REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
FACULTE DE GENIE ELECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire de Fin D'études

Master Académique

Domaine : **Mathématiques et Informatique**
Filière : **Informatique**
Spécialité : **Réseau, mobilité et systèmes embarqués**

Présenté par :
TOUZI Yasmine
LARBI Khadidja

Thème

Mise en place d'une sécurité réseau basée sur l'utilisation des VLANs et des VACLs au niveau de l'entreprise ENIEM

Devant le jury compose de:

…… …, Président.

Mr OUALLOUCHE Fethi , Maitre de conférences B, UMMTO, Encadreur.

Mr TALEB Ferhat, Chef de département, ENIEM, Co-encadreur

……, Examinateur.

2016/2017

Remerciements et dédicaces

Tout d'abord on tien a remercier avant tout, Dieu de nous avoir donné la patience, ainsi que la volonté et le courage de réalisé ce travail.

On tien a exprimer nos sincères remerciements à notre promoteur Mr OUALLOUCHE Fethi, pour avoir accepté de nous encadrer et pour sa disponibilité, son soutien et ses conseils qui nous ont permis de mener à bien ce projet.

Nos remerciements sincères s'adressent également à notre encadreur Mr TALEB Ferhat, pour son suivi, et à Mr YACINE pour ces motivations et ces conseils qui nous ont beaucoup servies.

Je dédie ce modeste travail :

À mes très chers parents en témoignage de reconnaissance et d'affection ;

À mes très chères frères Meziane et Abdeslam ;

À mes soeurs :
Djidji, Nadia, Hassiba, Hadjira et Dyhia ;

À Sidali qui a toujours cru en moi ;
A tous les matwaychiches que je n'oublierai jamais : Azwaw ,Karim Hammoudi, Nassim , Moh, Azwaw, Ghiles, Sabrina, Abdou, Smail, Tina, Tawes, Thinhinane et Malik;

À toute la famille Hammoudi ;

À tous ceux qui me connaissent.

Ldjar

Je dédie ce modeste travail :
À mes très chers parents en témoignage
de reconnaissance et d'affection ;

À ma sœur Assia :

À mes très chères frères : Tarik et Youcef ;

À mes chères amies, qui m'ont toujours soutenue
et aidé dans les moments les plus difficiles ;

A toute la famille TOUZI ;

À tous ceux qui me connais et je connais.

Yasmine

Table des matières

Table des matières

Table des matières

Table des matières

Table des matières

Chapitre03 : **Réalisation**

Table des matières

Table des matières

Table des matières

Liste des figures

Liste des figures

Liste des figures

Liste des figures

Introduction générale

Introduction générale

Actuellement, le bon fonctionnement d'une entreprise repose sur la solidité de son réseau local. Ce dernier met en relation des équipements terminaux (ordinateurs, imprimantes, stations de travail, terminaux passifs), et des serveurs et tous ces éléments sont entièrement sous la responsabilité d'un administrateur réseau.

Avec l'intégration du service internet dans l'entreprise et le nombre de machine qui est important et proportionnel à l'informatisation de services, l'approche des réseaux locaux présente des limites rigoureuses qui peuvent engendrer des pertes d'informations importantes.

A cet effet, un réseau peut toujours être sécurisé avec différents outils tels que les pare-feu et les anti-malveillances. Toutefois, pour une petite ou moyenne entreprise, la première solution qui est préconisée par les experts réseaux est la segmentation VLAN (Virtual Local Area Network) puis associer d'autres outils qui permettent de limiter les accès à quelques machines du réseau.

L'entreprise ENIEM fait partie des moyennes entreprises qui utilise un réseau local. Ce réseau présente quelques défaillances de sécurité. Dans le cadre de notre projet de fin d'études, nous nous sommes intéressés à étudier ce réseau et appliquer la segmentation par VLAN. Pour limiter l'accès aux machines du réseau ENIEM, nous avons optés pour l'utilisation des VACLs (Virtual Local Area Network). Ce choix est motivé par le cahier des charges de départ qui insister sur la nécessité d'avoir des accès différents aux machines appartenant au même VLANs.

Pour présenter notre travail, nous avons structuré le présent mémoire en trois chapitres :

- Dans le premier chapitre, nous présenterons les notions de base de sécurité dans les réseaux informatiques, les déférentes attaques et malveillances existantes, ainsi que les différentes techniques de protection.
- Dans le deuxième, une étude des VLANs, des ACLs et des VACLs sera exposée.
- Ensuite, dans le troisième chapitre, nous ferons une étude des failles du réseau existant et de la solution proposée.

  Enfin, nous terminerons par une conclusion générale.

Introduction générale

CHAPITRE I

Elements de base sur la sécurité informatique

Chapitre I Eléments de base sur la sécurité informatique

I. Introduction

Dans ce chapitre, nous allons introduire les notions de base de la sécurité informatique : les différentes menaces, risques et malveillances. Ainsi que les différentes techniques et méthodes de protection.

II. Sécurité d'un réseau

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 possèdent uniquement les droits qui leurs ont été accordés. [4]

La sécurité informatique a pour objectifs :

- **La prévention :** Prendre des mesures afin d'empêcher des attaques ;
- **La détection :** Prendre des mesures afin de détecter quand, comment, par qui une attaque a été réalisée et les actifs ou les biens qui ont été endommagés ;
- **La réaction :** Prendre des mesures après une attaque de sécurité, afin de pouvoir restaurer les biens et les actifs, ou réduire l'impact de l'attaque.

II.1. Les causes de l'insécurité

On distingue généralement deux types d'insécurité :

1. **L'état actif d'insécurité :** c'est la non-connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisible (par exemple la non désactivation de services réseaux non nécessaires à l'utilisateur) ;

2. **L'état passif d'insécurité :** c'est lorsque l'administrateur (ou l'utilisateur) d'un système ne connait pas les dispositifs de sécurité dont il dispose. [4]

II.2. Les services de sécurité [1]

Un service de sécurité est un service qui augmente la sécurité des traitements et des échanges de données d'un système. Un service de sécurité utilise un ou plusieurs mécanismes de sécurité.

Chapitre I Eléments de base sur la sécurité informatique

Il existe cinq services de sécurité qu'on peut implémenter dans une organisation, ces services ne sont pas tous requis, et on peut en implémenter quelques-uns en fonction des objectifs de la sécurité requis. Ces services sont :

- **L'authentification :** l'identité des acteurs de la communication est vérifiée.
  Mécanismes utilisés : Cryptage, signature numérique, Notarisation ;
- **La confidentialité :** les données (et l'objet et les acteurs) de la communication ne peuvent pas être connues d'un tiers non-autorisé.
  Mécanisme utilisé : Cryptage ;
- **L'intégrité des données :** les données de la communication n'ont pas été altérées.
  Mécanismes utilisés : cryptage, signature numérique, contrôle d'accès, contrôle d'intégrité ;
- **Le non répudiation des données :** Empêche l'émetteur ou le receveur de nier avoir transmis ou reçu un message.
  Mécanismes utilisés : signature numérique, notarisation ;
- **La disponibilité :** les acteurs de la communication accèdent aux données dans de bonnes conditions.
  Mécanismes utilisés : Filtrage (pare-feu), antivirus, contrôle d'accès ;

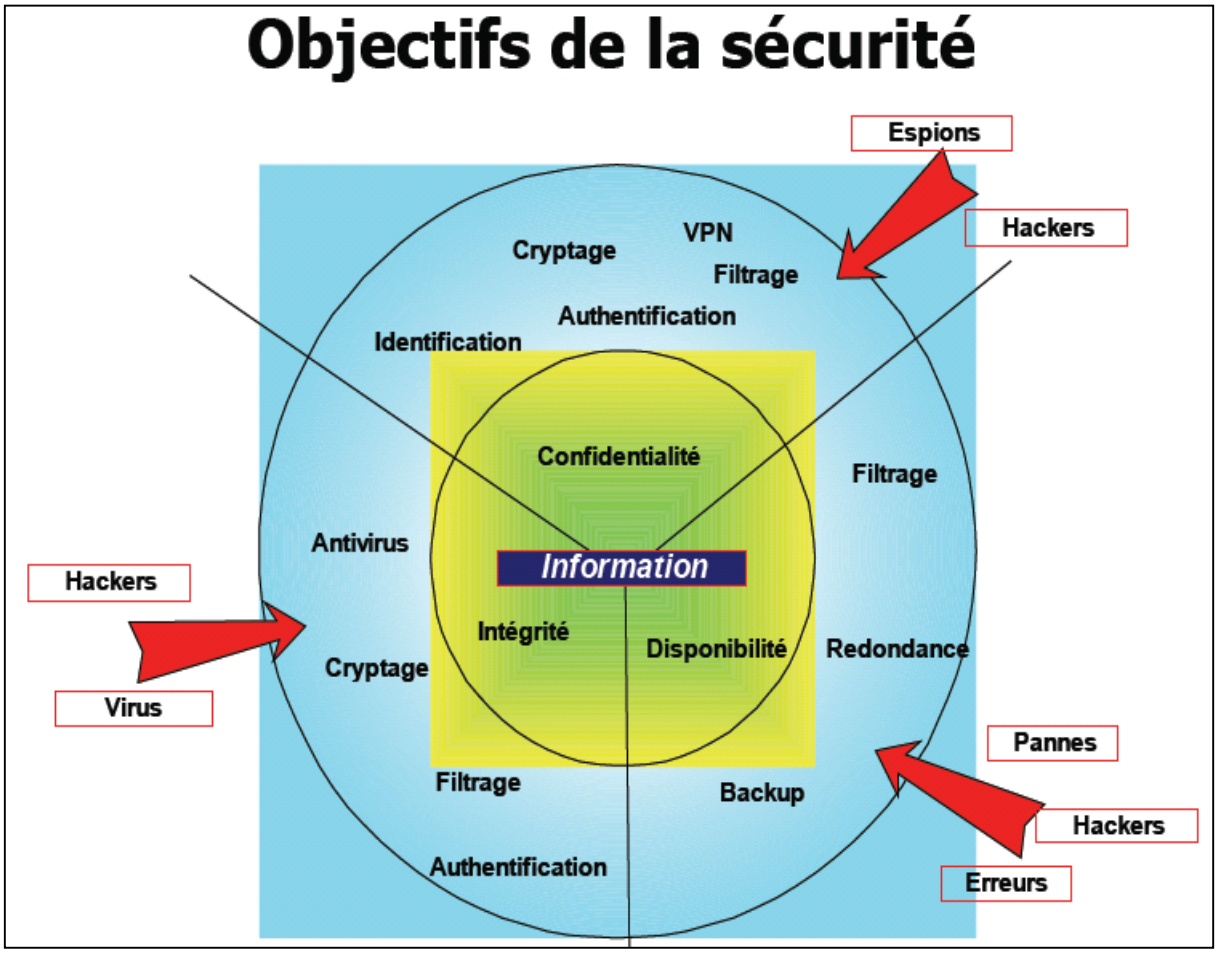

Figure I.1 : les objectifs de la sécurité

III. Les pirates informatiques

A l'origine « hacker » est un mot anglais qui veut dire « bricoler » ou encore « bidouilleur ». En informatique ce terme est utilisé pour définir les programmeurs débrouillards, avec des connaissances techniques élevées. Ces programmeurs sont avant tout passionnés par ce qu'ils font, ils ne se posent pas de limites pour les connaissances ou pour assouvir leurs curiosité.

Les hackers sont également capables de détourner un objet ou un logiciel de son fonctionnement originel. Ils utilisent leurs savoirs pour découvrir les choses auxquels ils ne sont pas censés avoir accès. Mais la communauté de hacker va également au-delà de la connaissance technique.

Chapitre I Eléments de base sur la sécurité informatique

Etre un hacker correspond davantage à un état d'esprit plus qu'au fait de programmer. Ainsi, les hackers sont généralement des personnes cultivés qui connaissent à la fois l'historique de leur statut, les grands acteurs du mouvement, qui se tient de tout ce qui s'apparente à leur domaine et qui ont soif de connaissances.

Le jargon informatique classe les hackers en plusieurs catégories en fonction de leurs objectifs, de leurs compétences et de la légalité de leurs actes. Ce vocabulaire fait référence aux films de western, où le héros porte un chapeau blanc, et les méchants portent des chapeaux noirs.

- **Les chapeaux blancs** ou white hat : professionnels de la sécurité informatique (consultants en sécurité, administrateurs réseaux…) effectuant des tests d'intrusions en accord avec leurs clients et la législation en vigueur afin de qualifier le niveau de sécurité des systèmes. Certains hackers se considèrent comme white hat alors qu'ils transgressent les lois, leur but étant de prévenir les responsables des failles de leurs systèmes. Certains d'entre eux s'infiltrent dans les systèmes de sécurités les plus coriaces juste pour la connaissance, pour se dire qu'ils savent le faire ;
- **Les chapeaux bleus** ou blue hat : consultants en sécurité informatique chargés de vérifier l'absence de bogues et de corriger d'éventuels exploits avant le lancement d'un site web en ligne ou système d'exploitation sur le marché. Le terme est notamment employé par Microsoft, désignant ses hackers et ingénieurs en sécurité informatique qui ont pour rôle de trouver les vulnérabilités de Windows ;
- **Les chapeaux noirs** ou black hat : créateurs de virus, cyber-espions, cyber-terroristes ou cyber-escrocs, agissant la plupart du temps hors-la-loi dans le but soit de nuire, de faire du profit ou d'obtenir des informations. Ces hackers n'ont pas la même éthique que les white hats et sont souvent malveillants. Les plus malveillants sont alors appelés crashers ;
- **Les chapeaux gris** ou grey hat : s'ils n'hésitent pas à pénétrer dans les systèmes sans y être autorisés, ils n'ont pas de mauvaises intentions. C'est souvent « l'exploit informatique » qui les motive, une façon de faire la preuve de leur agilité. Cette catégorie recouvre le large panel de personnes se situant entre le black hat et le white hat. Cela dit, le fait de ne pas obtenir d'autorisation préalable rend l'acte illégal ;

- **Les script kiddies** ou lamer, littéralement « gamins qui utilisent des scripts » : sans grande compétence, ceux-ci piratent en utilisant des programmes codés par d'autres. Ces personnes ne sont pas à proprement parler des hackers, mais elles peuvent se considérer comme tels ;
- **Les hacktivistes** : agissant afin de défendre une cause, ils peuvent transgresser la loi pour attaquer des organisations afin de les paralyser ou d'obtenir des informations, ainsi qu'attaquer des plateformes gouvernementales dans le cadre de conflits en cours ou passés. [2]

IV. Malveillance informatique

Parmi les multiples procèdes d'attaques contre le système d'information, il convient de réserver une place spéciale à une famille de logiciel malveillant (les anglophones ont créé à leur intention le néologisme malware), qui se répondent en générale par le réseau, soit par accès direct à l'ordinateur attaqué, soit cachés dans un courriel ou sur un site web attrayant. Mais aussi éventuellement par l'intermédiaire d'une clé USB ou d'un CD-Rom. la destination de ces logiciels est de s'installer sur l'ordinateur dont ils auront réussi à violer les protections, pour y commettre des méfaits, et aussi pour se propager vers d'autres victimes.

IV.1. Logiciels malveillants

IV.1.1. Les Virus

Un virus est un programme qui se réplique lui-même. Il se dissémine en se copiant lui-même sur l'ordinateur ou en insérant du code informatique dans les fichiers programmes ou les fichiers du système d'exploitation. Les virus n'endommagent pas toujours les fichiers ou les ordinateurs, mais ils affectent souvent les performances et la stabilité de l'ordinateur.

A des degrés divers, un virus peut entraîner un ralentissement de l'ordinateur, mais aussi détruire données et programmes. Dans le pire des cas, les virus suppriment ou modifient les données et les programmes de votre ordinateur. Certains virus transmis par courrier électronique envoient des messages contenant des informations confidentielles lorsqu'ils se propagent. Même lorsqu'un virus n'endommage pas directement des informations, le processus de réplication peut ralentir notre ordinateur et notre connexion Internet.

IV.1.2. Les Vers

Un ver est un code autonome particulièrement dangereux, qui se réplique et propage sans aucune action de la part de l'utilisateur. La plupart des vers se cachent dans les pièces jointes du courrier électronique et contaminent l'ordinateur dès leur ouverture.

Le ver recherche dans l'ordinateur infecté des fichiers tels que des carnets d'adresses ou des pages Web temporaires contenant des adresses électroniques. Il utilise ces adresses pour envoyer des messages électroniques infectés et, souvent, il imite l'adresse (ou usurpe l'identité) des expéditeurs pour nous faire croire que les messages infectés proviennent d'une connaissance. Les vers se propagent ensuite automatiquement à travers les courriers électroniques, les réseaux ou les failles des systèmes d'exploitation, inondant souvent ces systèmes avant d'être détectés.

Les vers ne détruisent pas systématiquement le contenu des ordinateurs, en général, ils affaiblissent les performances et la stabilité des ordinateurs et des réseaux.

IV.1.3. Cheval de Troie

Un cheval de Troie est un logiciel malveillant qui se cache à l'intérieur des autres programmes. Il pénètre dans l'ordinateur caché dans un programme inoffensif, par exemple un écran de veille. Ensuite, il injecte du code dans le système d'exploitation, ce qui permet à un pirate informatique d'accéder à l'ordinateur infecté. En règle générale, les chevaux de Troie ne se propagent pas tous seuls, ils sont portés par des virus, des vers ou des logiciels téléchargés.

IV.1.4. Porte dérobée

Une porte dérobée (backdoor) est un logiciel de communication caché, installé par exemple par un virus ou par un Cheval de Troie, qui donne à un agresseur extérieur accès à l'ordinatrice victime par le réseau.

IV.1.5. Bombe logique

Une bombe logique est une fonction cachée dans un programme en apparence honnête, utile ou agréable, qui se déclenchera à retardement, lorsque sera atteinte une certaine date, ou

lorsque surviendra un certain événement. Cette fonction produira alors des actions non désirées, voire nuisibles.

IV.1.6. Logiciel espion

Un logiciel espion peut afficher des publicités, collecter des informations nous concernant ou modifier les paramètres de notre ordinateur, généralement sans notre consentement explicite. Par exemple, il peut installer des barres d'outils, des liens ou des favoris non souhaités dans notre navigateur Web, modifier notre page d'accueil par défaut ou afficher fréquemment des fenêtres publicitaires.

Avec certains logiciels espions, aucun symptôme ne permet de détecter leur présence, ce qui ne les empêche pas de collecter en secret des informations sensibles, tels que les sites Web qu'on visite ou le texte qu'on tape. La plupart des logiciels espions sont installés en même temps que les logiciels gratuits qu'on télécharge, mais dans certains cas, une simple visite sur un site Web peut entraîner une infection par un logiciel espion.

IV.2. Courrier électronique non sollicité (spam)

Le spam, courriel indésirable ou pourriel : est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

Le spam par courrier électronique est le type de spam le plus répandu. Le coût d'envoi d'un courrier électronique étant négligeable, il est facile d'envoyer un message à des millions de destinataires. Les destinataires assument le coût de réception et de stockage en boîte aux lettres, ce qui peut causer des coûts non négligeables aux prestataires de services, à cause du volume pris par le spam qui est considérable.

IV.3. Injection SQL [3]

La faille SQLi, abréviation de « SQL Injection », est un groupe de méthodes d'exploitation de faille de sécurité d'une application interagissant avec une base de données. Elle permet d'injecter dans la requête SQL en cours un morceau de requête non prévu par le système et pouvant en compromettre la sécurité. Il existe plusieurs types d'injection SQL :

- La méthode « **blind based**» , qui permet de détourner la requête SQL en cours sur le système, et d'injecter des morceaux qui vont retourner caractère par caractère ce que l'attaquant cherche à extraire de la base de données. La méthode **blind based** se base sur la réponse du serveur : si la requête d'origine renvoie bien le même résultat qu'à l'origine (et indique donc que le caractère est valide) ou ne renvoie pas le même résultat (et indique donc que le caractère testé n'est pas le bon) ;
- La méthode « **error based** », qui permet de détourner la requête SQL en cours sur le système et d'injecter des morceaux qui vont retourner champ par champ ce que l'on cherche à extraire de la base de données. Cette méthode profite d'une faiblesse des systèmes de base de données permettant de détourner un message d'erreur généré par le système de base de données , et préalablement volontairement provoquée par l'**injection SQL** pour lui faire retourner une valeur précise récupérée en base de données ;
- La méthode « **union based** », qui permet de détourner la requête SQL en cours sur le système et d'injecter des morceaux qui vont retourner un ensemble de données directement extraites de la base de données. Cette méthode profite de certaines méthodes afin de détourner entièrement le retour de la requête SQL d'origine afin de lui faire retourner en une seule requête un important volume de données, directement récupéré en base de données ;
- la méthode « **Stacked queries** », la plus dangereuse de toutes. Profitant d'une erreur de configuration du serveur de base de données, cette méthode permet d'exécuter n'importe quelle requête SQL sur le système ciblé, ce qui ne se limite pas seulement à récupérer des données comme les trois précédentes. En effet, quand ce type de requête n'est pas désactivé, il suffit d'injecter une autre requête SQL, et elle sera exécutée sans problème, qu'elle aille chercher des données, ou en modifier directement dans la base de données.

V. Les attaques réseau

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système. Les attaques réseau peuvent être classées comme suit :

V.1. Attaques permettent de dévoiler le réseau

Ont pour objectif de découvrir les artères du réseau (le routage), les machines présentes dans un réseau, les ports ouverts sur un serveur et toutes autres informations pertinentes pour mener une attaque contre un réseau cible.

1. Attaques par cartographie du réseau

Elles permettent de découvrir les artères de communication d'un futur système cible, en utilisant traceroute par exemple. Traceroute utilise l'option TTL du paquet IP pour émettre un message *ICMP time_exceeded* pour chaque routeur qu'il traverse.

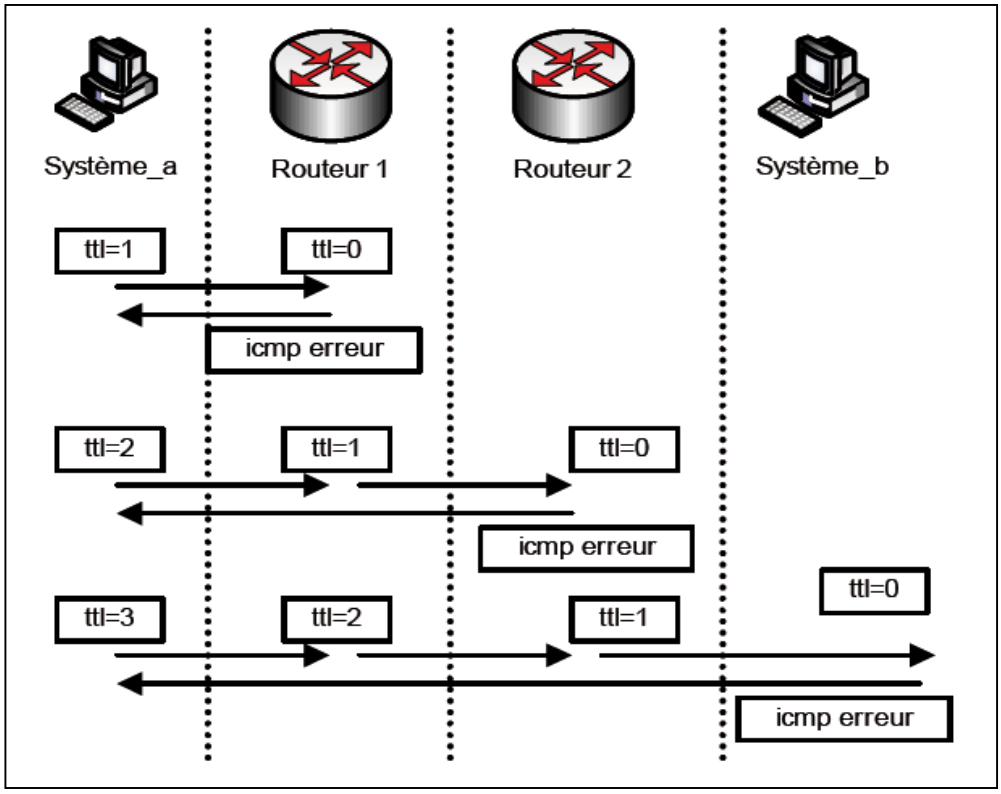

Figure I.2 : Fonctionnement de l'outil Traceroute .

2. Attaque par balayage TCP

Le client envoie une requête *TCP SYN* vers une adresse IP et *Num Port*, s'il reçoit une réponse *SYN/ACK* alors une application écoute sur le port S'il reçoit *RST*, ceci signifie qu'aucune application n'utilise ce port.

La figure suivante illustre une attaque par balayage TCP :

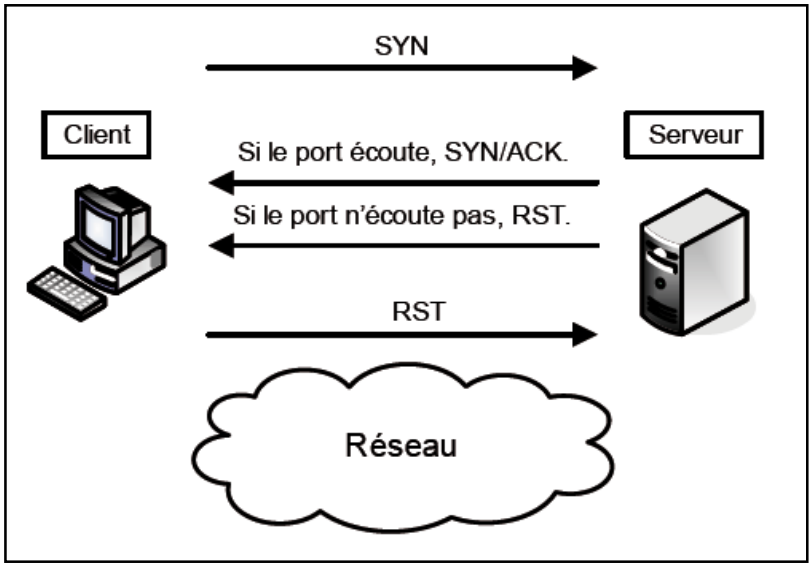

Figure I.3 : Le balayage TCP

V.2. Attaques permettant d'écouter le trafic réseau

Cette technique est utilisée pour écouter des informations sensibles comme des mots de passe.

1. Attaque par Sniffing

Dans un réseau fonctionnant en mode broadcast (le cas d'Ethernet) le flux atteint toutes les cartes réseau connectées au réseau. En temps normal, seules les trames destinées à la machine sont lues, les autres étant ignorées Grâce à une table d'écoute (sniffer) il est possible d'intercepter les trames reçues par la carte réseau.

Un sniffer comme Ethereal ou WinDump/TCPDump ou Wireshark, permet de récupérer tous les paquets IP et analyser leur contenu, qui peut être un paquet TCP contenant un paquet HTTP renfermant des données HTML.

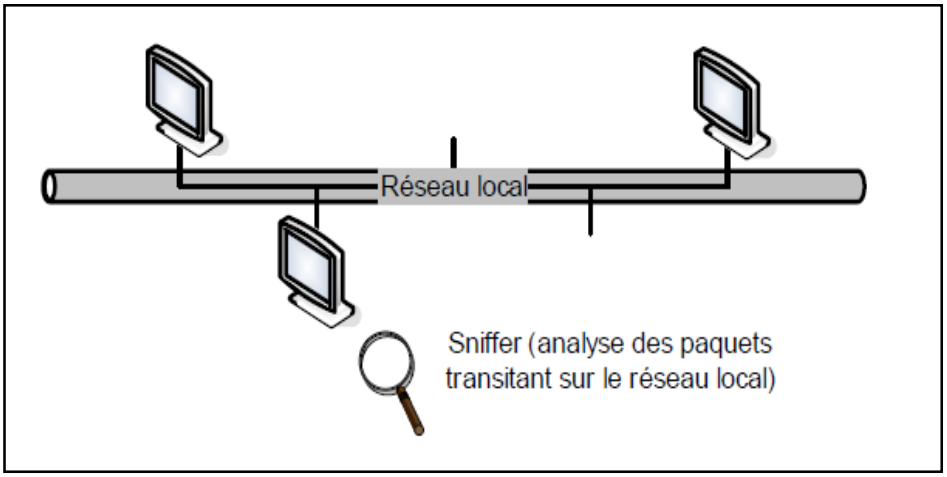

Figure I.4 : Attaque par Sniffing

2. Attaque de commutateur [3]

Le commutateur (switch) a pour fonction de permettre la cohabitation de différents sous réseaux physiques, qui ne communiquent pas nécessairement entre eux, sur le même équipement.

Pour atteindre cet objectif, le principe du VLAN (Virtual LAN) a été développé. À la base, un port du commutateur est assigné à un VLAN particulier, et seuls les ports du même VLAN peuvent s'échanger de l'information. Dans le but d'améliorer le confort pour l'administrateur et la qualité de service (redondance, etc.), des fonctionnalités supplémentaires ont vu le jour, avec leurs faiblesses. Ainsi, une attaque ARP spoofing peut permettre à une machine de recevoir des données qu'elle n'est pas censée recevoir.

Le protocole IEEE 802.1q a pour fonction principale de permettre à des commutateurs de s'échanger des données entre des VLAN partagés par plusieurs commutateurs. Certaines faiblesses de ce protocole sont cependant exploitables par quiconque est susceptible d'initier et de générer du trafic 802.1q avec le commutateur (ce qui constitue techniquement une faiblesse de configuration).

Par exemple, la technique dite du saut de VLAN (VLAN hopping) consiste pour le pirate à envoyer vers son port des paquets 802.1q ou ISL (Inter Switch Link) afin qu'il devienne un

port « trunk », port utilisé par les commutateurs pour partager des VLAN. C'est ce qu'illustre la figure suivante :

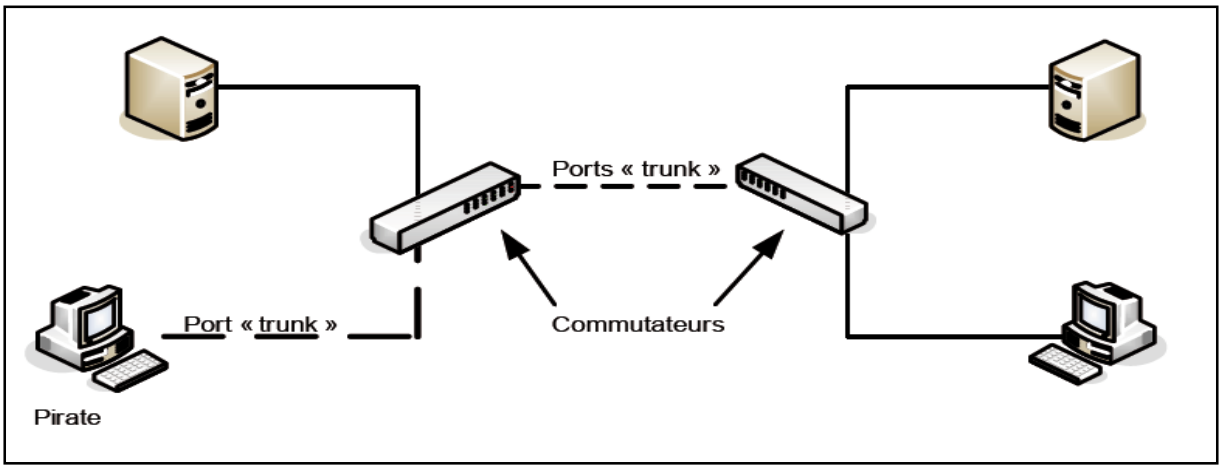

Figure I.5 : L'attaque VLAN Hopping

V.3. Attaques d'interférence avec une session réseau

1. ARP Spoofing

ARP (Address Resolution Protocol) permet de faire la correspondance entre une adresse IP et MAC afin de communiquer avec les systèmes voisins.

La faiblesse d'authentification de ARP permet à un système pirate d'envoyer des paquets ARP réponse au système cible indiquant que la nouvelle adresse MAC correspondant à l'adresse IP d'une passerelle est la sienne. Le Pirate reçoit donc tout le traffic à destination de la passerelle. Il lui suffit d'écouter ou de modifier massivement le traffic et de router ensuite les paquets vers leur véritable destination.

2. IP Spoofing

L'attaque IP spoofing consiste à se faire passer par un autre système en falsifiant son adresse IP. Le pirate commence par choisir le système qu'il veut attaquer. Après avoir obtenu le maximum de détails sur ce système cible, il détermine les systèmes ou adresses IP autorisés à se connecter au système cible.

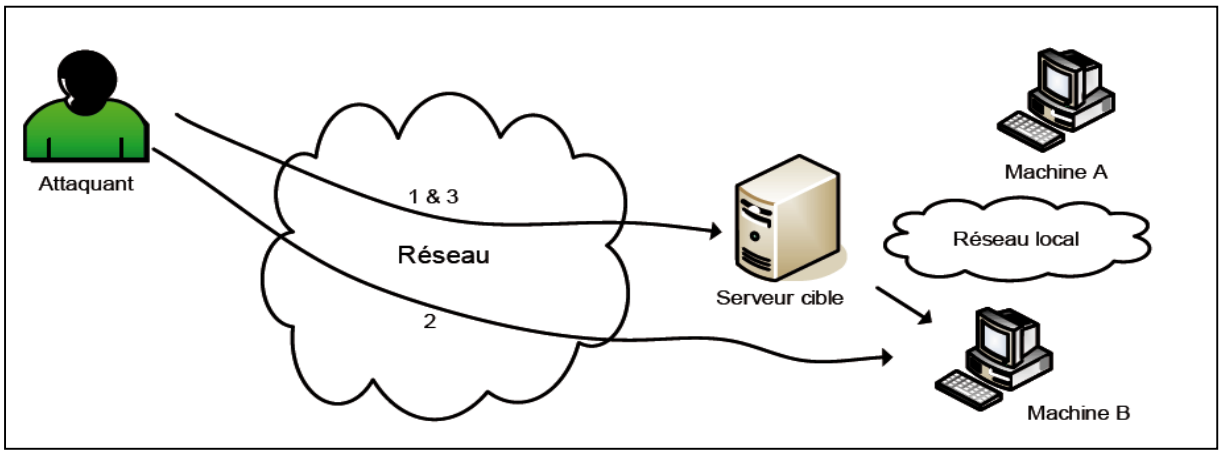

Figure I.6 : l'attaque IP Spoofing

V.4. Attaques de Déni de Service

1. Attaque Smurf

Pour attaquer une cible, le pirate inscrit l'adresse de la cible comme adresse source d'un ICMP echo request qu'il envoie à une destination (pour amplifier l'attaque, le pirate envoie la requête à une adresse de diffusion). La figure suivante illustre une telle attaque.

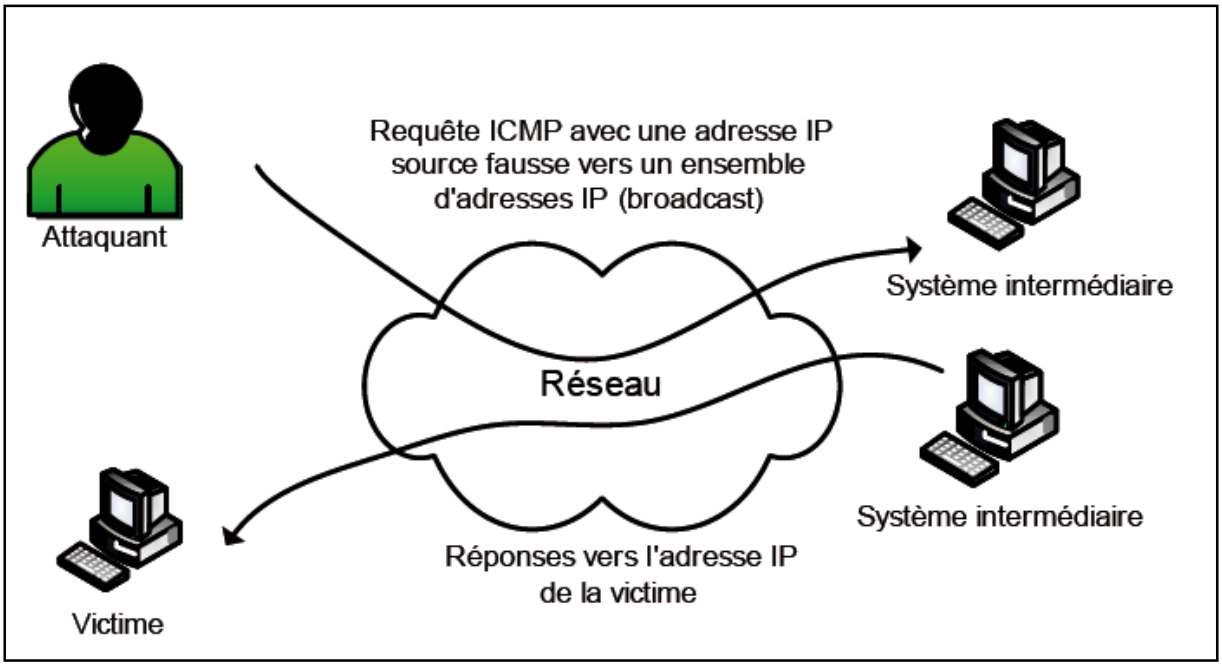

Figure I.7 : Attaque Smurf

2. Attaques par déni de service distribué (DDoS)

Le DDoS consiste à avoir à ses ordres un grand nombre de machines qui vont simultanément attaquer une seule cible.

Le pirate profite d'une vulnérabilité dans le logiciel d'un nombre important de machines pour y installer un client qui s'exécute d'une manière cachée sur les machines infectées. Les machines compromises sont appelées les « bots » (robots) ou des zombies. Ils ne communiquent pas directement avec le Pirate, ils se connectent à un serveur sur lequel se connecte aussi le Pirate (Serveur Chat, P2P, Twitter, ...) pour faire communiquer les bots et bostmaster afin de recevoir l'ordre d'attaques. La figure suivante illustre une telle attaque :

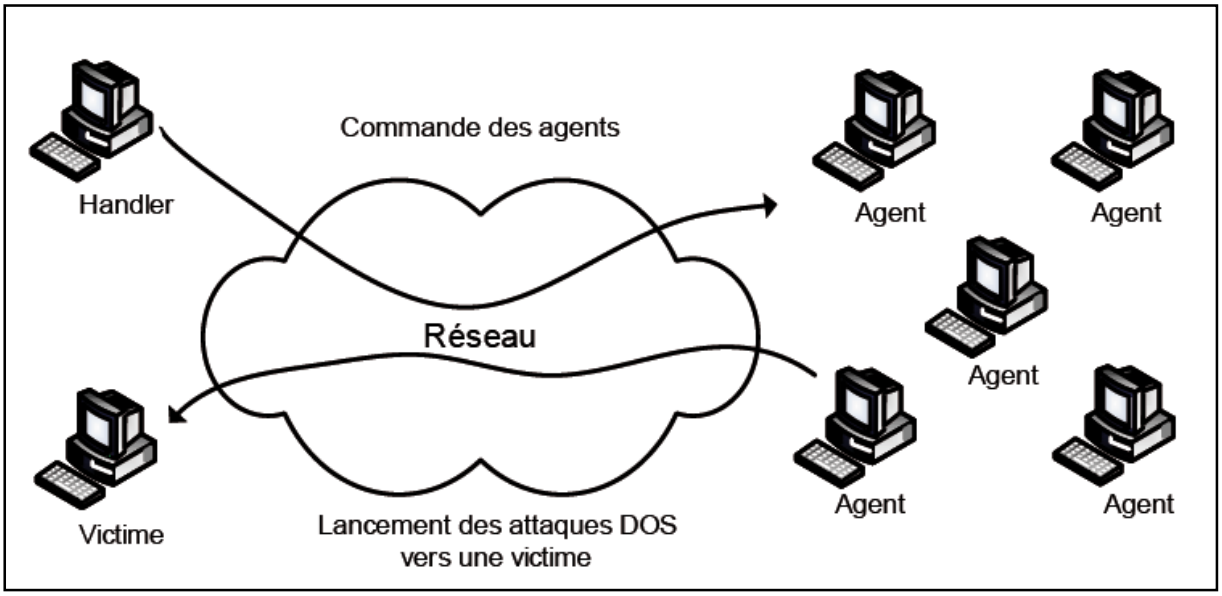

Figure I.8 : Attaques par déni de service distribué

V.5. Attaques de modification du routage réseau

Les protocoles de routage ont pour rôle de maintenir des tables de routage Pour cela, les routeurs s'échangent périodiquement des informations de routage (état de liens, coût de routes, etc.).

Toute attaque du routage peut impacter la disponibilité du réseau ou permettre le détournement du trafic à des fins de vol d'information. Il existe plusieurs attaques selon le protocole de routage utilisé. Parmi ces attaques, on peut citer :

- **Black hole:** un routeur qui annonce des routes qui ne lui appartiennent pas ou avec un coût minimal . Ceci permet l'attraction de tout le trafic vers cette destination ;

- **Man in the middle :** annonce de routes attrayantes pour faire passer le trafic par le pirate, puis le router vers la vrai destination ;

- **Numéro de séquence maximal :** dans OSPFv2 le **num seq** est utilisé pour détecter les annonces obsolètes ou doubles. Un **num seq** plus grand est favorisé. Un pirate qui fait une annonce (LSA) avec **num seq** maximal provoque l'ajustement du routage.

V.6. Attaques permettant d'utiliser des accès distants Wi-Fi

1. Attaque par modification de paquet

WEP qui est un Protocole pour sécuriser les réseaux sans fil de type Wi-Fi, utilise un checksum pour s'assurer de l'intégrité d'un paquet. Cependant, WEP utilisant une fonction linéaire pour calculer ce checksum, il est possible de modifier le contenu d'un paquet (et de son checksum) sans aucune détection possible de la part du récepteur.

Cette attaque est également connue sous le nom de Bit Flipping Attack, une variante consistant simplement à déplacer les bits.

2. Attaque par redirection d'adresse IP

Cette attaque nécessite que le point d'accès permette l'accès au réseau Internet, ce qui est fréquemment le cas. Elle suppose en outre que le pirate contrôle un ordinateur sur Internet. La séquence des événements est la suivante :

1. Le pirate modifie l'intégrité d'un paquet en remplaçant l'adresse IP destination par l'adresse de l'équipement qu'il contrôle. Il s'appuie pour cela sur un paquet capturé et la méthode dite du « bit flipping » ;
2. Il garde une copie du paquet chiffré ;
3. Le paquet est déchiffré par le point d'accès puis envoyé en clair sur le réseau vers l'adresse IP destination (donc l'ordinateur sous contrôle du pirate), laquelle reçoit la version en clair du paquet de données ;
4. Le pirate récupère cette version en clair .

Le pirate possédant la version chiffrée et déchiffrée du paquet, il peut commencer une attaque de type « texte déchiffré connu » pour trouver la clé WEP.

VI. Protection des accès réseau

VI.1. Contrôler les connections réseau

Tout accès d'un réseau externe à un réseau d'entreprise doit faire l'objet d'un contrôle d'accès afin de ne laisser passer que le trafic autorisé. L'objectif d'un tel contrôle est à la fois de créer un périmètre de sécurité, de limiter le nombre de points d'accès afin de faciliter la gestion de la sécurité, mais aussi de disposer de traces systèmes en cas d'incident de sécurité.

De manière plus générale, l'interconnexion entre deux réseaux de niveau de sécurité différent : l'interconnexion du réseau d'entreprise à internet, par exemple, doit faire l'objet d'un contrôle d'accès spécifique.

VI.2. le pare-feu

VI.2. 1. Définition

Un pare-feu est un logiciel ou un matériel qui vérifie les informations provenant d'Internet ou d'un réseau, puis les empêche d'accéder à l'ordinateur ou les y autorise, selon nos paramètres de pare-feu définis.

Lorsque des données sont envoyées ou reçues d'un ordinateur à un autre via Internet, les informations entrent et sortent par des portes virtuelles appelées « ports ». Chaque ordinateur dispose de 65 536 ports.

Ces « entrées » sont autant de possibilités pour pénétrer le système d'information de l'entreprise. Si bien qu'en l'absence de pare-feu, des pirates informatiques ont tout loisir d'infecter ou de détruire les données d'un ordinateur (virus, vers) ou de récupérer des informations via un cheval de Troie.

Un pare-feu joue un rôle de douanier vis-à-vis des ports : il contrôle les flux de données entrant et sortant de l'ordinateur ou du réseau de l'entreprise.

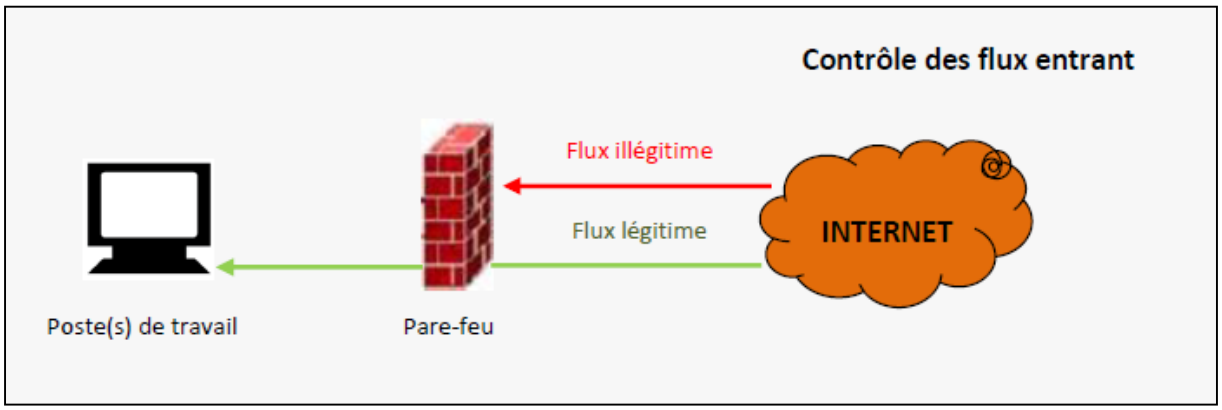

Figure I.9 : Contrôle des flux de données entrant

Les flux illégitimes depuis l'extérieur sont bloqués. Un tiers malveillant ne peut atteindre la porte dérobée, installée sur l'ordinateur par un cheval de Troie.

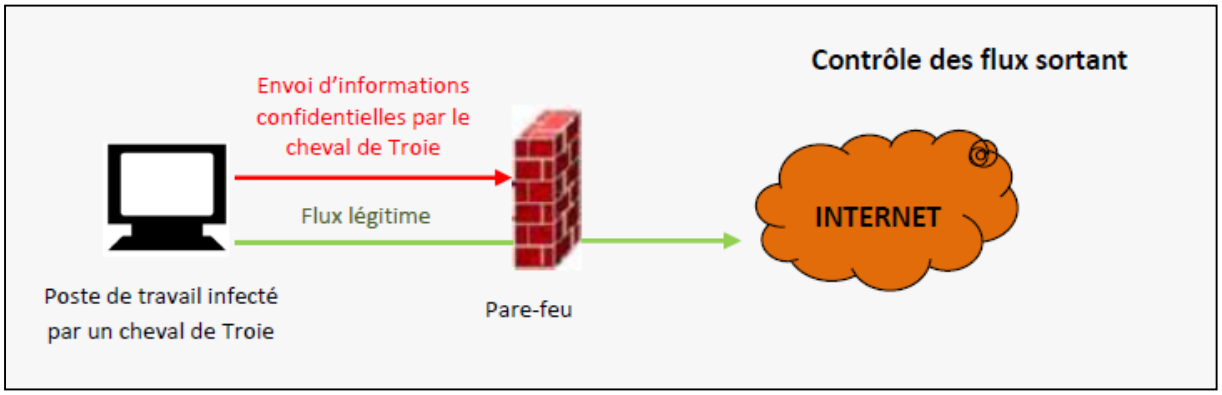

Figure I.10 : Contrôle des flux de données sortant

VI.2. 2. Catégories de pare-feu [4]

Il existe principalement deux catégories de pare-feu :

- **Les pare-feu personnels** : sont des logiciels installés sur des postes informatiques. Ils contrôlent uniquement les flux entrant et sortant des ordinateurs sur lesquels ils sont installés. Ce type de firewall est également utilisé par les particuliers. Windows en comporte un, par défaut.

- **Les pare-feu « réseau »** : se matérialisent généralement sous forme de boîtier. Ce type de firewall est souvent placé entre un accès externe et un réseau d'entreprise afin de protéger ce dernier des différentes menaces d'Internet.

VI.2. 3. Le filtrage

Les flux de données circulent par blocs de données appelés « paquets ». Un firewall analyse chacun de ces paquets sur la base d'un certain nombre de caractéristiques :

- L'adresse IP de l'émetteur du flux ;
- L'adresse IP du récepteur du flux ;
- Le type de transport de données ou protocole (IP, UDC, TCP ou ICMP) ;
- Le service (imprimante partagée par exemple) ou port demandé.

Lors de la configuration du pare-feu, un certain nombre de règles vont être définies à partir de ces caractéristiques. Chaque règle va, soit accepter explicitement certains flux (**accepté**), soit refuser explicitement certains flux (**refusé**).

VI.3. SHH (Secure Shell)

La commande SSH est une version sécurisée de RSH (Remote Shell) et rlogin. Elle se situe au niveau de la couche application du modèle OSI et permet d'obtenir un interprète de commande (Shell) distant sécurisé avec un système cible donné.

Le protocole SSH s'insère entre les couches applicatives et les couches réseau TCP afin d'offrir ces services de sécurité. Il reste possible de ne pas utiliser le protocole SSH. Les couches applicatives se connectent alors directement à la couche réseau TCP.

VI.4. les réseaux privés virtuels (VPN)

Un VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers de réseaux peu sûrs comme peut l'être le réseau internet. Cette technologie, de plus en plus utilisée dans les entreprises, permet de créer une liaison virtuelle entre deux réseaux physiques distants de manière transparente pour les utilisateurs concernés. Les données

envoyées au travers de ces liaisons virtuelles sont chiffrées, ceci garantit aux utilisateurs d'un VPN qu'en cas d'interception malveillante les données soient illisibles.

VI.5. Antivirus

L'antivirus sont des programmes capables de détecter la présence de virus sur un Ordinateur, ainsi que de nettoyer celui-ci dans la mesure du possible si jamais un ou des virus sont trouvés. Nettoyer signifie supprimer le virus du fichier sans l'endommager. Mais parfois, ce nettoyage simple n'est pas possible.

VII. Sécurité des équipements réseau

La protection des systèmes réseau concerne à la fois la configuration des systèmes et les protocoles utilisés pour le routage et l'administration du réseau.

La sécurité d'un réseau repose avant tout sur la sécurité des équipements ou systèmes réseau qui le composent. Cette dernière concerne principalement les domaines suivants :

- **Sécurité physique :** il s'agit de la protection des équipements réseau face aux menaces de feu, d'inondation, de panne de courant, etc. des équipements de protection tels qu'extincteurs, onduleurs, etc., permettent de se protéger de ces menaces.

- **sécurité de système d'exploitation :** il s'agit de se prémunir des faiblesses de sécurité ou des bogues du système d'exploitation qui s'exécutent sur l'équipement réseau. Seuls des tests de non-régression et de sécurité permettent de détecter certaines de ces faiblesses.
- **Sécurité logique :** il s'agit de se prémunir des faiblesses de configuration de l'équipement ou du système réseau. Seuls des règles de configuration sécurisées permettent de se prémunir contre ce type d'erreur ;

La sécurité de système d'exploitation est difficile à maitriser, du fait que ce dernier est généralement propriétaire et que les sources ne sont pas disponibles. En revanche, la

sécurité physique et la sécurité logique des équipements réseau et des systèmes sont des axes majeurs de la politique de sécurité réseau.

VIII. Assurer la confidentialité des connexions

La confidentialité des informations transitant sur un réseau ne peut être assurée que par le chiffrement des données avant leur émission.

VIII.1. Algorithmes cryptographiques

La cryptographie est l'ensemble des techniques (algorithmes, matériels, logiciels) permettant de protéger une communication au moyen d'un code secret.

La cryptographie moderne repose sur des fondements mathématiques très solides et permettent de réaliser des crypto-systèmes difficiles à casser dans des délais raisonnables avec la technologie actuelle.

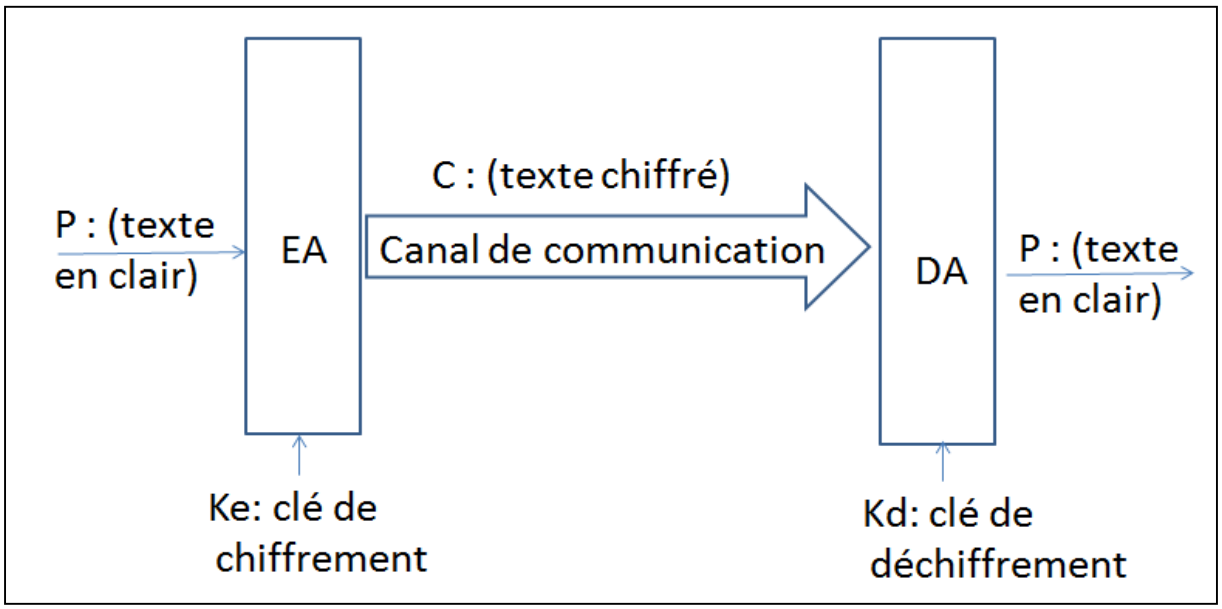

Figure I.11 : Principe de cryptographie

Les services fournis par la cryptographie sont :

1. **la confidentialité,** qui offre la garantie que seul le destinataire est capable de lire le message envoyé ;
2. **l 'authentification**, qui permet aux interlocuteurs d'une transaction de s'identifier avec certitude ;
3. **l'intégrité des données**, qui permet au destinataire de vérifier que le message reçu et le même que celui qui a été envoyé par la source ;
4. **la non répudiation des données,** qui interdit à l'émetteur d'un message de nier le fait d'avoir envoyé le dit message.

Les algorithmes cryptographiques peuvent être classés selon le type de clés en deux catégories :

- **Cryptage symétrique (à clé privée)**
  - La même clé est utilisée pour le cryptage et le décryptage ;
  - La clé doit rester secrète et être partagée par les deux interlocuteurs ;
  - Les algorithmes symétriques sont en général plus rapides ;
  - Les clés sont assez courtes ;
  - Toutefois, il faut une clé pour chaque communication bidirectionnelle (pour n utilisateurs il faut n (n-1)/2 clés différentes) ;
  - Problème de gestion des clés.

- **Cryptage asymétrique (à clé publique)**
  - La clé de chiffrement est différente de la clé de déchiffrement ;
  - La clé de chiffrement est publique, connue de tous, tandis que la clé de déchiffrement est privée, connue de son seul propriétaire ;
  - La gestion des clés est considérablement simplifiée. La clé de chiffrement publique est la seule qui doit être transmise. La clé secrète de déchiffrement reste au niveau de son propriétaire ;
  - Les algorithmes sont très longs et les clés doivent être longues également.

VIII.2. Les certificats numériques

Vérifier la signature numérique d'un document prouve seulement que ce dernier a été crypté avec la clé privée correspondant à la clé publique de décryptage. La signature numérique ne prouve pas que les clés (privées ou publiques) correspondent aux personnes qui les détiennent.

Un certificat numérique est un document qui prouve qu'un couple de clés privée-publique appartiennent à un individu (ou une entité) bien déterminé. Il est délivré par une autorité reconnue par tous les utilisateurs comme une autorité de confiance. Cette autorité est dite autorité de certification.

Un certificat numérique contient :

- Un numéro de série ;
- Le nom du détenteur ;
- La clé publique du détenteur ;
- Le nom de l'autorité qui a délivré le certificat ;
- La signature numérique de l'autorité ayant délivré le certificat ;
- D'autres informations personnelles ou commerciales.

VIII.3. fonctions de hachage

Les fonctions de hachages construisent une empreinte d'une chaine de données, à partir de laquelle il est impossible de revenir à la chaine de données initiale. La probabilité que deux chaines de données aient une empreinte identique est très faible.

Ces fonctions sont utilisées, par exemple, pour la vérification de l'intégrité des massages transmis. On crée pour cela une empreinte du message à transmettre, puis on transmet le message et l'empreinte. A la réception du message, on calcule l'empreinte du message reçue et on la compare à l'empreinte initiale. Si les deux empreintes correspondent, c'est que le message n'a pas pu être modifié.

IX. Protection de la gestion réseau

Par une bonne maitrise de la gestion réseau, il est possible de se prémunir de la plupart des problèmes de la sécurité réseau. Cela recouvre les services qui gravitent autour de la gestion du réseau, tels les services (routage, supervision, etc.) de résolution de noms de domaines, de synchronisation des horloges des équipements réseau, etc.

X. Conclusion

Les attaques réseau reposent sur un ensemble de faiblesses de sécurités touchant différentes domaines, toutefois, il y a des contres mesures de sécurité, des protocoles et applications qui permettent de contrecarrer les attaques des agresseurs, ou au moins, les limiter.

CHAPITRE II

Généralités sur les VLANs et les VACLs

I. Introduction

Ce chapitre présente des notions de bases sur les réseaux locaux virtuels ACL et les VACLs. Ainsi que leurs utilisations et configuration**.**

II. Réseau local

Un réseau local LAN (Local Area Network) est un réseau d'ordinateurs situés sur un même site.

Les communications sur ce type de réseau y sont généralement rapides et gratuites puisqu'elles ne passent pas par les services d'un opérateur de télécommunication. Le fait que le réseau soit sur un site bien délimité n'implique pas nécessairement qu'il soit de taille très réduite. **Il** est souhaitable de le segmenter en sous-réseaux quand le nombre de nœuds y devient important. L'ensemble reste un réseau local tant qu'il est indépendant des services d'un opérateur extérieur. **[2]**

III. Réseau local virtuel

III.1. Définition

Un Réseau Local Virtuel VLAN (Virtual Local Area Network) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

En effet, dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

III.2. Intérêts des VLANs

- **Augmentation des performances :** La segmentation créée par les VLANs réduit la taille des domaines de broadcast et de ce fait le nombre de collisions sur ces domaines. De plus, les VLANs se basent sur la commutation (et non le routage) pour segmenter les domaines de diffusion ce qui permet un traitement bien plus rapide ;

- **Réduction des coûts :** L'utilisation de VLANs permet de simplifier l'administration du réseau. l'utilisation des VLANs entraîne souvent la réduction du nombre de routeurs nécessaires, or les routeurs sont plus onéreux que les switches ;
- **Formation de groupes virtuels :** Il est courant de retrouver, dans les entreprises, des groupes de développement, de travail sur un projet spécifique, composés de membres qui viennent de différents départements.
  Ces groupes sont souvent formés pour un temps défini et à courte durée. Dans ce cas de figure, un VLAN pourrait être implémenté (sans avoir à déplacer les individus) pour les besoins ponctuels de ce groupe. Ce qui permet de créer des groupes de travail de manière transparente vis-à-vis de l'architecture physique du réseau ;
- **Gain de sécurité :** les groupes contenant des données sensibles sont séparés du réseau.

III.3. Types de VLANs [2]

Il existe trois types de VLANs :

1. VLAN de données

Un VLAN de données est un réseau local virtuel configuré pour transmettre le trafic généré par l'utilisateur. Un VLAN acheminant du trafic de voix ou de gestion ne peut pas faire partie d'un VLAN de données. Il est d'usage de séparer le trafic de voix et de gestion du trafic de données. Un VLAN de données est parfois appelé un VLAN utilisateur. Les VLAN de données sont utilisés pour diviser un réseau en groupes d'utilisateurs ou de périphériques.

2. VLAN par défaut

Le vlan par défaut pour les commutateurs Cisco est vlan1. Le vlan1 ne peut ni être renommé ni être supprimé. Par défaut, tout le trafic de contrôle de couche 2 est associé au vlan1.

3. VLAN natif

Les ports trunk sont les liaisons entre les commutateurs qui prennent en charge la transmission du trafic associée à plusieurs VLAN (trafic étiqueté), ainsi que le trafic qui ne provient pas d'un VLAN (trafic non étiqueté).

Les trames non étiquetées reçues sur le port trunk 802.1Q deviendront des membres du réseau local virtuel natif. Dans les commutateurs Cisco, le vlan natif est le vlan1.

III.4. Typologie de vlan

Pour attribuer un équipement à un réseau VLAN, Trois méthodes sont généralement utilisées :

- Les réseaux VLAN basés sur les ports ;
- Les réseaux VLAN basés sur les adresses MAC ;
- Les réseaux VLAN basés sur les protocoles.

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

1. VLAN niveau 1

Un VLAN de niveau 1 (aussi appelés VLAN par port, en anglais Port-Based VLAN) définit un réseau virtuel en fonction des ports de raccordement sur le Switch ou commutateur.

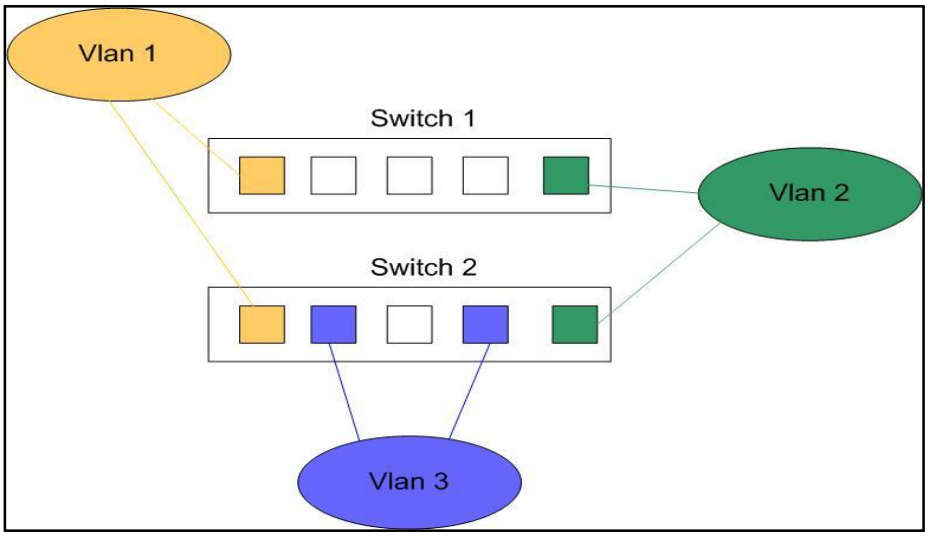

Figure II.1 : VLAN par port

Avantages :

- l'avantage principale du Vlan par port est qu'il permet une étanchéité maximale des Vlans. Une attaque extérieure ne pourra se faire qu'en branchant le PC pirate sur un port taggé. Le pirate a donc besoin d'avoir accès à la machine physique pour pénétrer le Vlan ;
- L'administrateur peut sans difficulté choisir les ports à tagger sans avoir d'information de la part des machines auxquelles sont reliés les ports.

Inconvénients :

- Le principal inconvénient du Vlan par port est qu'il nécessite une configuration lourde et contraignante sur chaque Switch. A chaque déplacement de poste, il faut modifier les Switchs correspondants pour maintenir une qualité de service ;

- Le mécanisme de Vlan par port ne possède pas d'architecture centralisée qui pourrait permettre d'éviter la lourdeur de la configuration. Chaque Switch possède sa table de correspondance indépendamment du contenu des autres Switchs.

2. VLAN niveau2

(Également appelé **VLAN MAC**, VLAN par adresse IEEE ou en anglais MAC Address-Based VLAN) consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station ;

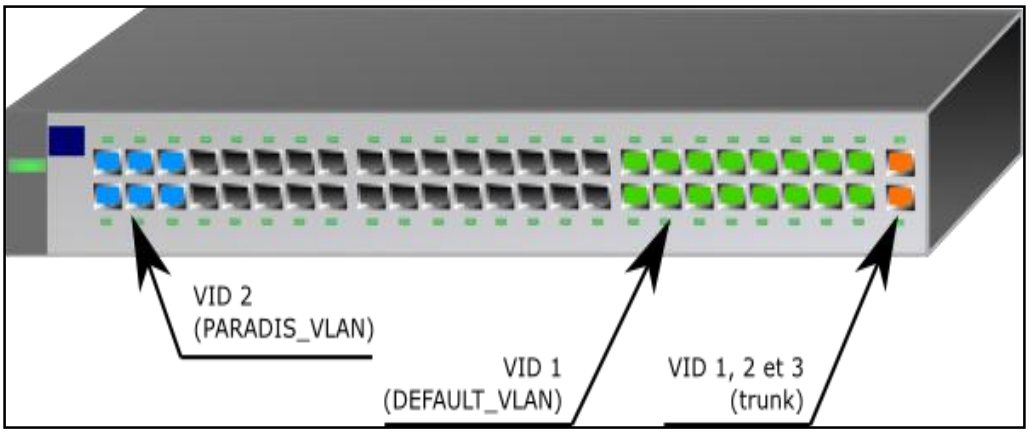

Figure II.2 : VLAN niveau 2

Avantages :

- Les Vlans de niveau 2 permettent une sécurité au niveau de l'adresse MAC, c'est à dire qu'un pirate souhaitant se connecter sur le Vlan devra au préalable récupérer une adresse MAC du Vlan pour pouvoir entrer ;

- Les Vlans de niveau 2 offrent des possibilités de centralisation des tables Vlans adresses MAC. Chaque Switch interroge ensuite cette table pour connaitre les informations nécessaires à une adresse MAC donnée.

Inconvénients :

- Le Vlan de niveau 2 offre une sécurité moindre que le Vlan par port de par la possibilité de spoofer l'adresse MAC. De plus, il n'y a pas de contrôle de flux prévu ce qui nécessite un bon dimensionnement du réseau.

3. VLAN niveau 3 (vlan par sous – réseaux)

Les Vlans de niveau 3 permettent de regrouper plusieurs machines suivant le sous réseau auquel elles appartiennent. La mise en place de Vlan de niveau 3 est conditionnée par l'utilisation d'un protocole routable (IP, autres protocoles propriétaires ...).

L'attribution des Vlans se fait de manière automatique en décapsulant le paquet jusqu'a l'adresse source. Cette adresse va déterminer à quel Vlan appartient la machine.

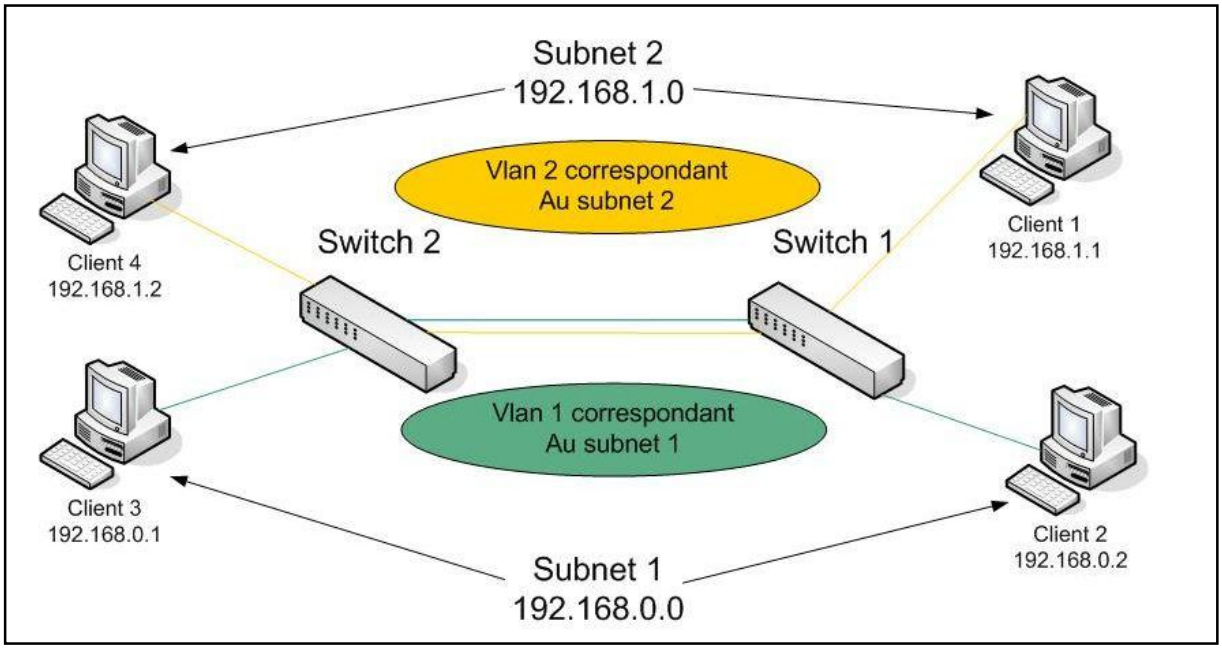

Figure II.3 : VLAN niveau 3

Avantages :

- L'avantage principal du Vlan de niveau 3 est qu'il permet une affectation automatique à un Vlan suivant une adresse IP. Par conséquent, il suffit de configurer les clients pour joindre les groupes souhaités. Il est aussi possible de séparer les protocoles par Vlan.

Inconvénients :

- Les Vlans de niveau 3 souffrent de lenteur par rapport aux Vlans de niveau 1 et 2. En effet, le switch est obligé de décapsuler le paquet j'jusqu'a l'adresse IP pour pouvoir détecter à quel Vlan il appartient.

- Les Vlans de niveau 3 sont restreints par l'utilisation d'un protocole de routage pour avoir l'identifiant niveau 3, et ainsi se joindre au Vlan correspondant.

III.5. Le routage inter VLAN

III.5. 1. Trunks

Les réseaux locaux sont distribués sur les différents équipements via des liaisons logiques dédiées appelées trunks. Le trunk est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels. Les trames qui traversent le trunk sont complétées avec un identificateur de réseau local virtuel (VLAN id). Grâce à cette identification, les trames sont conservées dans un même VLAN (ou domaine de diffusion).

Les trunks peuvent être utilisés :

- **Entre deux commutateurs :** C'est le mode de distribution des réseaux locaux le plus courant ;
- **Entre un commutateur et un hôte :** C'est le mode de fonctionnement à surveiller étroitement. Un hôte qui supporte le trunking a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels ;
- **Entre un commutateur et un routeur :** C'est le mode fonctionnement qui permet d'accéder aux fonctions de routage, donc à l'interconnexion des réseaux virtuels par routage inter-VLAN.

III.5.2. Le Protocol VTP

1. Présentation [8]

VTP ou VLAN Trunking Protocol est un protocole de niveau 2 utilisé pour configurer et administrer les VLAN sur les périphériques Cisco.

Au fur et à mesure que les réseaux s'agrandissent et gagnent en complexité, il devient essentiel de centraliser gestion de la structure des réseaux locaux virtuels. Le Protocol VTP est un protocole de messagerie de couche 2 qui fournit une méthode de distribution et de gestion de la base de données de réseau local virtuel à partir d'un serveur centralisé dans un segment de réseau. Les routeurs ne transmettent pas les mises à jour VTP.

Si un réseau d'entreprise comportant des contraintes de réseaux locaux virtuels n'est pas géré automatiquement, chaque réseau local virtuel doit être configure manuellement sur chaque commutateur. Toute modification apportée à la structure de réseau local virtuel requiert une configuration manuelle supplémentaire. Si un nombre n'est pas tapé correctement, des incohérences de connectivité peuvent se produire sur l'ensemble du réseau.

Pour résoudre ce problème, Cisco a créé le protocol VTP qui permet d'automatiser de nombreuses fonctions de configuration des réseaux locaux virtuels. Ce protocol garantit que la configuration est gérée de manière cohérente sur tout le réseau, et il réduit la tache de gestion et de surveillance des réseaux locaux virtuels.

Avec le protocol VTP, chaque commutateur annonce des messages sur ces ports agrégés. Ces messages incluent le domaine de gestion, le numéro de révision de la configuration, les réseaux locaux virtuels connus et les paramètres pour chaque réseau local virtuel. Ces trames d'annonce sont envoyées à une adresse de multidiffusion, de sorte que tous les périphériques voisins puissent recevoir les trames.

Chaque commutateur VTP enregistre une base de données de réseau local virtuel dans la mémoire vive non volatile qui comprend un numéro de version. Si un protocol VTP reçoit un message de mise a jour dont le numéro de version est supérieur à celui stocké dans la base de

données, le commutateur met à jour sa base de données de réseau local virtuel avec ces nouvelles informations.

Le numéro de version de la configuration VTP commence à zéro. A chaque changement effectué, ce numéro augmente d'un chiffre. Le numéro de version continue d'augmenter jusqu'à 2 147 483 648. Une fois ce numéro atteint, le compteur est remis à zéro. (Le redémarrage du commutateur réinitialise également le numéro de version).

Si un individu insère dans le réseau un commutateur présentant un numéro de version plus élevé sans auparavant redémarrer le commutateur un problème se produira avec le numéro de version. Les commutateurs étant par défaut des serveurs, des informations nouvelles, mais erronées, écrasent les informations de réseau privé virtuel légitimes sur tous les autres commutateurs.

Pour se protéger de cette situation critique, il suffit de configurer un mot de passe VTP pour valider le commutateur. Lors de l'ajout d'un nouveau commutateur sur un réseau existant, et redémarrer le commutateur immédiatement avant de l'ajouter au réseau, afin de réinitialiser le numéro de version. Par ailleurs, si vous ajoutez un commutateur à un réseau qui comporte déjà un commutateur serveur, vérifiez que le nouveau commutateur est configuré en mode client ou transparent.

2. Les modes VTP

Le switch possède 3 modes VTP : client, transparent ou server (actif par défaut) :

- **En mode client** : Il est associé à un domaine VTP. La déclaration des VLANs s'effectue sur le serveur. Il tient à jour la liste des VLANs déclarés et la diffuse à l'ensemble des clients ;
- **En mode transparent :** Il transmet les informations VTP aux autres switchs mais ne les traite pas. Ces switchs sont autonomes et ne participent pas aux VTP ;
  Il est associé à un domaine VTP. Il reçoit la liste des VLANs, il la propage aux autres clients auxquels il est connecté et met à jour sa propre liste.

- **En mode serveur :** il diffuse ses informations sur les VLAN à tous les autres switchs appartenant au même VTP domain. Ces informations sont stockés en NVRAM et sur un tel switch, il est possible de créer, modifier ou détruire un VLAN du VTP domain.

Il est associé à aucun domaine VTP. Sa liste de VLAN est locale et n'est pas mis à jour lorsqu'il reçoit une trame VTP. Cependant il propage les listes de VLAN qu'il reçoit.

3. Les messages VTP [8]

Les messages VTP se présente de diverses manières :

a) Annonces de type résumé

Les commutateurs émettent des annonces de type résumé toute les 5 minutes ou à chaque changement dans la base de données de réseau local virtuel. Les annonces de type résumé contiennent le nom de domaine VTP et le numéro de révision de la configuration ;

b) Annonce de type sous-ensemble

Une annonce de type sous-ensemble suit l'annonce de type résumé. Elle comprend une liste des informations du réseau local virtuel. Comprend les nouvelles informations de VLAN basées sur l'annonce de type résumé. Si plusieurs réseaux locaux virtuels sont présents, ils requièrent plusieurs annonces de type sous-ensemble ;

c) Requêtes d'annonces

Des clients VTP utilisent des demandes d'annonces pour obtenir des informations de réseau local virtuel. Les requêtes d'annonces sont requises si le commutateur a été réinitialisé ou si le nom de domaine a été modifié. Le commutateur reçoit une annonce de type résumé VTP dont le numéro de version de la configuration est supérieur au sien ;

4. La synchronisation

A chaque création, suppression ou modification de VLAN, une variable appelée RN (Revision Number) s'incrémente (initialement 0 puis 1 puis 2…). A chaque création, suppression ou modification de VLAN, le switch Server envoie un message VTP avec la nouvelle valeur du RN. Les autres switchs compare le RN reçu du switch Server avec le RN qu'ils stockent en local, si ce dernier est plus petit (logiquement) alors les switchs se synchronisent avec le Server et récupère la nouvelle base de données des VLANs.

Par défaut, le RN est envoyé automatiquement dès une création, suppression ou modification de VLAN puis envoyé toutes les 5 minutes.

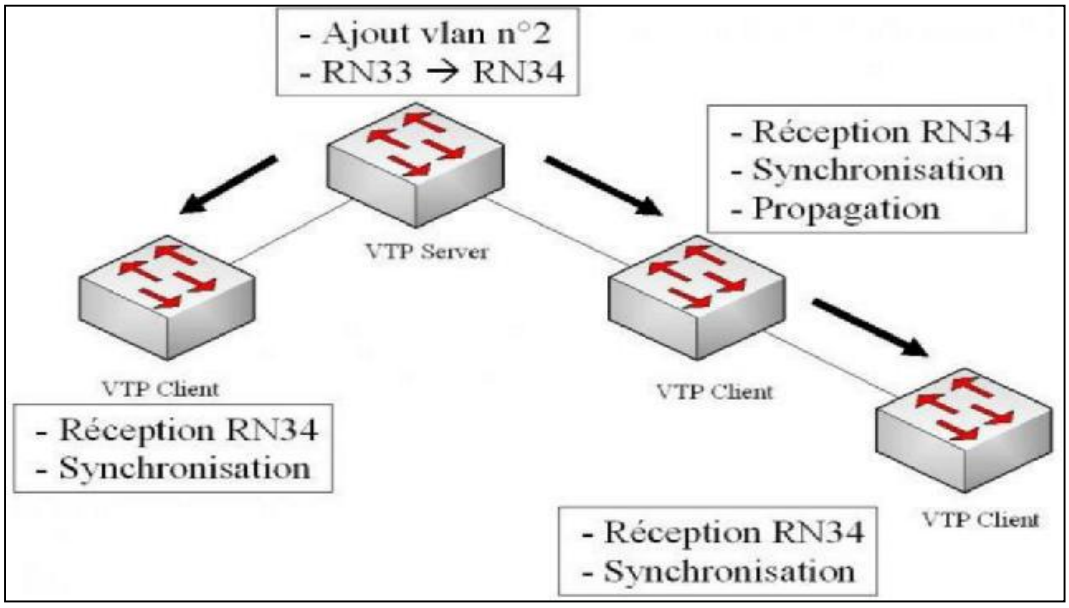

Figure II.4 : la synchronisation

5. Procédure de configuration

Pour configurer le protocole VTP sur un Switch Cisco, on suit les étapes suivantes :

- Configurer un domaine VTP qui permet à tous les switchs d'être dans le même « groupe » ;
- Configurer le mode VTP du Switch (Server, Client ou Transparent) ;
- Configurer un mot de passe pour sécuriser les messages VTP (Configuration optionnel).

VI. Les listes de contrôle d'accès « ACLs »

VI.1. Présentation

Les listes de contrôle d'accès sont des instructions qui expriment une liste de règles supplémentaires sur les paquets reçus et transmis par le routeur. Elles peuvent être utilisées pour implémenter la sécurité dans les routeurs.

Les listes de contrôle d'accès sont capables :

- d'autoriser ou d'interdire des paquets, que ce soit en entrée ou en sortie des interfaces
- Filtrer le traffic en entrée ou en sortie du routeur ;
- Restreinte l'utilisation à des personnes ou à des utilisateurs ;

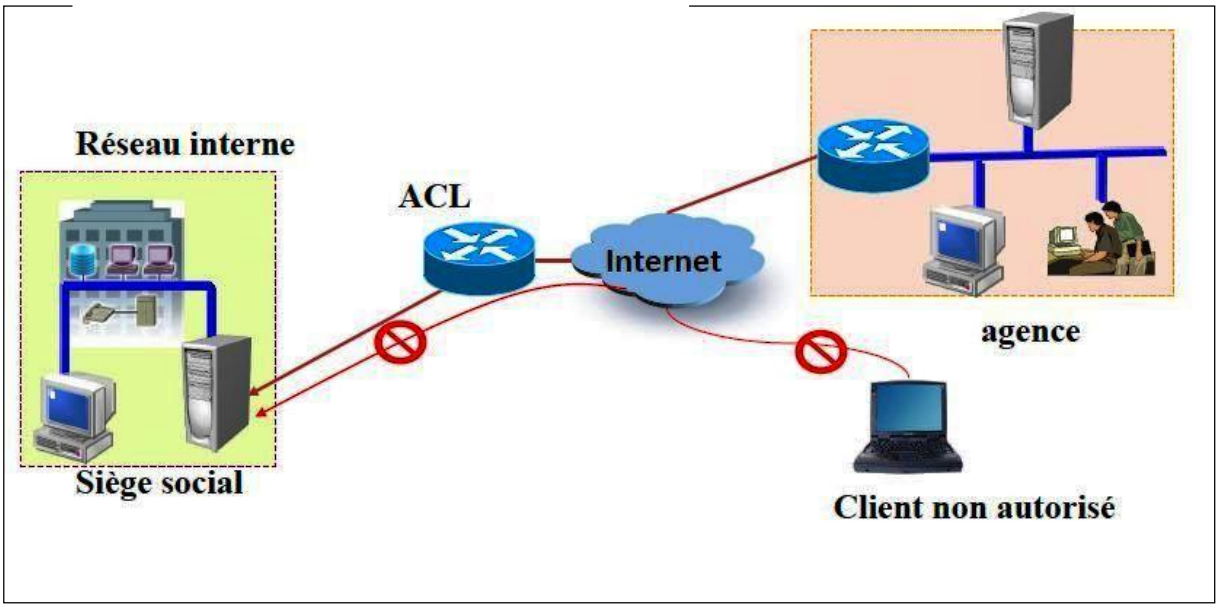

Figure II.5 : principe de fonctionnement des ACLs

Elles opèrent selon un ordre séquentiel et logique, en évaluant les paquets à partir du début de la liste d'instructions. Si le paquet répond au critère de la première instruction, il ignore le reste des règles et il est autorisé ou refusé.

L'ACL s'exécute dans la direction indiquée par le mot IN ou OUT. A un deny implicite à la fin. Aussi si le paquet ne satisfait à aucune règle il est rejeté.

VI.2. Nommage des ACLs

Les listes de contrôle d'accès nommées permettent d'identifier les listes de contrôle d'accès IP standards et étendues par des chaînes alphanumériques plutôt que par la représentation numérique actuelle.

On peut utiliser les listes de contrôle d'accès nommées dans les situations suivantes :

- Identifier intuitivement les listes de contrôle d'accès à l'aide d'un code alphanumérique.
- Configurer plusieurs ACL standard et plusieurs ACL étendues dans un routeur pour un protocole donné

VI.3. Numérotation des ACLs

Une liste de contrôle d'accès est identifiable par son numéro, attribué suivant le protocole et le type

```
Type de liste          Plage de numéros

     Listes d'accès IP standard 1 à 99 et 1300 à 1999
     Listes d'accès IP étendues 100 à 199 et 2000 à
  2699
     Listes d'accès Appletalk      600 à 699
     Listes d'accès IPX standard   800 à 899
     Listes d'accès IPX étendues   900 à 999
     Listes d'accès IPX SAP     1000 à 1099
```

Figure II.6 : classification des ACLs

VI.4. Types d'ACL

VI.4.1. ACL standard

Une ACL standard permet d'autoriser ou d'interdire des adresses spécifiques ou bien un ensemble d'adresses ou de protocoles, sachant que dans les instructions d'une ACL standard, on ne peut indiquer que les adresses sources.

Ce sont les ACLs les plus simples et, par conséquent, les moins gourmandes en ressources CPU. Elles sont par exemple utilisées pour autoriser ou interdire toute une plage d'adresse réseaux ou encore pour le filtrage des informations contenues dans des mises à jour de routage.

VI.4.2. ACL Etendue

Une ACL étendue permet de faire un filtrage plus précis qu'une ACL standard. En effet, une ACL étendue permet de filtrer en fonction de :

- Protocole utilisé (couche 3 et 4) ;
- Adresse source ;
- Adresse de destination ;

- Numéro de port.

VI.4.3. ACL nommée

Depuis la version 11.2 d'IOS, il est possible d'utiliser les ACLs nommées permettant l'identification par des chaines alphanumériques plutôt que par la représentation numérique actuelle. Une ACL nommée peut être de type standard ou étendue.

VI.5. Algorithme de vérification

Lorsque le routeur détermine s'il doit acheminer ou bloquer un paquet, la plate-forme logicielle **Cisco IOS** examine le paquet en fonction de chaque instruction de condition dans l'ordre dans lequel les instructions ont été créées.

Si le paquet arrivant à l'interface du routeur satisfait à une condition, il est autorisé ou refusé (suivant l'instruction) et les autres instructions ne sont pas vérifiées.

Si un paquet ne correspond à aucune instruction dans l'ACL, le paquet est jeté. Ceci est le résultat de l'instruction implicite **deny any** à la fin de chaque ACL.

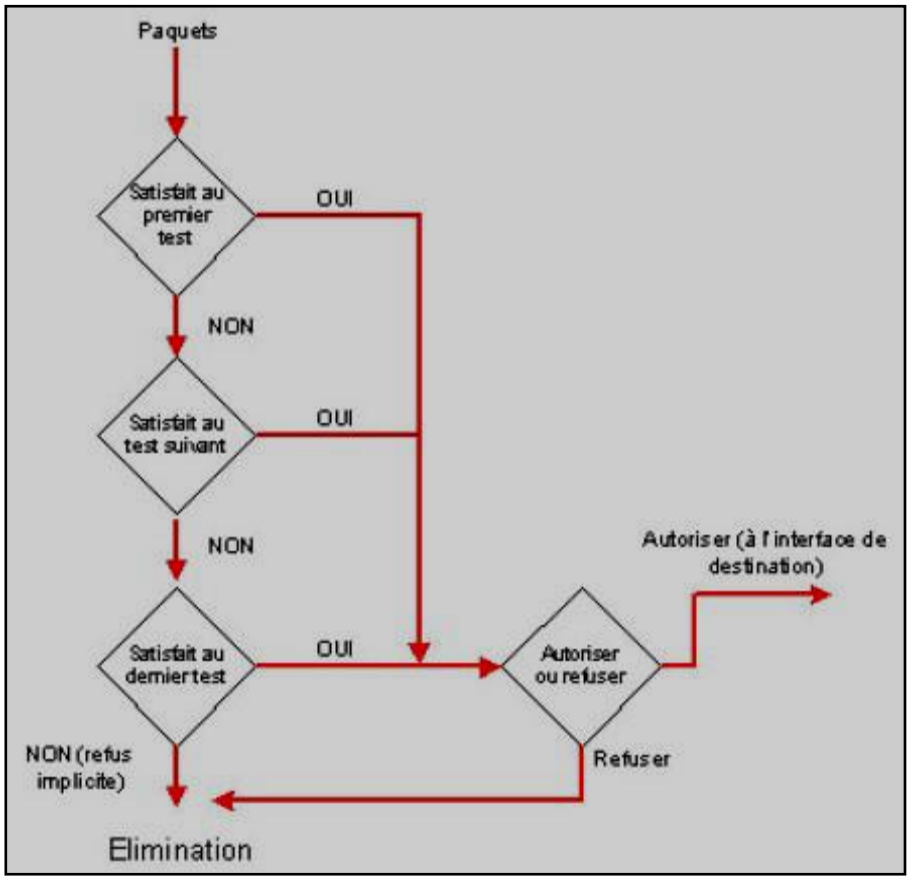

Figure II.7 : l'algorithme de vérification des ACLs

VI.6. Masque générique [7]

Un masque générique est une quantité de 32 bits divisés en quatre octets contenant chacun 8 bits.

- 0 signifie " vérifier la valeur du bit correspondant "
- 1 signifie " ne pas vérifier (ignorer) la valeur du bit correspondant "

Les listes de contrôle d'accès utilisent le masquage générique pour identifier une adresse unique ou plusieurs adresses dans le but d'effectuer des vérifications visant à accorder ou interdire l'accès.

Si le $X^{ième}$ bit est à 0 dans le masque, alors les $X^{ième}$ bits de l'adresse du paquet et de l'adresse de la liste doivent correspondre

Si le $X^{ième}$ bit est à 1 dans le masque, alors aucune correspondance n'est exigée entre les $X^{ième}$ bits de l'adresse du paquet et de l'adresse de la liste.

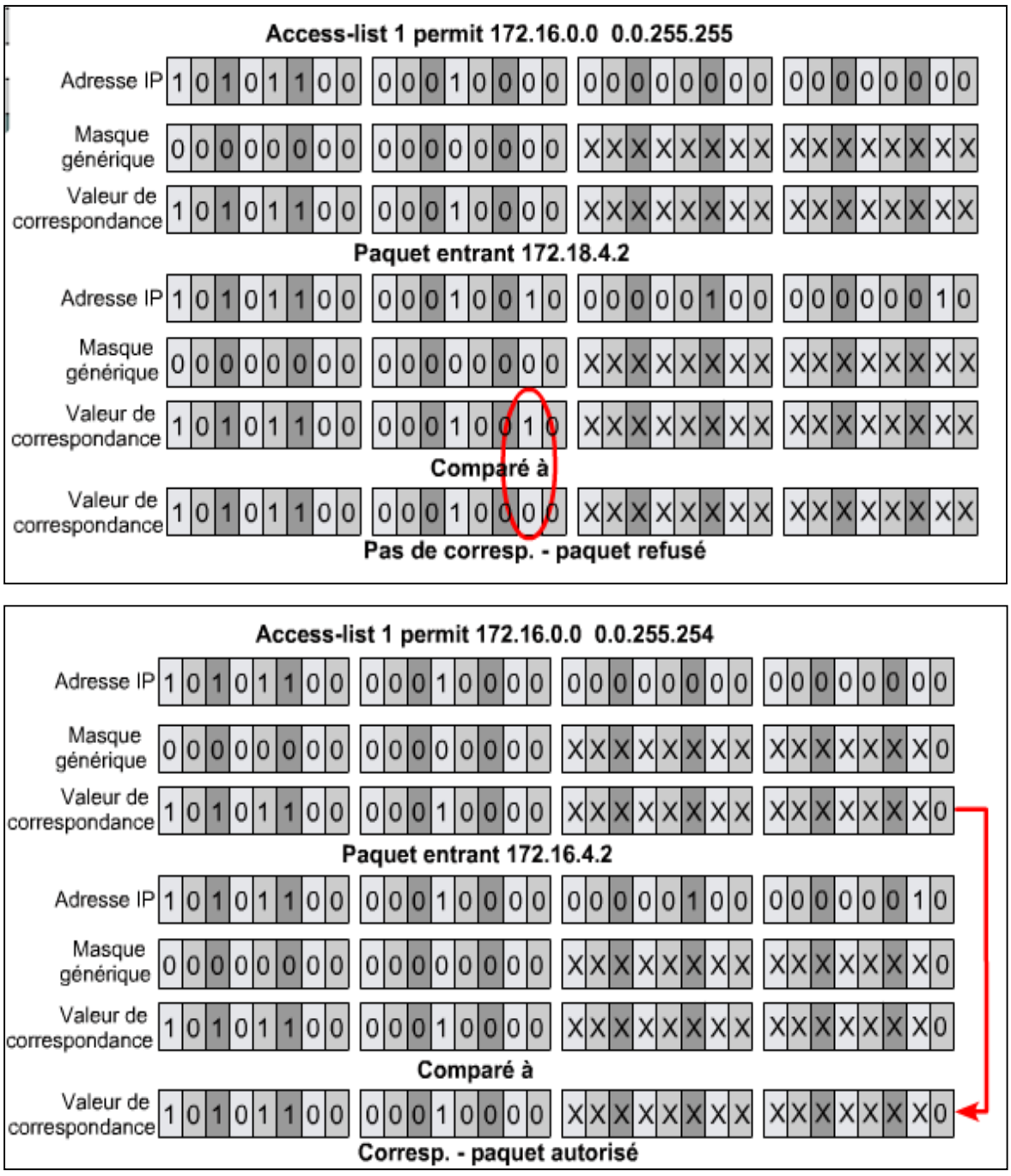

Figure II.8 : Application du masquage générique

VI.7. Configuration des ACLs

Les étapes pour la mise en œuvre des ACLs sont :

1. Création de l'ACL ;
2. Application de l'ACL sur une interface réseau.

VI.7.1. configuration des ACLs standards

Pour configurer une instruction pour une ACL standard pour IP, il faut utiliser la commande suivante dans le mode de configuration globale :

Access-list {numéro} {permit|deny} {préfixe} {masque générique} [log]

Access-list {numéro} {remark}] {commentaire}

- Si le masque générique n'est pas précisé, le masque générique par défaut 0.0.0.0 est utilisé ;
- **log** permet de garder en mémoire le nombre de paquets correspondant à l'instruction en cours ;
- Le mot clé **remark** suivi d'un commentaire permet d'indiquer l'utilité de l'instruction.

L'ordre de parcours des instructions dépend de l'ordre dans lequel on a configuré les instructions. Une nouvelle instruction est donc obligatoirement ajoutée à la fin de la liste, et il est impossible de supprimer une instruction particulière.

VI.7.2. configuration des ACLs étendues

Pour configurer une instruction pour une ACL étendue pour IP, il faut utiliser la commande suivante dans le mode de configuration globale.

Access-list {numéro} {permit|deny} {protocole} {préfixe source} {masque source}

[{opérateur} {opérande}] {préfixe destination} {masque destination}

[{opérateur} {opérande}] {icmp-type} [log] [established]

- **Protocole** peut être soit le nom (IP, TCP, UDP, ICMP, IGRP , etc.) soit le numéro du protocole (de 0 à 255).
- Le paramètre **established** ne peut être utilisé que pour le protocole TCP et permet de faire correspondre uniquement les sessions TCP déjà établies (drapeux ACK, FIN, PSH, RST, SYN ou URG).

- Le paramètre **icmp-type** ne peut être utilisé que pour le protocole ICMP, et correspond au nom ou au numéro du type de message ICM devant être vérifié.

Pour l'ordre de parcours ou la modification, les règles sont les mêmes qu'avec une ACL standard.

VI.7.3. Configuration des ACLs nommées

Pour configurer une instruction pour une ACL nommée pour IP, il faut utiliser la commande suivante dans le mode de configuration globale :

Ip access-list { standard|extended } {nom}

- Permet de créer une ACL nommée standard ou étendue ;
- Permet de passer dans le mode de configuration de l'ACL nommée.

{permit|deny} { stapréfixe} [masque] [log]

- Mode de configuration d'ACL nommée standard ;
- Les paramètres sont identiques que pour une ACL standard numérotée.

{permit|deny} {protocole} {préfixe source} {masque source} [{opérateur} {opérande}] {préfixe destination} {masque destination} [{opérateur} {opérande}] {icmp-type} [log] [established]

- Mode de configuration d'ACL nommée étendue ;
- Les paramètres sont identiques que pour une ACL étendue numérotée.

remark {commentaire}

- Mode de configuration d'ACL nommée (standard ou étendue) ;
- Fournit un commentaire pour indiquer l'utilité de l'ACL.

VI.7.4. Mise en place et vérification des ACLs

La création des ACLs étant faite, il faut maintenant les appliquer en utilisant les commandes suivantes :

- **Ip access-group {numéro|nom} {in|out}**
  - Mode de configuration d'interfaces ;
  - Applique une ACL sur l'interface pour filtrer le trafic entrant.

- **Ip access-class {numéro|nom} {in|out}**
  - Mode de configuration de ligne;
  - Applique une ACL sur la ligne pour filtrer les accès à cette dernière.

- **No access-list {numéro}**
  - Mode de configuration globale ;
  - Supprime complètement une ACL numérotée.

Les commandes suivantes servent à vérifier le placement des ACLs, ainsi que leurs instructions :

- **Show access-lists {numéro|nom}**
  - Affiche la liste des ACLs crées sur le routeur, leurs instructions ainsi que le nombre de correspondances pour chaque instruction.

- **Show ip interface[{type} {numéro}]**
  - Permet entre autres de voir quells sont les ACLs appliquées sur les interfaces et pour quelle direction.

VI.8. Avantages et inconvénients des ACLs

L'avantage principal des ACLs est donc de fournir une base de sécurité réseau en filtrant les trafics traversant un routeur.

Le principal inconvénient est malheureusement un traitement supplémentaire à effectuer pour chaque paquet entrant ou sortant du routeur, rallongeant ainsi à la latence réseau et à la surcharge CPU.

V. Les listes de contrôle d'accès virtuelles « VACLs »

V.1. Définition [6]

Les VLAN ACL (*pour VLAN Access Control List*) s'apparentent aux ACL de niveau trois c'est à dire aux ACL qui s'appliquent sur les interfaces routées. Mais comme leur nom l'indique, elles s'apposent dans des VLAN ou plus exactement à tous les paquets qui y entrent. Il est ainsi possible de limiter le trafic au sein même d'un VLAN.

Les VLAN ACL (ou VACL) sont définies dans la configuration par une suite de séquences numérotées. Chaque séquence comprend une identification du trafic à traiter et une action à lui administrer, le tout est ensuite appliqué au VLAN à protéger.

V.2. fonctionnement

Les VACLs peuvent fournir un contrôle d'accès pour tous les paquets qui sont reliés dans un VLAN ou qui sont acheminés vers ou hors d'un VLAN ou d'une interface WAN pour la capture de VACL. Contrairement aux ACLs classiques ou étendues de Cisco IOS configurées uniquement sur les interfaces de routeur et appliquées uniquement sur les paquets routés, les VACLs s'appliquent à tous les paquets et peuvent être appliqués à toute interface VLAN ou WAN. Les VACLs sont traitées en matériel. Les VACLs utilisent les ACLs Cisco IOS. Les VACLs ignorent les champs ACL Cisco IOS qui ne sont pas pris en charge par le matériel.

Lorsque on configure une VACL et qu'elle l'applique à un VLAN, tous les paquets entrant dans le VLAN sont vérifiés contre cette VACL. Si on applique une VACL au VLAN et une ACL à une interface routée dans le VLAN, un paquet entrant dans le VLAN est d'abord

vérifié contre le VACL et, s'il est autorisé, est ensuite vérifié contre l'ACL d'entrée avant qu'il soit traité par l'Interface routée. Lorsque le paquet est acheminé vers un autre VLAN, il est d'abord vérifié par rapport à l'ACL de sortie appliquée à l'interface routée et, si cela est autorisé, la VACL configurée pour le VLAN de destination est appliquée. Si une VACL est configurée pour un type de paquet et qu'un paquet de ce type ne correspond pas à la VACL, l'action par défaut est refusée.

V.3. Configuration des VACLs

Les VACLs utilisent les ACLs Cisco IOS IP et IPX standard et étendues et les ACL nommées par MAC Layer et les cartes d'accès VLAN.

Les étapes pour la mise en œuvre des VACL sont :

- La programmation d'une ou plusieurs ACL classiques qui sont examinées l'une après l'autre en séquence ;
  Ces ACL sont basées sur des adresses IP ou MAC ;
- La création de la VACL qui appelle l'ACL précédemment définie et décide d'une action ;
- L'application de la VACL au VLAN dans lequel on souhaite filtrer le trafic.

Pour utiliser le contrôle d'accès pour le trafic acheminé et généré, on peut utiliser VACL seul ou une combinaison de VACL et ACL. On peut définir des ACLs sur les interfaces VLANs pour utiliser le contrôle d'accès pour le trafic acheminé et généré en sortie. On peut définir une VACL pour utiliser le contrôle d'accès pour le trafic ponté.

Les cartes d'accès VLAN peuvent être une application aux VLANs ou aux interfaces WAN pour la capture VACL. Les VACL attachées aux interfaces WAN prennent en charge uniquement les ACLs Cisco IOS IP standards et étendues.

Les VACLs ont un refus implicite à la fin de la carte; Un paquet est refusé s'il ne correspond à aucune entrée ACL, et au moins une ACL est configurée pour le type de paquet.

Pour définir une carte d'accès VLAN, on effectue cette tâche :

Commander	Objectif
Routeur (config) # **vlan accès-map** *map_name* [*0-65535*]	Définit la carte d'accès VLAN. En option, vous pouvez spécifier le numéro de séquence de carte d'accès VLAN.
Router (config) # **no vlan accès-map** *map_name 0-65535*	Supprime une séquence de carte à partir de la carte d'accès VLAN.
Routeur (config) # **no vlan accès-map** *map_name*	Supprime la carte d'accès VLAN.

Figure II.9 : définition d'une carte d'accès VLAN

Lors de la définition d'une carte d'accès VLAN, on note les informations suivantes :

- Pour insérer ou modifier une entrée, il faut spécifier le numéro de séquence de la carte.
- Si on ne spécifie pas le numéro de séquence de la carte, un numéro est automatiquement attribué ;
- On peut spécifier une seule clause de correspondance et une seule action par séquence de carte ;
- On utilise le mot-clé **non** avec un numéro de séquence pour supprimer une séquence de carte ;
- On utilise le mot-clé non sans numéro de séquence pour supprimer la carte.

La clause d'action dans une VACL peut être avancée, déposer, capturer ou rediriger. Le trafic peut également être enregistré. Les VACL appliquées aux interfaces WAN ne prennent pas en charge les actions de redirection ou de journalisation.

Pour configurer une clause de correspondance dans une séquence de carte d'accès VLAN, on effectue cette tâche :

Commander	Objectif
Routeur (config-accès-map) # **match** { **adresse ip** { **1-199** | **1300-2699** | *Acl_name* } | **Adresse ipx** { **800-999** | *Acl_name* } | **Adresse mac** *acl_name* | Ipv6}	Configure la clause de correspondance dans une séquence de carte d'accès VLAN.
Routeur (config-accès-map) # **pas de correspondance** { **adresse ip** { **1-199** | **1300-2699** | *Acl_name* } | **Adresse ipx** { **800-999** | *Acl_name* } | **Adresse mac** *acl_name* / Adresse ipv6 acl_name}	Supprime la clause de correspondance dans une séquence de carte d'accès VLAN.

Figure II.10 : configuration d'une clause de correspondance.

Lorsqu'on configure une clause de correspondance dans une séquence de carte d'accès VLAN, on note les informations suivantes :

- On peut sélectionner une ou plusieurs ACL ;
- On utilise le mot-clé non pour supprimer une clause de correspondance ou des ACL spécifiées dans la clause.

Pour configurer une clause d'action dans une séquence de carte d'accès VLAN, on exécute cette tâche :

Commander	Objectif
Routeur (config-accès-map) # **action** { **drop** [**log**]} | { **Forward** [**capture**]} | { **Redirection** {{ethernet | Fastethernet | Gigabitethernet | Tengigabitethernet} slot / port} | {Port-channel channel_id}}	Configure la clause d'action dans une séquence de carte d'accès VLAN.
Routeur (config-accès-map) # **no action** { **drop** [**log**]} | { **Forward** [**capture**]} | { **Redirection** {{ethernet | Fastethernet | Gigabitethernet | Tengigabitethernet} slot / port} | {Port-channel channel_id}}	Supprime la clause d'action à partir de la séquence de la carte d'accès VLAN.

Figure II.11 : configuration d'une clause d'action.

IV. Conclusion

Les VLANs et les VACLs sont utiles et importants pour sécuriser les réseaux informatiques. En effet, Les VLANs facilitent la gestion du réseau, réduit la quantité de trafic inutile sur le réseau et augmente les performances. Aussi, l'utilisation des VACLs limite le trafic au sein d'un même VLAN et augmente la quantité de données à analyser.

CHAPITRE III

Analyse et implémentation de la solution

I. Introduction

Au niveau de ce chapitre nous allons faire une étude préalable du réseau existant de l'entreprise ENIEM, l'étude de réseau actuel et les critiques de la situation.

On donne par la suite les solutions proposées, les outils utilisée et on termine par l'illustration de quelques exemples d'application.

II. Présentation de l'ENIEM

II.1 Historique :

ENIEM : est une entreprise publique économique, elle est le leader de l'électroménager en Algérie, possédant des capacités de production et une expérience plus de 30 années dans la fabrication et le développement différentes branches de l'électroménager, notamment :

- Les appareils ménagers domestiques :
- Les lampes d'éclairages :
- Les produits sanitaires.

ENIEM résulte d'un contrat établi dans le cadre du premier plan quadriennal, et signé le 21 Aout 1971 avec un groupe d'entreprise allemandes représentées par le chef de D.I.A.G 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.

Elle œuvre dans le cadre national du développement économique et social, de la gestion de l'exploitation et de développement des activités de production d'appareils électroménagers grâce à ces directions et unités de productions.

II.2 Mission de l'entreprise :

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 réfrigération et de congélation par l'unité froid
- Les appareils de cuisson par unité cuisson
- Les appareils de climatisation par l'unité climatisation
- Les produits sanitaires par unité d'AIN DEFLA.

II.3 Organisation

L'organisation structurelle de l'ENIEM se présente comme suit :

- Elle est administrée par un conseil d'administration et dirigé par le directeur général.
- Le directeur générale exerce son autorité hiérarchique et fonctionnelle sur l'ensemble des directions et des unités.

Le schéma suivant résume l'organisation générale de l'entreprise ENIEM :

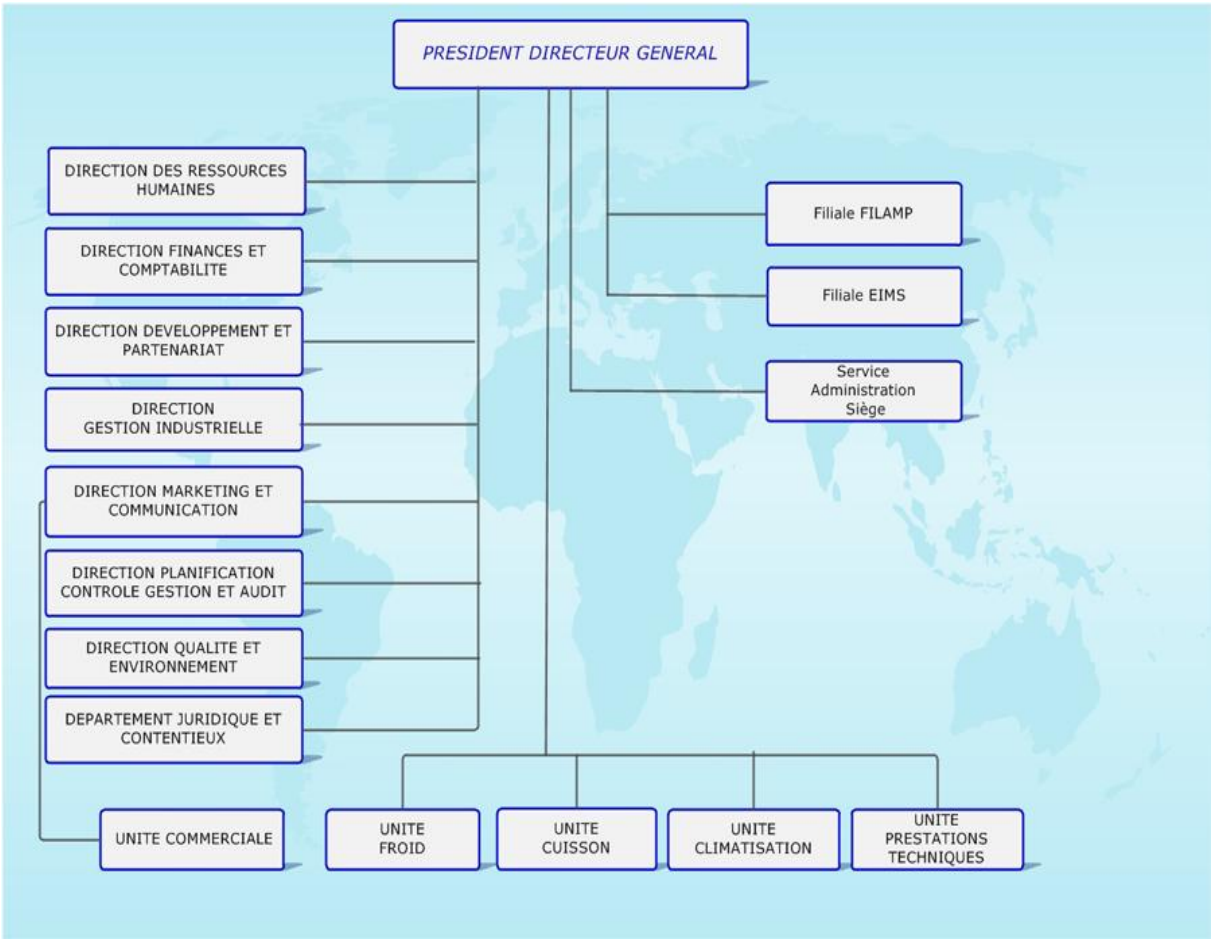

Figure III.1 organigramme générale de l'ENIEM

II.4 Les unités

1. Unité froid (UF)

Elle est l'unité la plus importante du point de vue effectif elle produit plusieurs modèles de réfrigérateurs et congélateurs. Le processus de fabrication est assure pat huit (08) ateliers qui sont :

- Atelier d'injection plastique ;
- Ateliers presses et soudures ;
- Atelier de refondée et de mise en longueur ;
- Atelier de traitement et de revêtement des surfaces ;
- Atelier de fabrication de pièces métalliques ;
- Atelier de thermoformage ;
- Atelier de montage final.

Et un laboratoire central composé de trois (03) sections :

- Laboratoire de chimie ;
- Laboratoire de métallurgie ;
- Laboratoire d'essais produits.

2. Unité cuisson (UCUIS)

Cette unité a pour mission la production et le développement des produits de cuisson à gaz, électrique ou mixte et tout produit de technologie similaire, elle produit des cuisinières à gaz 04 et 05 feux. Comporte (04) ateliers de fabrication :

- Atelier mécanique : s'occupe de la fabrication de composants d'alimentation en gaz et des différentes grilles de cuisinières.
- Atelier tôlerie : s'occupe de la fabrication des différentes pièces en tôle ;
- Atelier d'assemblage ;
- Ainsi qu'un laboratoire essais gazinières.

3. Unité climatisation (UCL)

Cette unité fait dans la production et le développement des produits de climatisation, de chauffage et annexe :

- Equipements de climatisation individuels et collectifs ;
- Activités annexes : chauffe-eau, chauffe bain et radiateur à gaz butane.

Composée essentiellement de quatre (04) ateliers de fabrication :

- Atelier tôlerie ;
- Atelier peinture ;

- Atelier montage final ;
- Atelier montage d'appareils de chauffage.

4. Unité prestation technique (UPT)

Chargée principalement de gérer et d'exploiter les moyens communs (production d'énergie et utilités) utilisés dans le processus de production des autres unités, ainsi que de la gestion des totalités des infrastructures communes (bâtiments, voirie, éclairage…).

Cette unité assure également, les pièces mécaniques nécessaires à l'entretien des équipements de production, la conception et la fabrication de nouveau moyens (moules, outils, gabarits…)

Elle est constituée d'ateliers de mécanique et de deux (02) stations :

- Station de production d'énergie et des fluides, elle produit de l'eau surchauffée, de la vapeur et de l'air comprimé ;
- Station de neutralisation, s'occupe de traitement des rejets industriels avant leur évacuation ;
- Et un laboratoire de métrologie qui se charge de l'étalonnage et de la vérification des mesures.

5. Unité commerciale

Elle est chargée de la commercialisation des produits de l'entreprise, de la promotion des exportations et de la gestion du réseau SAV (service après-vente). Composée essentiellement, d'une direction commerciale.

Cette direction a sous sa tutelle sept départements qui collaborent pour mettre en œuvre la stratégie commerciale

- Département vente : il se compose de trois services :
  - Service client ;
  - Service vente ;
  - Service synthèse et recouvrement.
- Département distribution : composé de deux services :
  - Service magasin produits finis ;
  - Service programmation.

- Service marketing ;
- Département service après-vente ;
- Département finance et comptabilité : composé de deux services ;
  - Un service comptabilité générale ;
  - Un service finances.
- Département administration générale et ressources humaine (AGRH) : composé de deux services :
  - Service gestion du personnel ;
  - Service moyens généraux.
- Département contrôle de Gestion.

6. Unité FILAMP (filiale)

L'unité FILAMP de Mohammedia (ULM) qui a commencé en février 1979 la fabrication des lampes d'éclairage domestique ainsi que des lampes de réfrigérateurs. Elle est devenue filiale à 100% ENIEM le 01 janvier 1997.

III. Présentation du domaine d'étude (UPT)

Notre travail au sein de l'entreprise ENIEM va s'effectuer principalement dans l'unité prestation technique. 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.
- Travaux de menuiserie.
- Travaux de nettoyage.
- Prestation informatique.

Le schéma suivant présente l'organisation **de** l'unité de prestation technique **:**

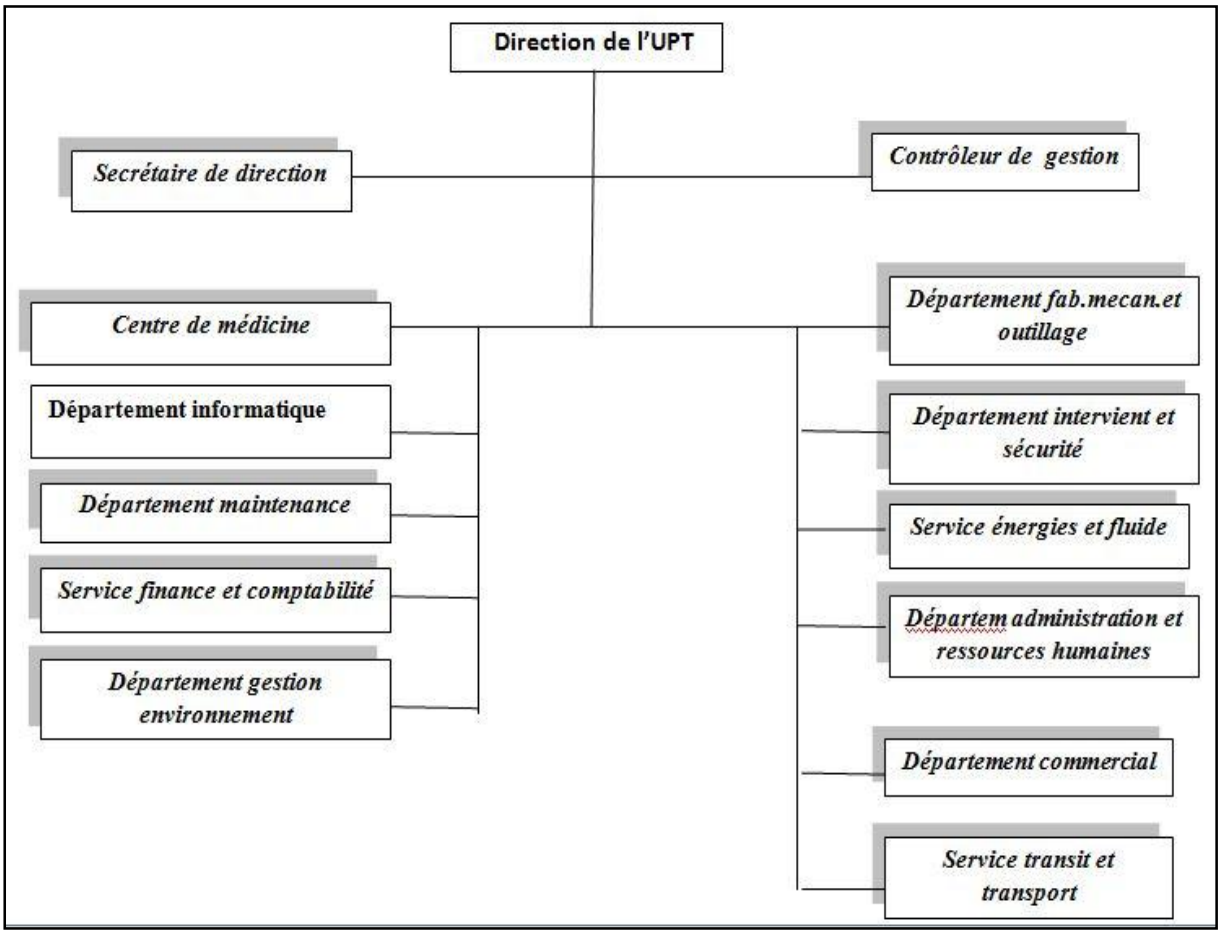

Figure III.2 : Organigramme de l'unité de prestation technique

IV. Présentation du réseau existant

L'architecture du réseau actuel de l'entreprise ENIEM est représentée dans la figure suivante :

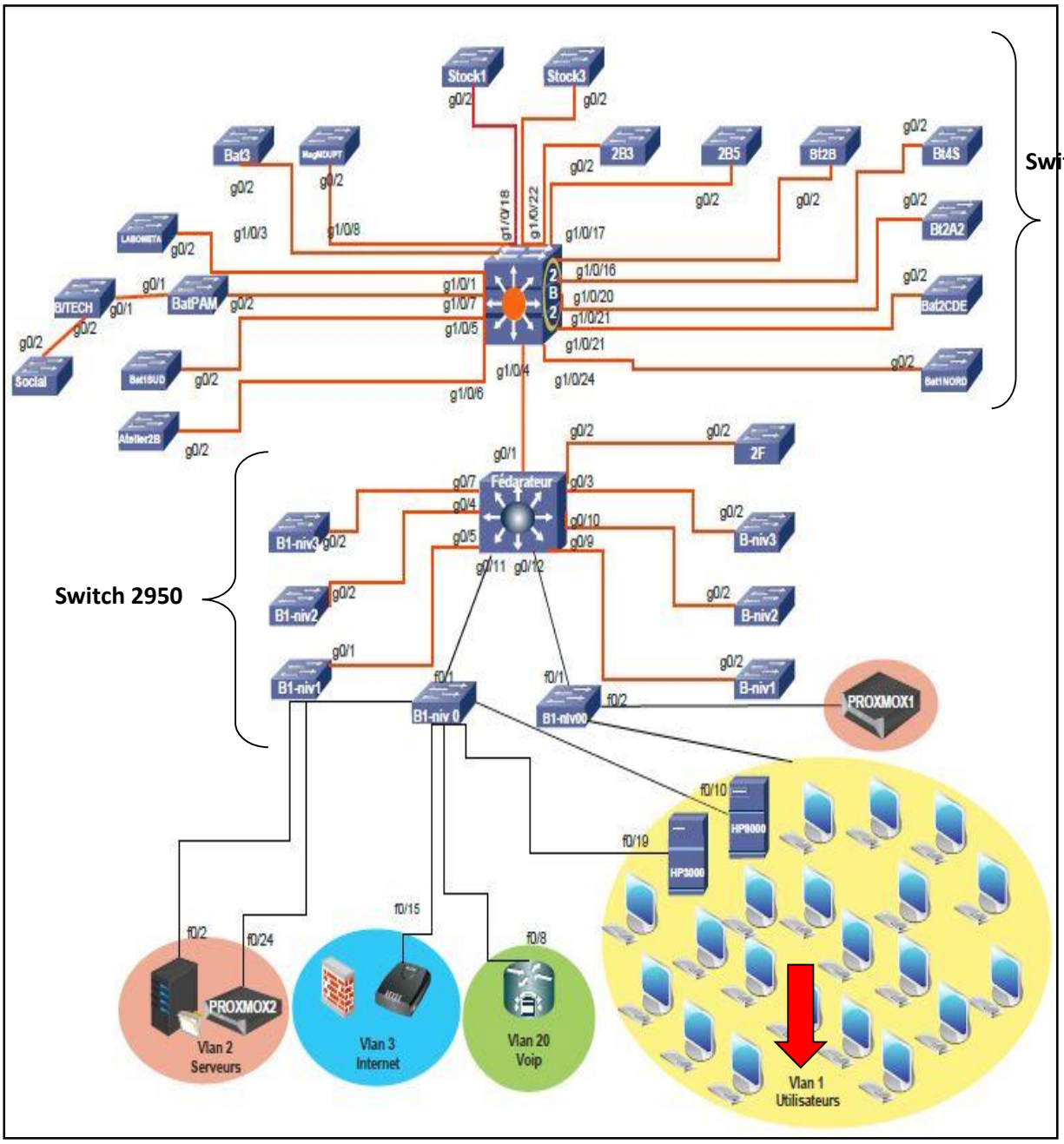

Figure III.3 : l'architecture de réseau existant

IV.1. Aspect matériel

Comme le montre la figure, le réseau existant contient deux blocs :

1. L'ancien bloc (le bloc administratif), qui contient :
    - Neufs commutateurs Ethernets 2950 ;
    - Un switch fédérateur 35600 (de niveau 3) ;
    - Un serveur pare-feu ;

- Un modem pour une connexion au réseau internet ;
- Deux serveurs HP3000 et HP9000 pour faire communiquer tous les utilisateurs.
- Des ordinateurs.

2. Le nouveau bloc (les ateliers), qui contient :
    - Un switch 3750 (de niveau 03) ;
    - 17 commutateurs Ethernets 2960 ;
    - Des ordinateurs.

IV.1.1. Le serveur HP3000 /A500

Le serveur HP3000 /A500 caractériser par deux faces :

1. La face avant

Elle est composée de :

- Lecteur de cassettes DRT DLT.
- Lecteur DVD.
- Lecteur de cassettes DAT DDS.

Figure III.4 : La face avant de serveur HP3000/A500.

2. La face arrière

La face arrière du serveur est principalement composée de

- DTC (Data Terminal Circuit) qui gère deux types de panneaux
  - DDP (Panneau de Distribution Directe) ;
  - MDP (Panneau de Distribution Modem).
- Les ports sur les DDP sont du type RJ45N (norme RS423) ;
- Les ports sur le MDP sont du type :
  - RJ45 (norme RS423) et numérotés de 100 à 115, de 200 à 215 pour les ports écran et de 300 à 315 pour les ports imprimantes.
  - DB25 (norme RS422) et numérotés de 400 à 415, de 500 à 515 pour les ports écran et de 600 à 615, pour les ports imprimantes.
- .Il est aussi équipé d'une unité centrale.

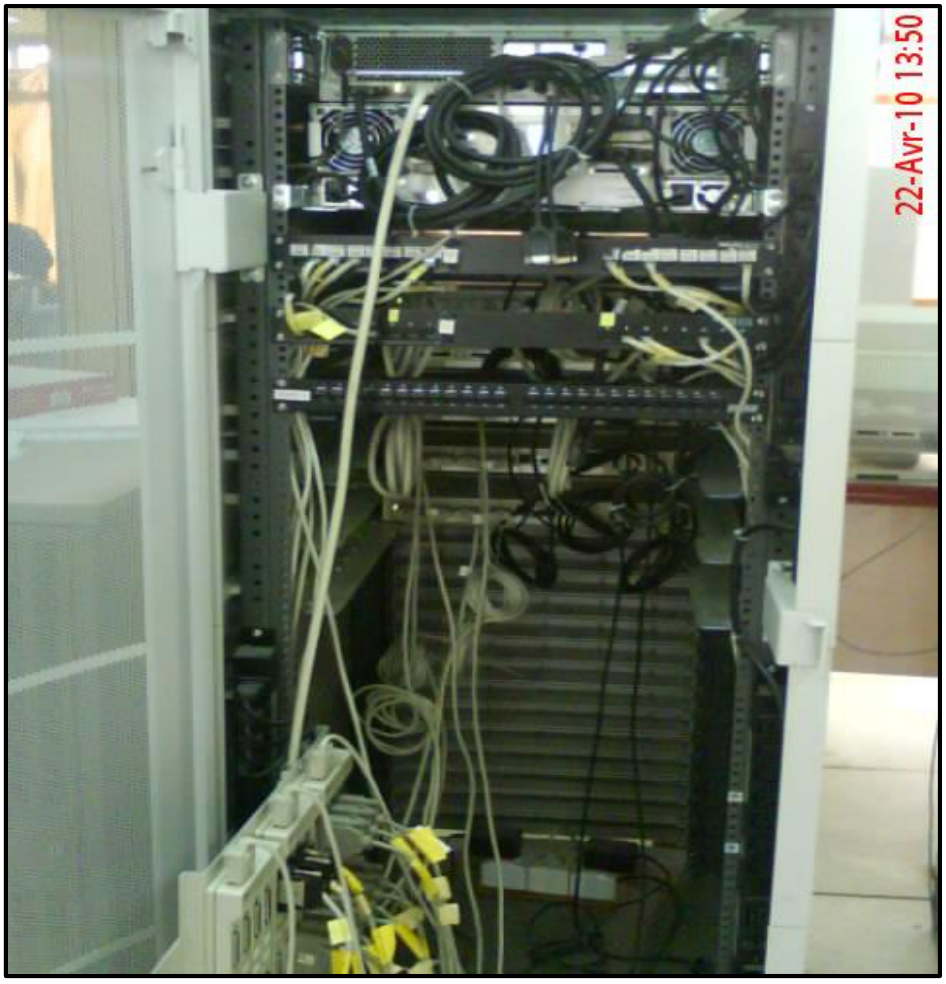

Figure III.5 : La face arrière de serveur HP3000/500.

IV.1.2. Serveur HP9000

HP 9000 est une série de Serveurs informatiques PA-RISC sous HP-UX produits par Hewlett-Packard depuis 1982 pour succéder à la série HP 3000 des années 1970. Il était concurrent des serveurs Sun, Apollo et IBM AS400.

IV.2. Aspect logiciel

Différents Les logiciels sont utilisés :

- **IMAGE/3000** : pour la gestion de bases de données ;
- **Réflexion x :** est un émulateur d'accès au serveur depuis les différentes PC des utilisateurs ;
- **EASY :** application installée au niveau du serveur pour gérer la comptabilité des différentes unités ;
- **ACPAE** : Gestion de la paie**.**
- **COBOL** : langage de programmation avec lequel toutes les applications opérationnelles sont développées.
- **Système MM3000 pour la gestion de production** : Il se charge de la production et tenue du stock des matières première et pièce de recharges ;
- **Système MM30909 :** 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 à la fonction achat ;
- **Gestion de la comptabilité :** la comptabilité clients, fournisseur, générale et d'autres ;
- **Windows serveur 2008 :** installé sur le serveur ;
- **Windows 7 :** installé sur les autres machines clientes.

IV.3. Aspect réseau

Le réseau actuel d'ENIEM est structuré en deux réseaux :

- Le réseau point à point des ateliers ;
- Le réseau local du bloc administratif.

a. Réseau point à point :

Ce réseau se trouve au niveau des ateliers. Il est composé de 39 terminaux dont 27 écrans de type HP (modèle 2563B, 2934A, RUGGED WRITER 480) et 12 imprimantes HP reliés au serveur HP3000/A500 par liaisons :

- **Directe** pour des distances inférieures ou égales 1200 mètres.
- **Modem-modem** avec des lignes téléphoniques (4 fils) pour des distances supérieures à 1200 mètres.
- **Multiplexeur Modem /Modem démultiplexeur** pour les installations de plusieurs terminaux distants.

b. Réseau local

La topologie choisie est en étoile vu la configuration du site, à savoir : deux bâtiment en forme de T (bâtiment A et bâtiment B ou se trouve notre champ d'étude).

Le schéma général du câblage et 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 tout 170 prises. Toutes les prises d'un même étage et de chaque bâtiment sont reliées à un Switch contenu dans une armoire de brassage, cette dernière est reliée par un câble Fabre Optique à un Switch dit FEDERATEUR contenu dans une armoire centrale installée au niveau de la salle machine au sous-sol du bâtiment B.

Le réseau est composé de 06 armoires de brassage départagées dans 02 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

V. Les critiques du réseau existant

Apres avoir étudié le fonctionnement du réseau local existant de l'entreprise ENIEM, nous sommes arrivés à extraire les critiques suivantes :

- Impossibilité de segmenter le réseau utilisateur en VLANs à cause du serveur HP3000 qui ne possède pas de Gateway ;
- Absence d'une stratégie de sécurité. En effet, tous les services se trouvent dans un même réseau, ce qui expose ce dernier au danger en cas de propagation d'une malveillance informatique. par exemple, un virus qui infecte une machine appartenant à une unité quelconque va se propager vers le réseau intégral de l'UPT d'une façon rapide, et paralyser ainsi tous les services voisins.

VI. Solutions proposées

A l'issu d'une étude préalable de l'unité prestation technique au sein de l'entreprise, nous avons opté pour l'implémentation du plan de sécurité suivant :

- Suppression du serveur HP3000 et le remplacer par des Switch ;
- Création des VLANs (segmentation du réseau en plusieurs VLANs) ;
- Création d'un pool DHCP pour chaque VLAN afin d'attribuer dynamiquement les adresses IP, la passerelle et l'adresse du serveur DNS ;
- Utilisation des ACLs pour interdire la communication entre deux VLANs et l'autoriser entre les autres ;
- Appliquer les VACLs à l'échelle d'un VLAN.

VII. Réalisation des tests

Pour simuler le réseau de l'ENIEM et pouvoir lui attribuer les configurations adéquates pour réussir la segmentation VLAN et sa sécurisation, nous avons utilisé le logiciel émulateur **GNS3.**

VII.1. Présentation du logiciel utilisé (GNS3)

GNS3 est un logiciel utilisé pour simuler différents périphériques virtuels et dispositifs réels comme les routeurs, commutateurs... Il est la suite logique de packet tracer : contrairement aux autres émulateurs, GNS3 utilise un véritable IOS entièrement fonctionnel. On y retrouve toutes les commandes réelles du matériel mais surtout : il donne la possibilité de mettre ces éléments (virtuels) dans le même réseau que les équipements réels de notre réseau (machines, Switch, téléphones IP,…). GNS3 est composé principalement d'un espace de travail et de 05 sous-menus (figure 1) :

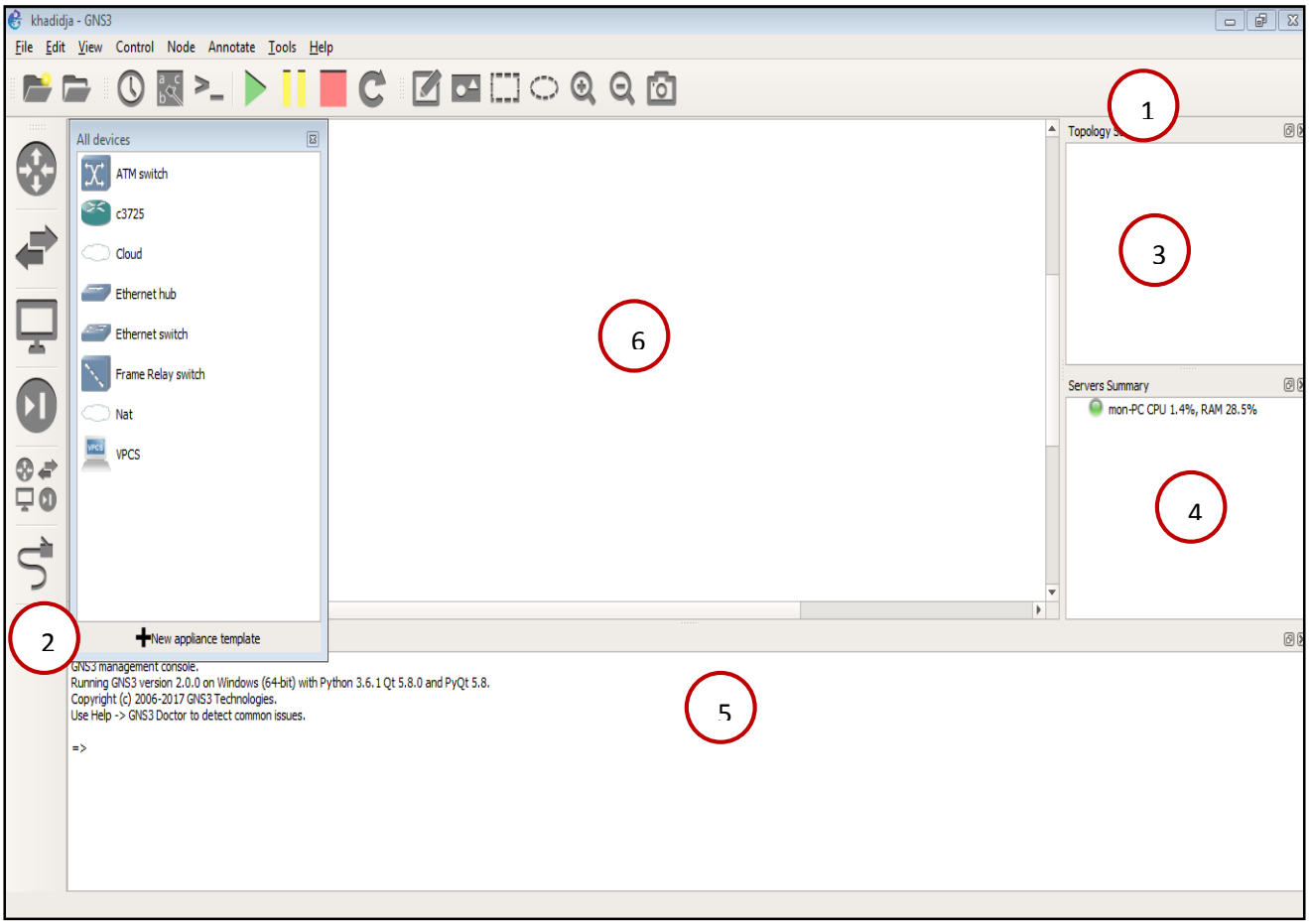

Figure III.6 : l'environnement GNS3

1. **La barre d'outils GNS3 :** ou l'on trouve des icones d'accès rapide comme le triangle vert utilise pour démarrer un composant.
2. **La barre d'outils des équipements réseaux** : qui permet d'ajouter des routeurs, Switch ou autre équipement utilisable.
3. **La barre d'outils *topology summary* :** qui permet d'avoir à tout moment un aperçu sur l'état des équipements réseaux de notre topologie.
4. **La barre d'outils *server summary*** : indique quel serveur est utilisé lors de la simulation
5. **La barre d'outils *consol* :** permet d'administrer sous forme CLI (command line interface) c'est-à-dire par commande texte les équipements réseaux.
6. **L'espace de travail :** l'espace alloué pour la réalisation de nos topologies réseau à partir de la barre d'outils des équipements

VII.2. Réalisation des tests

Comme la figure le montre, on a utilisé dans l'architecture :

- Des pc virtuels, des switch de niveau 2 et 2 switch de niveau 3.
- Une machine virtuelle « test »pour se connecter au serveur web « XAMP» et au serveur « DNS ».
- Un Cloud pour interconnecter la machine physique avec la machine virtuelle de « gns3 » pour cela on a créé une carte de bouclage Microsoft.

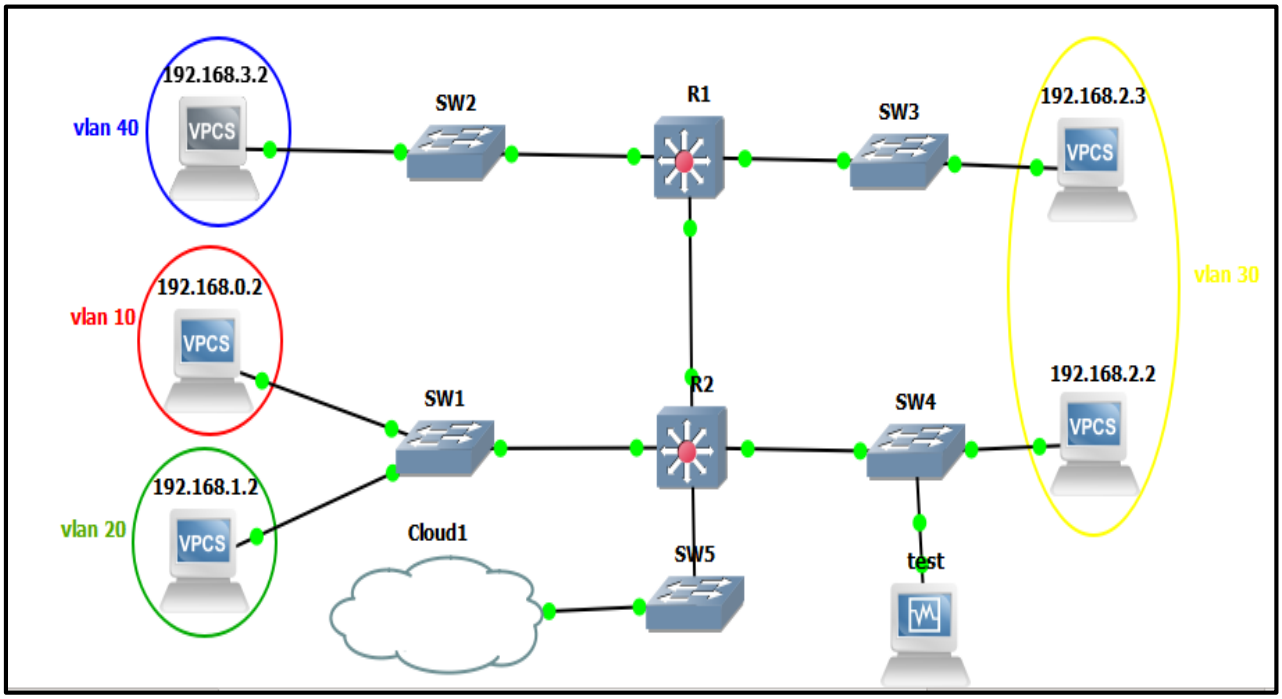

***Figure III. 7: l'architecture minimale du réseau d'ENIEM sous* GNS3**

1. La segmentation du réseau en 5 Vlan

```
R2#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/4, Fa1/5, Fa1/6, Fa1/7
                                                Fa1/8, Fa1/9, Fa1/10, Fa1/11
                                                Fa1/12, Fa1/13, Fa1/14, Fa1/15
10   froid                            active
20   cuisson                          active
30   clim                             active
40   upt                              active
60   INTERNET                         active
```

Figure III.8 : segmentation de réseau en plusieurs VLANs

- Création de Vlan 10 pour l'unité Froid avec la plage d'adresses 192.168.0.0 /24.
- Création de Vlan 20 pour l'unité Cuisson avec la plage d'adresses192.168.1.0 /24.

- Création de Vlan 30pour l'unité Climatisation avec la plage d'adresses 192.168.2.0 /24.
- Création de Vlan 40 pour l'unité UPT avec la plage d'adresses192.168.3.0 /24.
- Création de Vlan 60pour la connexion a un serveur web avec la plage d'adresses 10.10.10.0 /24.

2. Création de la machine virtuelle « test»

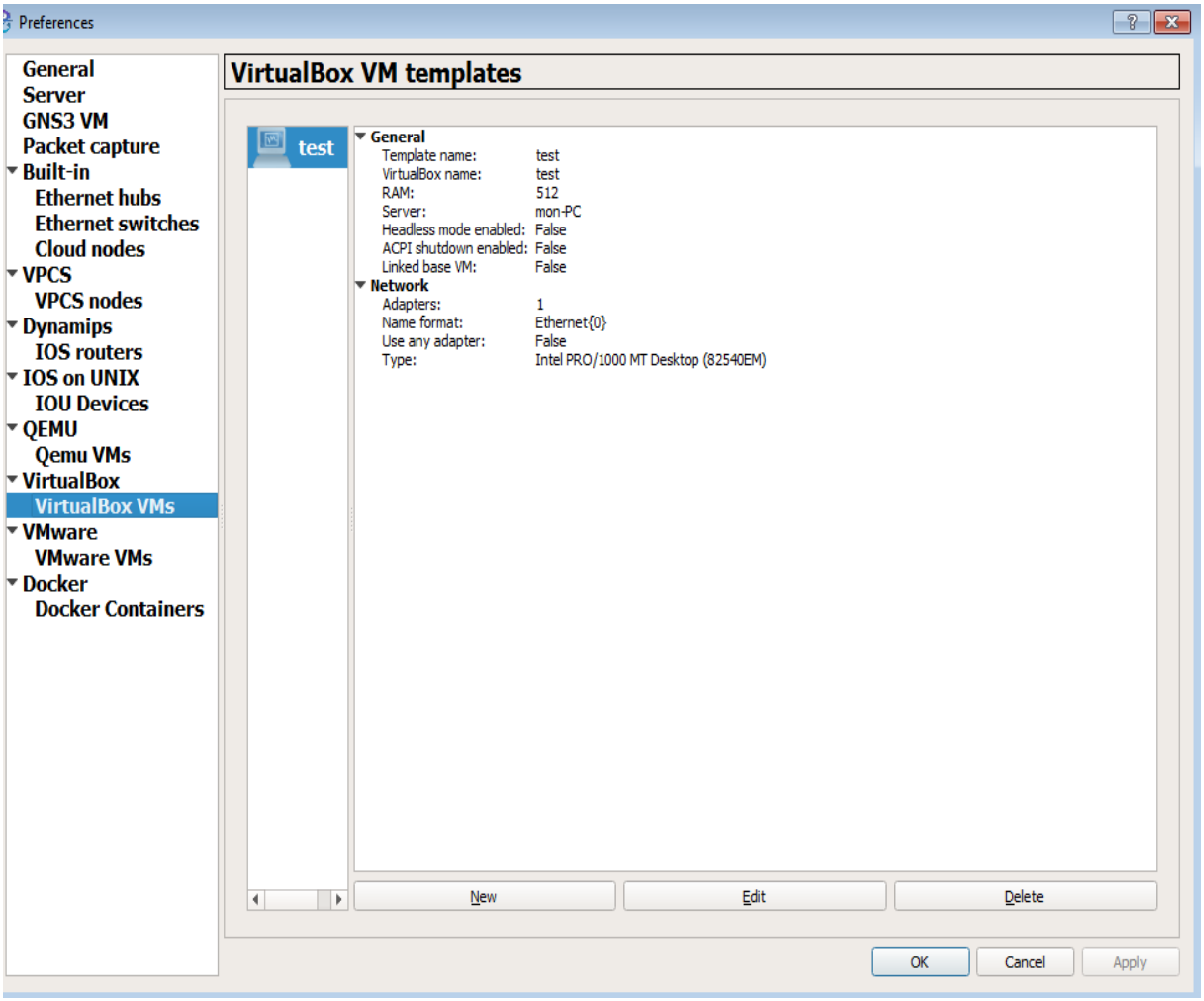

Figure III.9 : création d'une machine virtuelle

3. Vérification de la connexion entre les 4 vlan

- Ping de la machine du vlan 10 vers les autre vlan et le serveur DNS.

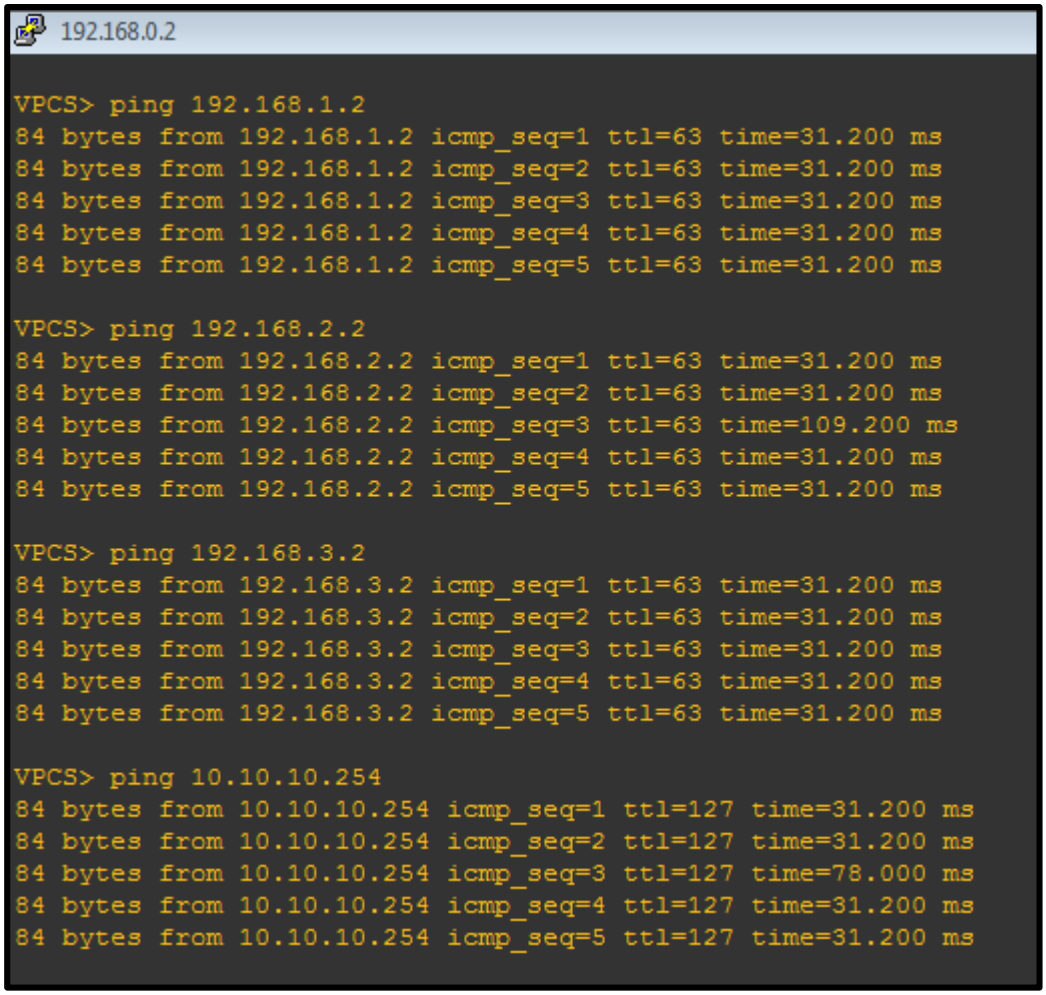

Figure III.10 : Ping de la machine du vlan 10 vers les autre vlan et le serveur DNS.

On a la machine d'adresses 192.168.0.2 du « vlan 10 » qui ping (envoie des paquets icmp) vers :

- La machine d'adresses 192.168.1.2 du « vlan 20 ».
- La machine d'adresses 192.168.2.2 du « vlan 30 ».
- La machine d'adresses 192.168.3.2 du « vlan 40 ».
- L'adresse10.10.10.254 du « vlan 60 » qui est le serveur DNS.

- **Ping de la machine du vlan 20 vers les autre vlan et le serveur DNS.**

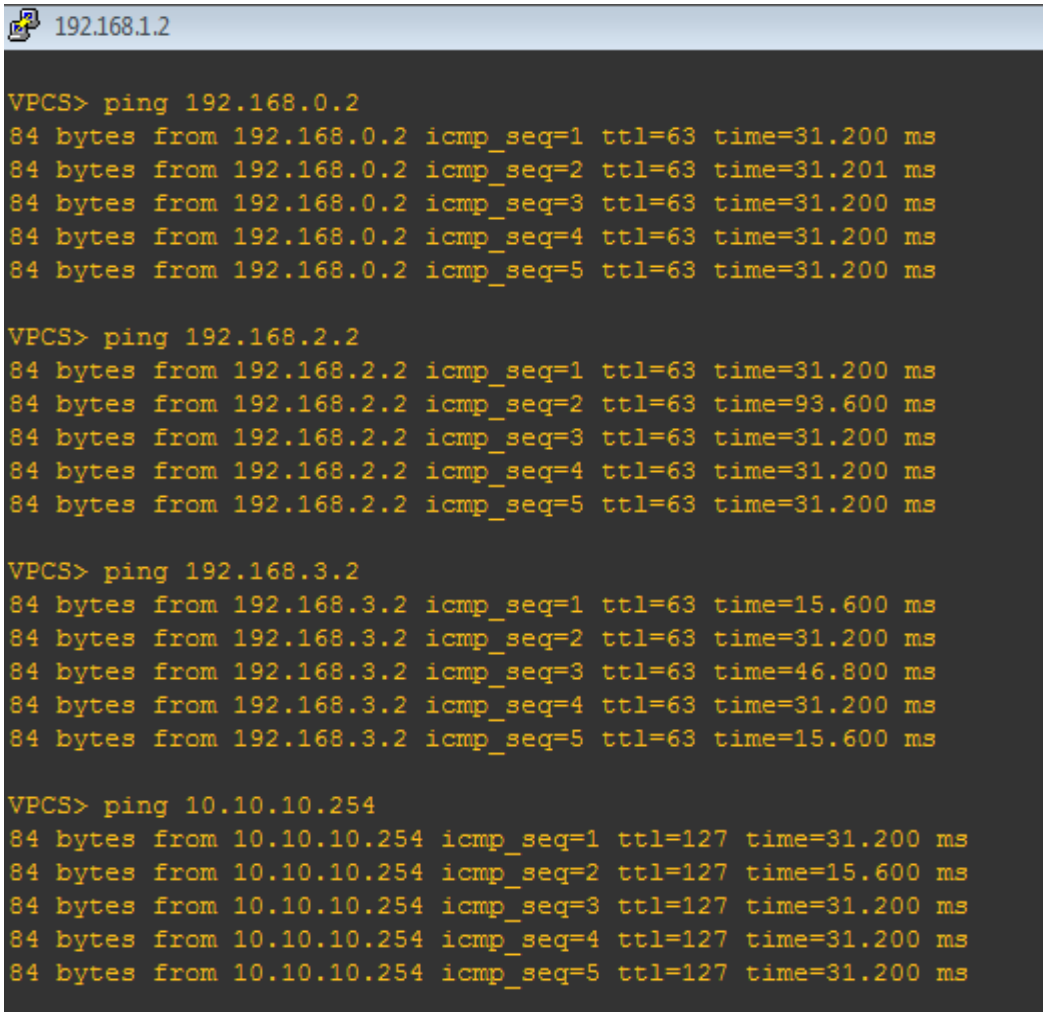

Figure III.11 : Ping de la machine du vlan 20 vers les autre vlan et le serveur DNS.

On a la machine d'adresses 192.168.1.2 du « vlan 20 » qui ping (envoie des paquets icmp) vers :

- La machine d'adresses 192.168.0.2 du « vlan 10 ».
- La machine d'adresses 192.168.2.2 du « vlan 30 ».
- La machine d'adresses 192.168.3.2 du « vlan 40 ».
- L'adresse10.10.10.254 du « vlan 60 » qui est le serveur DNS.

- Ping de la machine du vlan 30 vers les autre vlan et le serveur DNS.

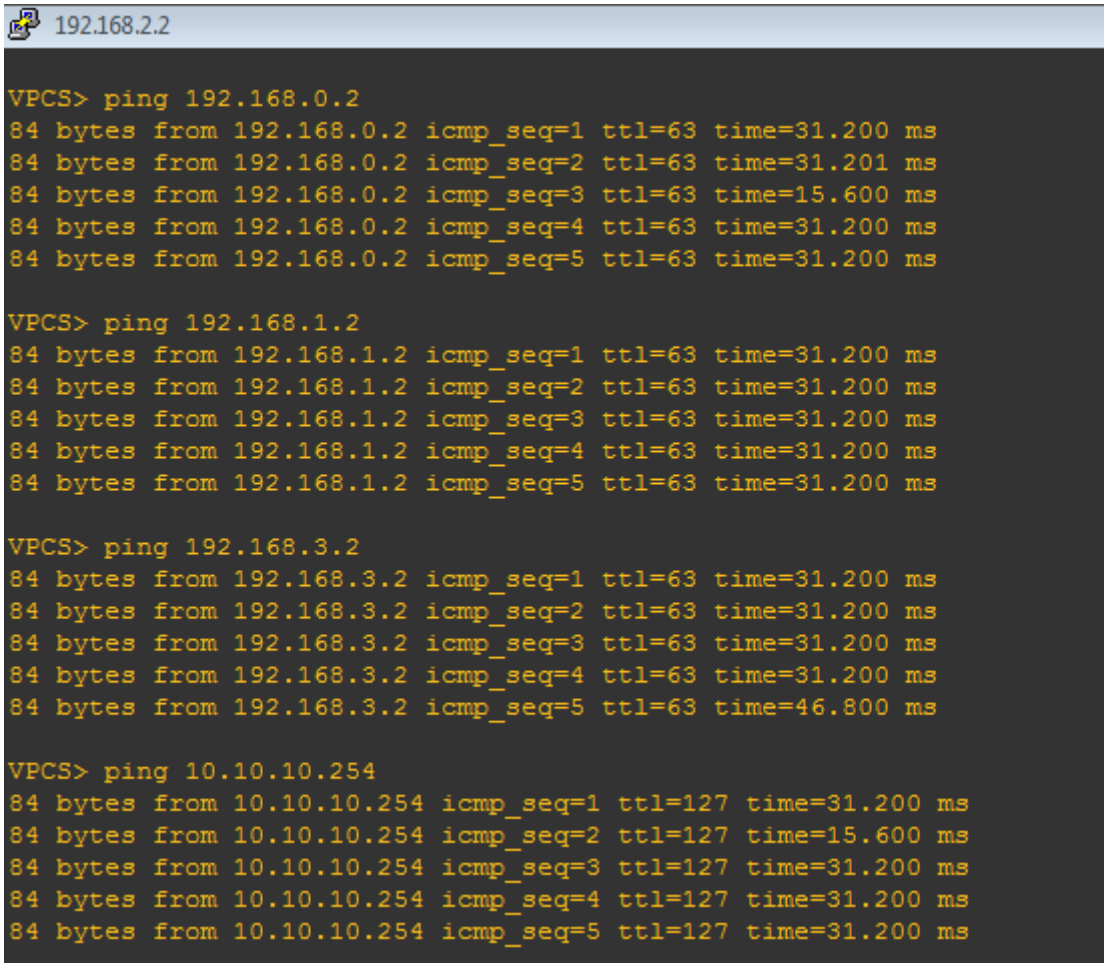

Figure III.12 : Ping de la machine du vlan 30 vers les autre vlan et le serveur DNS

On a la machine d'adresses 192.168.2.2 du « vlan 30 » qui ping (envoie des paquets icmp) vers :

- La machine d'adresses 192.168.0.2 du « vlan 10 ».
- La machine d'adresses 192.168.1.2 du « vlan 20 ».
- La machine d'adresses 192.168.3.2 du « vlan 40 ».
- L'adresse10.10.10.254 du « vlan 60 » qui est le serveur DNS

- Ping de la machine du vlan 40 vers les autre vlan et le serveur DNS.

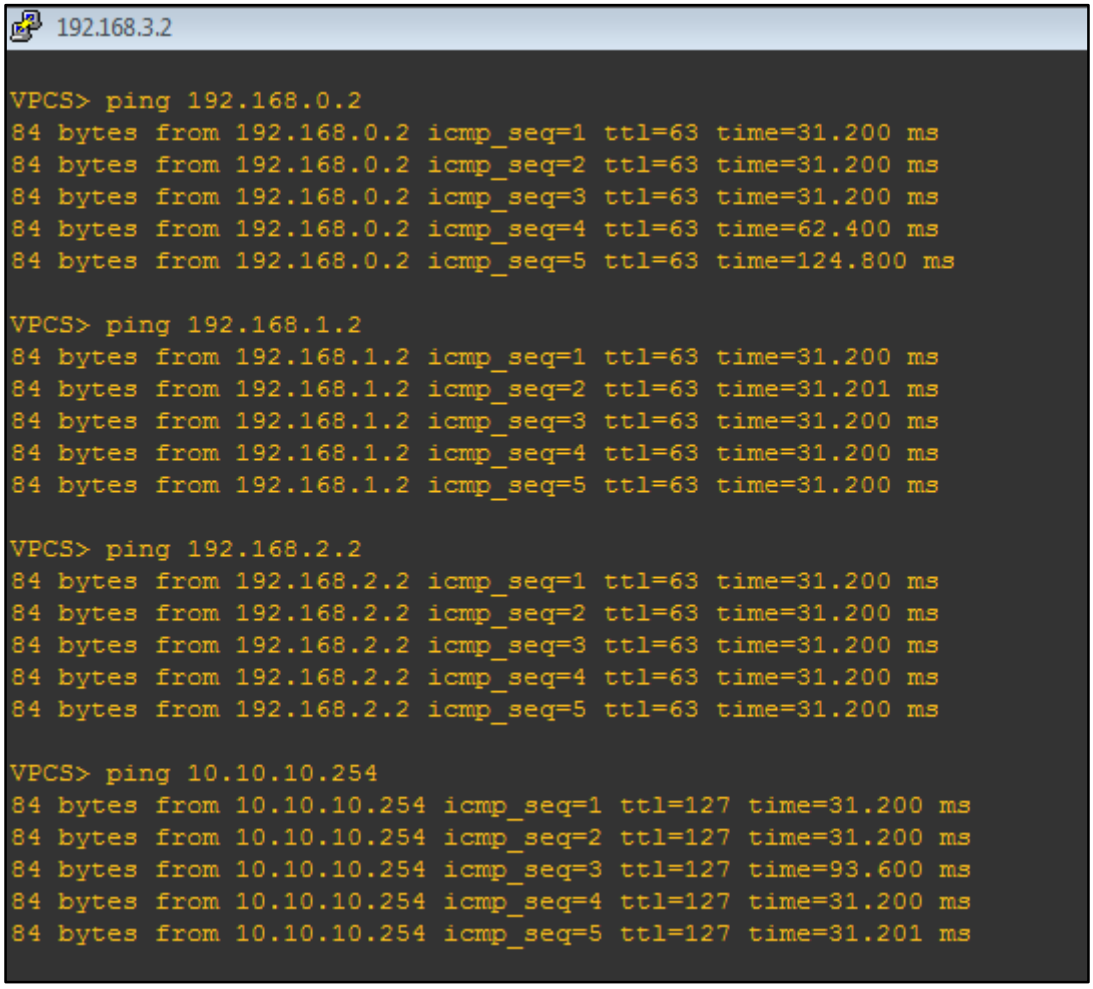

Figure III.13 : Ping de la machine du vlan 40 vers les autre vlan et le serveur DNS.

On a la machine d'adresses 192.168.3.2 du « vlan 40 » qui ping (envoie des paquets icmp) vers :

- La machine d'adresses 192.168.0.2 du « vlan 10 ».
- La machine d'adresses 192.168.1.2 du « vlan 20 ».
- La machine d'adresses 192.168.2.2 du « vlan 30 ».
- L'adresse 10.10.10.254 du « vlan 60 » qui est le serveur DNS.

- **Ping de la machine virtuelle du VirtuelBox du vlan 10 vers les autre vlan et le serveur DNS.**

L'affichage d'adresse, masque sous réseau et la passerelle de la machine virtuelle**« test »:**

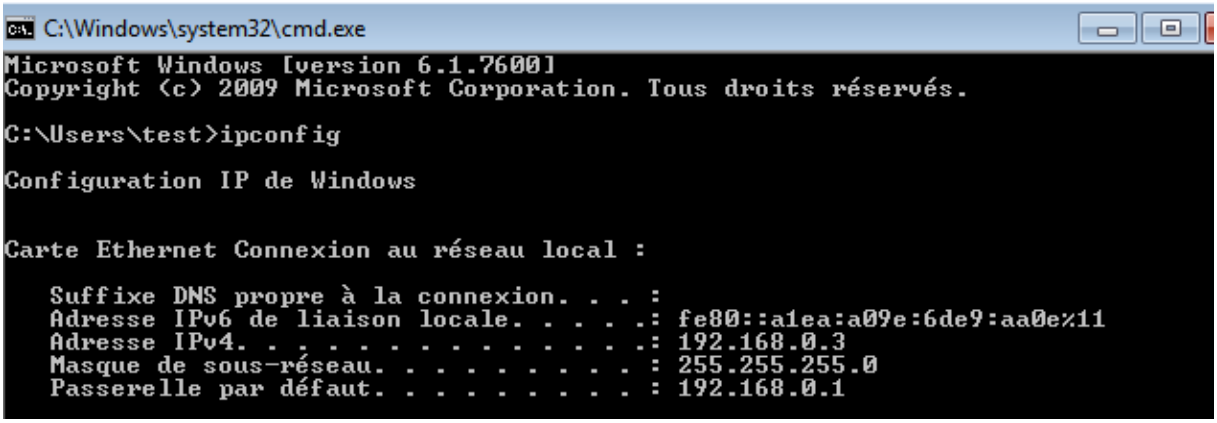

Figure III.14 : L'affichage d'adresse, masque sous réseau et la passerelle de la machine virtuelle« test ».

On a la machine virtuelle d'adresses 192.168.0.3 du « vlan 10 » qui ping vers la machine d'adresse 192.168.0.2 du « vlan 10 ».

Figure III.15 : Ping vers la machine d'adresse 192.168.0.2

La machine virtuelle d'adresses 192.168.0.3 du « vlan 10 » qui ping vers la machine d'adresses 192.168.1.2 du « vlan 20 ».

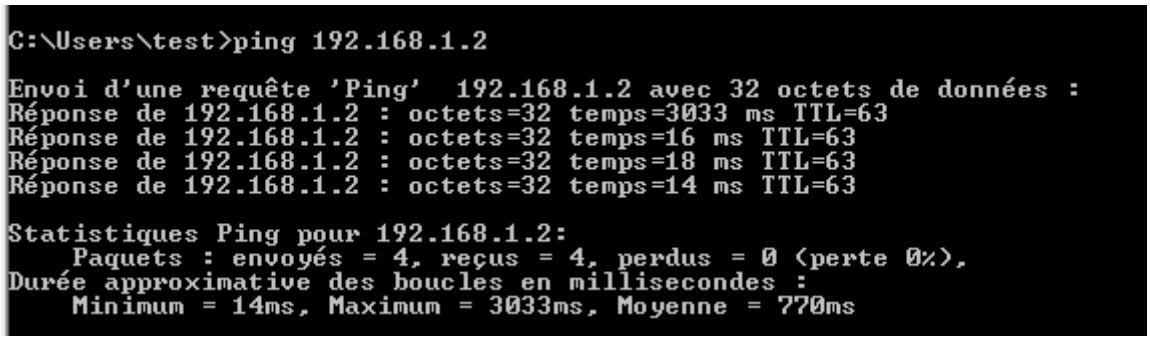

Figure III.16 : Ping vers la machine d'adresse 192.168.1.2

La machine virtuelle d'adresses 192.168.2.3 du « vlan 10 » qui ping vers la machine d'adresses 192.168.2.2 du « vlan 30 ».

```
C:\Users\test>ping 192.168.2.2

Envoi d'une requête 'Ping'  192.168.2.2 avec 32 octets de données :
Réponse de 192.168.2.2 : octets=32 temps=3024 ms TTL=63
Réponse de 192.168.2.2 : octets=32 temps=16 ms TTL=63
Réponse de 192.168.2.2 : octets=32 temps=15 ms TTL=63
Réponse de 192.168.2.2 : octets=32 temps=16 ms TTL=63

Statistiques Ping pour 192.168.2.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 15ms, Maximum = 3024ms, Moyenne = 767ms
```

Figure III.17 : Ping vers la machine d'adresses 192.168.2.2

La machine virtuelle d'adresses 192.168.0.3 du « vlan 10 » qui ping vers la machine d'adresses 192.168.3.2 du « vlan 40 ».

```
C:\Users\test>ping 192.168.3.2

Envoi d'une requête 'Ping'  192.168.3.2 avec 32 octets de données :
Réponse de 192.168.3.2 : octets=32 temps=14 ms TTL=63
Réponse de 192.168.3.2 : octets=32 temps=18 ms TTL=63
Réponse de 192.168.3.2 : octets=32 temps=14 ms TTL=63
Réponse de 192.168.3.2 : octets=32 temps=18 ms TTL=63

Statistiques Ping pour 192.168.3.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 14ms, Maximum = 18ms, Moyenne = 16ms
```

Figure III.18 : Ping vers la machine d'adresses 192.168.3.2

La machine virtuelle d'adresses 192.168.0.3 du « vlan 10 » qui ping vers l'adresses 10.10.10.254du serveur DNS du « vlan 60 ».

```
C:\Users\test>ping 10.10.10.254

Envoi d'une requête 'Ping'  10.10.10.254 avec 32 octets de données :
Réponse de 10.10.10.254 : octets=32 temps=13 ms TTL=127
Réponse de 10.10.10.254 : octets=32 temps=19 ms TTL=127
Réponse de 10.10.10.254 : octets=32 temps=22 ms TTL=127
Réponse de 10.10.10.254 : octets=32 temps=15 ms TTL=127

Statistiques Ping pour 10.10.10.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 13ms, Maximum = 22ms, Moyenne = 17ms
```

Figure III.19 : Ping vers l'adresse 10.10.10.254 du serveur DNS du « vlan 60 ».

La machine virtuelle d'adresses 192.168.0.3 du « vlan 10 » qui ping vers Le nom du domaine « test.lan » du serveur DNS.

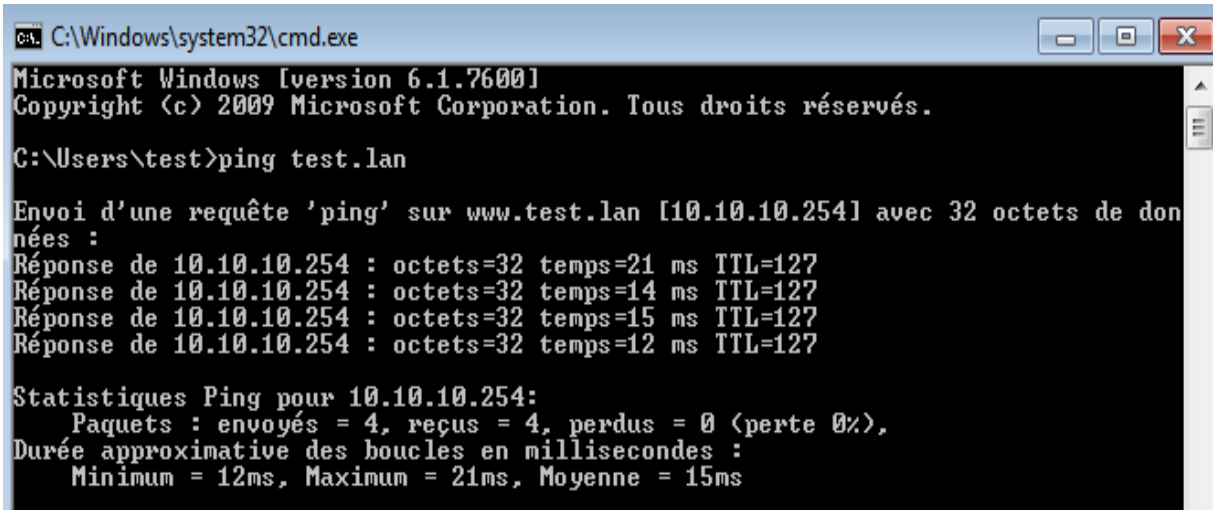

Figure III.20 : Ping vers le nom du domaine « test.lan » du serveur DNS.

4. La mise d'une ACL entre le vlan 20 et vlan30

- Ping de la machine du vlan 20 vers les machines du vlan 30 :

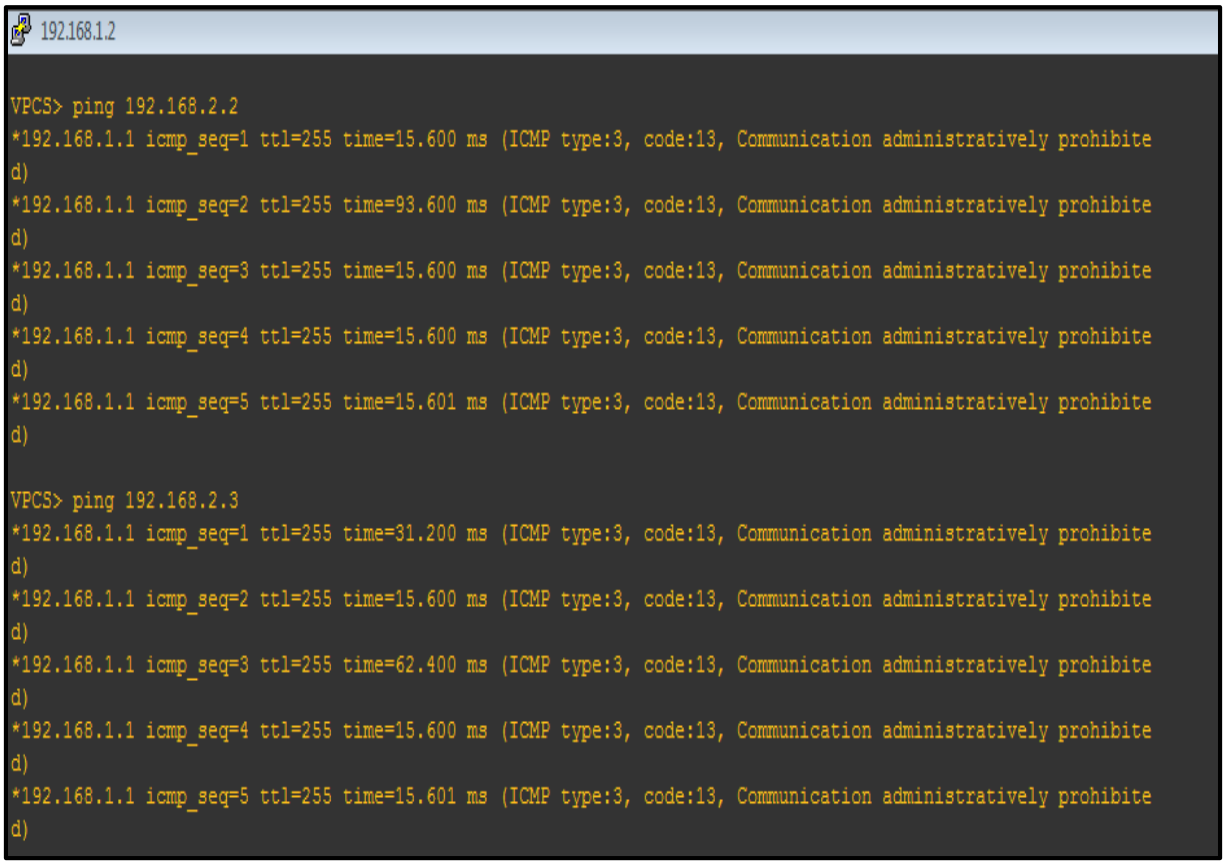

Figure III.21 : Ping de la machine du vlan 20 vers les machines du vlan 30.

On a la machine d'adresses 192.168.1.2 du « vlan 20 » qui ping vers la machine d'adresses 192.168.2.2 et la machine d'adresses 192.168.2.3 du « vlan 30 », et on voie que l'ACL a interdit l'envoie de ping des machines du « vlan 30 », alors pas de communication avec le « vlan 20 » et le « vlan 30 ».

- Ping de la machine du vlan 30 vers la machine du vlan 20 :

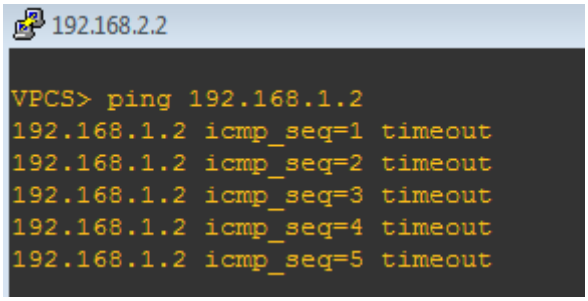

Figure III.22 : Ping de la machine du vlan 30 vers la machine du vlan 20

On a la machine d'adresses 192.168.2.2 du « vlan 30 » qui Ping vers la machine d'adresses 192.168.1.2 du « vlan 20 » et on voie que l'ACL a interdit la communication entre le « vlan 30 » et le « vlan 20 ».

- Ping de la machine du vlan 30 vers la machine du vlan 20 ;

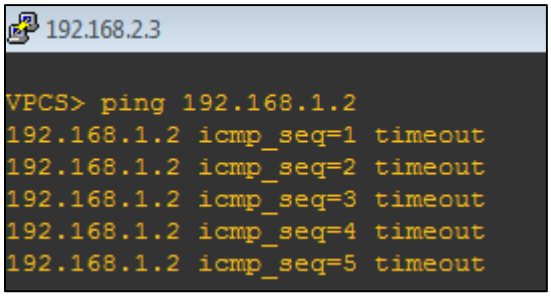

Figure III.23 : Ping de la machine du vlan 30 vers la machine du vlan 20.

On a la machine d'adresses 192.168.2.3 du « vlan 30 » qui ping vers la machine d'adresses 192.168.1.2 du « vlan 20 » et on voie que l'ACL a interdit la communication entre le « vlan 30 » et le « vlan 20 ».

5. **La mise d'une ACL qui permet au vlan 10 d'envoyer des Ping vers tous les vlan même le server DNS mais d'interdire le trafic UDP sur le serveur DNS :**

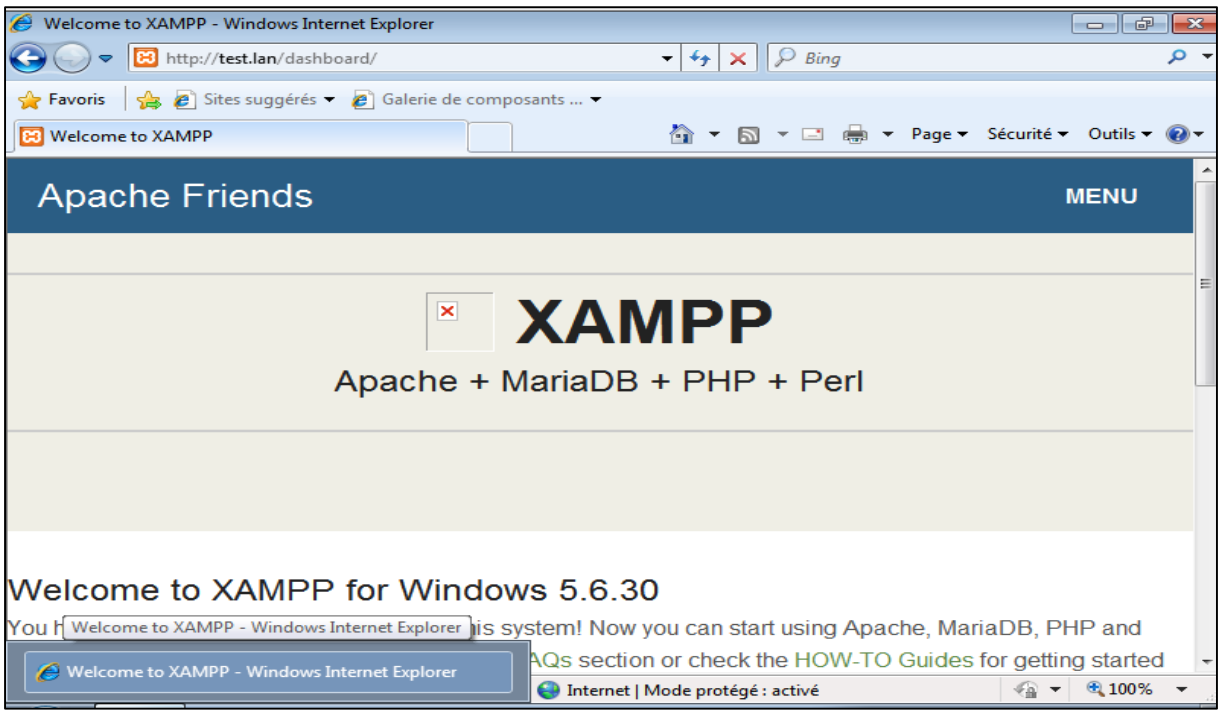

Figure III.24 : La connexion de la machine virtuelle« test »au server web xamp avec le nom de domaine « test.lan »avant la mise de l'ACL.

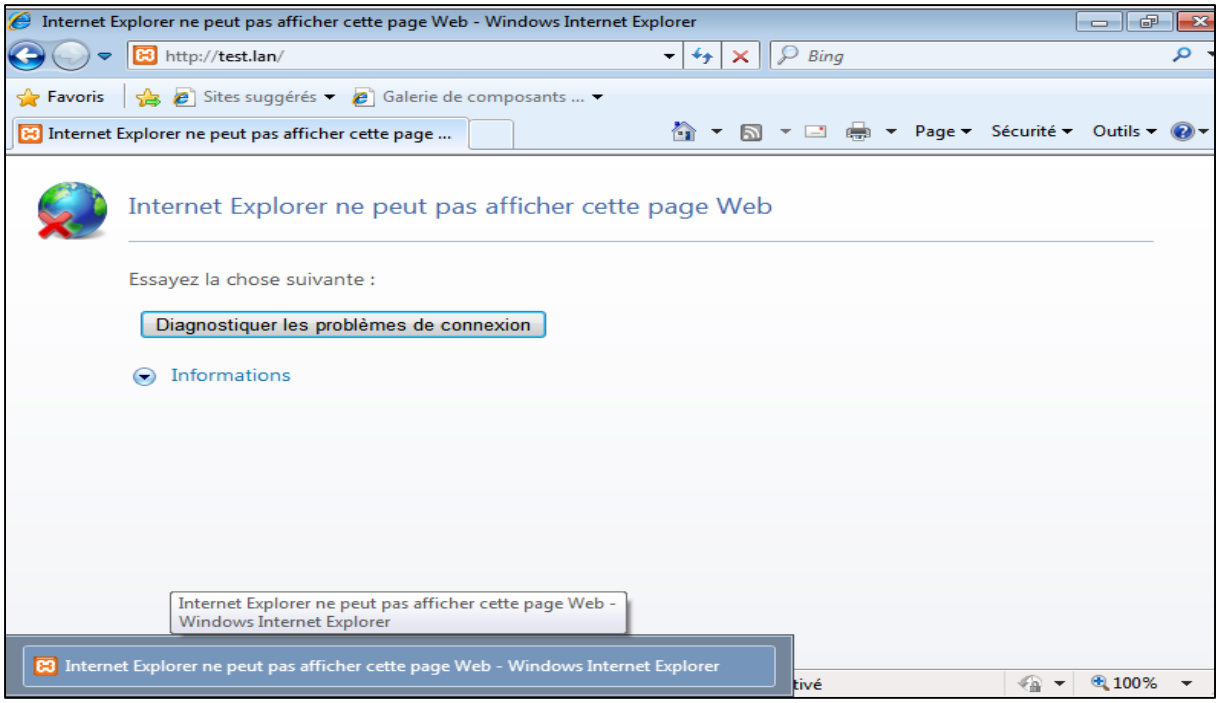

Figure III.25 : La connexion de la machine virtuelle« test »au server web xamp avec le nom de domaine « test.lan » après la mise de l'ACL.

6. La mise d'une VACL dans le Vlan 30 :

En ce moment, il n'est pas possible d'imiter les commutateurs Catalyst avec Dynamips / GNS3. Ceci est dû à l'impossibilité d'imiter les processeurs ASIC utilisés dans ce type de périphériques. Cependant on peut utiliser le module EtherSwitch avec les séries 2600, 3600 et 3700. En gardant à l'esprit que ce module fonctionne différemment (utilise la base de données vlan, etc.) et ne supporte pas la liste de contrôle d'accès VLAN (VACL) alors on va faire le test sur un switch federateur reel.

- On crée en premier lieu, une ACL étendu « VLAN30» qui permet d'identifier le trafic entre la machine d'adresse 192.168.2.2, et la machine d'adresse 192.168.2.3 du vlan 30 parce que nous voulons le bloquer. Donc il faut une règle « **permit »** qui y corresponde.

```
R2(config)# ip access-list extended VLAN30
R2(config-ext-nacl)# permit ip host 192.168.2.2 host 192.168.0.3
R2(config-ext-nacl)# permit ip host 192.168.2.3 host 192.168.2.2
R2(config- ext-nacl)#exit
```

Figure III. 26 : création d'une ACL étendu « VLAN30»

- On créer une **Vlan Access Map** qui est un élément qui combine les matches avec les actions, munie de deux règles.

1. Le trafic correspondant à l'acl « VLAN30 » doit être « droppé » **n° de séquence 10**
2. Le reste du trafic doit être « forwardé » **n° de séquence 20**

```
R2(config)#vlan access-map VMAP-VLAN30 10
R2(config-access-map)#match ip address VLAN30
R2(config-access-map)#action drop
R2(config-access-map)#exit
R2(config)#vlan access-map VMAP-VLAN30 20
R2(config-access-map)#action forward
R2(config-access-map)#exit
```

Figure III.27 : création de Vlan Access Map.

- On applique ces règles au **Vlan 30**

```
R2(config)# vlan filter VMAP-VLAN30 vlan-list 30
```

Figure III.28 : application du filtre

- La machine d'adresse 192.168.2.2 ping vers machine d'adresse 192.168.2.3, on voie que le trafic est bloqué.

```
VPCS#ping 192.168.2.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
VPCS #
```

Figure III.29 : Ping vers machine d'adresse 192.168.2.3

Conclusion

Sans VLAN un Switch considère toutes ces interfaces comme étant dans le même LAN et donc dans le même domaine de broadcast. Alors qu'avec les VLANs et les VACLs, un Switch peut mettre certaines de ces interfaces dans un domaine de broadcast. Ainsi, nous avons opté pour cette solution pour sécuriser le réseau de l'entreprise ENIEM.

Conclusion générale

Conclusion générale

Dans le cadre de notre projet de fin d'études, nous nous sommes penchés sur un des aspects majeurs des réseaux d'entreprises qui est la sécurité. A cet effet, nous avons testés l'utilisation conjointe des VLANs et des VACLs dans le réseau de l'entreprise ENIEM. Les différents droits d'accès aux machines et aux services est administrés selon le cahier des charges de l'entreprise ENIEM.

L'utilisation des VLANs permet de segmenter le réseau de l'entreprise en quatre sous-réseaux correspondant aux quatre unités de l'entreprise. Puis, afin de limiter les accès entre les différentes unités, nous avons mis en place des ACLs. Enfin, pour renforcer la sécurité, nous avons créés des VACLs pour limiter quelques accès entres les services (ressources humaine et commerciale) au sein d'un même Vlan.

D'après les tests de notre simulation, il apparaît que la segmentation d'un réseau en utilisant les VLANs facilite la gestion du réseau, réduit la quantité de trafic inutile sur le réseau et augmente les performances. Aussi, l'utilisation des VACLs limite le trafic au sein d'un même VLAN et augmente la quantité de données à analyser car tout le trafic de la couche 2 qui entre dans un VLAN est capturé.

Au terme des différents tests effectués, nous pouvons affirmer que l'utilisation des VLANs, des ACLs, et des VACLs comme solution pour formaliser le domaine de la sécurité informatique du réseau locale de l'entreprise, s'avère très efficace.

Comme perspective de notre travail, nous proposons de renforcer la sécurité du réseau en ajoutant un autre outil de sécurité, qui est le pare-feu niveau applicatif ou filtre d'application. En effet, ceci va permettre à l'administrateur d'avoir un contrôle complet des services utilisables, et il donne les différents détails des connexions et offre la possibilité d'authentification des utilisateurs.

Références bibliographiques

Bibliographie

[1] **C. Lorens, L, Levier,D. Valois. « Tableau de bord de la sécurité réseau». 2eme édition. 61, bld Saint-Germain 75240 Paris Ceex 05 : EDITION EYROLLES, 2006, 583 pages.**

[2] **Jean-François PILLOU, « Tout Sur Les Réseaux et Internet », DUNOD 2006. , 482 pages.**

[3] **Bernard Cousin. « Sécurité des réseaux informatiques », Rennes .1ere édition, 2005, 203 pages.**

[4] **http://www.commentcamarche.com**

[5] **http://www.courstechinfo.be/**

[6] **http://www.cisco.com/**

[7] **http://www.ciscoMadesimple.com/**

[8] **cours Cisco CCNA.**