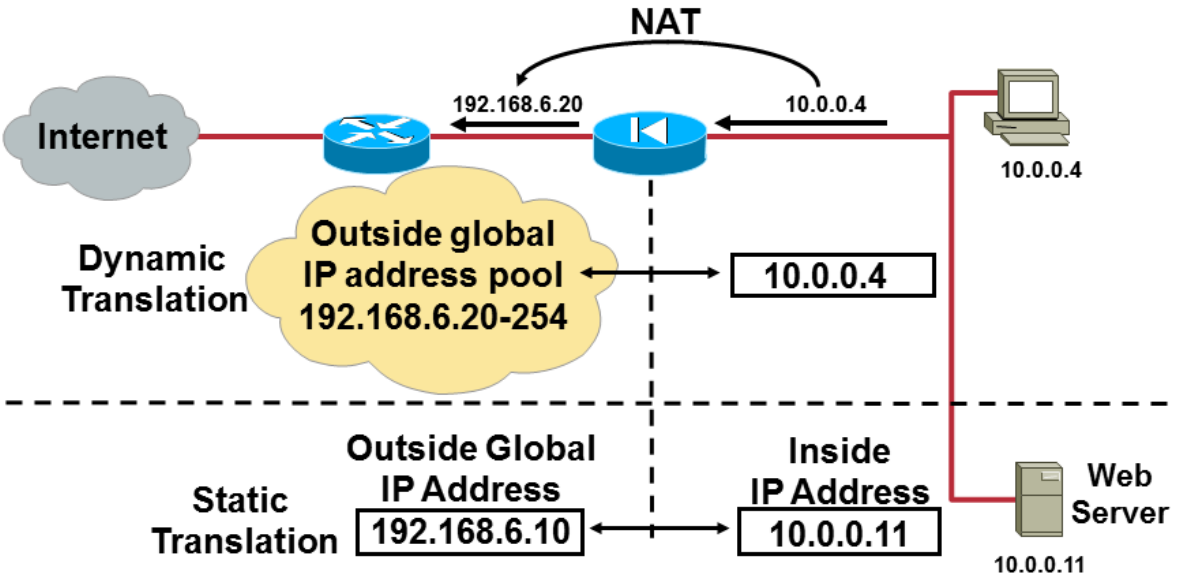


Figure III.9 : Présentation de principe du NAT

III.7.2.2.2.Désignation des interfaces lors du configuration de NAT

Les éléments (firewall,routeur ,..) configurés pour la NAT tiennent à jour une table appelée table NAT. Chaque entrée de cette table contient cinq champs :

- ✓ Protocole :repère le protocole IP dont la connexion doit être traduite en utilisant les

adresses IP contenue dans l'enregistrement.

- ✓ Adresses IP internes locales : c'est des adresse IP du réseau local (interne)
- ✓ Adresses IP internes globales : sont les adresses en lesquelles les adresses IP locales

internes sont traduites.

- ✓ Adresses IP externes locales : ce sont les adresses IP de l'espace d'adressage interne

par lesquelles sont connues les machines connectées aux réseaux externe.

- ✓ Adresse IP externes globales :sont les adresses de machines connectées aux réseaux externe.

II.7.2.2.3.Types de NAT

Il existe deux types de traduction NAT : dynamique et statique.

- **NAT dynamique**

La fonction NAT dynamique utilise un pool d'adresses publiques et les attribue selon la méthode du premier arrivé, premier servi. Lorsqu'un hôte ayant une adresse IP privée demande un accès à Internet, la fonction NAT dynamique choisit dans le pool une adresse IP qui n'est pas encore utilisée par un autre hôte. Cette description est celle du mappage

- **NAT statique :**

La fonction NAT statique utilise un mappage biunivoque des adresses locales et globales ; ces mappages restent constants. Cette fonction s'avère particulièrement utile pour les serveurs Web ou les hôtes qui doivent disposer d'une adresse permanente, accessible depuis Internet. Ces hôtes internes peuvent être des serveurs d'entreprise ou des périphériques réseau.

Les fonctions NAT statique et dynamique nécessitent toutes deux qu'il existe suffisamment d'adresses publiques disponibles pour satisfaire le nombre total de sessions utilisateur simultanées donc dans ce cas ,une entreprise qui a un grand réseaux par exemple doit envisager d'acheter plusieurs adresses publiques pour faire sortir beaucoup d'utilisateurs au même temps ,mai sur le plan économique cette solution revient plus chère pour cette entreprise , et c'est ce qui a fait apparaitre la solution de translation de ports d'adresses PAT (ou bien surcharge NAT) dont le principe de fonctionnement est expliqué c'est dessous :

Le PAT mappe plusieurs adresses IP privées à une seule adresse IP publique ou à quelques adresses. Grâce au PAT, plusieurs adresses peuvent être mappées à une ou quelques adresses car chaque adresse privée est également suivie par un numéro de port. Lorsqu'un client ouvre une session TCP/IP, le routeur NAT attribue un numéro de port à son adresse source. La surcharge NAT s'assure que les clients utilisent un numéro de port TCP différent pour chaque session client avec un serveur sur Internet. Lorsqu'une réponse revient du serveur, le numéro de port source, qui devient le numéro de port de destination lors du retour, détermine le client auquel le routeur achemine les paquets. Il confirme également que les paquets entrants étaient demandés, ce qui ajoute un niveau de sécurité à la session.

II.7.2.2.4.Configuration de la NAT

Les figures :**II.10 ,11,12**montrent les étapes de configuration du NAT statique ,NAT dynamique et le PAT respectivement :

Étape	Action	Remarques
1	Établissez la traduction statique entre une adresse locale interne et une adresse globale interne. `Router(config)#ip nat inside source static ip-locale ip-globale`	Entrez la commande globale **`no ip nat inside source static`** pour supprimer la traduction source statique.
2	Spécifiez l'interface interne. `Router(config)#interface numéro type`	Entrez la commande **`interface`**. L'invite d'ILC passe de `(config)#` à `(config-if)#`.
3	Signalez l'interface comme connectée à l'intérieur. `Router(config-if)#ip nat inside`	
4	Quittez le mode de configuration d'interface. `Router(config-if)# exit`	
5	Spécifiez l'interface externe. `Router(config)#interface numéro type`	
6	Signalez l'interface comme connectée à l'extérieur. `Router(config-if)#ip nat outside`	

Figure III.10 :Configuration du NAT statique

Étape	Action	Remarques
1	Définissez un pool d'adresses globales à attribuer selon les besoins. `Router(config)#ip nat pool nom ip-début ip-fin {netmask masque-réseau | prefix-length longueur-préfixe}`	Entrez la commande globale **no ip nat pool** *nom* pour supprimer le pool d'adresses globales.
2	Définissez une liste d'accès standard autorisant les adresses qui doivent être traduites. `Router(config)#access-list numro-liste-d' accs permit source [ masque-gnrique-source]`	Entrez la commande globale **no access-list** *numéro-liste-d'accès* pour supprimer la liste d'accès.
3	Établissez une source dynamique de traduction, en spécifiant la liste d'accès définie à l'étape précédente. `Router(config)#ip nat inside source list numéro-liste-d'accès pool nom`	Entrez la commande globale **no ip nat inside source** pour supprimer la source dynamique de traduction.
4	Spécifiez l'interface interne. `Router(config)#interface numéro type`	Entrez la commande **interface**. L'invite ILC passe de `(config)#` à `(config-if)#`.
5	Signalez l'interface comme connectée à l'intérieur. `Router(config-if)#ip nat inside`	
6	Spécifiez l'interface externe. `Router(config)#interface numéro type`	
7	Signalez l'interface comme connectée à l'extérieur. `Router(config-if)#ip nat outside`	
8	Quittez le mode de configuration d'interface. `Router(config-if)# exit`	

FigureIII.11: Configuration du NAT dynamique

Étape	Action	Remarques
1	Définissez une liste d'accès standard autorisant les adresses qui doivent être traduites. `Router(config)#access-list numéro-liste-contrôle-d'accès permit source [masque-générique-source]`	Entrez la commande globale **`no access-list`** *`numéro-liste-d'accès`* pour supprimer la liste d'accès.
2	Spécifiez l'adresse globale, en tant que pool, à utiliser pour la surcharge. `Router(config)#ip nat pool nom ip-début ip-fin {netmask masque-réseau | prefix-length longueur-préfixe}.`	
3	Établissez la traduction de surcharge. `Router {config} #ip nat inside source list numéro-liste-contrôle-d'accès pool nom overload.`	

4	Spécifiez l'interface interne.
	`Router(config)#interface type numéro`
	`Router(config-if)#ip nat inside`
		Entrez la commande **`interface`**. L'invite d'ILC passe de `(config)#` à `(config-if)#`.

5	Spécifiez l'interface externe.
	`Router(config-if)#interface type numéro`
	`Router(config-if)#ip nat outside`	

Figure II.12.: Configuration du PAT

IV.1.Introduction

Le but de ce chapitre est de presenter un plan de sécurité pour l'appliquer au niveau de réseau d'ENIEM de façon a assurer la sécurité de ce réseau. Pour commencer on a présenter les deux simulateurs « PACKET TRACERT » et « GNS3»,le premier est utilisé pour la configuration des éléments que contient le réseau(switch, federateur, et les routeurs),le deuxiéme c'est pour la configuration du firewall(PIX) installé.En suite,après avoir présenté le réseau existant on a etudié ses failles et dans ce qui suit on a proposé une solution basé sur l'administration du réseau ainsi qu'un filtrage des addresses IP en utilisant la configuration des listes de contrôle d'accè (ACL).

IV.2.1.les logiciels de simulation

IV.2 .1.1 Le logiciel « PACKET TRACERT »

- **Définition**

Packet Tracer est un logiciel fournit par Cisco, il nous permet de concevoir, configurer et simuler des réseaux.

Il nécessite pour son fonctionnement le matériel suivant :

- ✓ Intel Pentium 200 MHZ
- ✓ 64 MB de RAM.
- ✓ 30 MB de disque dur.

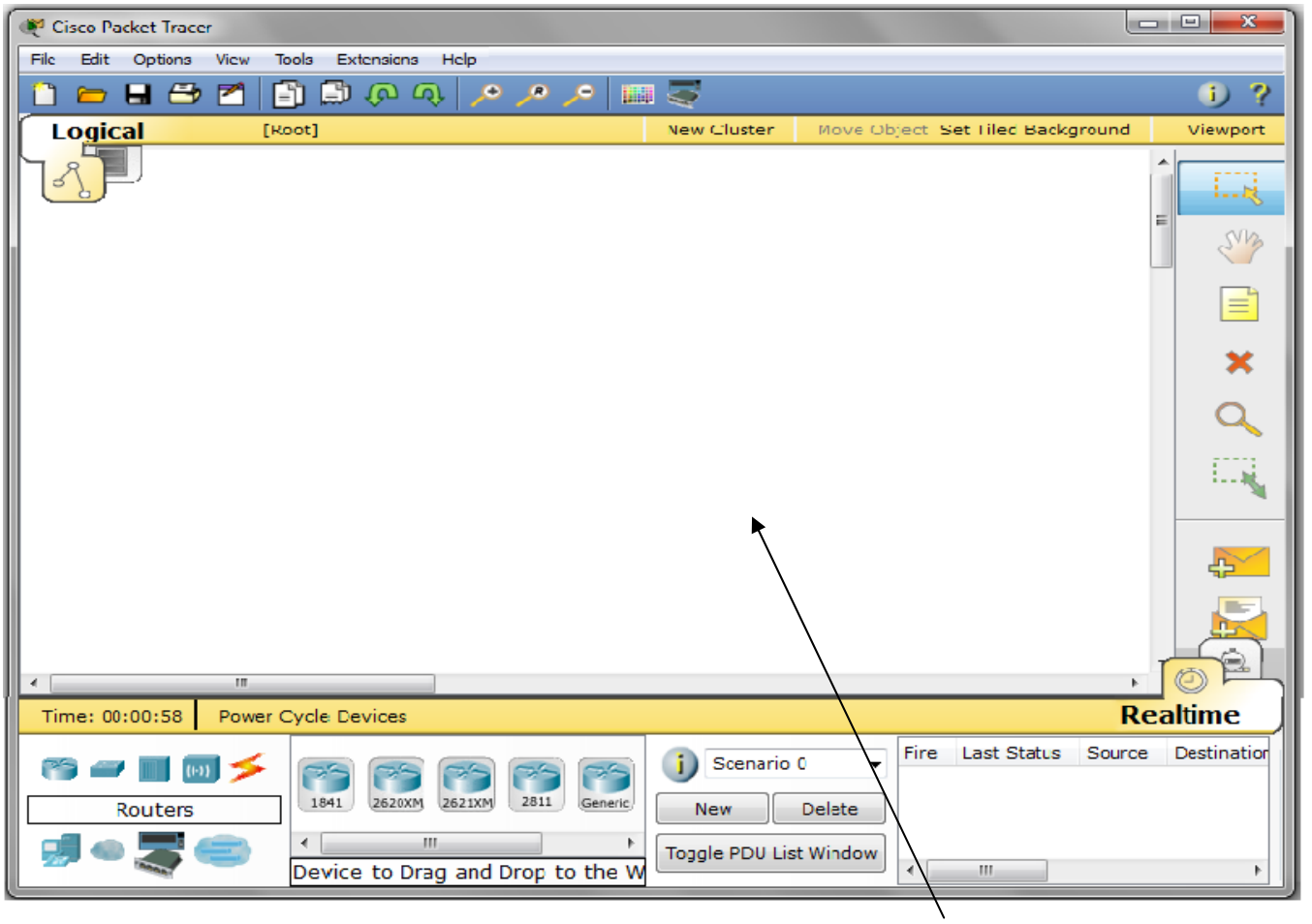
Packet Tracer fonctionne sous les systèmes d'exploitation suivants : WIN 98, XP, WIN7.

- **Technologie et protocoles supportés :**

Packet Tracer supporte toute sorte de câbles (câble série, faste Ethernet, Gigabit Ethernet, Fibre optique) ainsi que les technologies suivantes : VLAN, ACL, VLSM, DHCP, comme il introduit les couches du modèle OSI lors de l'acheminement du paquet.

Il supporte les équipements suivants : PC,routeur, Switch,point d'accès,hub, nuage, pont,serveur,imprimante,répétiteur.

Quand on œuvre Packet Tracer, la fenêtre de la figure IV.1 s'œuvre :



Espace où on crée notre réseau

Figure IV.1: La page principale du Packet Tracer

Les éléments de sa barre d'outils sont :

New open save print copy paste

Les icones des différents éléments à utiliser pour créer le réseau se trouve dans l'emplacement que la figure montre et il suffit juste de cliquer et sur l'un de ces éléments et lui faire glisser sur l'espace réserver pour créer le réseau.

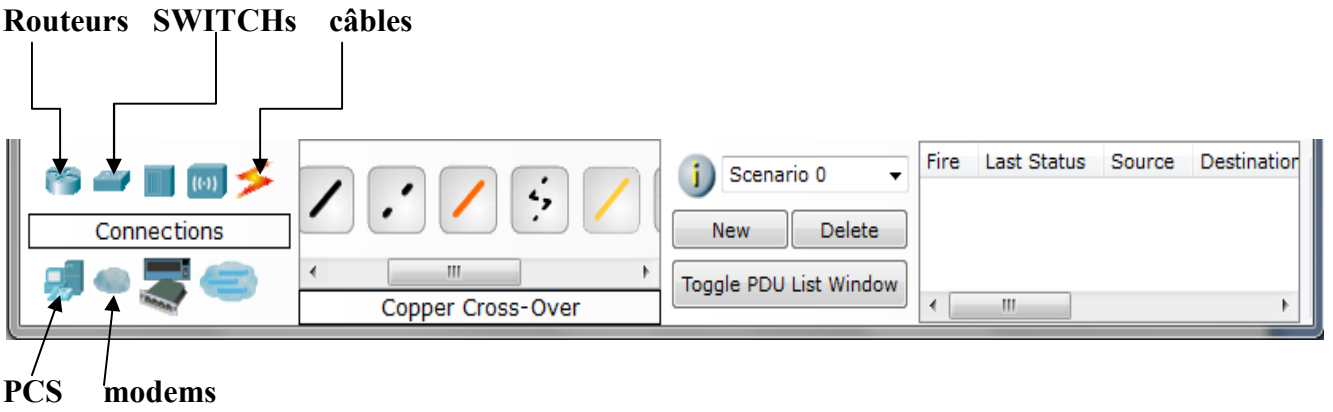


Figure IV.2: barre des équipements réseau

- **Modes de Packet Tracer**

A.Mode topologique :

Pour créer un réseau.

Ce mode introduit les types de connexions suivants :

- Copper straight-through :

C'est un standard Ethernet pour connecter différents équipements

Exemple : Hub ⟶ Routeur

Switch ⟶ PC

Routeur ⟶ Hub

La connexion peut être réalisée par les ports suivants : 10 MBS Copper (Ethernet) ,100 MBS Copper (Faste Ethernet) et 1000 MBS Copper (GB Ethernet).

- Copper cross-over

C'est un standard Ethernet pour connecter deux équipements de même couche OSI.

- Fibre

Elle est utilisée pour mettre des connexions entre ports fibre (100 MBS et 1000 MBS)

- Wireless

N'est établie qu'entre les PC et les points d'accès, plusieurs PC peuvent être connectés à un seul pont d'accès.

- Phone

C'est une connexion établie entre PC Routeur, PC Switch, elle est utilisée pour la configuration à distance.

B.Simulation mode

Pour tester des différentes situations configurées en mode topologie. On peut créer des nouveaux scénarios en cliquant sur le bouton « NEW». Pour ajouter un autre paquet en clique sur  ,dans ce mode on peut voir le parcours d'un paquet dans les différentes couches de modèle OSI ainsi que sa durée de vie.

- Les différentes situations d'un paquet le long de son chemin :

L'arrivée d'un paquet avec succès est représenté par : 

L'arrivée d'un paquet avec sans succès est représenté par : 

Si un paquet entre dans la file d'attente il sera représenté comme suit : 

IV.2.1.2 Le logiciel « GNS3 »

GNS3 est un simulateur graphique d'équipement réseaux qui nous permet de créer des topologies de réseaux complexes et d'en établir des simulation.De plus, il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco .L'Ios c'est le système d'exploitation des routeursetSwitch et firewall Cisco et pour enttrer dans l'interface graphique de chaque éléments il faut télécharger son IOS,GNS3 est compatible avec :Windows, Linux,…

La figure IV.3 c'est la premiere figure qui s'œuvre lorsque on click sur le logiciel « GNS3»,cette figure nous présentes l'emplacement des différentes icones qu'on utilise pour créer un réseau :

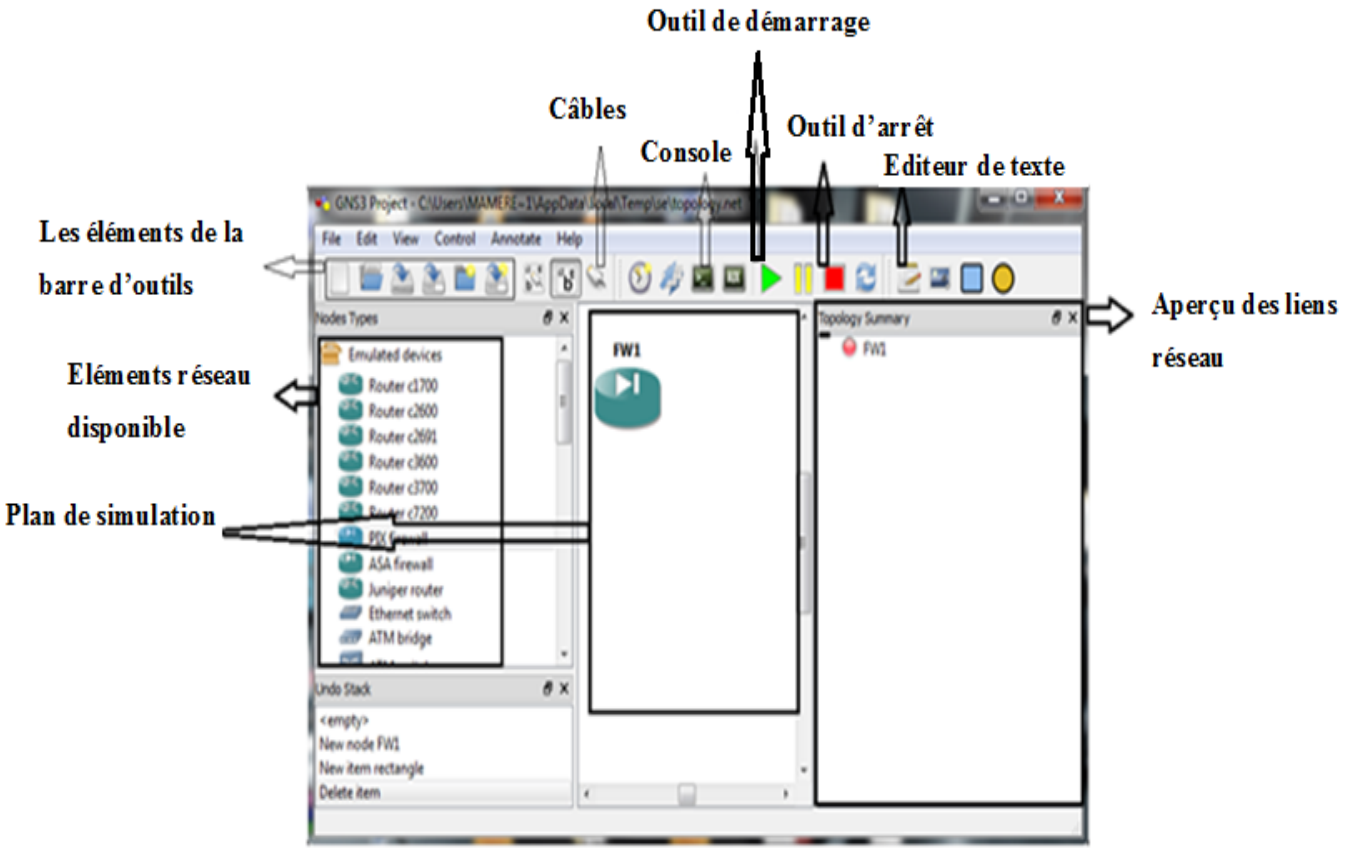


Figure IV.3 : Détail de la fenêtre du simulateur

Pour ce qui concerne la configuration d'un firewall(PIX),on click sur EDIT ⟶Péférence et la figure IV.4 s'œuvre . puis en suit les étapes suivante :

- Sélectionner l'onglet **Qemu.**
- Dans le champ binary image on click sur parcourir (…) pour indiquer l'emplacement de l'IOS du PIX
- On click sur « APPLY» puis « OK»

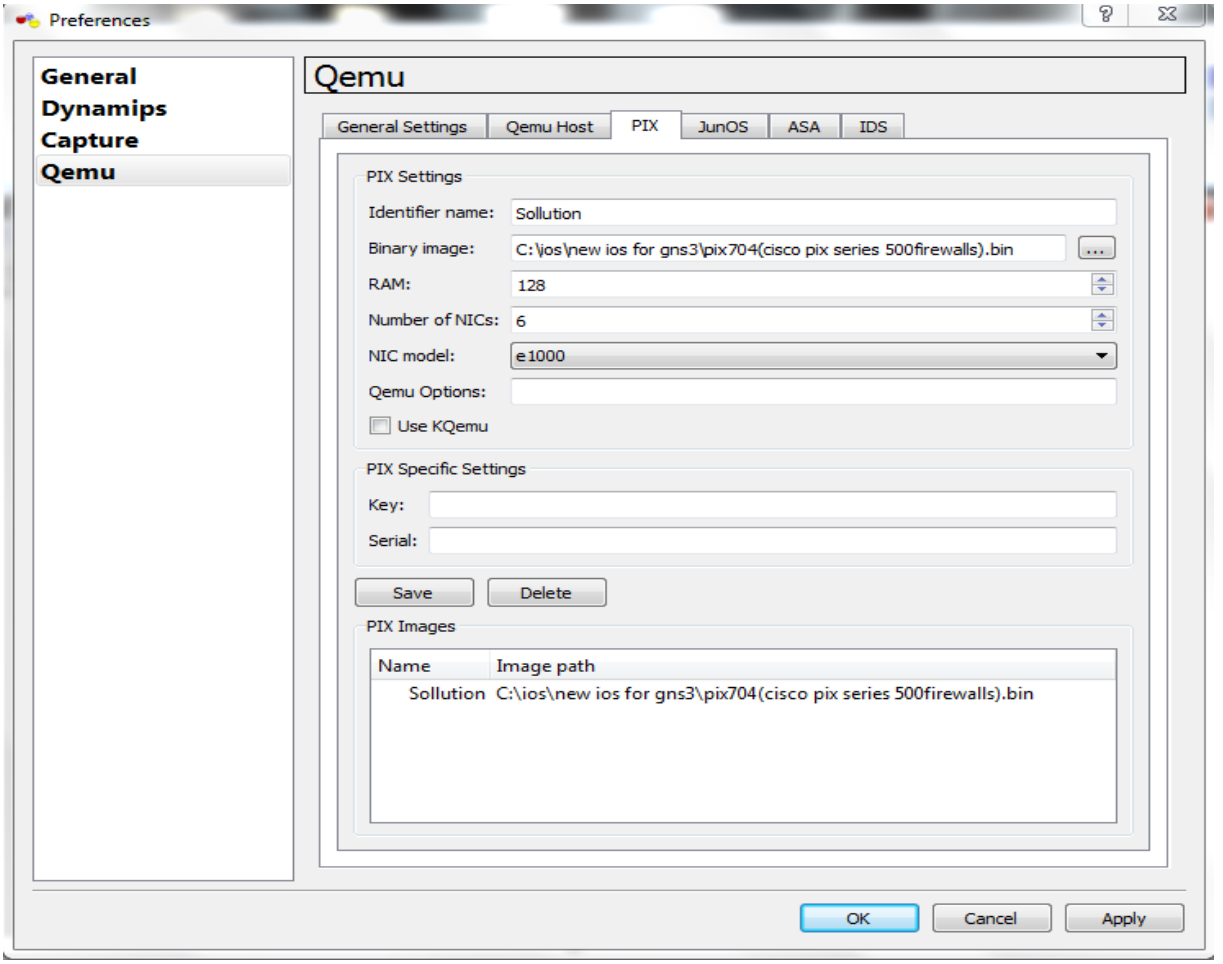


Figure IV.4. : Localisation du binaire de Qemu

IV.3.Présentation du réseau existant

Comme la figure IV.5 le montre le réseau existant contient :

- Sept SWITCHs
- Un server de base de données
- Un serveur web
- Un switch fédérateur
- Des ordinateurs (PC)
- Un modem pour une connexion au réseau internet

En effet, six SWITCHs de ce réseau sont départagés dans deux batiments et chaque batiment est composé de trois étages (donc en tout on a six étages) et il y aun SWITCH dans chaque étage de chaque batiment ,et ils désigne les unités de l'ENIEM suivantes :Unité froid ,unité climatisation ,unité cuisson, et département informatique tandisque le sptieme SWITCH appartient a l'unité préstation technique qui se trouve au sous sol du batiment .

Tout les SWITCHs des unités appartiennent à des armoires dites armoiresde brassages sauf le SWITCH de l'unité informatique qui appartienne à l'armoire d'étage où se trouve le SWITCH fédérateur auquel sont relié les six autres SWITCHs par la fibre optique.

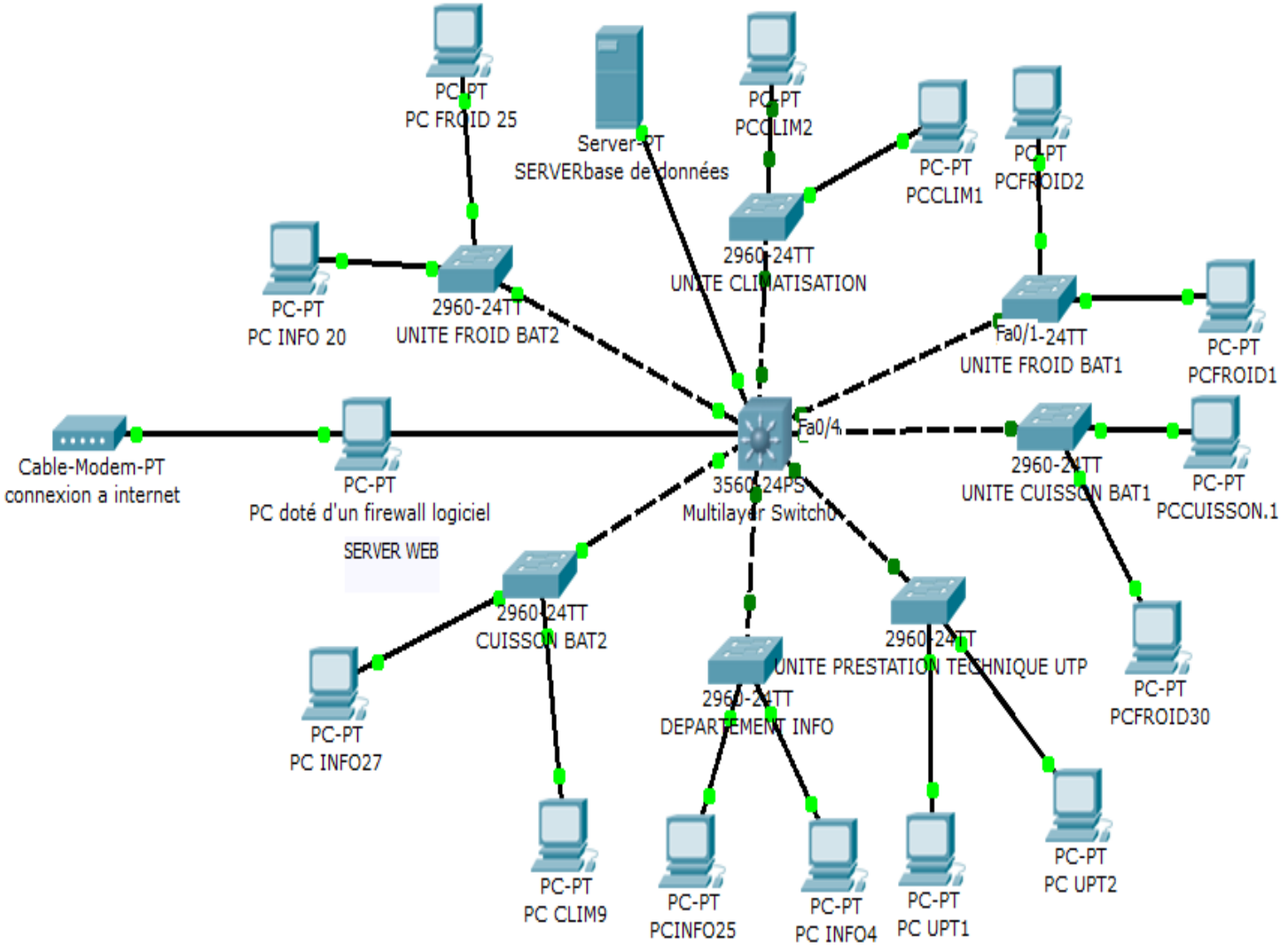


Figure.IV.5 :Présentation du réseau existant

V.2.1.Fonctionnement du réseau existant

Le fonctionnement de ce réseau est illustré dans la figureIV.2.1 :

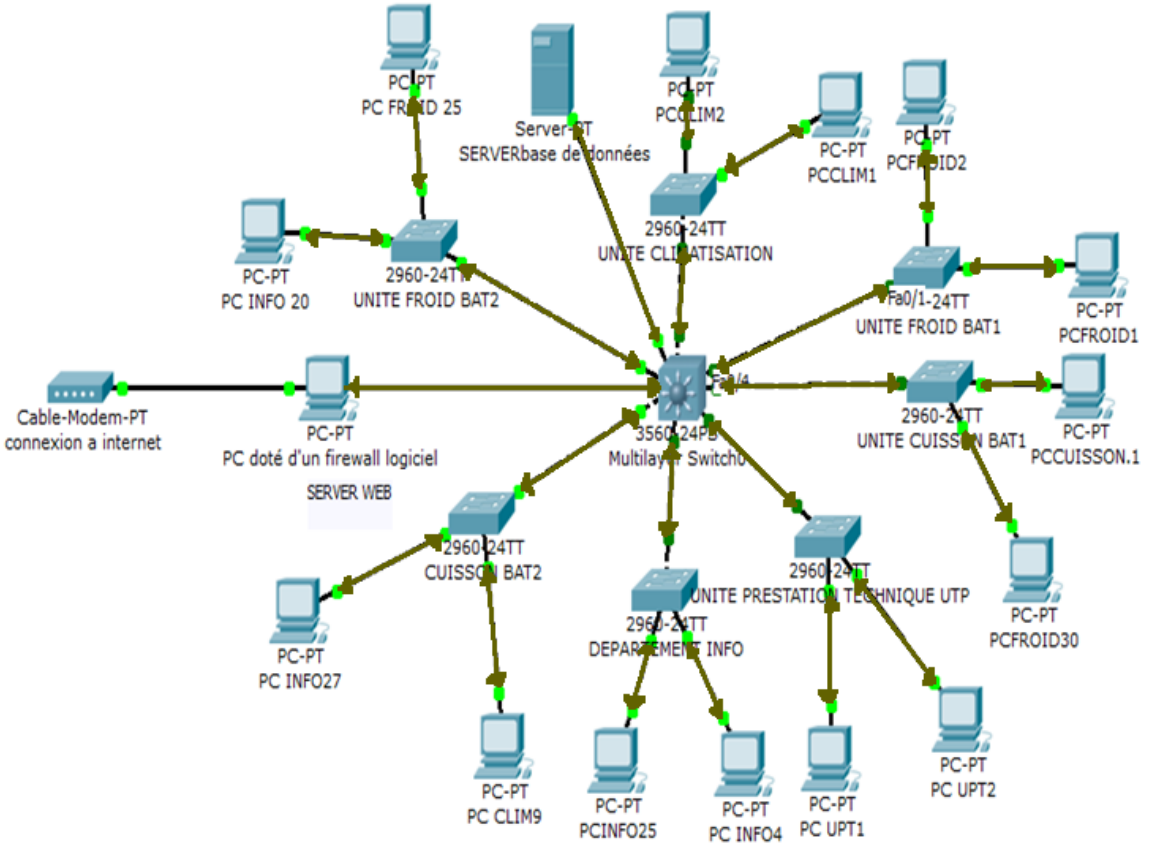


Figure IV.6 : Fonctionnement du réseau existant

- **Indications**

 : indique que l'accès est permis de chaque unité émettrice vers n'importe quelles unité destinataire (accès non limité).

Ainsi le réseau mis en œuvre dans la figure V.2.1 indique qu'un ordinateur peut émettre un trafic vers n'importe quel destinataire voulu et aussi recevoir du n'importe quelle source. donc tout les PC se connectent entre eux.

- **Explication**

La configuration de tous les équipements d'interconnexions (les SWITCHs, le fédérateur) présentés dans la figure IV.2.1 est dite : configuration basique cela veut dire que cette configuration est limité a l'utilisation d'un seul VLAN par défaut (natif) et que la configuration des switchs n'utilise que des mots de passes et une adresse IP , autrement dit tous les SWITCHs se trouvent dans un seul sous réseau et c'est ce que explique le fait que tous les SWITCHs , ainsi que tous les ordinateur connectés a leurs déférents ports peuvent se voir et se connectés entre eux .

La figure IV.2.1 nous montre aussi que dans un SWITCH d'une unité considérée on peut trouver des ordinateurs d'une autre unité qui lui y sont reliés, sachant que ces ordinateurs se trouvent tous dans un même sous réseau , par exemple l'ordinateur PCfroid.30 appartient a l'unité froid mais comme les ports de ce dernier sont tous utilisés donc il est reliés a l'un des ports libres qui se trouvent dans le switch de l'unité cuisson .

- **Remarque :**le réseau existant contient beaucoup plus d'ordinateurs que ce qu'est

présenté dans la figure IV.2.1 ;et comme on peut pas présenté tout les ordinateurs existant, on a pris un exemple de deux à trois ordinateurs pour chaque unité et cela suffit pour illustrer le fonctionnement du réseau .

IV.2.2. Les Critiques du reseau existant

Apres avoir expliqué le fonctionnement du reseau local de l'entreprise ENIEM ,nous avons arrivé à extraire les critique suivantes :

Critique1 : Les switchs du réseau sont configurables mais non configurés.

Exemple1 : Tout les switchs sont considérés comme des switchs simples .

Critique2 Le réseau est installé anarchiquement et non administré

Exemple2 : Des fonctions de différentes unités se trouvent sur le même switch et non administrés.

Critique 3 : Le réseau installé est non sécurisé contre les intrusions d'une façon fiable .

Exemple 3:La sécurité du réseau existant est basée uniquement sur l'utilisation d'un firewell logiciel .

Critique 4 : Manque d'une interconnection entre l'entreprise ENIEM et sa direction genérale.

IV.4.Solutions proposées

A l'issu d'une étude préalable de l'unité prestation technique au sein de l'entreprise nous avons opté pour l'implimentation du plans de sécurité suivants :

- Administration et ordonnancement du réseau local.
- Installation d'un routeur pour relier l'entrprise ENIEM au routeur de sa direction générale (DG), et configuration d'un processus d'encapsulation des données entre ces deux retours en utilisant le protocole « FRAME RELAY» .
- Installation et configuration d'un firewall .

L'architecture du réseau avec les solutions proposées dans ce plan de sécurité est présentéepar la figure **IV.7**.

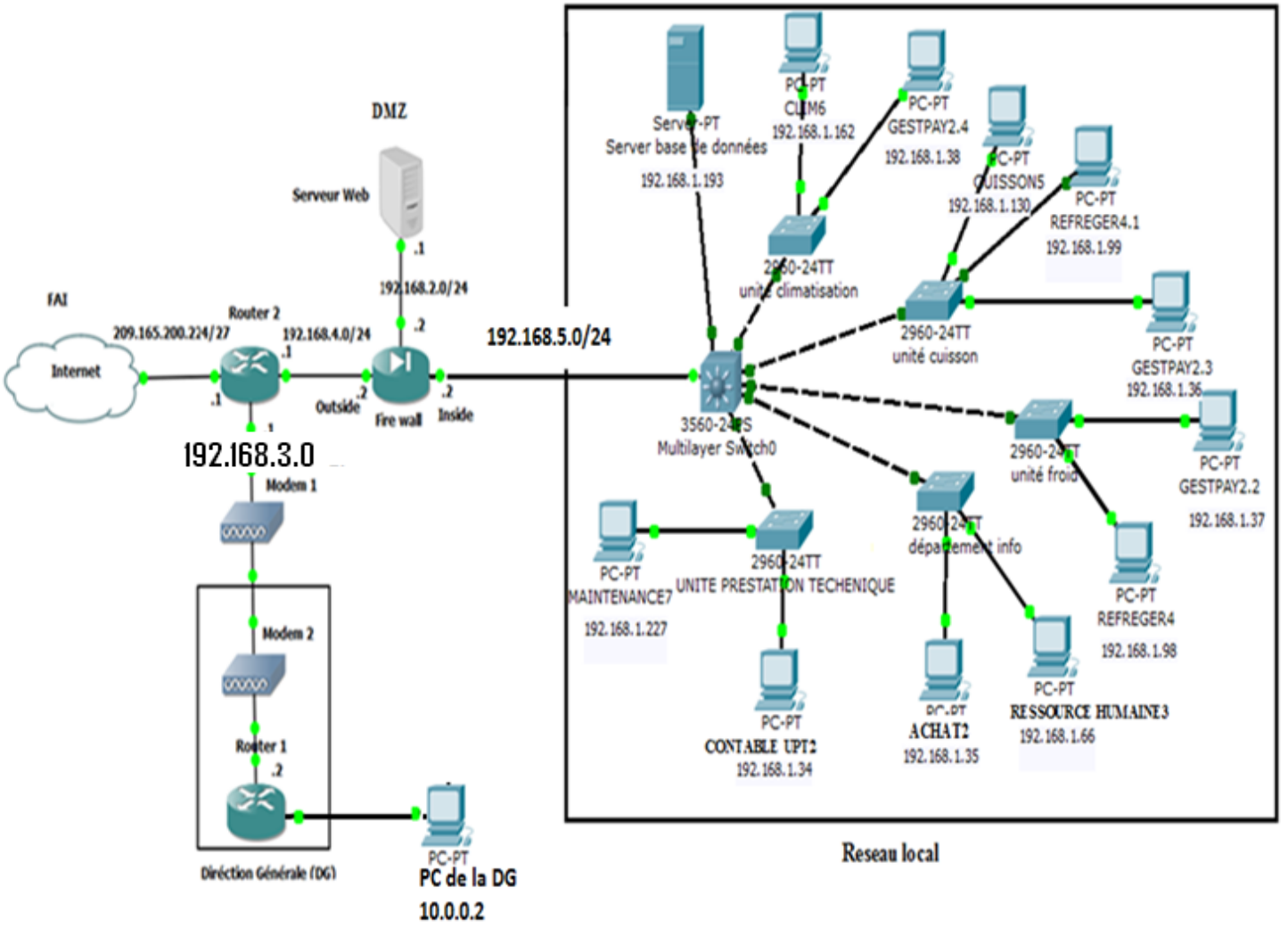


FIGURE IV.7 :architecture du réseau avec le plan de solution proposé

IV.4.Mise en œuvre du plan de sécurité proposé

La méthode suivie pour appliquer le principe de sécurité que ce plan a portéconsiste à commencer par l'administration du réseau local, ensuite la configuration de routage et le protocole Frame Relay au niveau du routeur2 et a la fin on a configuré le firewall(PIX).

IV.4.1. Administrations et organisations du réseau local

Cette solution suggère l'utilisation des sous réseaux VLANs pour chaque fonction de quelconque unité et désigner un Switch pour chaque unité et les configurés selon les besoins nécessaires(figure IV.8) . Le réseau local ainsi présenté contient : les SWITCHs des différentes unités qui sont reliés au SWITCH fédérateur ,un serveur de base de données , et quelques ordinateurs pour illustrer le résultats dus a l'application de cette solution.

- **Remarque** :dans l'architecture du réseau existant,avant d'appliquer la solution, le

serveur WEB a été inclut dans le réseau local et cela donne une occasion aux pirates d'acceder vers le réseau interne , par contre dans cette solution, le serveur web n'apparait plus dans le réseau local mais on lui a fait changer de place vers une zone isolée dite zone délimitarisée afin d'atteindre un pourcentage de sécurité maximum.

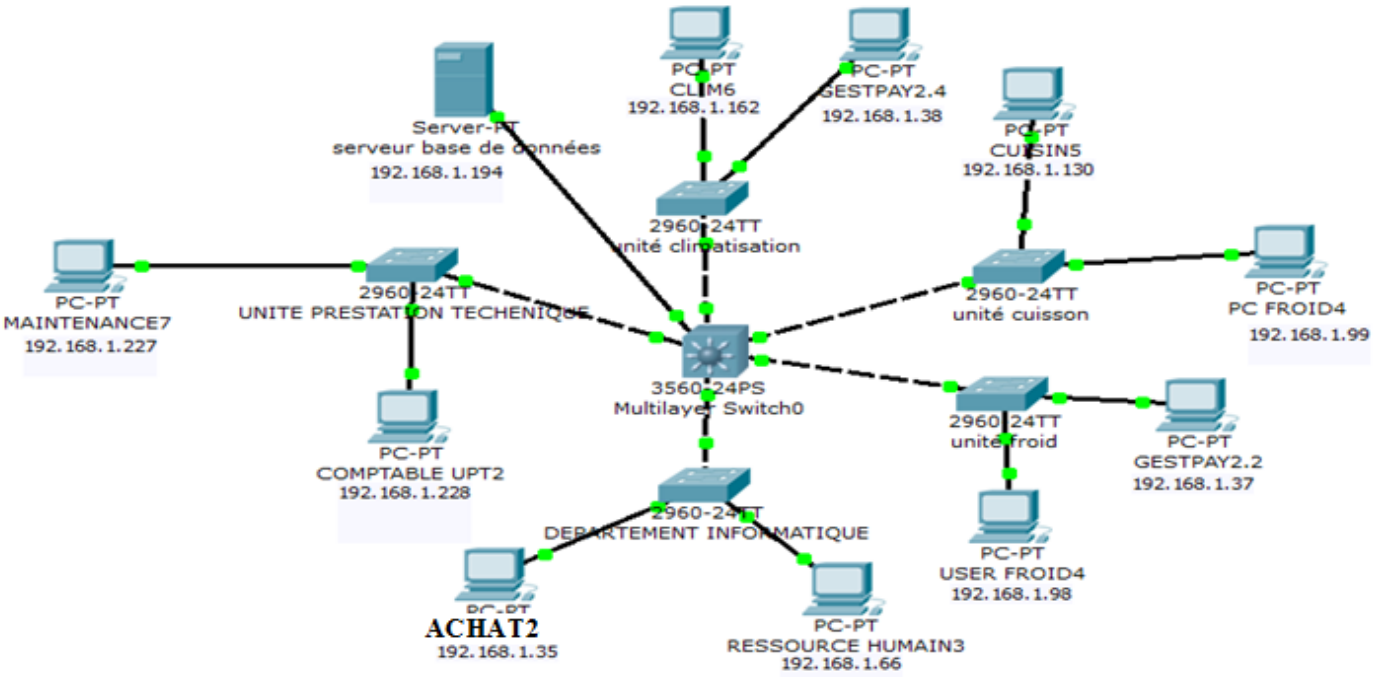


Figure IV.8 : réseau local avec la solution proposée

1V.4.1.1.Explication des étapes de la mise en œuvre de la solution

Les étapes de la procédure suivit pour appliquer la solution proposée sont les suivantes :

1V.4.1.1.1.Etape N°1 : proposition d'un plan d'adressage

Pour notre architecture on a opté pour le plan d'adressage suivant :

- **Switch federateur :**

Interfaces	Adresse IP	Masque de sous réseau
VLAN 1	192.168.1.2	255.255.255.224
VLAN 2	192.168.1.33	255.255.255.224
VLAN 3	192.168.1.65	255.255.255.224
VLAN 4	192.168.1.97	255.255.255.224
VLAN 5	192.168.1.129	255.255.255.224
VLAN 6	192.168.1.161	255.255.255.224

VLAN 7	192.168.1.225	255.255.255.224
VLAN 8	192.168.1.192	255.255.255.224

- **Unité préstation techenique**

Périphériques	Interface	Adresse IP	Masque de sous réseau	Passerelle par défaut
Switch	Vlan 1	192.168.1.1	255.255.255.224	/
PC prestation technique 7	Carte réseau	192.168.1.227	255.255.255.224	192.168.1.225 (VLAN 7)
PCComptable upt7	Carte réseau	192.168.1.34	255.255.255.224	192.168.1.228 (VLAN 7)

- **Departement informatique**

Périphériques	interface	Adresse IP	Masque de sous réseau	Passerelle par défaut
Switch	VLAN 1	192.168.1.3	255.255.255.224	/
PC gestion de payement 2.1	Carte réseau	192.168.1.35	255.255.255.224	192.168.1.33 (VLAN 2)
PC ressource humaine 3	Carte réseau	192.168.1.66	255.255.255.224	192.168.1.65 (VLAN 3)

- **Unité froid**

Périphériques	Interface	Adresse IP	Masque de sous réseau	Passerelle par défaut
Switch	Vlan 1	192.168.1.5	255.255.255.224	/
PC gestion de payement 2.2	Carte réseau	192.168.1.37	255.255.255.224	192.168.1.33 (VLAN 2)
PC USER FROID4	Carte réseau	192.168.1.98	255.255.255.224	192.168.1.97 (VLAN 4)

- **Unité cuisson**

Périphériques	Interface	Adresse IP	Masque de sous	Passerelle par

			réseau	défaut
Switch	VLAN 1	192.168.1.6	255.255.255.224	/
PC FROID4	Carte réseau	192.168.1.36	255.255.255.224	192.168.1.66 (VLAN 4)
PC CUISIN5	Carte réseau	192.168.1.130	255.255.255.224	192.168.1.129 (VLAN 5)

- **Unité climatisation**

Périphériques	Interface	Adresse IP	Masque de sous réseau	Passerelle par défaut
Switch	VLAN 1	192.168.1.7	255.255.255.224	/
PC gestion de payement 2.4	Carte réseau	192.168.1.38	255.255.255.224	192.168.1.33 (VLAN 2)
PC climatise-ur 6	Carte réseau	192.168.1.162	255.255.255.224	192.168.1.161 (VLAN 6)

1V.4.1.1.2.Etape N°2 : désigner chaque unité par un switch

1V.4.1.1.3.Etape N°3 : créer les VLAN suivant :

VLAN 2, VLAN3, VLAN4, VLAN5, VLAN6, VLAN7 et VLAN8.

- VLAN2 : est le sous réseau pour la gestion de payement de chaque unité.
- VLAN3 : est le sous réseau pour designer le « departement informatique » .
- VLAN4 : est le sous réseau pour designer « l'unité froid»
- VLAN5 : est le sous réseau pour designer « l'unité cuisson »
- VLAN6 : est le sous réseau pour « l'unité climatisation »
- VLAN7 : est le sous réseau pour designer « l'unité préstation technique »
- VLAN8 : pour désigner le sous réseau au quel appartient le serveur base de données

IV.4.1.1.4.Étape N°4 : affecter les VLANs crées aux déférentes interfaces des SWITCHs aux quelles sont connectées les ordinateurs.

IV.4.1.1.5.Etapes N°5 : créer 03 listes de contrôle d'accès (ACL) pour spécifier les ordinateurs ou bien les sous réseaux qui doivent se contactés entre eux et les autres qui ne le doivent pas .Les exemples qu'on a pris pour l'application de ces listes de contrôle d'accés sont :

- ACL 1 : Bloquer l'accés Au « PC ressource humaine » du departement informatique d'accéder vers le « «PC conmtable UPT2» du l'unité prestation technique
- ACL 2 :permettre l'accés vers tout les unités du réseau pour « PCMAINTENANCE7» du l'unité prestation technique et cetteapplication est envisageable pour la maintenance des ordinateurs a distance sans se déplacer .
- ACL 3 :bloquer l'accès au « PCUSER4 »du l'unité froid vers le serveur base de données et permmettre l'accès pout tout les autres ordinateurs.

la configuration de ces étapes est données comme suit :

- **Configuration de switch fédérateur**

Switch>enable //*pour le passage en mode privilégié*//

Switch#configure terminal //*pour le passage en mode de configuration globale*//

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

Switch (config)#hostname fédérateur //*pour définir le nom du switch fédérateur *//

federateur (config)#interface vlan 1 //*pour le passage en mode de configuration de l' interface VLAN 1*//

federateur(config-if)#IP Address 192.168.1.2 255.255.255.224

federateur(config-if)#no shutdown //*pour activer l'interface*//

%LINK-5-CHANGED: Interface Vlan1, changed state to up

federateur(config-if)#exit //*pour quiter le mode actuel*//

federateur(config)#vtp mode server //*définir le federateur comme serveur VTP*//

Device mode already VTP SERVER.

federateur(config)#vtp domain ENIEM.fr

Changing VTP domain name from NULL to ENIEM.fr

federateur(config)#vtp version 2

federateur(config)#vlan 2 //*pour créer le VLAN 2*//

federateur(config-vlan)#name GESTIONDEPAYEMENT //*donner un nom au VLAN crée *//

federateur(config-vlan)#exit

federateur (config)#interface vlan 2 //*pour le passage en mode de configuration de l' interface VLAN 2*//

federateur(config-if)#IP Address 192.168.1.33 255.255.255.224

federateur(config-if)#no shutdown //*pour activer l'interface*//

%LINK-5-CHANGED: Interface Vlan1, changed state to up

federateur(config-if)#exit //*pour quiter le mode actuel*//

//*REMARQUE :il faut suivre juste ces memes derniéres 7lignes de configuration pour les autres VLANs *//.

federateur(config)#access list 101deny icmp host 192.168.1.66 host 192.168.1.228 //*pour creer l'ACL1*//

federateur(config)#access list 101 permit HOST 192.168.1.66 any

federateur(config)#interface vlan 3 //*pour associer l'ACL crée a l'interface VLAN3*//

federateur(config-if)#ip access-group 101 out

federateur(config-if)#exit

federateur(config)#access-list 102 permit icmp host 192.168.1.227 any //*pour creer l'ACL2 *//

federateur(config)#INTerface VLan 8

federateur(config-if)#IP ACcess-group 103 out

federateur(config-if)#exit

federateur(config)#ACcess-list 103 deny icmp host 192.168.1.98 HOST 192.168.1.194 //*pour creer l'ACL3 *//

federateur(config)#access list 103 permit HOST 192.168.1.98 any

federateur(config)#INTerface VLAN 4

federateur(config-if)#IP ACcess-group 101 OUT

federateur(config-if)#exit

- **Switch unité prestation techenique**

Switch>enable

Switch#configure terminal

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

Switch(config)#hostname UNITEPRESTATION

UNITEPRESTATION(config)#vtp mode client

Setting device to VTP CLIENT mode.

UNITEPRESTATION (config)#interface VLAN 1

UNITEPRESTATION (config-if)#ip address 192.168.1.1 255.255.255.224

UNITEPRESTATION (config-if)#no shutdown

UNITEINFORMATIQUE(config-if)#exit

UNITEPRESTATION (config)#interface fastEthernet 0/1

UNITEPRESTATION(config-if)#SWitchport Mode Trunk

UNITEPRESTATION (config-if)#NO SHutdown

UNITEPRESTATION (config-if)#exit

UNITEPRESTATION(config)#INTerface FastEthernet 0/2

UNITEPRESTATION(config-if)#switchport mode access //*pour mettre cette interface en mode accée*//

UNITEPRESTATION(config-if)#switchport access vlan 7 //*affecter le Vlan7 a l'interface*//

UNITEPRESTATION(config-if)#no shutdown

UNITEPRESTATION(config-if)#exit

UNITEPRESTATION(config)#INTerface FastEthernet 0/3

UNITEPRESTATION(config-if)#switchport mode access

UNITEPRESTATION(config-if)#switchport access vlan 2

UNITEPRESTATION(config-if)#no shutdown

UNITEPRESTATION(config-if)#exit

- **Switch unité climatisation**

Switch>enable

Switch#configure terminal

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

Switch(config)#hostname UNITEICLIMATISATION

UNITEICLIMATISATION (config)#vtp mode client

Setting device to VTP CLIENT mode.

UNITEICLIMATISATION (config)#interface VLAN 1

UNITEICLIMATISATION config-if)#ip address 192.168.1.7 255.255.255.224

UNITEICLIMATISATION (config-if)#no shutdown

UNITEICLIMATISATION (config-if)#exit

UNITEICLIMATISATION (config)#interface fastEthernet 0/1

UNITEICLIMATISATION (config-if)#SWitchport Mode Trunk

UNITEICLIMATISATION (config-if)#NO SHutdown

UNITEICLIMATISATION (config-if)#exit

UNITEICLIMATISATION (config)#INTerface FastEthernet 0/2

UNITEICLIMATISATION (config-if)#switchport mode access

UNITEICLIMATISATION (config-if)#switchport access vlan 6

UNITEICLIMATISATION (config-if)#no shutdown

UNITEICLIMATISATION (config-if)#exit

UNITEICLIMATISATION (config)#INTerface FastEthernet 0/3

UNITEICLIMATISATION (config-if)#switchport mode access

UNITEICLIMATISATION (config-if)#switchport access vlan 2

UNITEICLIMATISATION (config-if)#no shutdown

UNITEICLIMATISATION (config-if)#exit

- **Switch unité froid**

Switch>enable

Switch#configure terminal

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

Switch(config)#hostname UNITEFROID

UNITEFROID (config)#vtp mode client

Setting device to VTP CLIENT mode.

UNITEFROID (config)#interface VLAN 1

UNITEFROID (config-if)#ip address 192.168.1.5 255.255.255.224

UNITEFROID (config-if)#no shutdown

UNITEFROID (config-if)#exit

UNITEFROID (config)#interface fastEthernet 0/1

UNITEFROID (config-if)#SWitchport Mode Trunk

UNITEFROID (config-if)#NO SHutdown

UNITEICLIMATISATION (config-if)#exit

UNITEFROID (config)#INTerface FastEthernet 0/2

UNITEFROID (config-if)#switchport mode access

UNITEFROID (config-if)#switchport access vlan 4

UNITEFROID (config-if)#no shutdown

UNITEFROID (config-if)#exit

UNITEFROID (config)#INTerface FastEthernet 0/3

UNITEFROID (config-if)#switchport mode access

UNITEFROID (config-if)#switchport access vlan 2

UNITEFROID (config-if)#no shutdown

UNITEFROID (config-if)#exit

- **Switch unité cuisson**

Switch>enable

Switch#configure terminal

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

Switch(config)#hostname UNITECUISSON

UNITECUISSON (config)#vtp mode client

Setting device to VTP CLIENT mode.

UNITECUISSON (config)#interface VLAN 1

UNITECUISSON (config-if)#ip address 192.168.1.6 255.255.255.224

UNITECUISSON (config-if)#no shutdown

UNITECUISSON (config-if)#exit

UNITECUISSON (config)#interface fastEthernet 0/1

UNITECUISSON (config-if)#SWitchport Mode Trunk

UNITECUISSON (config-if)#NO SHutdown

UNITECUISSON (config-if)#exit

UNITECUISSON (config)#INTerface FastEthernet 0/2

UNITECUISSON (config-if)#switchport mode access

UNITECUISSON (config-if)#switchport access vlan 5

UNITECUISSON (config-if)#no shutdown

UNITECUISSON (config-if)#exit

UNITECUISSON (config)#INTerface FastEthernet 0/7

UNITECUISSON (config-if)#switchport mode access

UNITECUISSON (config-if)#switchport access vlan 2

UNITECUISSON (config-if)#no shutdown

UNITECUISSON (config-if)#exit

- **Switch unité departement informatique**

Switch>enable

Switch#configure terminal

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

Switch(config)#hostname UNITEDEPARTEMENTINFO

UNITEDEPARTEMENTINFO (config)#vtp mode client

Setting device to VTP CLIENT mode.

UNITEDEPARTEMENTINFO (config)#interface VLAN 1

UNITEDEPARTEMENTINFO(config-if)#ip address 192.168.1.3 255.255.255.224

UNITEDEPARTEMENTINFO (config-if)#no shutdown

UNITEDEPARTEMENTINFO (config-if)#exit

UNITEDEPARTEMENTINFO (config)#interface fastEthernet 0/1

UNITEDEPARTEMENTINFO (config-if)#SWitchport Mode Trunk

UNITEDEPARTEMENTINFO (config-if)#NO SHutdown

UNITEDEPARTEMENTINFO (config-if)#exit

UNITECOMMERCIALE (config)#INTerface FastEthernet 0/2

UNITECOMMERCIALE (config-if)#switchport mode access

UNITEDEPARTEMENTINFO (config-if)#switchport access vlan 2

UNITEDEPARTEMENTINFO (config-if)#no shutdown

UNITEDEPARTEMENTINFO (config-if)#exit

UNITEDEPARTEMENTINFO (config)#INTerface FastEthernet 0/3

UNITEDEPARTEMENTINFO (config-if)#switchport mode access

UNITEDEPARTEMENTINFO (config-if)#switchport access vlan 3

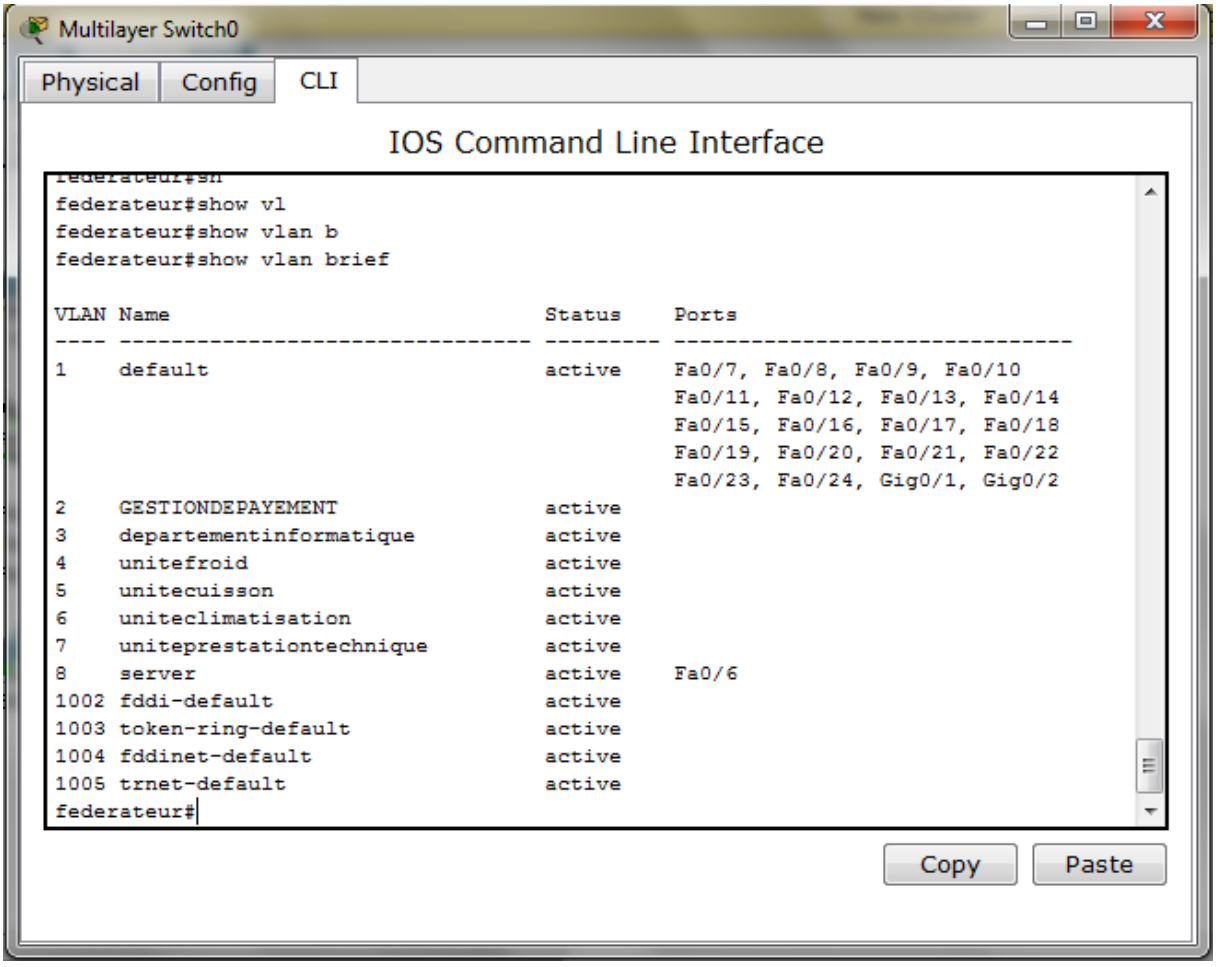
UNITEDEPARTEMENTINFO (config-if)#no shutdown

UNITEDEPARTEMENTINFO (config-if)#exit

1V.4.1.1.6.Etape N°6 : verification de la configuration

- Vérification de la creation des VLANs

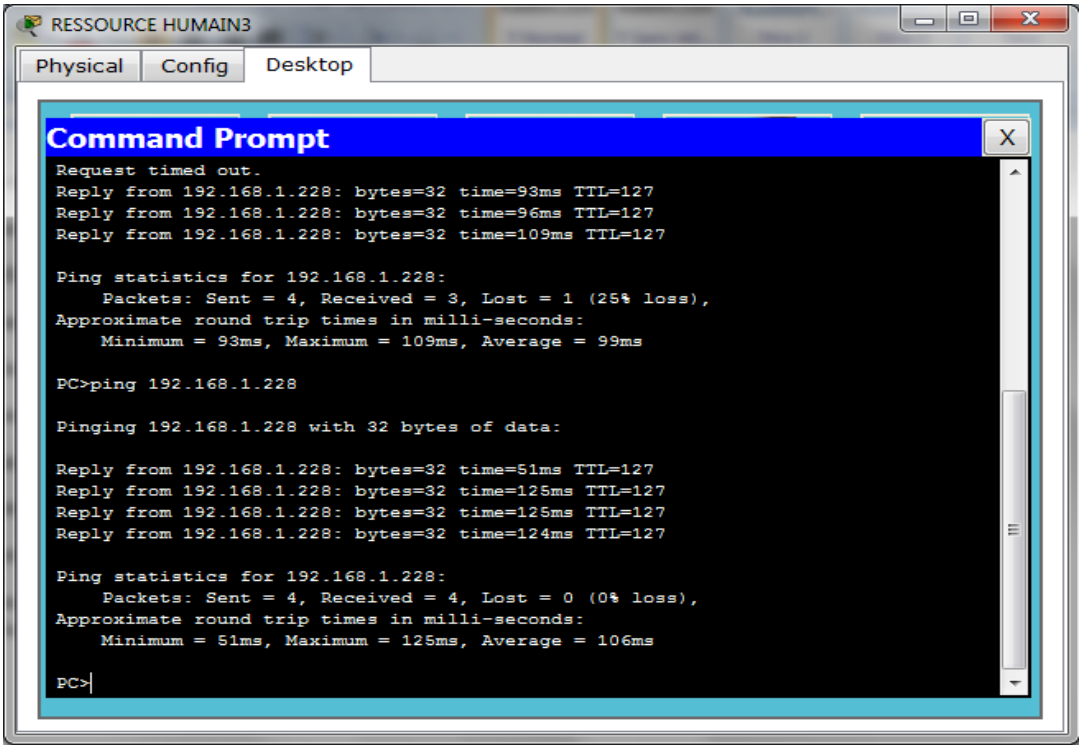
Pour vérifier la creation des VLANs on utilise la commande # show VLAn brief # en mode priviligié comme c'est ilustré dans la figure IV.9.A.



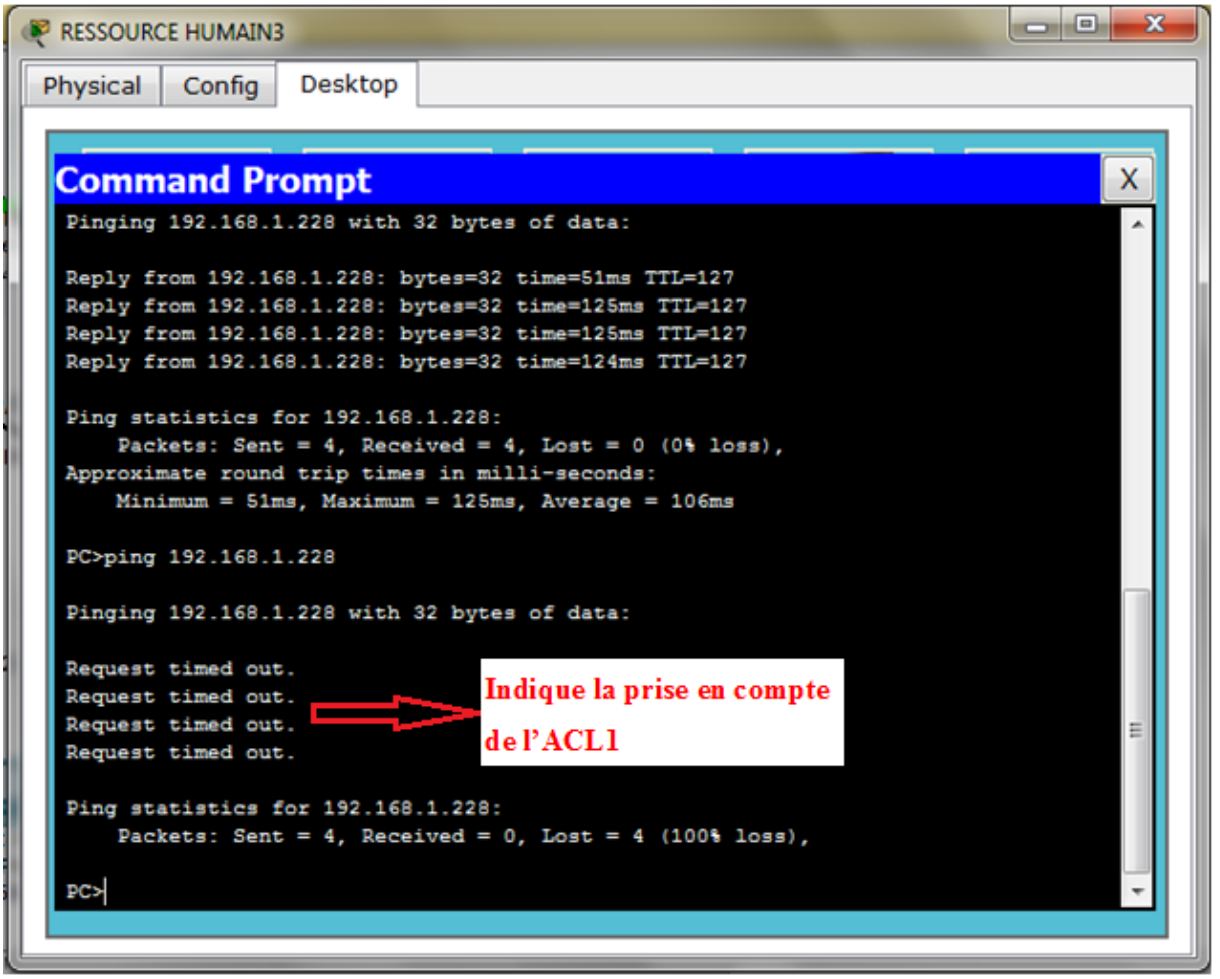
FigureIV.9 :Verification de creation des VLANs

- **Vérification des listes de contrôle d'accès**

Les figures IV.10 et IV.11 représentent les résultats obtenus lors d'un ping avant et après la creation de la premiere liste de control d'accés :



FigureIV.10 : Test avant la creation de l'CL1



FigureIV.11 : Test aprés la creation de l'ACL1

Les figures IV.12et IV.13 représentent les résultats obtenus lors d'un ping avant et après l'ACL2

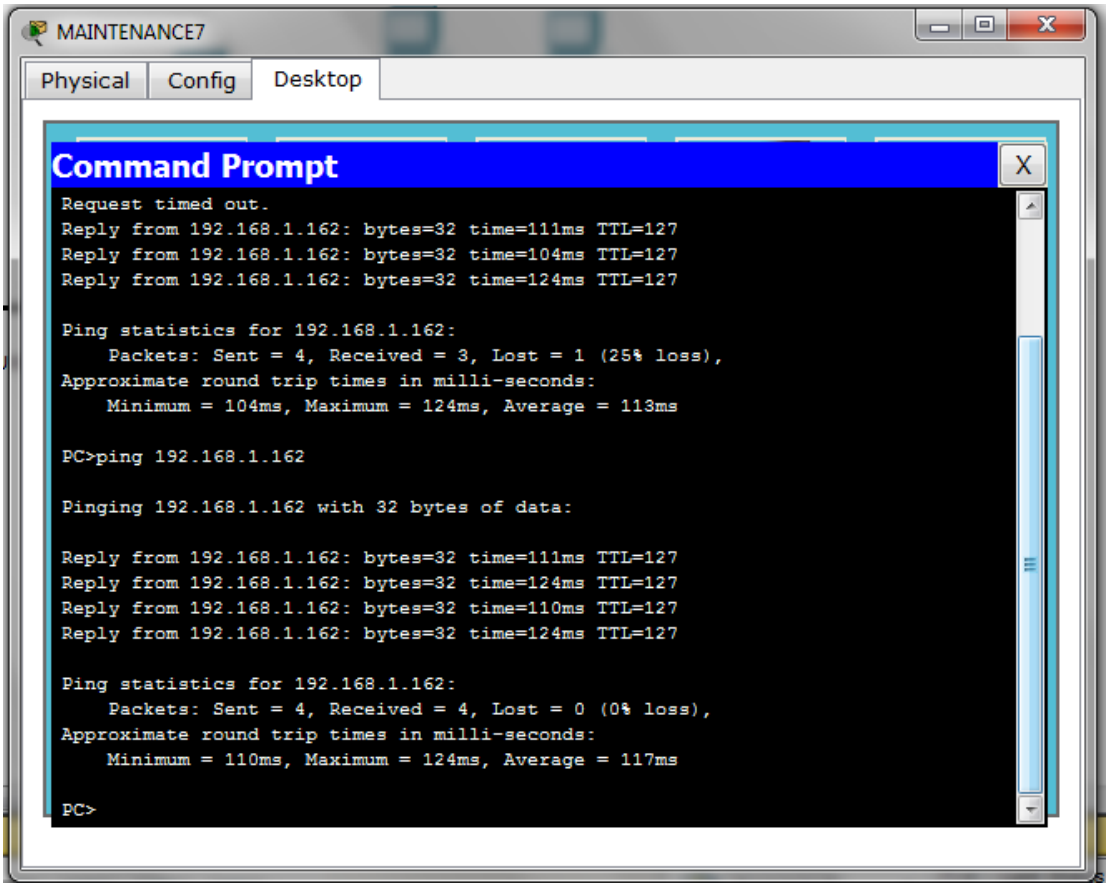


Figure IV.12 : Test avant la creation de l'ACL2

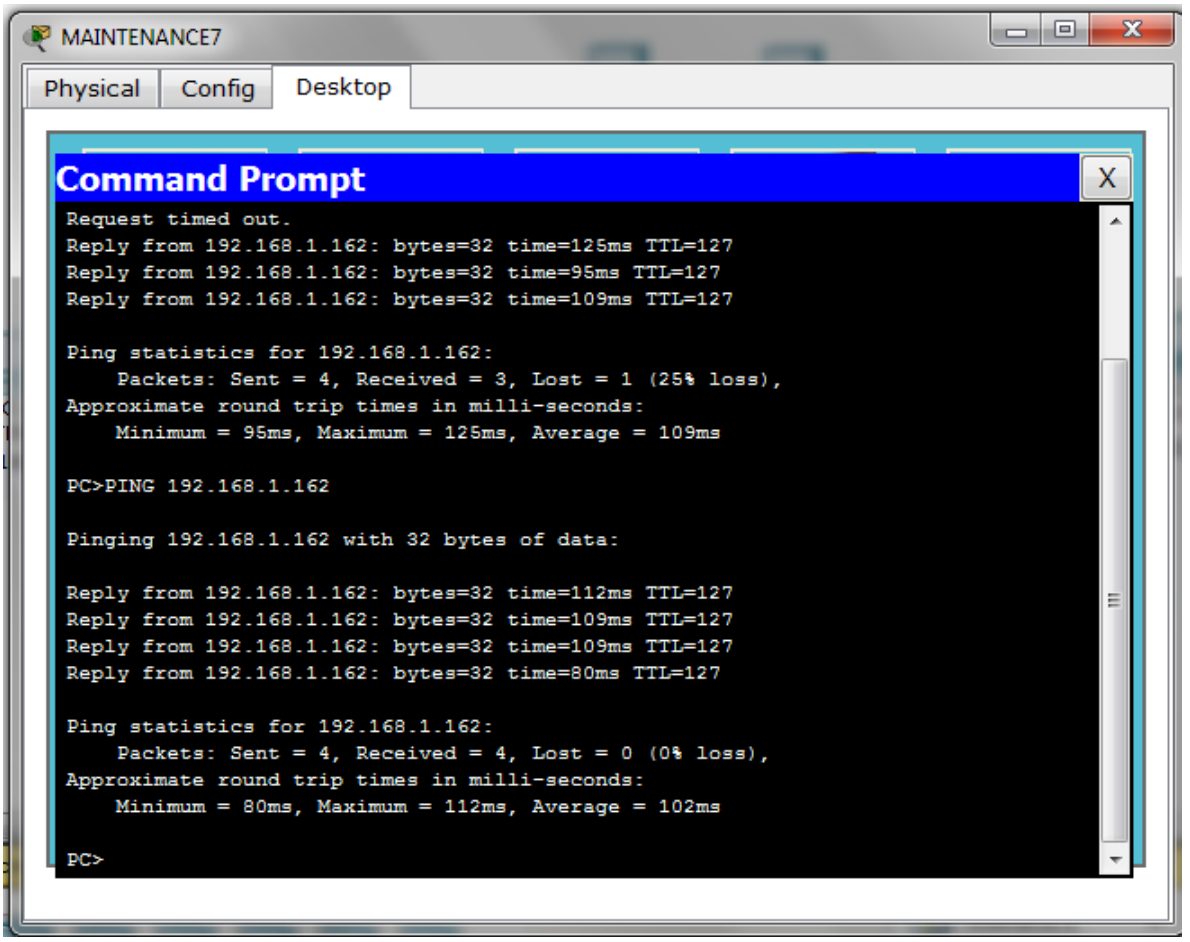
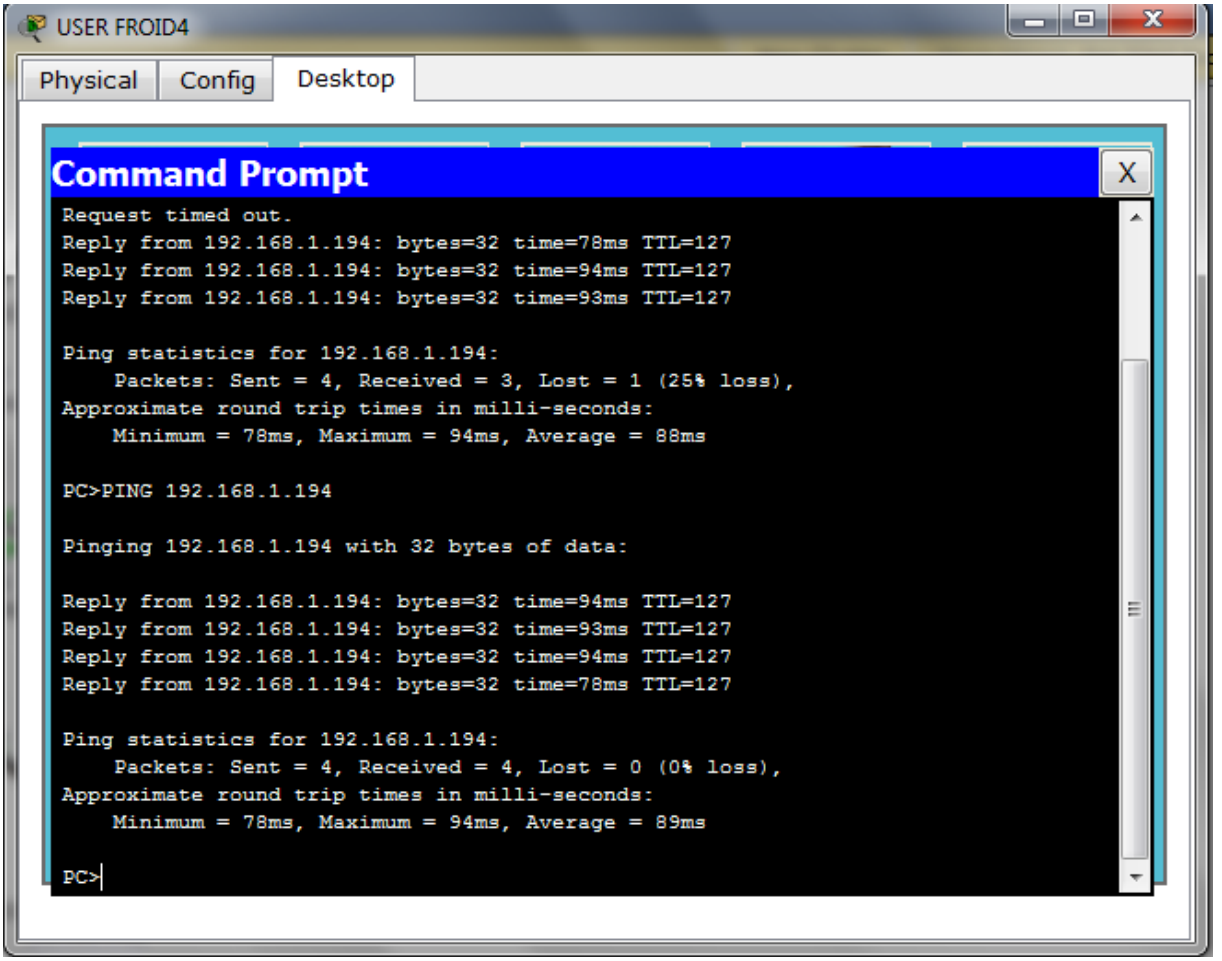


Figure IV.13 : Test aprés la creation de l'ACL2

Les **Figure IV.14 /15** vérifient l'etat de marche lors d'un ping de l'ACL3 crée :



FigureIV.14 : Test avant la creation de l'ACL3

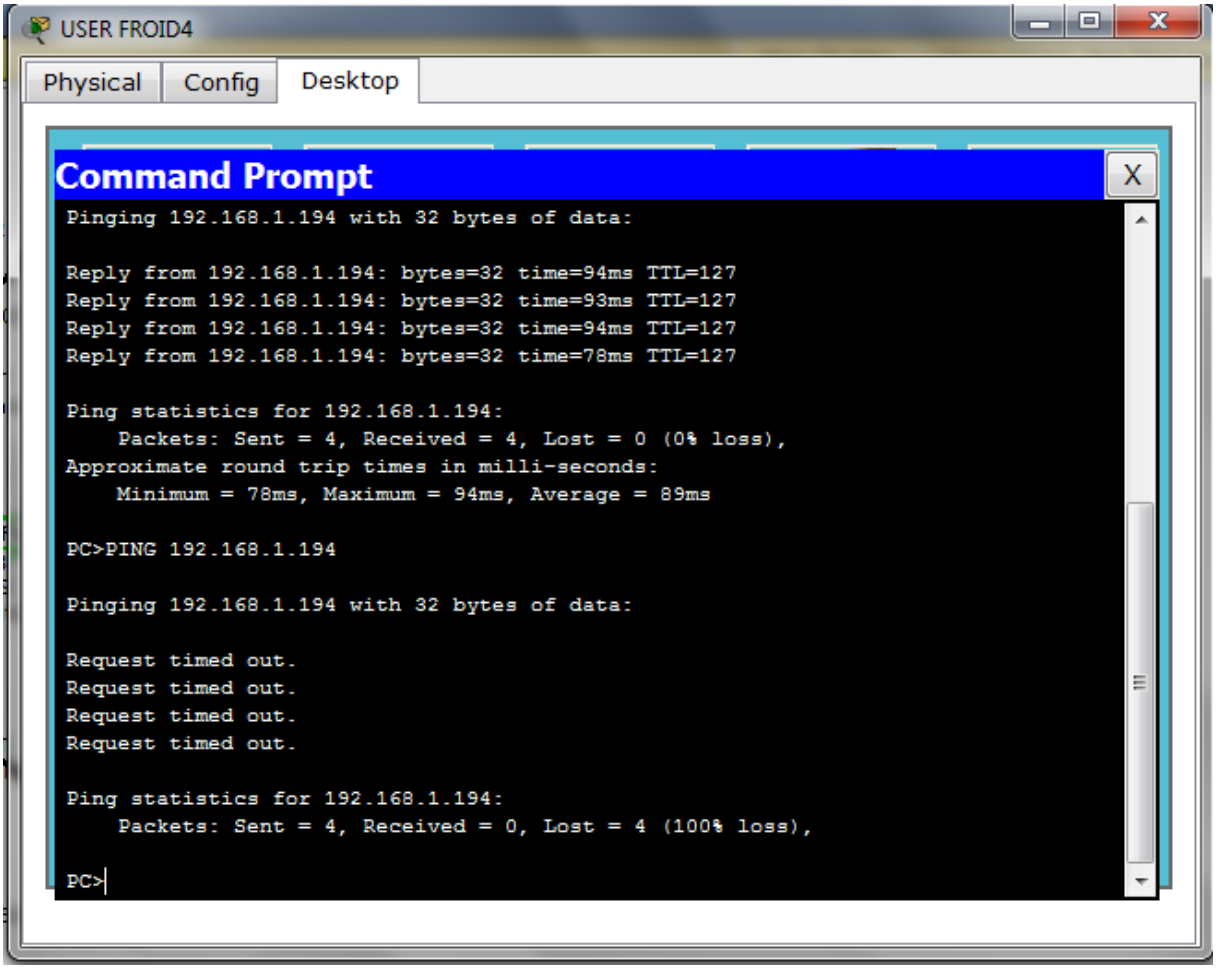


Figure IV.15 : Test aprés la creation de l'ACL3

IV.5.1. La configuration du routeur de l'entreprise

Ce routeur comme c'est indiqué dans la figure IV.4 est nomé « routeur2 ».

Comme le simulateur « GNS3 » demande un PC plus performant que ce qu'est mis a notre disposition pour arriver a configurer l'étape du routage et du protocole Frame Relay entre le retour de la DG , le routeur de FAI et le firewall, pour cela, on a donné l'exemple présenté par la figureIV.16 pour montrer comment configurer le routage dynamique et aussi pour vérifier cette configuration.

IV.5.1.1. La configuration du routage dynamique

Pour activer le routage entre les 03 réseaux connéctés au routeur de l'entreprise ona utlisé le protocole de routage « OSPF» et sa configuration et donnée par la figure suivante :

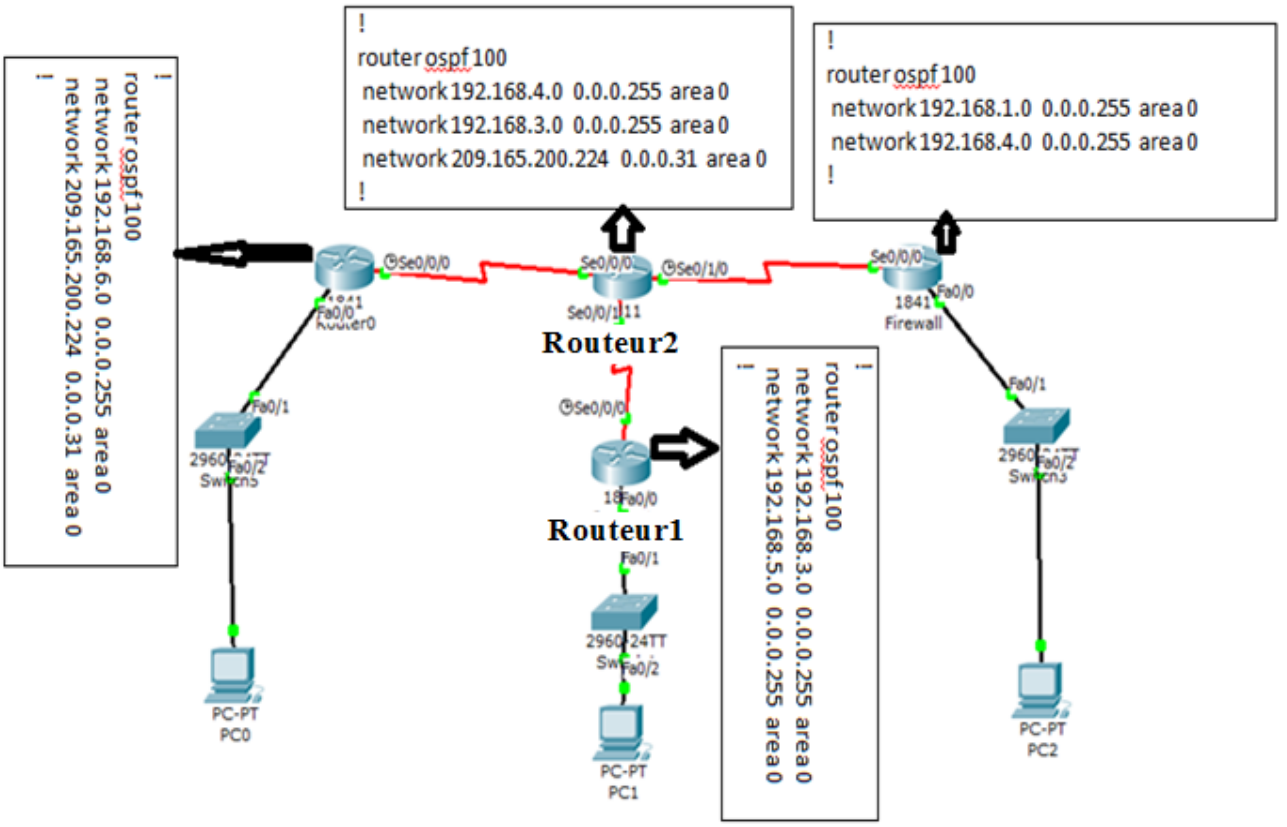


Figure IV.16 : Configuration du routage dynamique

- **Verification de la configuration du routage dynamique**

L'indication « Destination host unreachable » dans la figureIV.17nous montre que le Ping entre le PC2 et le PC1(voir figure IV.16) avant la configuration du protocole de routage a été echoué.Par contre la figure IV.18 montre que le Ping ,après avoir configuré le protocole de routage « OSPF »,entre ces deux ordinateurs a été fait avec succès.

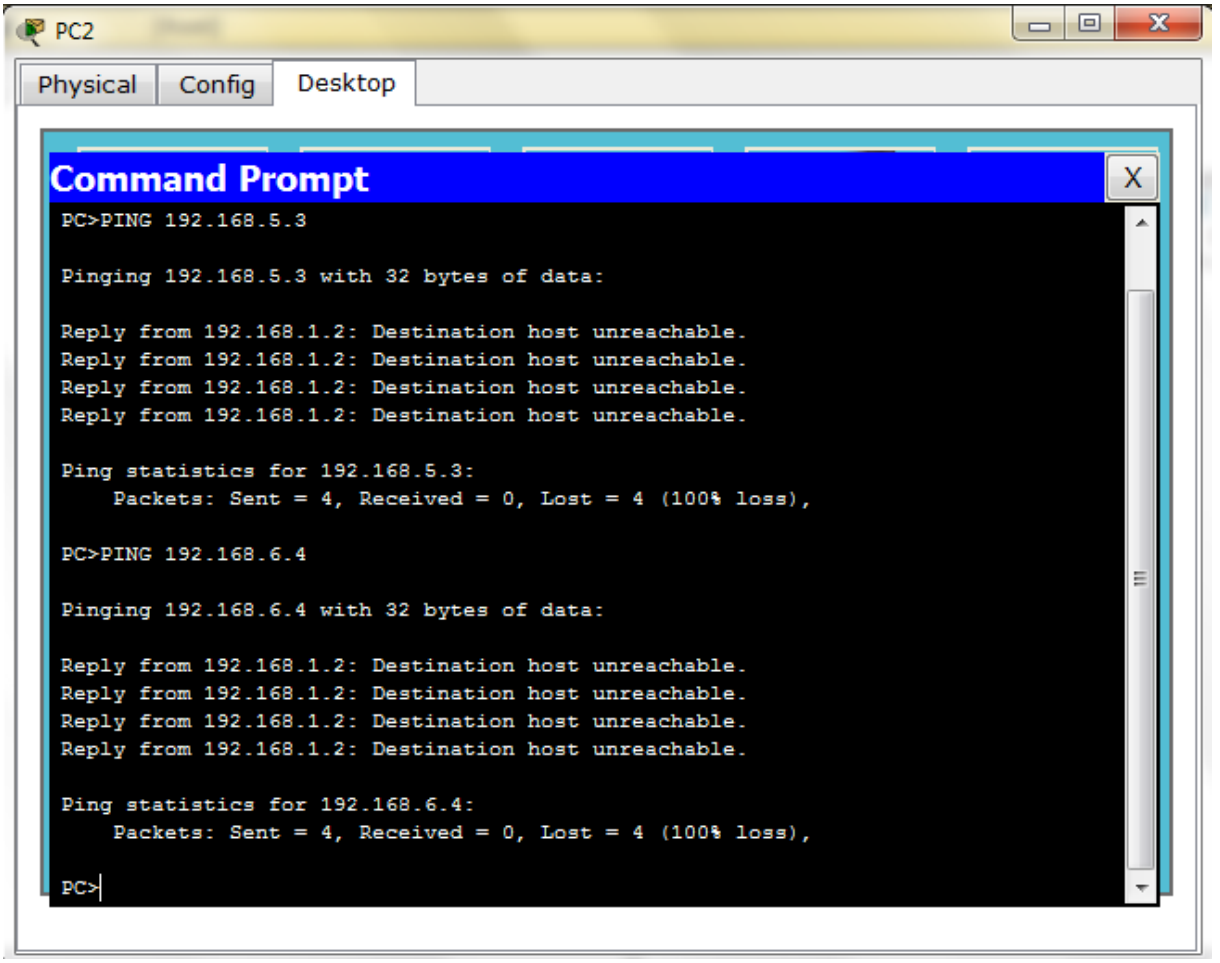


Figure IV.17 : resultat du pingavant la configuration de L'OSPF

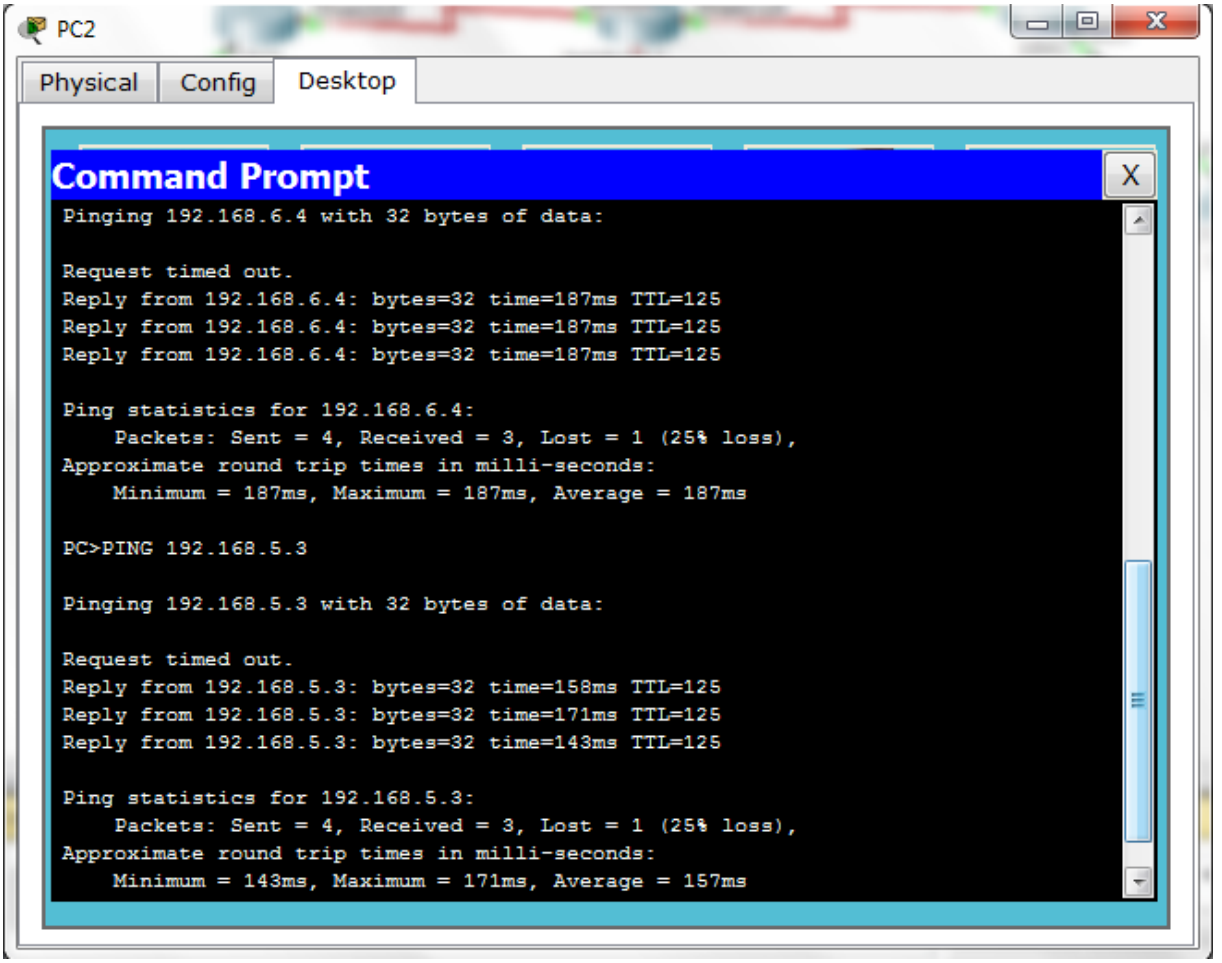


Figure IV.18 :le resultat du ping après la configuration de l'OSPF

IV.5.1.2. La configuration du Frame Relay entre routeur1 et routeur2

La figureIV.19illustre une ligne telephonique permettant de connecter le réseau de l'entreprise ENIEM qui se trouve au sein de la zone industrielle AISSAT - IDIR OUED - AISSI aux réseaux de sa direction générale qui se trouve au Chef-lieu de TIZI - OUZOU à proximité de la gare ferroviaire,et pour l'encapsulation des données on a utilisé le protocole Frame Relay.

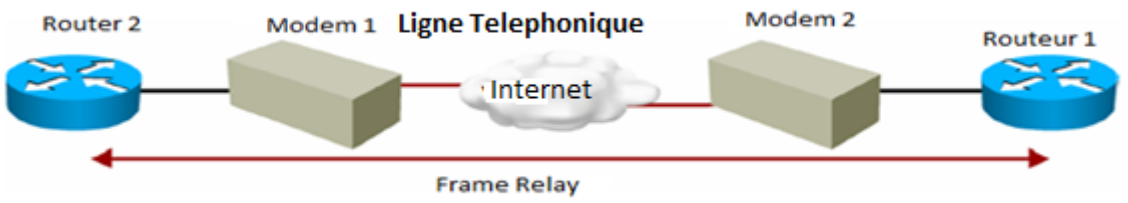


Figure IV.19 :La liaison entre l'entreprise ENIEM et sa direction générale

La figure IV.20 représente la configuration du frame Relay

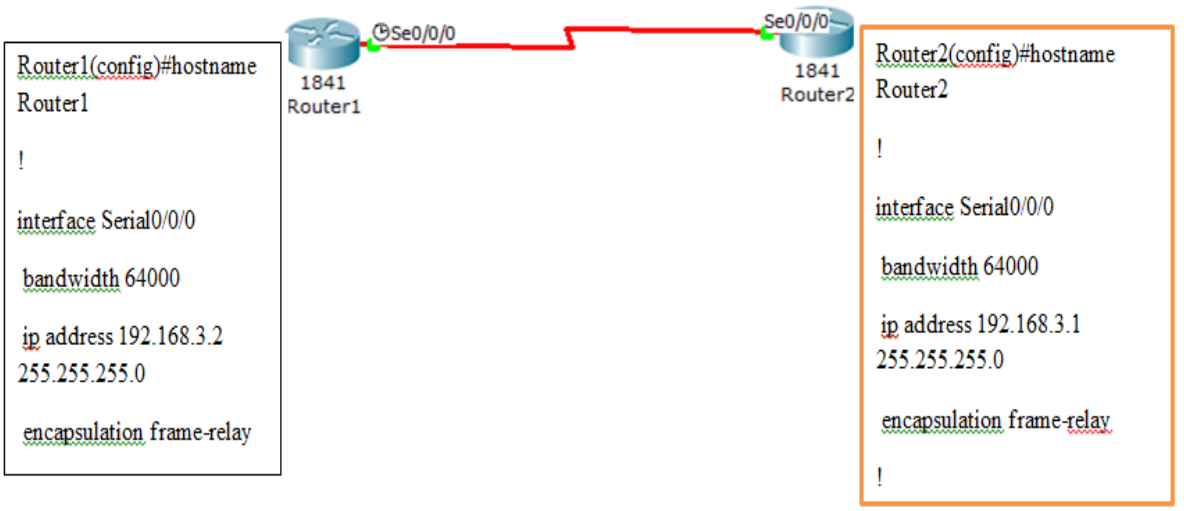
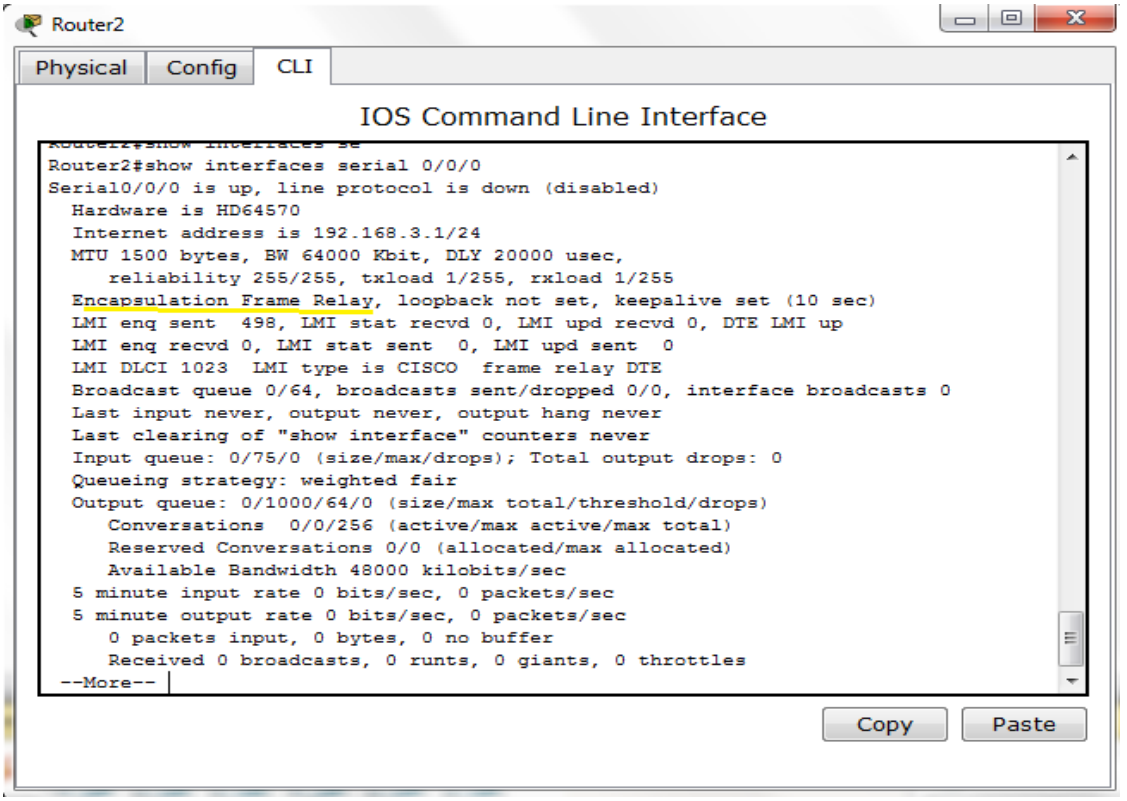


Figure IV.20 :Configuration du frame Relay

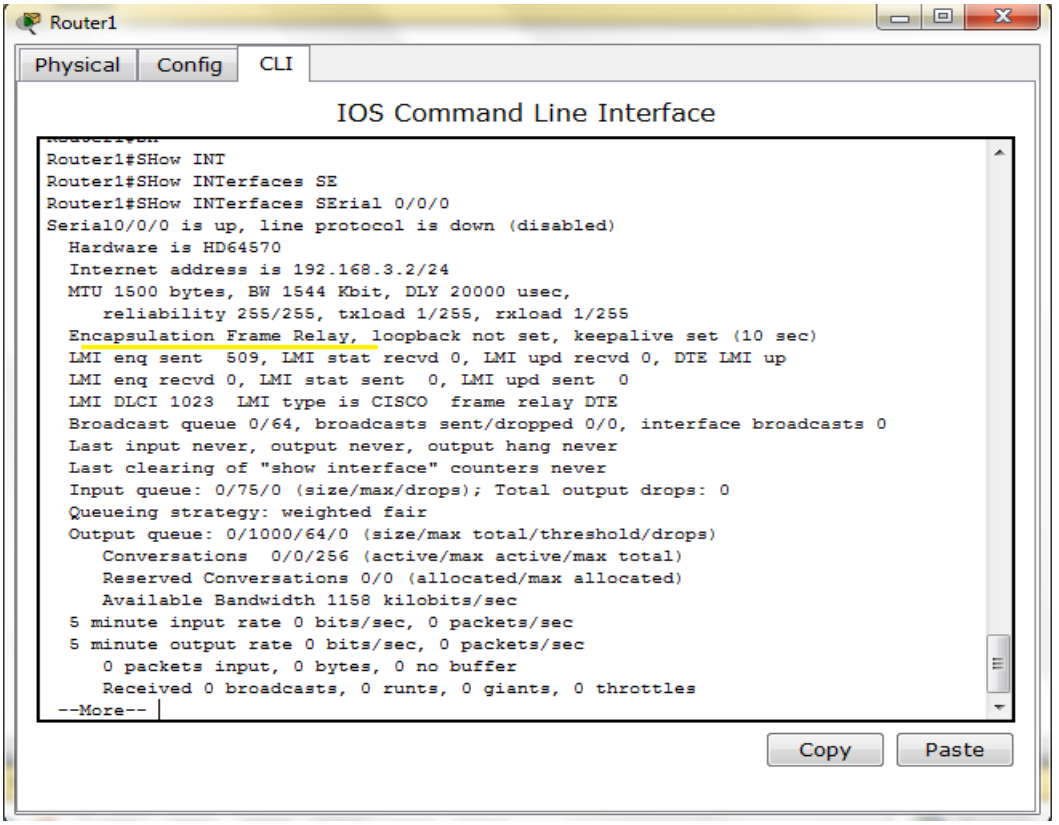
- **Vérification de la configuration du frame Relay**

La figure IV.21représente la vérification du la configuration du frame Relay en etulisant la commande « Show interface Serial 0/0/0 » au niveau du Router2 .



FigureIV.21 : Le résultat obtenu sur le Router2

La figure IV.22 représente la vérification du la configuration du frame Relay en etulisant la commande « Show interface Serial 0/0/0 » au niveau du Router1.



FigureV.22 : Le résultat obtenue sur le Router1

IV.6.1. Configuration d'un firewall (PIX)

Dans cette partie on s'interesse à la configuration d'un firewall(PIX) en utilisant le simulateur GNS3,ce firewall(PIX) posséde trois interfaces réseaux :une connectée au reseau local(inside, Ethernet1) , l'autre au rseau l'internet (outside, Ethernet0) et la troisiéme sur le serveur Web(DMZ, Ethernet2) comme le montre la figure IV.23

Les étapes suivantes nous illustre la configuration complette de ce firewall :

1. **Configuration des interfaces**

La première étape consiste à donner un nom, une adresse IP et le niveau de sécurité choisit pour chaque interface (figure IV.23)

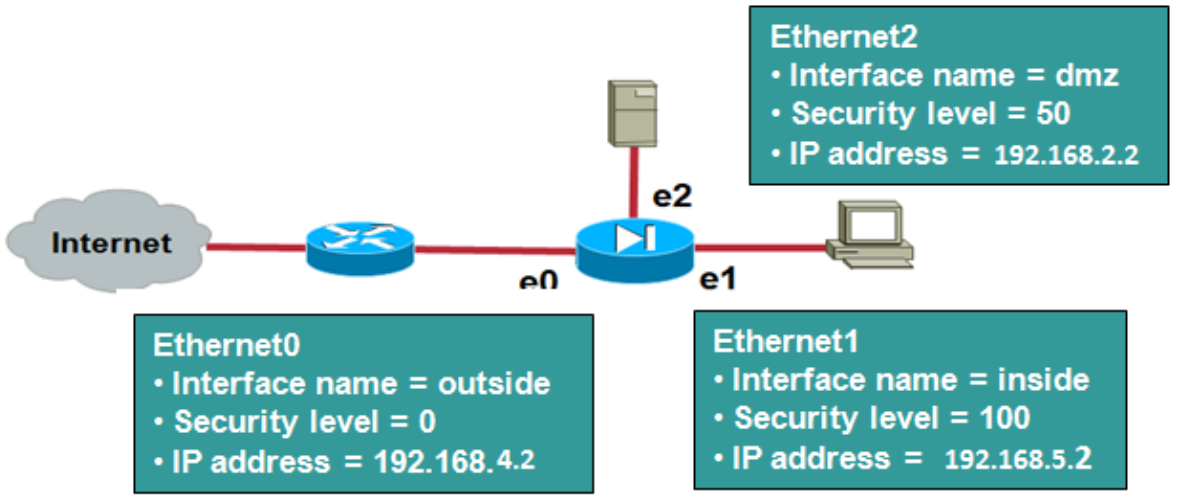
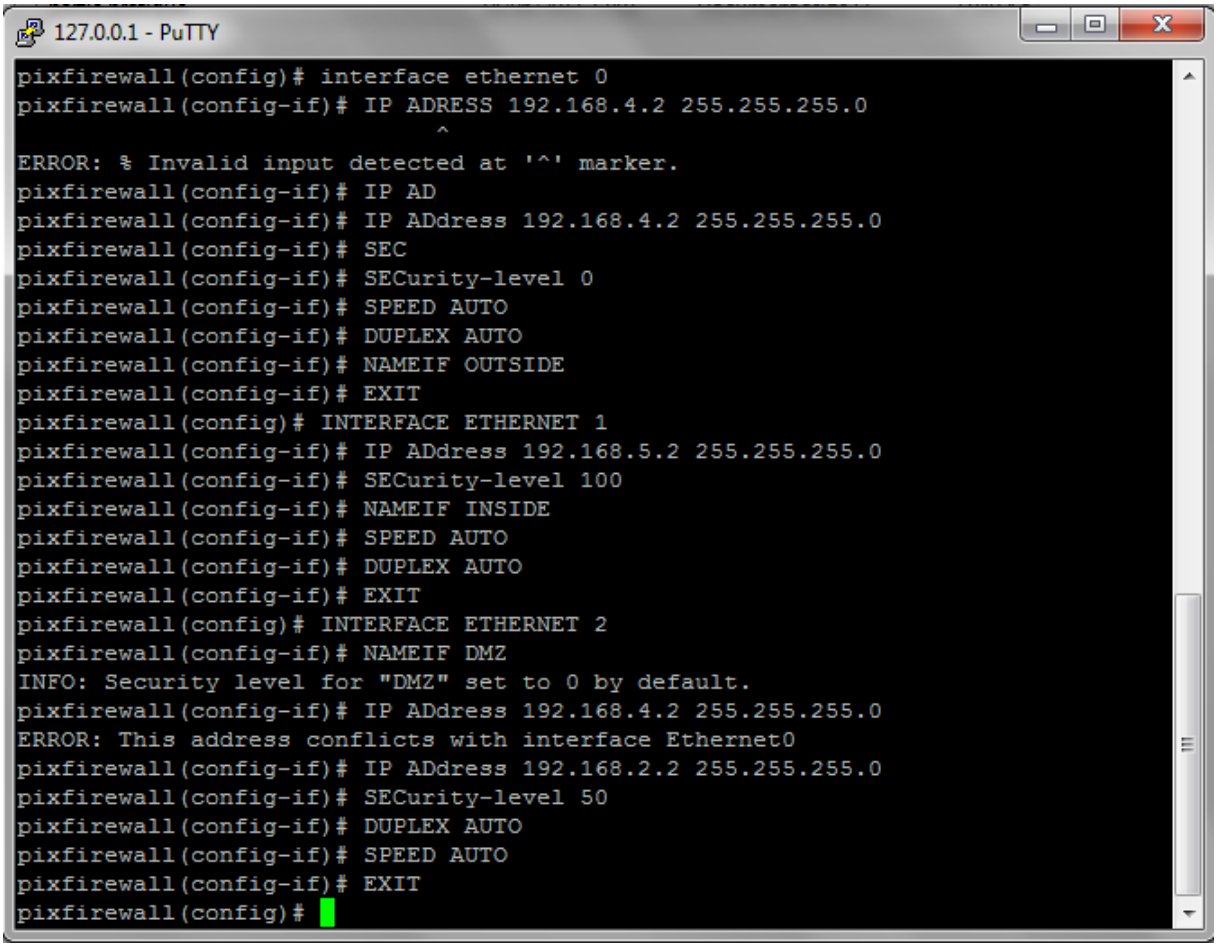


Figure IV.23 : les interfaces du firewall(PIX)

La figure IV.24 donne la configuration ces trois interfaces :



FigureIV 24 : configuration des interfaces du PIX

2. Configuration de la translation d'adresses

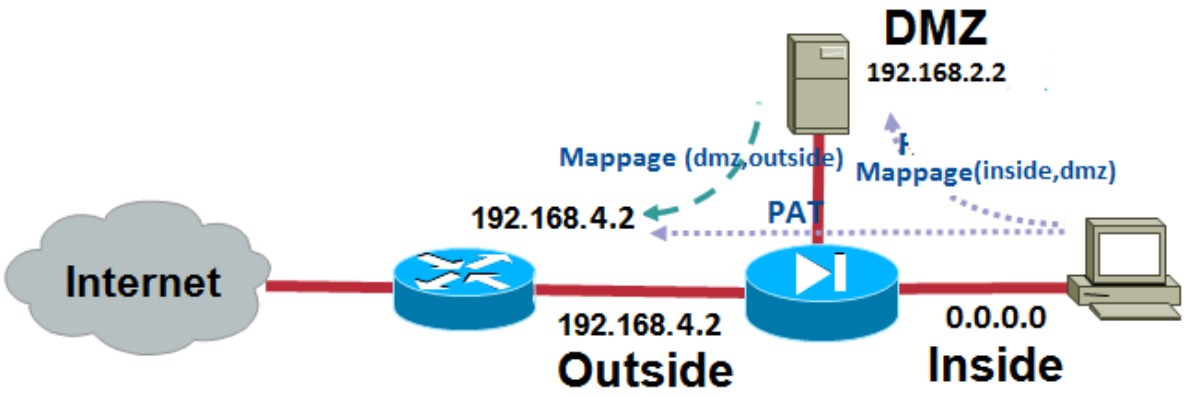


Figure IV.25 :Configuration du PAT et mapage

Comme la figure IV.25 le montre,il faut indiquer l'application du PAT (Port Translation Adresse) à n'importe quelle machine (**0.0.0.0 0.0.0.0**) venant de l'interface interne(**Inside**) pour sortir sur l'Interneten utilisant l'**IP** (publique) :192.168.4.2 de **l'interfaceoutside**

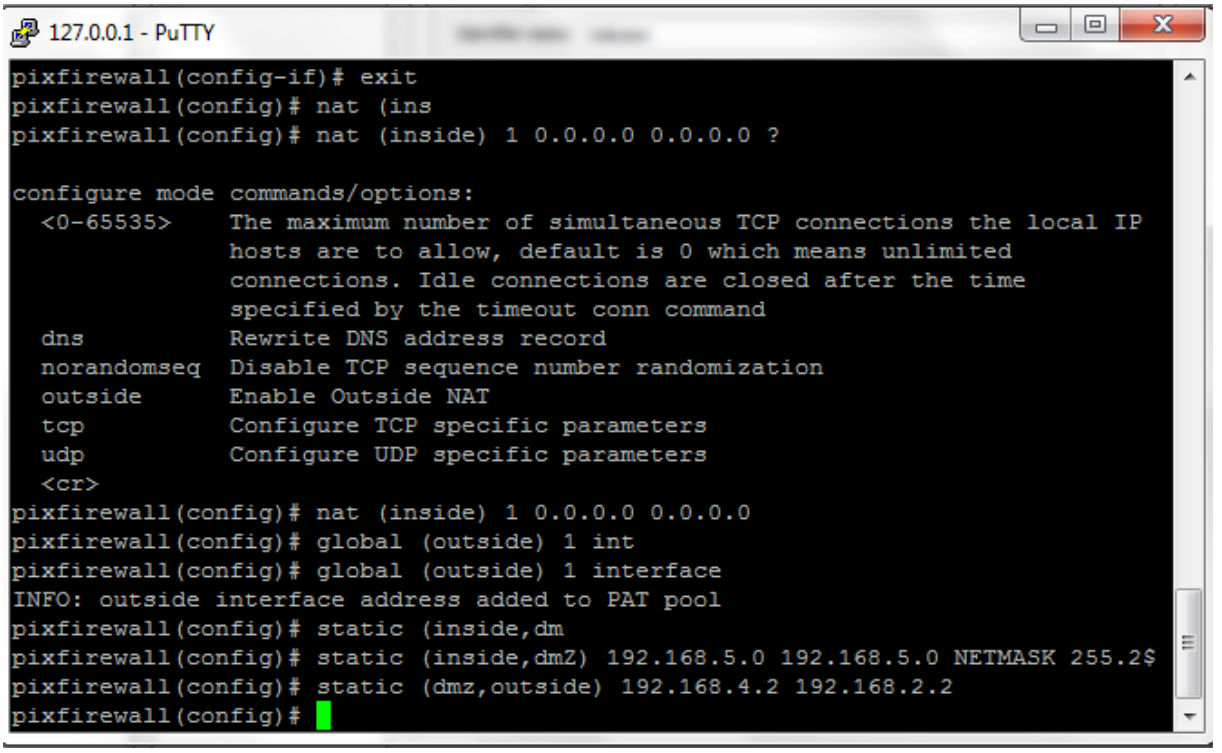
Interface : Signifie qu'on fera du PAT en utilisant l'IP de l'interface externe

Par contre il suffit juste d'appliquer le mappage (redirection) entre :

(Inside) et (DMZ) et aussi entre (DMZ) et (outside).

Static (dmz, outside) : pour la redirection des adresses venant de l'extérieure vers la DMZ

La figure IV.26 nous donne les commandes de configuration pour ce qu'est expliqué Ci-dessus :



FigureIV.25 : commandes de configuration du PAT et mappage

3. Configuration du routage

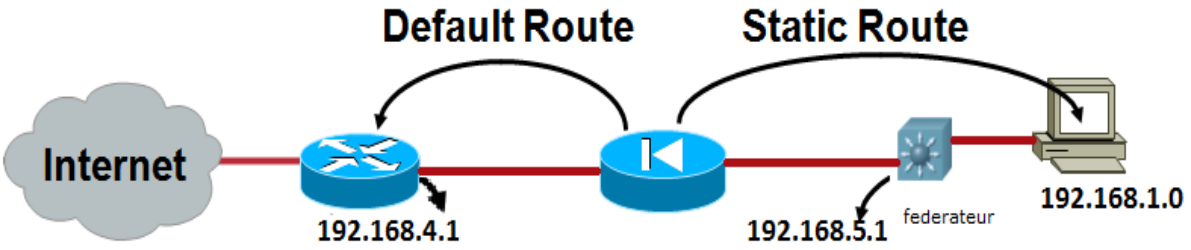
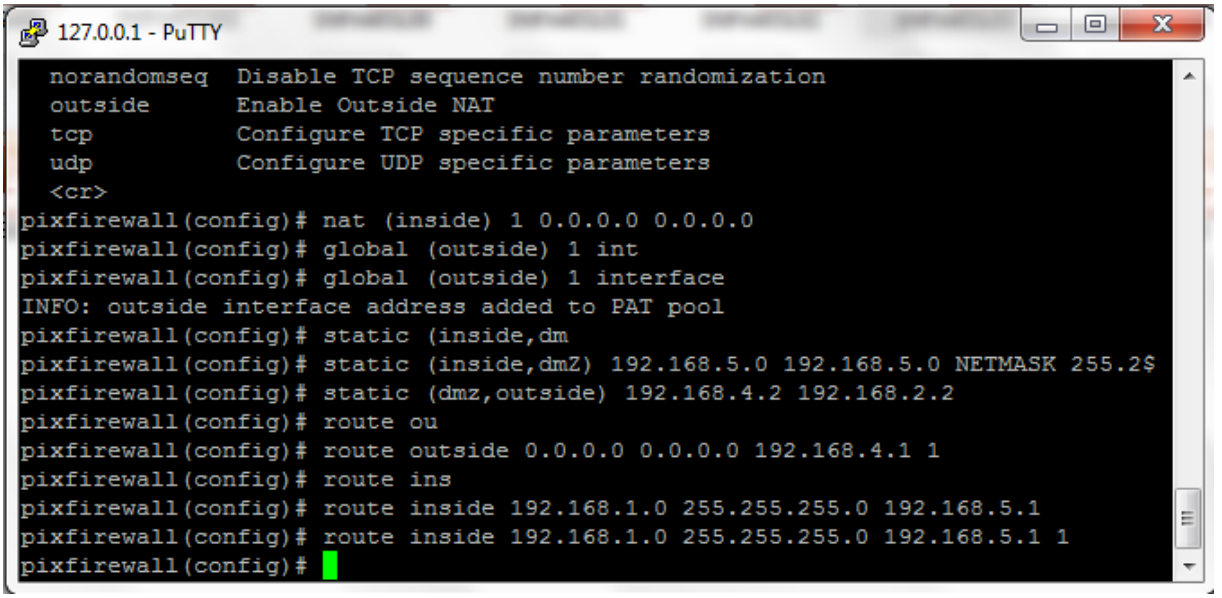


Figure IV.26 :routage dans le firewall

Cette troisiéme étape consiste à configurer le routage d'une sorte a indiquer au firewall que tout ordinateurs qui appartient au réseau 192.168.1.0 doit etre routé vers l'adresse IP 192.168.5.1, tandis qu'il faut spécifier la passerelle par defaut (192.168.4.1) pour tout ordinateur venant du firewall .

Les commandes de configuration du routage expliqué dans ce cas sont données réspectivement dans la figure suivante :



FigureIV.27:commandes de configuration du routage

4. Contrôler les accès de l'extérieur avec les ACLs

Un firewall, comme c'est indiqué dans la figure IV.28, bloque tout accès d'une zone moins sécurisée a une autre zone plus sécurisée, par contre il laisse passé tout accès d'une zone plus sécurisée vers une zone moins sécurisée, ainsi, dans notre cas de configuration des interfaces du firewall(PIX) on aura les deux situations suivantes :

- ✓ Le réseau local (INSIDE sécurité100) peut accéder vers l'extérieur (OUTSIDE sécurité 0) mais le sens inverse est impossible.
- ✓ le réseau OUTSIDE peut pas accéder vers la DMZ par contre de cette dernière on peut accéder vers l'extérieure.

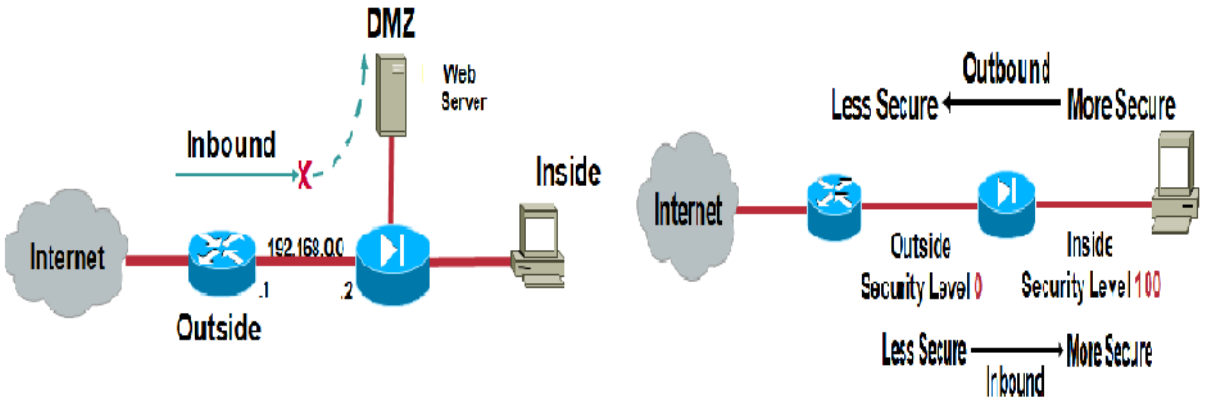


Figure IV.28 : Caractéristique d'un firewall

En effet deux problèmes se posent dans ce cas :

- ✓ Le premier est que les utilisateurs OUTSIDE (internet) ne peuvent pas avoirs

L'accèsvers le serveur WEB de l'entreprise s'ils veulent consulter son site pour voir, par exemple, la publicité de sa production.

- ✓ Le deuxième est que la direction générale (DG) ne peut pas accéder vers le réseau local(INSIDE).

Pour résoudre ces problèmes on doit configurer des listes de contrôles d'accès qui permettront d'autoriser l'accès dans ces deux cas. La figure IV.29 donne les commandes de configuration de ces listes de contrôles d'accès.

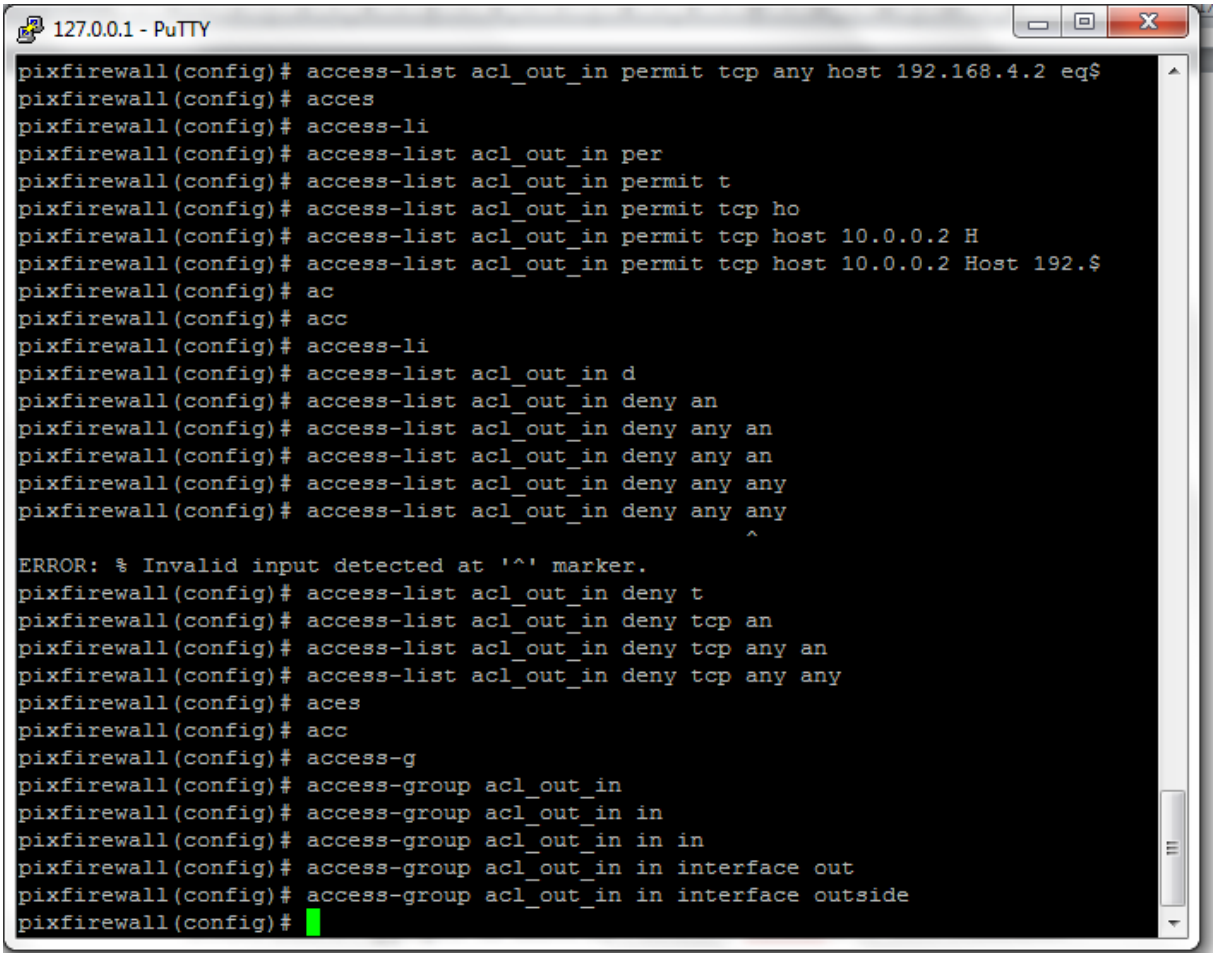


Figure IV.29 :commandes d'ACL du firewall

Ces03 lignes de commandes permettent de créer uneACL appelée acl_out_in.

Cette ACLautorise les services **http (web)** de n'importe quelle hôte (PC) vers la DMZet autorise l'accès au réseau de la direction générale vers le PC gestion de payement2.1 du département informatique et de refuser les autres d'accéder au réseau local.

IV.7.Conclusion

D'après les résultats de la simulation obtenue, on constate que la liste de contrôle d'accès qu'on a appliqué sur le fédérateur 3550 nous permit de sécuriser le réseau local de l'entreprise ENIEM et que la configuration du protocole Frame Relay et le routage dynamique pour le routeur externe de l'entreprise sont bien vérifiés et de ce que concerne la sécurité du réseau contre les intrusions externe on a configuré le firewall(PIX) en utilisant le logiciel de simulation « GNS3 » d'une façon a autoriser les utilisateurs extérnes d'avoir un accès vers le serveur WEB de l'entreprises et de bloquer leur accès vers le réseau local.

Conclusion générale

Les différentes menaces et attaques sur divers systèmes nous ont ramené à parler de la nécessité de garantir certains besoins de sécurisation : l'intégrité et la confidentialité des données transmises, l'authentification des acteurs, ainsi que la non répudiation des actes.

Dans notre mémoire ,nous nous sommes intéressés a une technique (méthode) qui nous aide a mettre en place et en marche une politique de sécurité dans le but de faire face a ces différentes menaces et attaques , cette politique de sécuritéqu'on proposée est basée sur l'installation et la configuration d'un firewall ainsi que la configuration des autres éléments d'interconnexions du réseau (routeur ,fédérateur , …) afin d'avoir plus de sécurité en utilisant des listes de contrôles d'accès (ACL) et la translation d'adresses de l'entreprise.

En effet, la sécurité est comme une chaine et elle est proportionnelle aux différentes menaces qui augmentent au fur et àmesure, c'est ce qui a fait de la sécurité un sujet très vastes et très important en mêmetemps, donc nous envisageons quelques perspectives pour la continuation de ce travail :

- S'intéresser à d'autres aspects de sécurité comme par exemple : la configuration d'un VPN pour relier le réseau de l'entreprise ENIEM avec sa direction générale
- Evaluer la solution en prenant en compte autres aspect de sécurité tel que : l'authentification en utilisant le protocole RADIUS.
- Conception d'un réseau sans fil pour ajouter l'unité commerciale au réseau de l'entreprise.

Ce projet nous a permis d'acquérir des connaissances dans de nombreux domaines. En effet, il nous a initiés au monde de la recherche sur les réseauxsurtout en ce qui concerne la sécurité ; Ainsi les différents modes de communication, leurs applications, ainsi que les protocoles qui les gèrent. Grâce notre modeste travail, nous avons eu l'occasion de voir beaucoup de choses de plus prés et d'enrichir nos connaissances ; nous avons aussi eu la chance de mettre nos capacités en valeur et de faire face aux situations les plus critiques et aux obstacles et apprendre comment procéder pour s'en sortir.

V.1.Introduction

Matériels et logiciels présentent de manière détaillée le matériel informatique et les différents systèmes d'exploitation. L'objectif de ce chapitre est d'apprendre les différentes fonctionnalités des composants matériels et logiciels et la méthode de configuration des différentes matérielles Cisco (Switch, routeur et firewall).

V.2. Les équipements Cisco

Les réseaux hétérogènes utilisant le matériel Cisco formant Interne sont reliés entre eux grâce à des dispositifs d'interconnexion (Switch, routeur, firewall) qui assurent le transfert des données.

V.2.1. les Switch Cisco(CATALYST Cisco)

Les commutateurs intelligents Cisco Catalyst, nouvelle famille de périphériques autonomes à configuration fixe, apportent aux postes de travail une connectivité FastEthernet et GigabitEthernet optimisent les services de LAN sur les réseaux d'entreprise.

Et ces caractéristiques sont :

- Fonctionnalités intelligentes à la périphérie du réseau, par exemple des listes de Contrôle d'accès (ACL) élaborées et une sécurité optimisée
- Sécurité du réseau assurée par une série de méthodes d'authentification, destechnologies de cryptage des données et le contrôle des admissions sur le réseau basé sur les utilisateurs, les ports et les adresses MAC.

Figure III.2 les Switch cisco

V.2.2. les Router Cisco

La fonction principale d'un routeur Cisco consiste à diriger les paquets destinés à des réseaux locaux et distants en :

- Déterminant le meilleur chemin pour l'envoi des paquets,
- Transférant les paquets vers leur destination.

Figure : Vue de l'arrière du routeur

V.2.3 Les firewalls Cisco

Dans cette partie, nous ne présenterons que le PIX 501, conçu pour les "petits" bureaux. Cinq autres modèles existent : 506, 515, 520, 525 et 535.

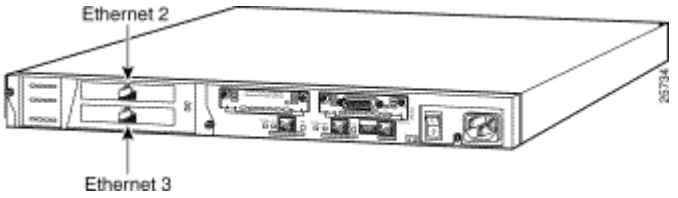


Fig2. L'interface Ethernet du Pare-feu Cisco PIX 501

Figure 3 : La face avant du PIX

Figure 4 : La face avant du PIX

V.2.3.1.Caractéristiques fonctionnelles.

Le PIX est un pare-feu à inspection d'état, il se base donc sur les couches 3 et 4 du modèle OSI et peut assurer le suivi des échanges et utilise l'ASA (Adaptive Security Algorithm) pour ce filtrage dynamique. Si les paquets d'une communication sont acceptés alors les paquets suivants de cette communication seront acceptés implicitement. De plus l'ASA permet d'affecter des niveaux de sécurité à vos interfaces. Ainsi un niveau égal à 0 équivaut à un réseau non sécurisé (internet), et un niveau égal à 100, à un réseau digne de confiance (réseau interne). Pour les PIX équipés de plus de 2 interfaces, des niveaux entre 1 et 99 peuvent être assignés : DMZ et autres réseaux plus vulnérables que le réseau local. Il peut aussi contrôler l'accès de différentes applications, services et protocoles et protège votre réseau contre les attaques connues et courantes.

Ce pare-feu gère également le VPN (IKE et IPSec). On peut ainsi créer des tunnels VPN entre sites.

Le PIX peut aussi faire office de serveur DHCP pour les équipements connectés au réseau interne et grâce au NAT, permet à ces "clients" de se connecter à Internet avec une même adresse IP publique.

V.3.Caractéristiques matérielles

Bien qu'il existe plusieurs types et modèles des équipements Cisco, chacun comporte, à la base, les mêmes composants matériels, et pour cela dans cette partie on présente sur les caractéristiques matériel d'un routeur et presque pareil pour le firewall et Switch.

La figure présente l'intérieur d'un routeur 1841. Pour voir les composants internes du routeur.

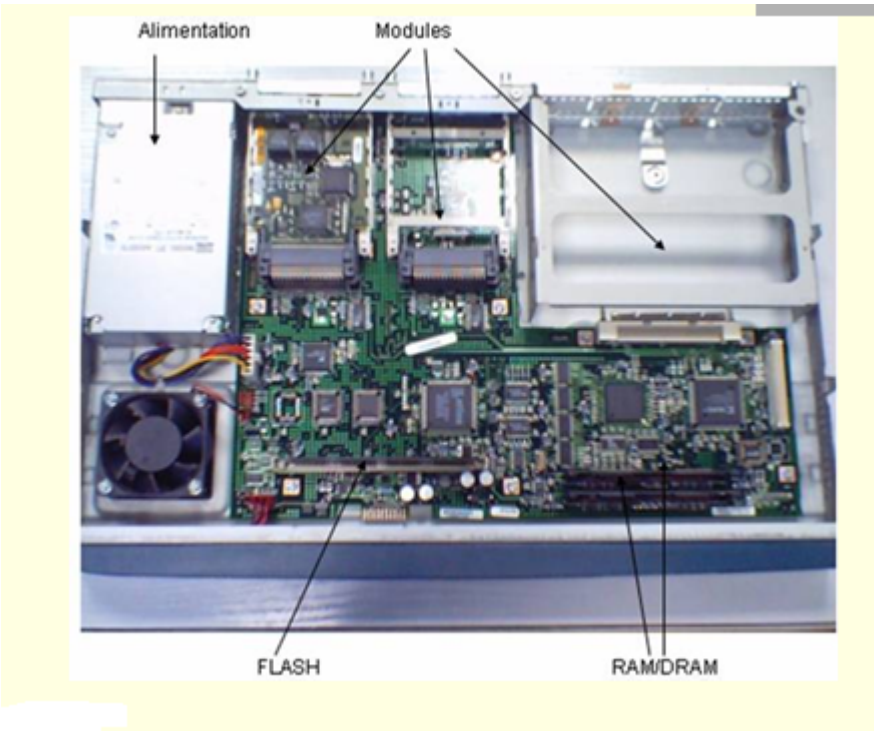


Figure 5 : Vue de l'intérieur du routeur

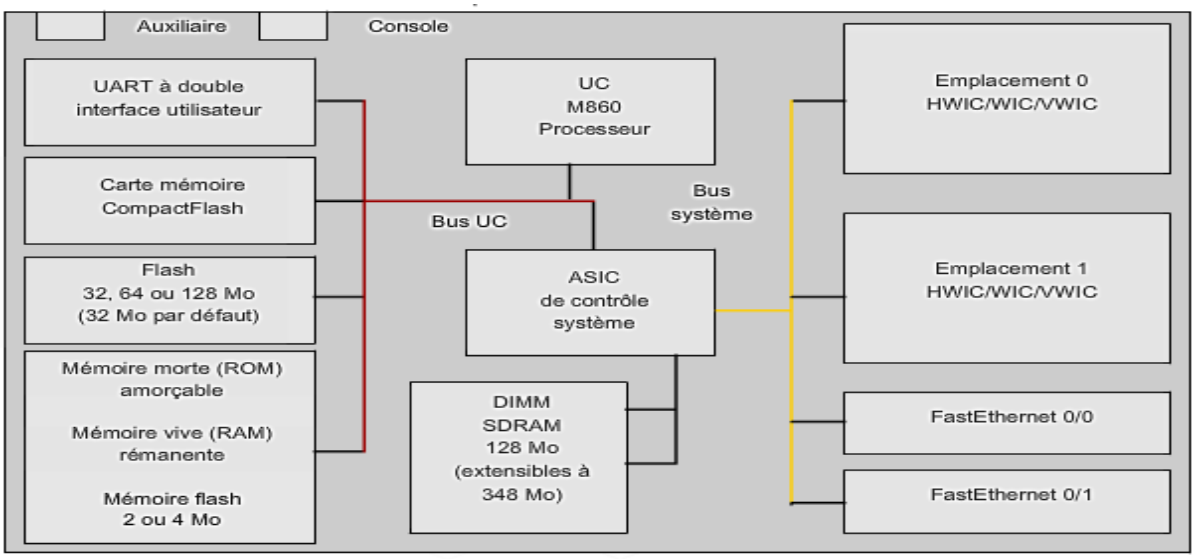


Figure 6 : composant matériel d'un routeur Cisco

Comme un PC, un routeur comprend également les éléments suivants :

- Unité centrale (UC)
- Mémoire vive (RAM)
- Mémoire morte (ROM)

V.3.1.Microprocesseur (UC)

Le Microprocesseur (CPU) L'unité centrale, ou le microprocesseur, est responsable de l'exécution du système d'exploitation du routeur.

V.3.2.Mémoire vive(RAM)

La mémoire vive stocke les instructions et données requises pour exécution par l'UC. La mémoire vive est utilisée pour enregistrer ces composants :

- **Système d'exploitation** : le système IOS (Internetwork Operating System) de Cisco est copié dans la mémoire vive pendant l'amorçage.
- **Fichier de configuration en cours** : il s'agit du fichier de configuration qui enregistre les commandes de configuration actuellement utilisées par l'IOS du routeur. À de rares exceptions près, toutes les commandes configurées sur le routeur sont enregistrées dans le fichier de configuration en cours, appelé running-config.
- **Table de routage IP** : ce fichier stocke des informations sur les réseaux directement connectés et les réseaux distants. Il permet de déterminer le meilleur chemin pour le transfert du paquet.
- **Cache ARP** : ce cache contient les mappages d'adresses IPv4 et MAC, de manière similaire au cache ARP d'un PC. Le cache ARP est utilisé sur les routeurs dotés d'interfaces de réseau local, telles que les interfaces Ethernet.

Mémoire tampon de paquets : les paquets sont stockés temporairement dans une mémoire tampon lors de leur réception sur une interface ou avant de quitter une interface.

La mémoire vive est une mémoire volatile : elle perd donc son contenu lorsque le routeur est mis hors tension ou redémarré. Cependant, le routeur contient également des zones de stockage permanent, comme la mémoire morte, flash et NVRAM.

V.3.2.Mémoire morte(ROM)

La mémoire morte est une forme de stockage permanent. Les périphériques Cisco utilisent la mémoire morte pour enregistrer les éléments suivants :

- Instructions d'amorçage
- Logiciel de diagnostic de base
- Version réduite d'IOS

La mémoire morte utilise un progiciel, qui est un logiciel incorporé dans le circuit intégré. Le progiciel inclut les logiciels qui n'ont habituellement pas besoin d'être modifiés ou mis à niveau, les instructions d'amorçage par exemple. La mémoire morte ne perd pas son contenu lorsque le routeur est mis hors tension ou redémarré.

- **Mémoire flash**

La mémoire flash est une mémoire non volatile pouvant être stockée et effacée électriquement. Elle sert de stockage permanent pour le système d'exploitation, Cisco IOS. Sur la plupart des modèles de routeurs Cisco, l'IOS est stocké de manière permanente dans la mémoire flash et copié dans la mémoire vive lors du processus d'amorçage, où il est ensuite exécuté par le processeur. La mémoire flash ne perd pas son contenu lorsque le routeur est mis hors tension ou redémarré.

- **Mémoire vive non volatile**

La mémoire vive non volatile ne perd pas les informations qu'elle contient lorsque le système est mis hors tension. Elle s'oppose aux formes les plus courantes de mémoire vive, telles que la mémoire vive dynamique (DRAM), qui nécessite une alimentation continue pour conserver les informations. La mémoire vive non volatile est utilisée par Cisco IOS comme stockage permanent pour le fichier de configuration initiale (startup-config). Toutes les modifications de configuration sont enregistrées dans le fichier de configuration en cours (running-config) dans la mémoire vive, et sont, à de rares exceptions près, immédiatement implémentées par l'IOS. Pour enregistrer ces modifications, au cas où le routeur serait redémarré ou mis hors tension, la configuration en cours doit être copiée dans la mémoire vive non volatile, où elle est enregistrée en tant que fichier de configuration initiale. La mémoire vive non volatile conserve son contenu, même si le routeur se recharge ou s'il est mis hors tension.

V.4.Network Operating System

Le logiciel du système d'exploitation utilisé dans les routeurs Cisco est appelé Cisco Internetwork Operating System (IOS). Comme tout système d'exploitation d'ordinateur, Cisco IOS gère les ressources matérielles et logicielles du routeur, notamment l'allocation de mémoire, les processus, la sécurité et les systèmes de fichiers. Cisco IOS est un système d'exploitation multitâche intégré aux fonctions de routage, de commutation, d'interconnexion et de télécommunications.

V.5.Les indicateurs LED

Le panneau avant d'un équipement Cisco comporte différents voyants permettant de surveiller les activités et les performances du système. Le panneau avant du commutateur comporte les LED suivantes:

- LED système
- LED pour le mode des ports
- LED pour l'état des ports

La LED système indique si le système est bien alimenté et s'il fonctionne correctement.

La signification des LED correspondant à l'état des ports varie en fonction de la valeur courante du LED Mode.

LED Stat :

- désactivé : aucune liaison
- vert fixe : liaison opérationnelle
- vert clignotant : envoi ou reçoit des données
- alternance vert et orange : liaison défectueuse
- orange fixe : port désactivé par l'admin, SpanningTre...

V.6.Les modes configuration de matériel Cisco

- mode utilisateur, accès restreint avec un prompt en '>'
- mode enable ou privilégie, accès par la commande 'enable' avec un prompt en '#'
- mode de configuration, accessible à partir de enable par la commande 'configure', prompt en 'configure#'; le mode de configuration le plus utilisé est 'configure terminal', il existe aussi 'memory' et 'network'

V.6.1. les commandes utiliser pour la configuration d'un Switch et d'un router

Le tableau suivant représente les différentes commandes utilisé pour la configuration d'un Switch et d'u routeur Cisco.

Commandes	*Descriptions*
configure terminal ou conf t ou confterm	Entre dans le mode de configuration globale
CTRL-Z	Permet de retourner à la racine du menu
exit	Sort et remonte d'un cran dans la hiérarchie des menus
hostname ou host <hostname>	Permet de modifier le nom de l'équipement réseau
enable secret <password>	Assigne un mot de passe encrypté à enable
interface ethernet | fastethernet | Serial | loopback <interface>ouint e | fa | s | lo	Entre dans le mode de configuration del'interface
ip address <address><mask>ouip add	Configure l'interface avec l'ip et le masque de réseau
bandwidth ou band	Indique une bande passante
encapsulation <encap> [<type]> ou encap	Fournit l'encapsulation de l'interface
no shutdown ou no shut	Active ou Désactive l'interface
Les commandes de sauvegarde :	
copy running-config startup-configou copy run star ou write mem	Sauvegarde la configuration courante en NVRAM
copy running-configtftpou copy run tftp	Sauvegarde la configuration courante vers un serveur TFTP
copy startup-configtftpou	Sauvegarde la configuration situé en
copy star tftp	NVRAM vers un serveur TFTP

copy tftp startup-configou copy tftp star	Charge un fichier de configuration d'un serveur TFTP en NVRAM
copy tftp running-configou copy tftp run	Charge un fichier de configuration d'un serveur TFTP dans la configuration courante
Commandes	***Descriptions***
erase startup-config ou erase star	Efface la configuration de la NVRAM
Configuration d'une connexion en telnet:	
router# conf t	
router(config)# line console 0	
router(config)# login	
router(config)# passwordxyz	
Les commandes de configurations du routage :	
router <xxx> [<process-id>,<autonomous system>] rip,ospf,bgp,igrp,eigrp,is-is,...	Configure le protocole de routage d'un routeur
exemple de configuration du routage RIP:	
router# conf t	
router(config)# router rip	
router(config-router)# version 1-2	la version 2 apporte le routage CIDR et l'utilisation de VLSM, un nombre de sauts à 128
router(config-router)#network *networknumber*	
exemple de configuration du routage OSPF:	
router# conf t	
router(config)# router ospf 10	
router(config-router)# network network number	
exemple de configuration du routage IGRP:	
router# conf t	
router(config)# router	

igrpautonomoussystem	
router(config-router)# network *networknumber*	
exemple de configuration du routage EIGRP:	
router# conf t	
router(config)# router eigrpautonomous system	
router(config-router)# network *networknumber*	
exemple de configuration du routage BGP:	
router# conf t	
router(config)# router bgp*autonomous system*	
router(config-router)# network *networknumber* [mask *network-mask*] [route-map *route-map-name*]	
D'autres commandes de routage	
ip multicast-routing	Permet de faire du routage multicast
ip rsvp bandwidth [*interface-kbps*] [*singleflow-kbps*]	Active la réservation RSVP sur une interface
Les commandes sur un Switch :	
vlan database vlan 1 name <vlan name>	Accès à la database et écriture dans le fichier vlan.dat
Exemple de configuration d'un vlan :	

switch# vlan database switch(vlan)# vlan<number><name> switch(vlan)# exit switch(config)#interface fa<iface-number> switch(config)#interface range fa... switch(config-if)#switchport mode access	affectation sur un port affectation sur un ensemble de ports on passe le mode de configuration de l'interface
Commandes	***Descriptions***
switch(config-if)# switchport access vlan <number-name>	on active le vlan sur le ou les interfaces
Activation du trunking sur l'interface	Le truncking sert dans l'extention d'un domaine VLAN sur d'autre switch, pour se faire CISCO utilise le protocole VTP VLAN Trunking Protocol
switchporttrunkencap dot1q	Il y a 2 protocoles utilisés dans l'étiquetage: le protocole ISL (CISCO) et le protocole 802.1q (IEEE)
switchport mode trunk	On active le mode trunk sur le port du commutateur serveur et client qui font le trunk le reste des ports sont en mode access
vlan database vtpdomain<domain-name> vtp server	Création d'un serveur VTP
vlan database vtpdomain<domain-name> vtp client	Création d'un client VTP
ip default-gateway <ip-gateway>	On peut définir une passerelle par défaut pour communiquer entre VLAN, pour se faire on utilise un routeur
encapsulation ISL | dot1q <vlan-number>	en mode interface on peut spécifier le type d'encapsulation sur le routeur
D'autres commandes communes :	
reload	Redémarre l'équipement réseau
setup	Passe en mode de configuration assisté
ping [<address>]	ping seul, permet de faire un ping étendu de spécifier une interface particulière..., ping + address IP ping l'interface avec l'interface directement connecté.
Les commandes show :	
show interfaces oushint	Donne une description détaillé sur les

	interfaces
show running-configoush run	affiche la configuration courante
Commandes	***Descriptions***
show startup-configoush star	affiche la configuration en NVRAM
show ip route oushіp route	affiche la table de routage
show ip<routing-protocol> [<options>]	affiche les informations sur le protocole de routage défini
show ipprotocols	affiche des informations sur les protocoles utilisés
show ?	donne toutes les commandes show disponibles

III.6.1. les commandes basiques pour la configuration d'un firewall

Pour une première configuration, il est conseillé de ne pas oublier certains points :

- ne pas répondre aux Ping sur l'interface externe.
- établir les routes par défaut
- configurer les interfaces
- établir les règles de redirection et de contrôle d'accès

Ensuite il faut tester la connectivité et si cela réussit, sauvegarder la configuration.

Détaillons à présent les commandes qui seront utiles pour cette configuration.

- hostname {nom}

- Mode de configuration globale.
- Spécifie le nom d'hôte du pare-feu.
- Exemple : hostname SupinfoPix001

domain-name {nom}

- Mode de configuration globale.
- Spécifie le nom de domaine auquel appartient le pare-feu.
- Exemple : domain-namesupinfo.lan

enablepassword {mot de passe} [encrypted]

- Mode de configuration globale.
- Mot de passe du mode privilégié.
- Sans le paramètre [encrypted], le mot de passe est écrit en clair dans le fichier de

configuration.

- Exemple : enablepasswordsupersecurepwdencrypted

clock set hh:mm:ss {mois jour | jour mois} année

- Configure l'horloge du pare-feu.

- clearclock

- Reconfigure l'horloge sur l'heure GMT (nécessaire dans le cas d'utilisation d'IPSec avec des certificats).

nameif {ethernet{n°} | gb-ethernet{n°}} {nom} security{level}

- Mode de configuration globale.

- Nomme l'interface et lui assigne son niveau de sécurité.

- Exemple : nameif ethernet0 outside security0

- Exemple 2 : nameif ethernet1 inside security100

-**interface {ethernet{n°} | gb-ethernet{n°}} [10baset | 10full | 100basetx | 100full | 1000sxfull | 1000basesx | aui | auto | bnc] [shutdown]**

- Mode de configuration globale.

- Configure la vitesse de l'interface spécifiée en argument et l'active.

- La vitesse est optionnelle.

shutdown : permet de désactiver l'interface (par défaut toutes les interfaces sont désactivées).

- Exemple : interface ethernet0 100full

ipaddress {nom_interface} {{ip} {masque} |{dhcp}}

- Mode de configuration globale.

- Configure l'adresse IP de l'interface.

- Exemple : ipaddressinside 10.0.0.2 255.0.0.0

- Exemple 2 : ipaddressoutsidedhcp

route {nom_interface} {ip} {masque} {ip_passerelle} [metric]

- Mode de configuration globale.

- Spécifie une route statique.

- Pour spécifier la route par défaut, il faut utiliser l'ip et le masque 0.0.0.0 ou 0.

- Exemple : route outside 0.0.0.0 0.0.0.0 82.226.244.238 1

- L'interface outside enverra tous les paquets sortant vers l'ip 82.226.244.238 (un routeur par

exemple).

- La métrique correspond au nombre de sauts jusqu'à la passerelle, par défaut 1

[no] rip {nom_interface} {defautl|passive} [version [1|2]] [authentication [text|md5] key {key_id}] - Dés/Active la réception des mises à jour des tables de routages RIP - icmp {permit|deny} {ip_source} [masque] {nom_interface}

- Autorise ou refuse le requête ping sur l'interface spécifié.
- Exemple : icmpdenyanyany
- Cet exemple refuse toutes les requêtes icmp.

Show interface {ethernet{n°} | gb-ethernet{n°}}

- Affiche les informations détaillées de l'interface.
- show ip
- Affiche la configuration IP des interfaces.

Show nat

- Affiche la configuration NAT : les interfaces autorisées à initier des connexions vers des interfaces moins sécurisées.

Show global

- Affiche les adresses à utiliser pour les translations.

Show xlate

- Affiche la table des adresses translatées dynamiquement. - show route
- Affiche les routes configurées.

Show access-list

- Affiche les ACL.

Show running config

- Affiche le fichier de configuration actif.

writememory

- Copie la configuration courante dans la mémoire Flash.
- Cette configuration sera utilisée au prochain démarrage.

reload

- Redémarre le PIX.

V.7. Configurer le périphérique Cisco (Switch ou routeur ou un firewall) avec HyperTerminal

V.7.1.Configuration d'HyperTerminal

- **Exemple pour la configuration d'un Switch**

Tout d'abord, vous avez besoin d'un câble console (câble RJ-45 vers Série) reliant le port série de votre ordinateur à la prise RJ-45 marqué « console » sur votre Switch comme il est donnée par la figure suivante.

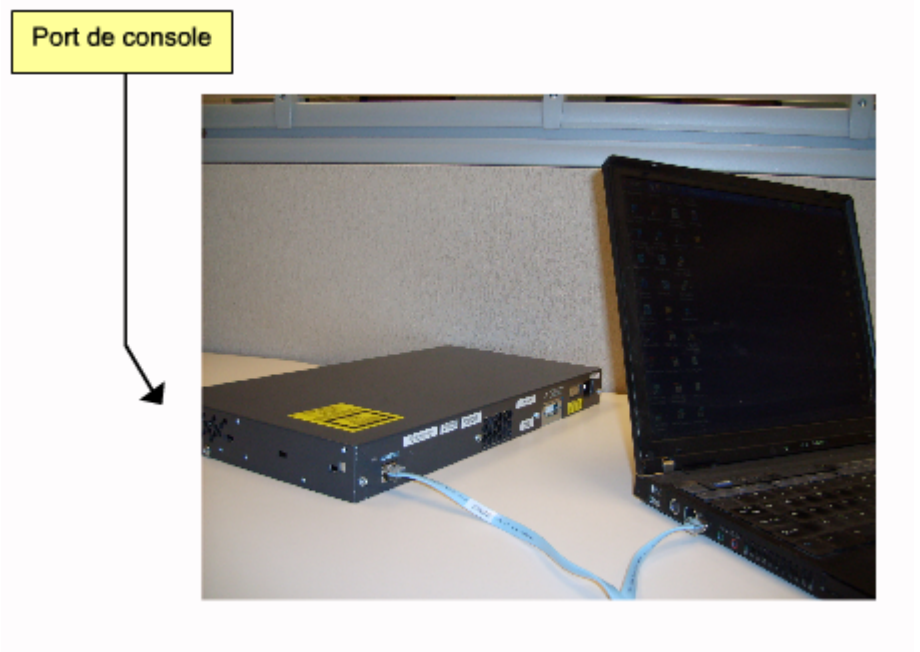
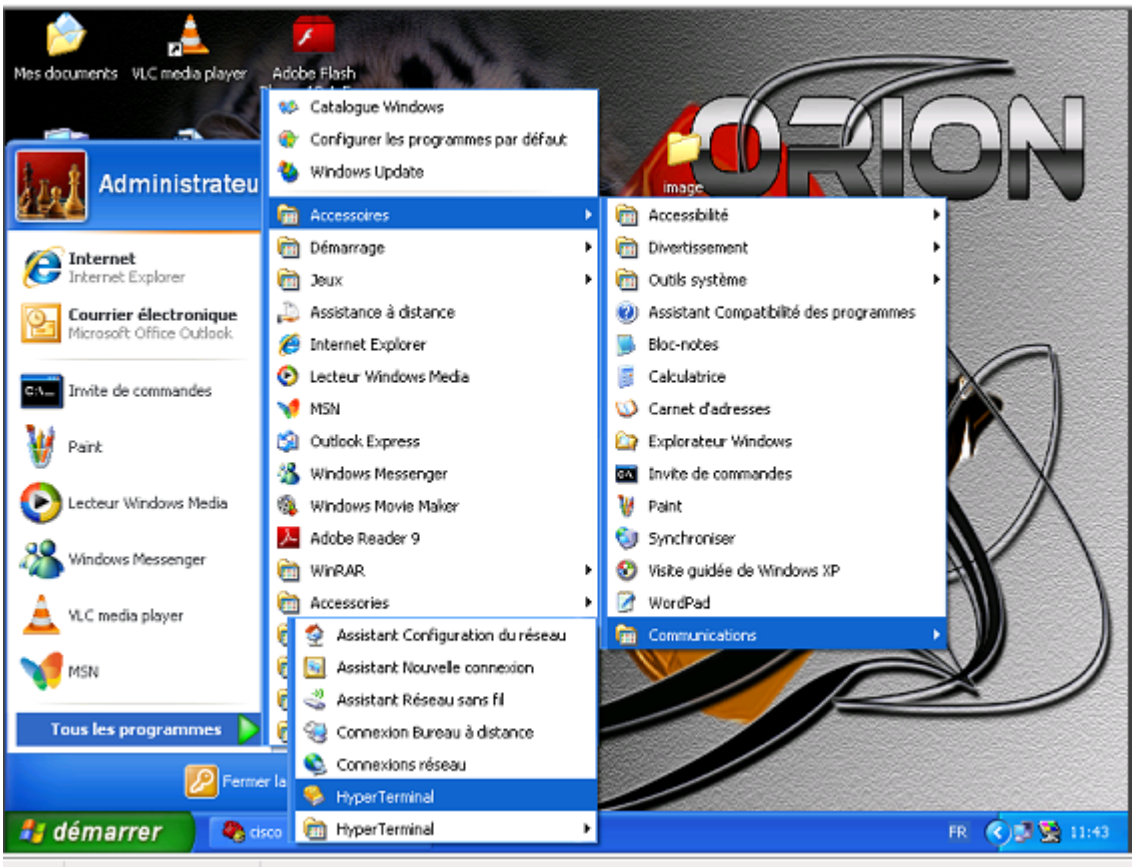
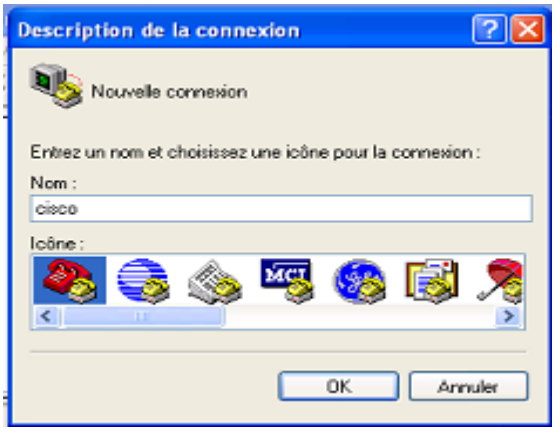


Figure 7 :L'interface de la console du Switch.

Ensuite, ouvrez Hyper-Terminal (Menu démarrer -> Tous les programmes -> accessoires -> communications ->Hyper-Terminal), puis entrez un nom pour votre nouvelle connexion ; sélectionnez le port série sur lequel est connecté le câble console et cliquez sur « paramètres par défaut » puis ok comme il est donnée par les figures (1), (2), (3), (4) et(5) successivement.



Figure(1)



Figure(2)

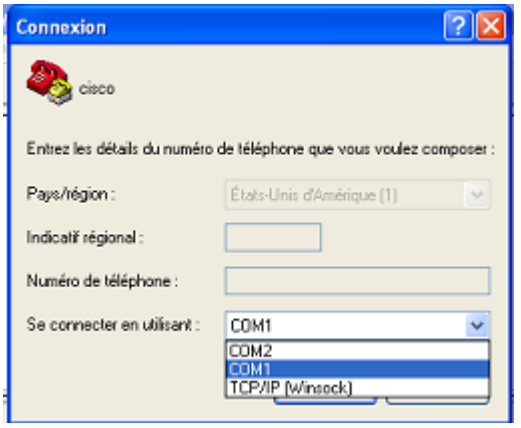
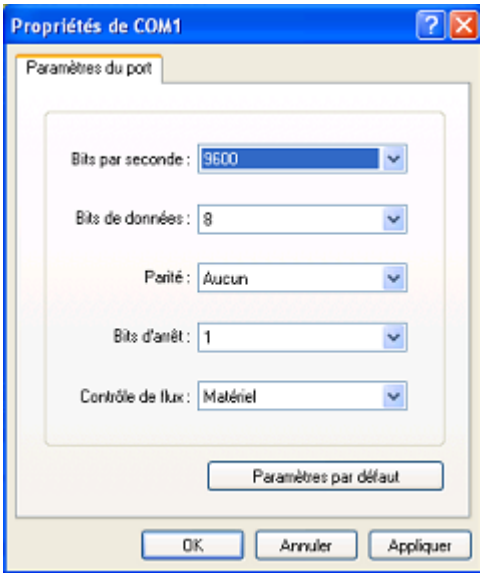
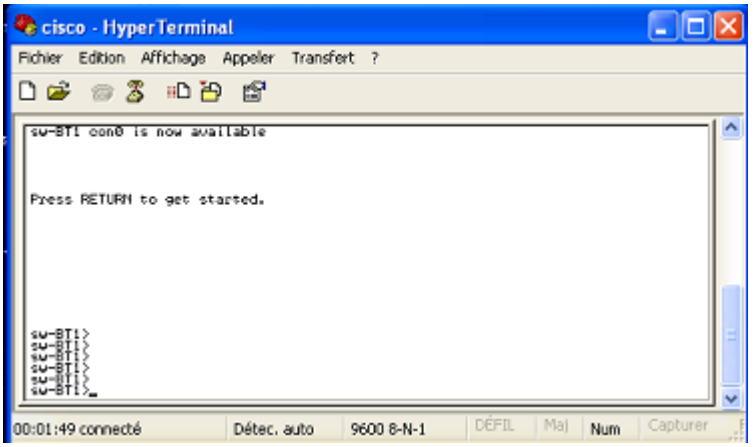


Figure (3)



Figure(4)



Figure(5)

Voilà, Nous somme connecté au Switch et à partir de maintenant nous pouvons le configurer.

Et pour la configuration d'un firewall on suit les même étapes de la configuration du Switch, mais pour la configuration d'un routeur lorsque vous terminez ces étapes, et S'il est allumé, faite un retour à la ligne, vous devriez voir apparaître une ligne vous demandant si vous voulez entrer dans outil de configuration initial, dans ce cas répondez « no » sinon, il vous affiche le nom du routeur suivi de ">" (ex: Routeur>).

. S'il est allumé, faite un retour à la ligne, vous devriez voir apparaître une ligne vous demandant si vous voulez entrer dans outil de configuration initial, dans ce cas répondez « no » sinon, il vous affiche le nom du routeur suivi de ">" (ex: Routeur>) ; dans ce cas tapez "en" pour enable et entrez le mot de passe s'il y en a un. Cette fois "Routeur>" change en "Routeur#" et vous pouvez commencer à taper des commandes de configuration.

III.8. Résultat d'un Ping à partir d'une hôte

Pour voir les résultats de la commande Ping, commencer per ouvrir une fenêtre d'inviter de commande et à exécuter une commande semblable à celle reproduite ci-dessus .en spécifiant une adresse IP valide sur votre réseau comme il est donnée par la figure suivante :

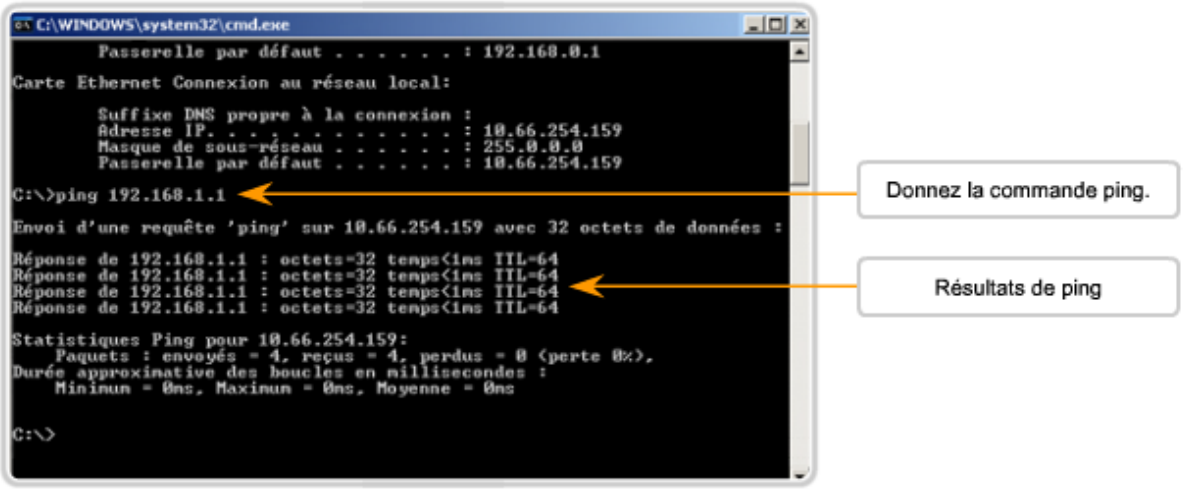


Figure 8: Résultat d'un Ping à partir d'une hôte

DG : direction générale de l'ENIEM ;.

Routeur 1 : routeur utilisé par DG.

Routeur 2 : routeur utilisé par l'entreprise ENIEM.

Routeur 0 : routeur utilise par le fournisseur d'accès

FAI : fournisseur Access internet.

Modem 1 : modem utilisé par ENIEM.

Modem 2 : modem utilisé par la direction générale.

Inside : interface deréseau local du firewall.

Outside : interface de réseau externe du firewall.

Pc0 : utilisateur externe.

Pc1 : utilisateur du la direction générale.

Pc2 : utilisateur de l'ENIEM.

.

- Tout sur la sécurité informatique, Pillou , Jean François, cote IA 201
- Tout sur le réseau informatique, Pillou , Jean François, cote IA 274
- Initiation aux réseaux, G.Pujolle, Eyrolles,2002
- Mémoire de fin d'études, Mr .Yazid FEKHAR , la sécurité dans les réseaux ,ING INFO 29 année 2006/2007 département informatique de la FGEI de l'UMMTO .
- Mémoire de fin d'études, M^{elle} : LARABI Drifa et M^{elle} : YAHIAOUI Karima, sécurité des réseaux ,ING INFO 63 année 2005/2006 département informatique de la FGEI de l'UMMTO .
- Mémoire de fin d'études ,M^{elle} :AMROUNI Hadjila et M^{elle} :ARIB Nassima , interconnexion des réseaux TCP/IP à base des routeur cisco,ING INFO 88 année 2006/2007 département informatique de la FGEI de l'UMMTO
- http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_book09186a0080172852.html :
- www.commentcamarche .com