République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université Abderrahmane Mira de Béjaïa

Faculté des Sciences Exactes

Département Informatique

Mémoire de fin de Cycle

En vue de l'obtention du diplôme de Master professionnel en informatique

Option : Administration et Sécurité des Réseaux

THÈME

Proposition de solution de sécurité pour le Réseau local de l'hôpital d'Amizour

Réalisé par :

Mr. Fares KHELOUFI
Mr. Yacine IKHLEF

Encadrés par :

M^me^ GHANEM Souhila

M^elle^ SADOU Malika

Jury :

Présidente : M^me^ GASMI Badrina

Examinatrice : M^me^ KHALED Hayette

2015 - 2016

Dédicaces

Ce modeste travail est dédié :

A nos chers parents qui nous ont soutenus et encouragés durant toute notre scolarité.

A nos frères et sœurs

A nos enseignants

A nos amis(e)

A toutes les personnes qui nous ont apportés de l'aide.

Remerciements

Nos premiers remerciements s'adressent à Dieu le tout puissant qui par sa bonté et sa miséricorde nous a permis d'avoir le courage, la foi et la volonté de mener à bien ce travail.

Nous tenons aussi à remercier notre encadreuse Madame GHANEM Souhila, et co-encadreuse Mademoiselle SADOU Malika qui ne nous a lésé d'aucune information, qui a été présente à tout moment de la réalisation de ce projet et surtout sans laquelle ce modeste travail n'aurait jamais vu le jour, ainsi que les membres du jury pour l'intérêt qu'ils ont portés à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.

Nous remercions également tous les professeurs qui ont contribués de près ou de loin à notre formation universitaire, sans oublier toute personne qui nous a aidés à mener à terme notre projet.

Merci à tous.

Table des matières

Listes des figures

Liste des Tableaux

Liste des abréviations

A

ACL	Access Control List
ARP	Adresse Resolution Protocol

C

CFI	Canonical Format Identifier
CLI	Commande Langage Interface

D

DES	Data Encryption Standard
DTP	Dynamic Trunking Protocol

E

EPH	Etablissement Public Hospitalier

F

FDDI	Fiber Distributed Data Interface
FTP	File Transfert Protocol

G

GVRP	GARP VLAN Registration Protocol

I

ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IPSec	Internet Protocol Security
IP	Internet Protocol
ISL	Inter Switch Link Protocol

L

LAN	Local Area Network
LLC	Logical Link Control
L2TP	Layer 2 Tunneling Protocol

M

MAC	Media Access Control
MAU	Multistation Access Unit
MAN	Métropolitains Area Network

O

OSI	Open Systems Interconnection

P

POP	Post Office Protocol
PPTP	Point-to-Point Tunneling Protocol
STP	protocole Spanning Tree

R

RARP	Reverse Address Resolution Protocol

S

SMTP	Simple Mail Transport Protocol

T

TELNET	TELe communication NETwork
TCP	Transmission Control Protocol
TCI	Tag Control Information
TPID	Tag Protocol Identifier

V

VID	VLAN ID
VLAN	Virtuel Local Area Network
VTP	Vlan Trunking Protocol
VPN	Virtual Private Network

W

WAN	Wide Area Network

Introduction Générale

L’humanité a longtemps imaginé un monde où nous contrôlons tout, un univers sans frontières ni limites où tout est possible, c’est de ces besoins qu’est née l’informatique, cette science qui met en œuvre des ensembles complexes de machines appelés Automates, Calculateurs, Ordinateurs, et Systèmes informatiques.

L’évolution de la technologie ne s’est pas arrêtée là, en effet un moyen de relier ces équipements informatiques fut élaborée, c’est ce qu’on appelle les réseaux informatiques, leur première apparition date de 1960, ces derniers permettent le partage d’informations et de données entre les équipements reliés entre eux.

Au départ les réseaux informatiques ont été conçus pour l’armée américaine, afin que cette dernière puisse protéger ses infrastructures informatiques contre d’éventuelles attaques, mais ces réseaux présentaient l’inconvénient de ne pouvoir couvrir que des distances géographiquement limitée.

Mais c’est surtout avec l’apparition d’internet que l’informatique a fait un bond en avant, les réseaux n’étaient plus limités, ils pouvaient enfin communiquer entre eux et ce indépendamment des distances, internet offre donc un grand éventail de possibilités, qui sont de plus en plus importantes de jour en jour, avec entre autre des connections haut débit comme le Câble ou l'ADSL.

Le rôle des réseaux a donc sensiblement évolué ces dernières années, la croissance phénoménale des établissements et entreprises au niveau architectural et financier a mené ces derniers à développer de nouveaux besoins pour la gestion et la coordination, et surtout la communication, la nécessité d’utiliser les réseaux et Internet était devenu plus qu’indispensable.

La sécurité des réseaux est donc devenue un des éléments-clés de la continuité des systèmes d'informations de l'entreprise quelle que soit son activité, sa taille et sa répartition géographique, ainsi l'hôpital d'Amizour nommé "**BENMERAD EL MEKKI**" ne fait pas exception à cette règle. En effet la nécessite de protéger les données sur les patients et les services disponibles, et la fragilité du réseau actuel aux différentes attaques internes et externes, nous ont poussé à réfléchir à comment sécuriser le réseau informatique de l'hôpital en question.

L'objectif de notre mémoire de fin de cycle est donc de proposer des solutions pour sécuriser le réseau local de l'hôpital d'Amizour avec l'implémentation d'une solution basée essentiellement sur les VLANs (Virtual Area Network).

Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, etc.) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

Dans le présent mémoire, nous présenterons en détail les étapes que nous avons suivies pour réaliser notre projet, illustrées en quatre chapitres organisés comme suit :

Le premier chapitre s'intitule « **Généralités sur les réseaux et la sécurité informatique** » où nous présenterons quelques concepts de base des réseaux informatiques, et certaines notions sur la sécurité informatique.

Dans le deuxième chapitre titré « **Introduction aux réseaux locaux virtuels**» nous définirons en premier lieu ce qu'est un réseau virtuel, ensuite nous parlerons de son fonctionnement et de ses objectifs. Nous finirons par citer les différents protocoles de mise en place, principalement VTP, sa compréhension nous aidera dans la réalisation.

Le troisième chapitre nommé «**Organisme d'accueil et conception de l'architecture LAN** » aura pour objectif de mieux comprendre l'organisme et sa structure hiérarchique, nous allons donc évoquer la problématique ainsi que la solution adéquate, nous finirons par présenter les différents équipements, interfaces et VLAN pour ensuite passer à l'étape de réalisation.

Dans le quatrième et dernier chapitre, nous allons enfin passer à la « **Réalisation** », cette phase est décomposée en deux parties, dans la première nous introduirons les outils et logiciels ayant servi à l'élaboration du projet, tout en expliquant les configurations, nous passerons ensuite à la deuxième partie qui sera principalement consacrée à la création des VLANs.

Enfin, dans la conclusion générale, nous ferons une récapitulation du travail effectué ainsi que l'expérience acquise durant ce projet.

Chapitre 1 : Généralités sur les réseaux et la sécurité informatique

CHAPITRE 1 : Généralités sur les réseaux et la sécurité informatique

Introduction

Pour mener à bien notre projet qui est de proposer des solutions de sécurité pour le réseau local d'Amizour, nous devons commencer par expliquer le fonctionnement des réseaux informatiques, et définir certains concepts de la sécurité informatique.

Nous avons divisé ce premier chapitre en deux grandes parties. Dans la première, nous allons aborder les concepts des réseaux informatiques, en l'occurrence la classification, caractéristiques des réseaux locaux, du modèle OSI et du protocole TCP/IP, puis dans la deuxième partie nous passerons à la sécurité informatique, ses objectifs et son utilisation au sein des réseaux informatiques.

Partie I : Les réseaux informatiques

Dans cette première partie, nous allons définir quelques notions sur les réseaux informatiques et plus particulièrement sur les réseaux locaux.

I.1 Définition d'un réseau

D'une manière générale, un réseau n'est rien d'autre qu'un ensemble d'objets ou de personnes connectés ou maintenus en liaisons et dont le but est d'échanger des informations ou des biens matériels [3].

Un réseau informatique est un ensemble des ressources de communication (matérielles et logicielles), d'ordinateurs et des clients cherchant à exploiter ces ressources afin de répondre à un besoin d'échange d'informations.

I.2 Classification des réseaux

Nous distinguons différents types de réseaux classifiés selon leurs tailles, leurs vitesses de transfert des données, ainsi que leurs étendues.

I.2.1 Les réseaux locaux : Local Area Network (LAN)

Un réseau local est un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau dont la taille est de quelque kilomètres. Le débit est généralement compris entre 1 Mbit/s et 100 Gbit/s.

I.2.2 Les réseaux métropolitains : Métropolitains Area Network (MAN)

Un réseau MAN interconnecte plusieurs LANs géographiquement proches (au maximum quelques kilomètres) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer. Un MAN est formée de commutateurs ou de routeurs interconnectés par des liens de hauts débits (généralement de fibres Optiques).

I.2.3 Les réseaux distants : Wide Area Network (WAN)

Les réseaux WAN interconnectent plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un MAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles contrairement aux WAN qui fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau.

I.3 Caractéristiques des réseaux locaux (LANs)

Un réseau local se caractérise principalement par sa topologie (physique et logique), les média utilisés pour le transport, ainsi que le mode transmission.

a. Media de transmission : Dans les réseaux locaux, nous pouvons trouver plusieurs medias de transport, et parmi ces medias nous citons :

- Le câble coaxial.
- La paire torsadée.
- La fibre optique.
- Les ondes hertziennes.

b. Mode de transmission : Selon le sens des échanges, nous distinguons trois modes de transmission :

- La liaison simplex.
- La liaison half-duplex.
- La liaison full-duplex.

I.3.1 Les topologies d'un réseau

Pour pouvoir utiliser un réseau, Il faut définir, en plus du type de réseau, une méthode d'accès entre les ordinateurs, ce qui nous permettra de connaître la manière dont les informations sont échangées.

Il existe deux types de topologies : topologie logique et topologie physique [2].

- **La topologie logique** : Elle représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet,

Token ring et FDDI.

- **La topologie physique** : la topologie physique est la façon dont les équipements sont connectés physiquement les uns aux autres grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels (cartes réseau, etc.)

Nous distinguons principalement trois grandes topologies physiques dans les réseaux locaux, la topologie en bus, en étoile, et en anneau qui peuvent être combinées pour obtenir des topologies hybrides.

1) Topologie en bus

Une topologie en bus (Figure I.1**)** est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau.

Figure I.1 : Topologie en bus

Cette topologie a pour avantages d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui sera affecté.

2) Topologie en étoile

Dans une topologie en étoile (Figure I.2 **)**, les ordinateurs du réseau sont reliés à un système matériel appelé *hub* ou *concentrateur*. Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles nous pouvons connecter les câbles en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

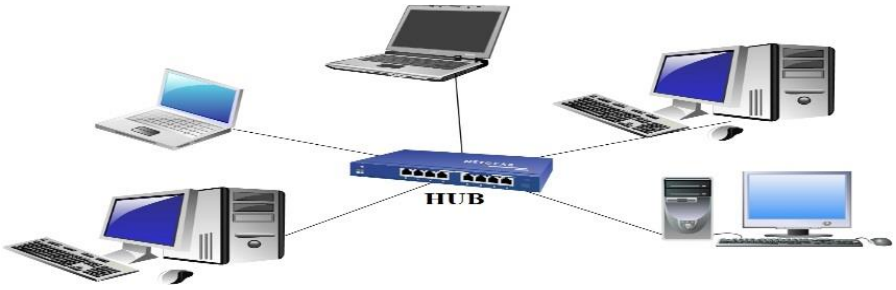

Figure I.2 : Topologie en étoile

Contrairement aux réseaux construits sur une topologie en bus, les réseaux à topologie en étoile sont beaucoup moins vulnérables car nous pouvons aisément retirer une des connexions en la débranchant du concentrateur sans pour autant paralyser le reste du réseau. En revanche, un réseau à topologie en étoile est plus coûteux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire à savoir le hub.

3) Topologie en anneau

Dans un réseau en topologie en anneau (Figure 1.3**)**, les ordinateurs communiquent chacun à leur tour, nous avons donc une boucle d'ordinateurs sur laquelle chacun d'entre-eux va avoir la parole successivement.

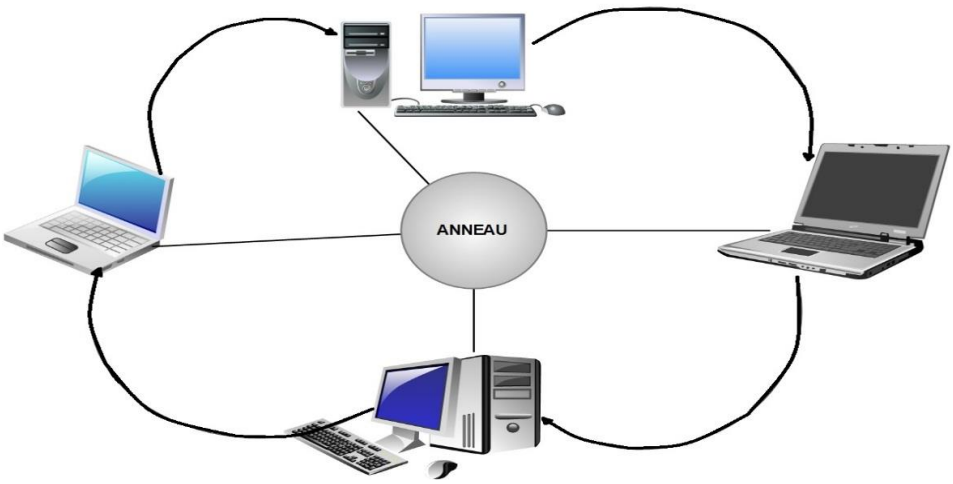

Figure I.3 : Topologie en anneau

En réalité les ordinateurs d'un réseau en topologie anneau ne sont pas reliés en boucle, mais sont reliés à un répartiteur appelé MAU (*Multistation Access Unit*) qui gère la communication entre les ordinateurs qui lui sont reliés en accordant à chacun d'entre-eux un temps de parole.

I.3.2 L'interconnexion d'un réseau local

La mise en place d'un réseau soulève de nombreuses questions sur les contraintes d'utilisation. Comment faire si le réseau à créer dépasse les distances maximales imposées par le type de câble utilisé ? Comment faire parvenir les informations à d'autres réseaux que le sien? Comment relier des réseaux utilisant des protocoles de communication différents? Toutes ces questions peuvent être résolue grâce à différents types de matériels qui sont [14]:

1. Répéteur: dispositif permettant d'étendre la distance de câblage d'un réseau local. Il amplifie et répète les signaux qui lui parviennent.

2. Pont : Un pont *(bridge)* est un dispositif permettant de relier des réseaux de même nature.

3. Routeur : Un routeur *(router)* est un dispositif permettant de relier des réseaux locaux de telle façon à permettre la circulation de données d'un réseau à un autre de façon optimale.

4. Passerelle : Une passerelle *(gateway)* est un dispositif permettant d'interconnecter des architectures de réseaux différentes .Elle assure la traduction d'un protocole d'un haut niveau vers un autre.

5. Concentrateur : Un concentrateur *(hub)* est un dispositif permettant de connecter divers élément de réseau.

6. Commutateur: Un commutateur *(Switch)* est un dispositif permettant de relier divers éléments tout en segmentant le réseau.

7. Adaptateurs: les adaptateurs *(adapter)* sont destinés à être insérés dans un poste de travail ou un serveur afin de les connecter à un système de câblage.

I.4 Le modèle de référence OSI

Un aspect important dans l'ouverture des réseaux a été la mise en place d'un modèle de référence, le modèle OSI (Open Systems Interconnection) (Figure I.4). Celui-ci définit en sept couches, présent sur chaque station qui désire transmettre. Chaque couche dispose de fonctionnalités qui lui sont propres et fournit des services aux couches immédiatement adjacentes. Même si le modèle OSI est très peu implémenté, il est toujours utilisé comme référence pour identifier le niveau de fonctionnement d'un composant réseau [6].

I.4.1 Principe du modèle

L'organisme ISO a défini en 1984 un modèle de référence, nommé Open System interconnections (OSI) destiné à normaliser les échanges entre deux machines. Il définit ainsi ce que doit être une communication réseau complète. L'ensemble du processus est ainsi découpé en sept couches hiérarchiques.

Ce modèle définit précisément les fonctions associées à chaque couche. Chacune d'entre elles se comporte comme un prestataire de service pour la couche immédiatement supérieure. Pour qu'une couche puisse envoyer une commande ou des données au niveau équivalent, elle

doit constituer une information et lui faire traverser toutes les couches inférieures, chacune d'elles ajoutant un en-tête spécifique, lesquels forment une sorte de train, à l'arrivée, cette information est décodée, la commande ou les données sont donc libérés.

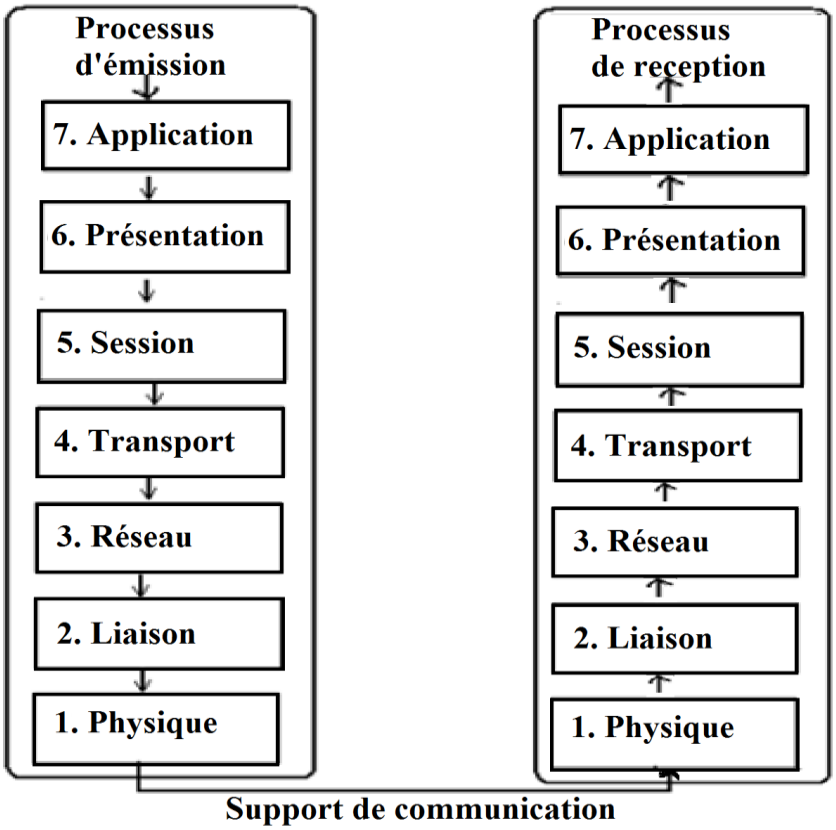

Figure I.4 : Modèle OSI.

I.4.2 Rôle des différentes couches

Chaque couche définie par le modèle a un rôle bien précis, qui va du transport du signal codant les données à la présentation des informations pour l'application du destinataire [4].

1. La couche physique : Elle convertit les signaux électriques en bits de données et inversement, selon qu'elle transmet ou reçoit les informations de la couche suivante.

2. La couche liaison : Elle est divisée en deux sous-couches :

- **La couche MAC** qui structure les bits de données en trames et gère l'adressage des cartes réseaux.
- **La couche LLC** qui assure le transport des trames et gère l'adressage des utilisateurs, c'est à dire des logiciels des couches supérieures.

3. La couche réseau : Elle traite la partie donnée utile contenue dans la trame. Elle connaît l'adresse de tous les destinataires et choisit le meilleur itinéraire pour l'acheminement. Elle gère donc l'adressage logique et le routage.

4. La couche transport : Elle segmente les données de la couche session, prépare et contrôle les taches de la couche réseau. Elle peut multiplier les voies d'accès et corriger les erreurs de transport.

5. La couche session : Son unité d'information est la transaction. Elle s'occupe de la gestion et la sécurisation du dialogue entre les machines connectées, les applications et les utilisateurs (noms d'utilisateurs, mots de passe, etc.)

6. La couche présentation : Elle convertit les données en informations compréhensibles par les applications et les utilisateurs ; syntaxe, sémantique, conversion des caractères graphiques, format des fichiers, cryptage, compression.

7. La couche application : c'est l'interface entre l'utilisateur ou les applications et le réseau. Elle concerne la messagerie, les transferts et partages de fichiers, l'émulation de terminaux.

I.5 Le modèle TCP/IP

Il est nommé ainsi car les protocoles de communications TCP et IP y sont les éléments dominants. Il faut noter que les protocoles TCP et IP ont été inventés bien avant le modèle qui porte leur nom et également bien avant le modèle OSI. Le modèle TCP/IP a été construit suite aux travaux du département de la défense américaine (Dod[2]) sur le réseau ARPANET, l'ancêtre d'internet, et sur le mode de communication numérique via des datagrammes. C'est suite à cette réalité technique qu'est venu se greffer la normalisation du modèle TCP/IP qui dans le principe et sur certaines couches s'inspire du modèle OSI [4].

I.5.1 Présentation du model TCP/IP

Les protocoles TCP/IP se situent dans un modèle souvent nommé "famille de protocoles TCP/IP".

I.5.2 IP (Internet Protocol)

IP est un protocole qui se charge de l'acheminement des paquets pour tous les autres protocoles de la famille TCP/IP. Il fournit un système de remise de données optimisées sans connexion. Le terme « optimisé » souligne le fait qu'il ne garantit pas que les paquets transportés parviennent à leur destination, ni qu'ils soient reçus dans leur ordre d'envoi. Ainsi, seuls les protocoles de niveau supérieur sont responsables des données contenues dans les paquets IP et de leur ordre de réception.

Le protocole IP travaille en mode non connecté, c'est-à-dire que les paquets émis sont acheminés de manière autonome (datagrammes), sans garantie de livraison.

I.5.3 TCP (Transmission Control Protocol)

TCP est le protocole IP de niveau supérieur. Il fournit un service sécurisé de remise des paquets. TCP fournit un protocole fiable, orienté connexion, au-dessus d'IP (ou encapsulé à l'intérieur d'IP). TCP garantit l'ordre et la remise des paquets, il vérifie l'intégrité de l'en-tête

des paquets et des données qu'ils contiennent. TCP est responsable de la retransmission des paquets altérés ou perdus par le réseau lors de leur transmission. Cette fiabilité fait de TCP/IP un protocole bien adapté pour la transmission de données basées sur la session, les applications client-serveur, et les services critiques tels que le courrier électronique.

La fiabilité de TCP a son prix. Les en-têtes TCP requièrent l'utilisation de bits supplémentaires pour effectuer correctement la mise en séquence des informations, ainsi qu'un total de contrôle obligatoire pour assurer la fiabilité non seulement de l'en-tête TCP, mais aussi des données contenues dans le paquet. Pour garantir la réussite de la livraison des données, ce protocole exige également que le destinataire accuse la réception des données**.**

Ces accusés de réception (ACK) génèrent une activité réseau supplémentaire qui diminue le débit de la transmission des données au profit de la fiabilité. Pour limiter l'impact de cette contrainte sur la performance, la plupart des hôtes n'envoient un accusé de réception que pour un segment sur deux ou lorsque le délai imparti pour un ACK expire.

Sur une connexion TCP entre deux machines du réseau, les messages (ou paquets TCP) sont acquittés et délivrés en séquence.

I.5.4 Description des couches TCP/IP

Les couches du modèle TCP/IP sont plus générales que celles du modèle OSI et elles sont comme suit :

1) Couche application : La Couche Application reprend les applications standards en réseau informatique et Internet. Elle dispose des protocoles suivants : SMTP (Simple Mail Transport Protocol), POP (Post Office Protocol), TELNET (TELe communication NETwork), FTP (File Transfert Protocol).

2) Couche transport : La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles, TCP (Transmission Control Protocol - protocole de contrôle de transmission), fournit d'excellents moyens de créer, en souplesse, des communications réseau fiables, circulant bien et présentant un taux d'erreurs peu élevé.

3) Couche Internet : La couche Internet est chargée de fournir le paquet des données. Elle définit les datagrammes et gère la décomposition / recomposition des segments. La couche Internet utilise les cinq protocoles suivants : IP (Internet Protocol), ARP (Adresse Resolution Protocol), ICMP (Internet Control Message Protocol), RARP (Reverse Address Resolution Protocol), IGMP (Internet Group Management Protocol).

4) Couche Accès réseau : Le nom de cette couche a un sens très large et peut parfois prêter à confusion. On lui donne également le nom de couche hôte-réseau. Cette couche se charge de tout ce dont un paquet IP a besoin pour établir une liaison physique, puis une autre liaison physique. Cela comprend les détails sur les technologies LAN et WAN, ainsi que tous les détails dans les couches physiques et liaison de données du modèle OSI.

La figure I.5 ci-dessous illustre les couches du model TCP/IP correspondantes au couches du modèle OSI.

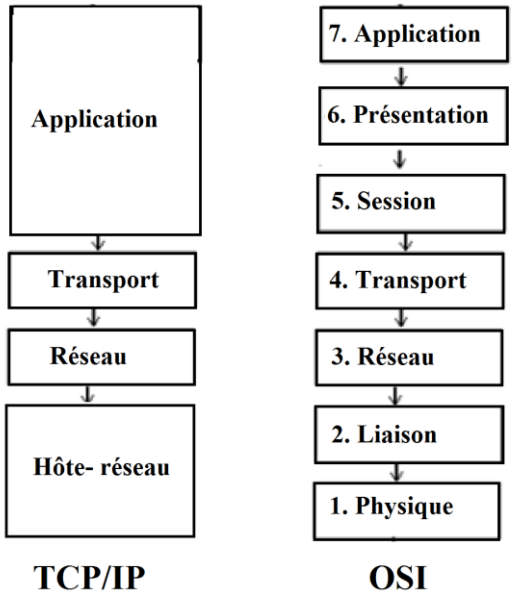

Figure I.5 : TCP/IP

Partie II : Sécurité informatique

La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

Nous allons maintenant parler de la sécurité informatique, ses objectifs et de son impact sur les réseaux.

II.1 Objectifs de la sécurité informatique

Le système d'information représente un patrimoine essentiel de l'organisation, qu'il convient de protéger.

La sécurité des systèmes d'information vise à assurer les propriétés suivantes [4] :

1. L'authentification : L'identification des utilisateurs est primordiale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

2. L'intégrité : S'assurer que les données ne sont pas être altérées de façon fortuite, les éléments considérés doivent être exactes et complets

3. La confidentialité : Limiter l'accès aux informations qu'aux personnes autorisées.

4. La disponibilité : Garantir le fonctionnement du système sans faille, et l'accès aux services et ressources installées avec le temps de réponse voulu.

5. La non-répudiation : C'est la propriété qui assure la preuve de l'authenticité d'un acte, c'est-à-dire qu'aucun utilisateur ne peut ensuite contester les opérations qu'il a réalisé, et qu'aucun tiers ne pourra s'attribuer les actions d'un autre utilisateur.

II.2 Terminologie de la sécurité informatique

L'ensemble des termes utilisés dans le domaine de la sécurité informatique peut se résumer ainsi [17] :

1) Vulnérabilité : Une vulnérabilité ou une faille est une faiblesse dans un système ou un logiciel permettant à un attaquant de porter atteinte à la sécurité d'une information ou d'un système d'information.

2) Menace : Ce sont les actions potentiellement nuisibles à un système informatique. Les menaces peuvent être le résultat de plusieurs actions en provenance de plusieurs origines.

3) Risque : Un risque désigne la probabilité d'un événement dommageable ainsi que les coûts qui s'ensuivent, le risque dépend également des montants des valeurs à protéger.

4) Attaque : Une attaque est l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant des systèmes et généralement préjudiciables. Et parmi les différentes attaques qui existent, nous pouvons citer : IP spoofing, Le Sniffing, lesVirus, les Ver, les attaques DoS, et Man in the middle.

II.3 La sécurité des réseaux informatiques

La sécurité des réseaux consiste à mettre en place des moyens en vue de garantir les propriétés de sécurité concernant des données critiques d'une entreprise, ainsi que de faire appliquer les règles définies dans une politique de sécurité, parmi lesquelles nous trouvons :

II.3.1 Pare-feu

Un pare-feu (Figure 1.6) est un système ou un groupe de systèmes qui gère les contrôles d'accès entre deux réseaux. Ces dispositifs filtrent les trames des différentes couches du modèle TCP/IP afin de contrôler leur flux et de les bloquer en cas d'attaques, celles-ci pouvant prendre plusieurs formes [1].

Le filtrage réalisé par le pare-feu constitue la première défense de la protection du système d'information. Il peut être composé de périphériques comportant des filtres intégrés dont la fonction principale est de limiter et de contrôler le flux de trafic entre les différentes parties des réseaux.

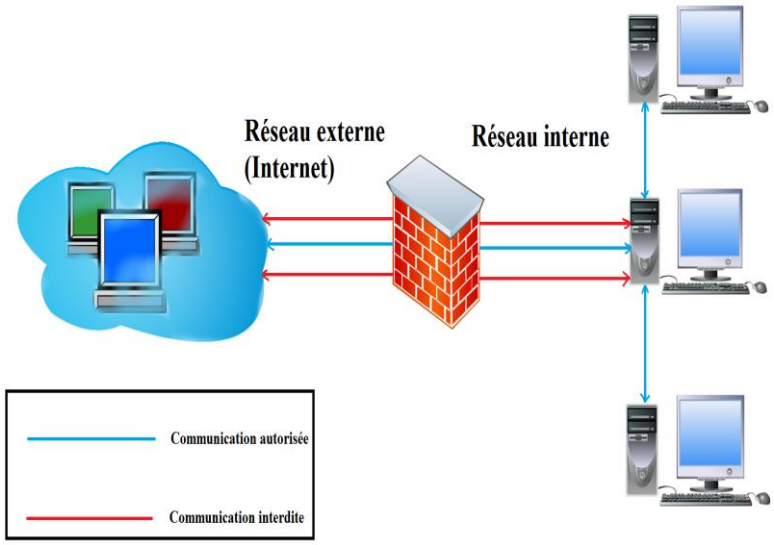

Figure I.6: Pare-feu

II.3.2 Les listes de contrôles d'accès (ACL)

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées généralement au trafic circulant via une interface de routeur (Figure I.7)

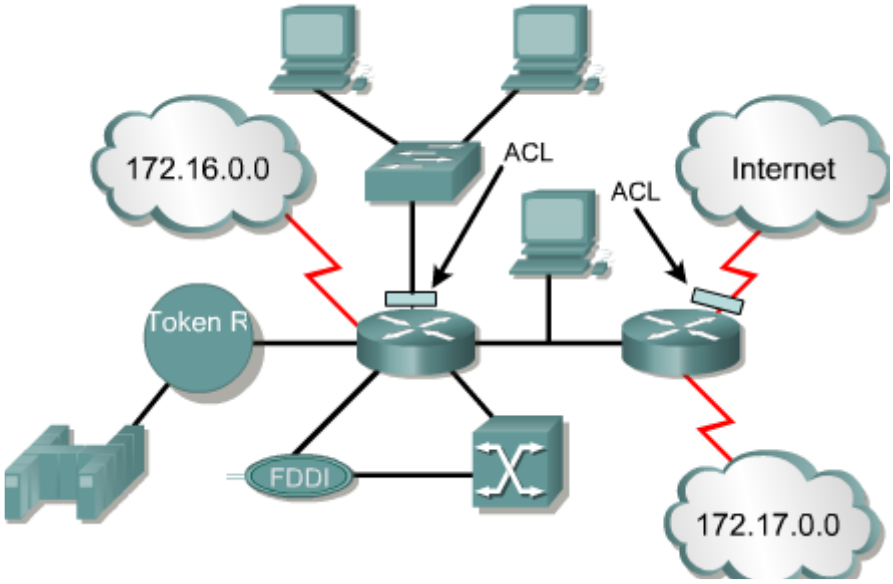

Figure I.7 : ACL

Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter. L'acceptation et le refus peuvent être basés sur des conditions précises. Les ACL permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie.

Des listes de contrôle d'accès peuvent être créées pour tous les protocoles routés, tels que les protocoles IP (Internet Protocol) et IPX (Internetwork Packet Exchange). Des listes de contrôle d'accès peuvent également être configurées au niveau du routeur en vue de contrôler l'accès à un réseau ou à un sous-réseau [13].

II.3.2.1 l'intérêt d'utiliser des ACL

Voici les principales raisons pour lesquelles il est nécessaire de créer des listes de contrôle d'accès :

- Limiter le trafic réseau et accroître les performances. En limitant le trafic vidéo, par exemple, les listes de contrôle d'accès permettent de réduire considérablement la charge réseau et donc d'augmenter les performances
- Contrôler le flux de trafic. Les ACL peuvent limiter l'arrivée des mises à jour de routage. Si aucune mise à jour n'est requise en raison des conditions du réseau, la bande passante est préservée
- Fournir un niveau de sécurité d'accès réseau de base. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section
- Déterminer le type de trafic qui sera acheminé ou bloqué au niveau des interfaces du routeur. Il est possible d'autoriser l'acheminement des messages électroniques et de bloquer tout le trafic via Telnet.
- Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.
- Filtrer certains hôtes afin de leur accorder ou de leur refuser l'accès à une section de réseau. Accorder ou refuser aux utilisateurs la permission d'accéder à certains types de fichiers, tels que FTP ou HTTP.

II.3.2.2 les types des listes contrôles d'accès

Il existe trois types d'ACL que voici :

a. Listes de contrôle d'accès standard : Les listes d'accès standard vérifient l'adresse d'origine des paquets IP qui sont routés. Selon le résultat de la comparaison, l'acheminement est autorisé ou refusé pour un ensemble de protocoles complet en fonction des adresses réseau, de sous-réseau et d'hôte.

b. Listes de contrôle d'accès étendues : Les listes d'accès étendues sont utilisées plus souvent que les listes d'accès standard car elles fournissent une plus grande gamme de contrôle. Les listes d'accès étendues vérifient les adresses d'origine et de destination du paquet, mais peuvent aussi vérifier les protocoles et les numéros de port. Cela donne une plus grande souplesse pour décrire ce que vérifie la liste de contrôle d'accès. L'accès d'un paquet peut être autorisé ou refusé selon son emplacement d'origine et sa destination, mais aussi selon son type de protocole et les adresses de ses ports.

c. Listes de contrôle d'accès nommées : Les listes de contrôle d'accès nommées IP ont été introduites dans la plate-forme logicielle Cisco IOS version 11.2, afin d'attribuer des noms aux listes d'accès standard et étendues à la place des numéros.

II.3.3 Proxy

Un système mandataire (Proxy) (Figure I.8) repose sur un accès à l'internet par une machine dédiée: le serveur mandataire ou Proxy server joue le rôle de mandataire pour les autres machines locales, et exécute les requêtes pour le compte de ces dernières [7].

Un serveur mandataire est configuré pour un ou plusieurs protocoles de niveau applicatif (http, FTP, SMTP, etc.) et permet de centraliser, donc de sécuriser, les accès extérieurs (filtrage applicatif, enregistrement des connexions, masquage des adresses des clients, etc.).

Les serveurs mandataires configurés pour http permettent également le stockage de pages web dans un cache pour accélérer le transfert des informations fréquemment consultées vers les clients connectés.

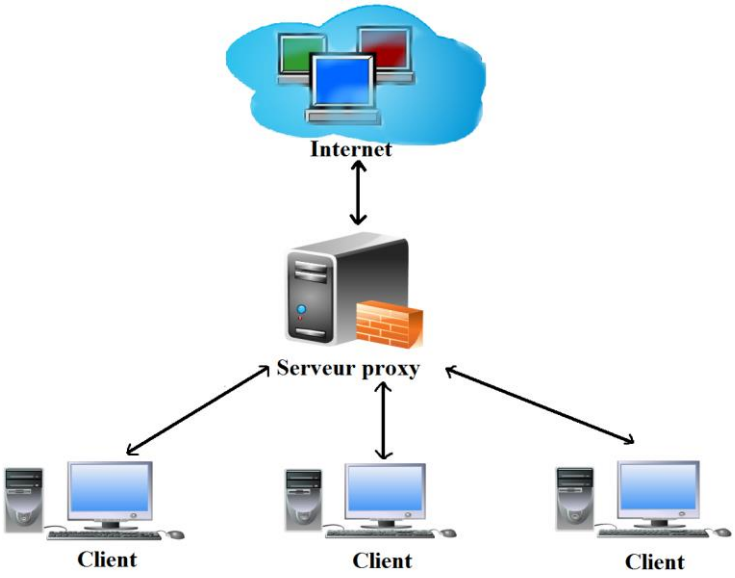

Figure I.8 : Proxy

II.3.4 Virtuel Local Area Network (VLAN)

Nombreuse sont les entreprises à recourir à la technologie VLAN, afin d'améliorer la sécurité et les performances de leur réseaux locaux.

Un VLAN ou réseau local virtuel est un regroupement de stations de travails indépendamment de la localisation géographique sur le réseau, ces dernières pourront communiquer comme si elles étaient sur le même segment.

Un VLAN permet de créer des domaines de diffusion (domaines de *broadcast*) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement, il existe plusieurs méthodes pour créer des VLAN [13]

a. VLAN par port : Également appelé VLAN de niveau 1, chaque port des commutateurs est affecté à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN.

b. VLAN par adresse MAC : ou VLAN par adresse IEEE sont des vlan de niveau 2, chaque adresse Mac est affectée à un VLAN, l'intérêt de ce type de VLAN est l'indépendance vis à vis de la localisation géographique.

c. VLAN par protocole : Dans ce cas, la communication ne se fera qu'entre les machines qui utilisent le même protocole, par application, c'est-à-dire par le numéro de port par exemple, ou par mot de passe suivant le login de l'utilisateur.

II.3.5 Cryptographie

La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage de données. Elle nous permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse les lire.

La cryptographie est divisée en deux types [5] :

a. cryptographie Symétrique : En cryptographie conventionnelle, également appelée cryptage de clé secrète ou de clé symétrique, une seule clé suffit pour le cryptage et le décryptage. La norme de cryptage de données (DES) est un exemple de système de cryptographie conventionnelle largement utilisé par le gouvernement fédéral des Etats-Unis. La Figure I.9 est une illustration du processus de cryptage symétrique.

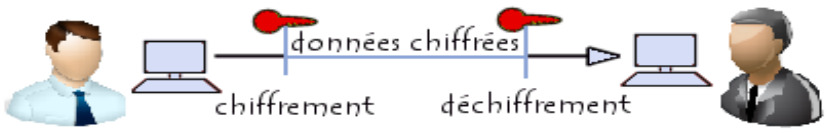

Figure I.9 : Cryptographie Symétrique

b. Cryptographie Asymétrique : La Cryptographie asymétrique (Figure I.10) ou à clé publique est un procédé asymétrique utilisant une paire de clés pour le cryptage : une clé publique qui crypte des données et une clé privée ou secrète correspondante pour le décryptage. Nous pouvons ainsi publier notre clé publique tout en conservant notre clé privée secrète. Tout utilisateur possédant une copie de notre clé publique peut ensuite crypter des informations que nous seuls pouvons lire.

D'un point de vue informatique, il est impossible de deviner la clé privée à partir de la clé publique. Tout utilisateur possédant une clé publique peut crypter des informations,

mais est dans l'impossibilité de les décrypter. Seule la personne disposant de la clé privée correspondante peut les décrypter

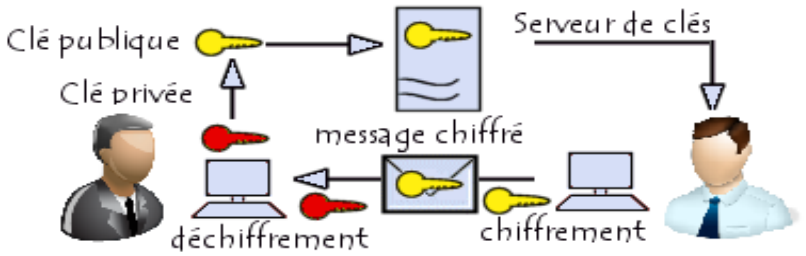

Figure I.10 : Cryptographie Asymétrique

c. Signature numérique : Les signatures numériques permettent au destinataire de vérifier authenticité des données, leur origine, mais également de s'assurer qu'elles sont intactes. Ainsi, les signatures numériques garantissent l'authentification et l'intégrité des données. Elles fournissent également une fonctionnalité de non répudiation. Ces fonctions jouent un rôle tout aussi important pour la cryptographie que la confidentialité, sinon plus. Une signature numérique a la même utilité qu'une signature manuscrite. Cependant, une signature manuscrite peut être facilement imitée, alors qu'une signature numérique est pratiquement infalsifiable. De plus, elle atteste du contenu des informations, ainsi que de l'identification du signataire.

d. Hachage : Le système décrit précédemment comporte certains problèmes. Il est lent et produit un volume important de données (au moins le double de la taille des informations d'origine). L'ajout d'une fonction de hachage à sens unique dans le processus permet d'améliorer ce système. Cette fonction traite une entrée de longueur variable afin d'obtenir en sortie un élément de longueur fixe, à savoir 160 bits. En cas de modification des données même d'un seul bit, la fonction de hachage garantit la production d'une valeur de sortie complètement différente.

II.3.6 Virtual Private Network (VPN)

Un VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers des réseaux peu sûrs comme peut l'être le réseau Internet. Les VPNs ont pour objectif de contribuer à la sécurisation des échanges de données privées, sensible sur les réseaux publics [12].

Un VPN fonctionne selon un système de tunnelisation privé, c'est-à-dire qu'un tunnel est créé, à l'intérieur duquel transitent toute la communication et ou toutes les données transmises qui sont cryptées. Un VPN est très fermé, un utilisateur non autorisé, ne peut en aucun cas avoir accès aux données transmises sur le réseau et en cas d'interceptions, les informations interceptées sont cryptées, illisibles, et donc inutilisables.

Le fonctionnement des VPN repose sur des technologies appelées protocoles de tunnelisation ou protocoles VPN et parmi eux nous retrouvons :

- Internet Protocol Security (IPSec).
- Layer 2 Tunneling Protocol (L2TP).
- Point-to-Point Tunneling Protocol (PPTP).
- Hybrid VPN.

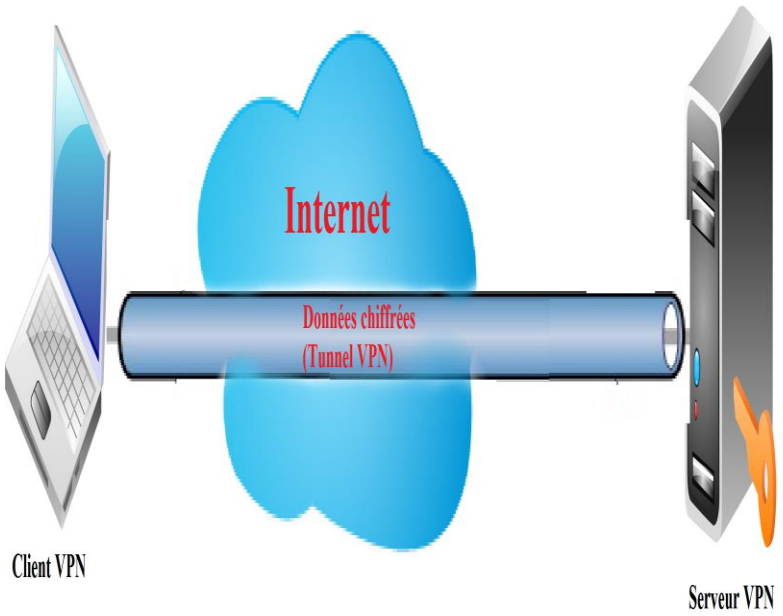

Figure I.11 : VPN

Conclusion

Ce chapitre nous a permis en premier lieu de découvrir et de mieux comprendre les notions et les aspects élémentaires des réseaux informatiques, où nous avons décrit les modèles OSI et TCP/IP, et en deuxième lieu de comprendre les concepts et objectifs de la sécurité informatique, et plus particulièrement la sécurité des réseaux où nous avons présenté brièvement les différentes politiques sécuritaires, comme les pare-feu, les proxys et surtout les VLANs que nous aborderons en détails dans le chapitre suivant.

Chapitre 2 : Introduction aux Réseaux Locaux Virtuels

CHAPITRE 2 : Introduction aux Réseaux Locaux Virtuels

Introduction

De nos jours, il est pratiquement devenu indispensable pour toute entreprise de posséder son propre parc de réseau informatique interne, permettant ainsi la communication de données ou tout simplement d'informations d'un pôle d'une entreprise à un autre, et se présentant sous la forme d'un ensemble de matériels réseaux (commutateurs, routeurs, etc.) reliés entre eux.

Cependant, il est parfois nécessaire de segmenter le réseau de façon logique pour des raisons sécuritaires principalement, et ce par la segmentation du réseau en plusieurs réseaux virtuels lesquels nous allons justement aborder dans ce chapitre (les différents types, raisons de leur utilisation, etc.). Mais avant tout, nous commencerons par un rappel sur le principe de la commutation.

2.1 Rappels sur la commutation

Les commutateurs ne sont rien d'autre que des ponts filtrants, certes équipés de fonctions plus nombreuses et de performances qui n'ont rien de comparable aux ponts que nous utilisons depuis plusieurs années [8].

Le travail de base d'un commutateur est de gérer des tables d'adressage : savoir sur quel port se trouve une adresse MAC afin d'éviter de diffuser le trafic inutile sur les segments des autres machines. Le nombre d'adresses MAC par port fait partie des caractéristiques du produit auxquelles l'administrateur du réseau doit s'intéresser afin de choisir le switch approprié.

Lorsque le réseau n'est pas bouclé (c'est à dire que pour aller d'un point à un autre du réseau il y a un et un seul chemin), cette gestion de tables d'adresses MAC est suffisante. Lorsqu'il peut y avoir plusieurs chemins pour aller d'un point à un autre du réseau il est nécessaire d'utiliser en plus des arbres de recouvrement (*spanning-tree* en anglais).

2.1.1 Spanning-Tree

Le protocole Spanning Tree (STP) est un protocole de couche 2 (liaison de données) conçu pour les commutateurs. Le standard STP est défini dans le document IEEE 802.1D-2004. Il permet de créer un chemin sans boucle dans un environnement commuté et physiquement redondant. STP détecte et désactive ces boucles et fournit un mécanisme de liens de sauvegarde. Le standard a été amélioré en incluant IEEE 802.1w Rapid Spanning Tree (RSTP).

Le protocole STP a pour but d'éviter les cycles (et donc des trames qui se baladent) et doit être recalculé à chaque modification de la topologie d'un réseau. Un effet visible de l'utilisation de cette technologie est les blocages de quelques secondes voire dizaines de secondes que les utilisateurs peuvent observer lorsqu'une machine est insérée dans un réseau sur lequel il y a un arbre de recouvrement (débranchez une machine d'un commutateur, rebranchez-la et observez : si votre réseau se bloque quelques temps c'est peut-être que votre commutateur recalcule son arbre de recouvrement) [10].

2.1.2 Domaine de Collision

Un domaine de collision est un ensemble d'entités (cartes réseaux) qui partagent le même média de communication. Tous les environnements à supports partagés, notamment ceux que vous créez au moyen de concentrateurs, sont des domaines de collision. Plus il y a de stations connectées par le biais d'un appareil fonctionnant au niveau 1 du modèle OSI, plus il y a de risques de collision. (Figure II.1) [16].

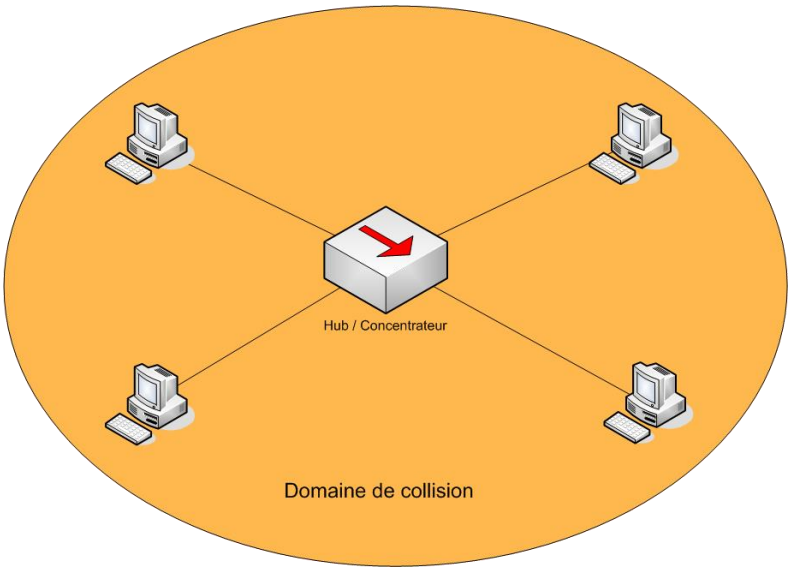

Figure II.1 : Domaine de Collision avec un Hub

Pour résoudre ce problème nous devons alors remplacer le hub par un commutateur(Switch), lequel crée une connexion réseau dédiée. Cette connexion est interprétée comme un domaine de collision individuel puisque le trafic reste indépendant de toutes les autres formes de trafic informatique, autrement dit il y aura alors un domaine de collision par port du switch, et le fait que le port du switch soit branché sur une unique carte réseau, élimine le risque de collision. (Figure II.2).

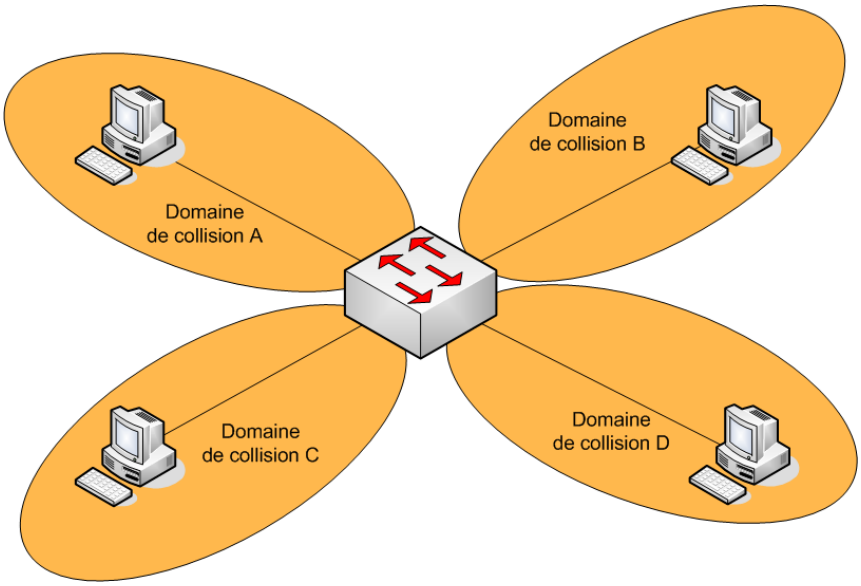

Figure II.2 : Domaine de collision avec un Switch

L'étendue et le nombre de domaines de collisions dépendent donc de l'équipement sur lequel les entités sont connectées.

2.1.3 Domaine de diffusion

Le domaine de diffusion sur la couche 2 est désigné par l'expression « domaine de diffusion MAC ». Ce domaine comprend tous les périphériques du réseau local qui reçoivent d'un hôte les trames de diffusion destinées à tous les autres ordinateurs du réseau local, il faut noter aussi qu'un domaine de diffusion englobe plusieurs domaines de collisions [11].

Quand on parle de domaine de broadcast, on prend l'hypothèse où l'entité émettrice souhaite envoyer une donnée à tout le monde, soit en broadcast. (Figure II.3).

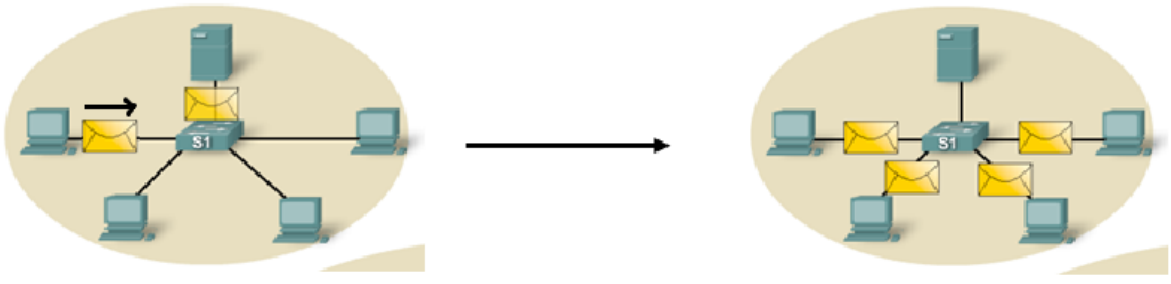

Figure II.3 : Domaine de diffusion

Dans le LAN, que ce soit avec un Hub, ou un Switch, la donnée sera propagée sur tous les ports parce que:

- Un hub ne lit pas le niveau 2 donc il transmet la donnée sur tous ses ports.
- Un Switch lit aussi le niveau 2 et comprend que la donnée est à destination de tout le monde (adresse MAC destination = ffff.ffff.ffff) donc il transmet cette donnée sur tous ses ports.

Il faut donc réduire le domaine de broadcast, et pour ce faire nous devons utiliser une fonctionnalité qui existe sur le Switch qui est la possibilité de "découper" le domaine de broadcast en plusieurs domaines de broadcast plus petits pour exploiter au maximum la bande passante de chaque domaine de collision. On ne parle plus alors de LAN mais de VLAN (Virtual LAN)**.**

2.2 Généralités sur les réseaux virtuels

L'idée de base des VLAN est de découper un seul réseau local (c'est à dire un ensemble cohérent d'infrastructures de niveau 2) en des réseaux logiques totalement disjoints : c'est comme si on avait plusieurs réseaux physiques totalement disjoints, un par VLAN. Ces réseaux partagent une même infrastructure [8] [9].

Nous nous situons bien ici au niveau de la couche liaison du modèle ISO, c'est à dire au niveau des trames (Ethernet, token-ring, FDDI pour citer quelques technologies). Pour utiliser des termes plus proches de la technologie ethernet on peut dire que chaque VLAN correspond à un domaine de diffusion indépendant des autres.

Les équipements modernes permettent à l'administrateur du réseau de construire des VLAN selon des critères techniques différents. Nous allons expliquer en quelques paragraphes à quoi correspondent les trois types de VLAN que l'on rencontre le plus fréquemment.

2.2.1 L'intérêt d'avoir des VLANs

Il existe plusieurs intérêts à avoir des VLAN dans un réseau, voici quelques exemples de besoins qui nécessitent l'utilisation des réseaux virtuels:

- **La sécurité** : Les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité.
- **Réduction des coûts :** Des économies sont réalisées grâce à l'utilisation plus efficace de la bande passante et des liaisons ascendantes existante.

- **Meilleures performances :** Le fait de diviser des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques (domaines de diffusion) réduit la quantité de trafic inutile sur le réseau et augmente les performances.

- **Atténuation des tempêtes de diffusion :** Le fait de diviser un réseau en plusieurs réseaux VLAN réduit le nombre de périphériques susceptibles de participer à une tempête de diffusion.

- **Efficacité accrue du personnel informatique :** Les VLAN facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseau similaires partagent le même VLAN.

- **Gestion simplifiée de projets ou d'applications** : La séparation des fonctions facilite la gestion d'un projet ou l'utilisation d'une application

2.2.2 Les différents types de VLAN

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

a. Les VLAN par port : Chaque port physique du commutateur est configuré par l'administrateur du réseau pour appartenir à un VLAN, et toute machine (ou ensemble de machines) qui se trouve branchée sur ce port fera partie de ce VLAN. C'est le mode de fonctionnement le plus simple et le plus déterministe, c'est à dire celui où potentiellement les défauts de logiciel sont le moins probable. Ce type de réseaux virtuels n'a rien de bien innovant. Lorsque les équipements réseau étaient simples et fiables, on faisait déjà des VLAN par port tout simplement en construisant des réseaux physiquement séparés, chacun ayant son câblage et ses propres équipements actifs. C'est bien le branchement physique sur un port d'un concentrateur plutôt qu'un port d'un autre concentrateur qui déterminait l'appartenance à un réseau.

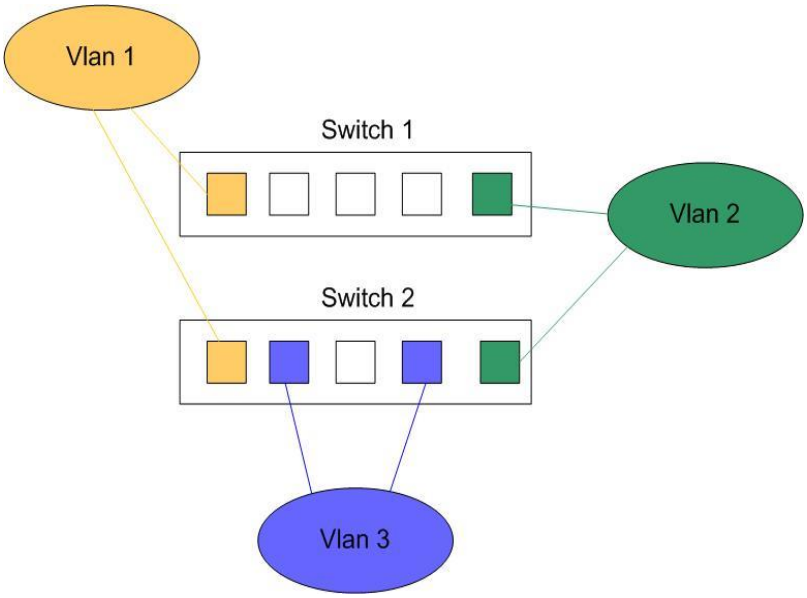

Figure II.4: VLAN par port

b. Les VLAN par adresse Mac : Dans ce modèle, le VLAN auquel appartient une station est déterminé par son adresse MAC. Les adresses MAC étant physiquement liée aux stations, ce modèle permet de conserver la répartition des VLANs même après le déplacement d'une station. Contrairement au modèle de VLAN basé sur le port, des stations appartenant à des VLAN différents peuvent être connectées au même port d'un commutateur. Une station peut théoriquement être membre de plusieurs VLANs différents. Le principal inconvénient de ce modèle est la mise à jour des correspondances entre les VLANs et les adresses MAC, qui peut être ardue dans des réseaux de grande taille.

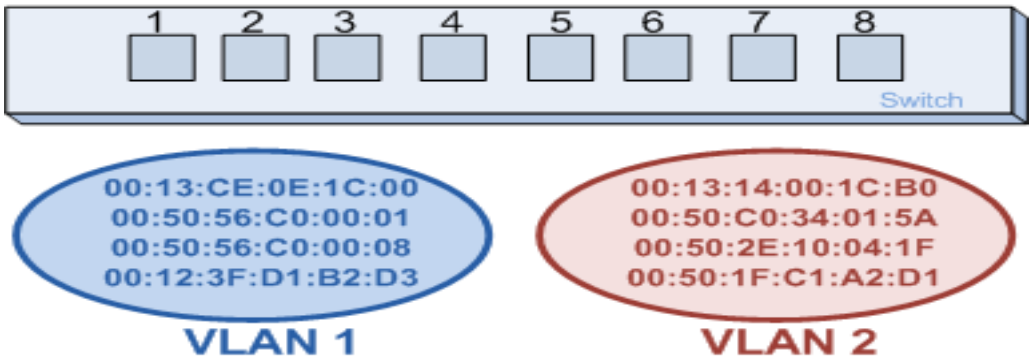

Figure II.5 : VLAN par adresse MAC

c. Le VLAN par protocole : Un VLAN par protocole, ou VLAN de niveau 3, est obtenu en associant un réseau virtuel par type de protocole rencontré sur le réseau. On peut ainsi

constituer un réseau virtuel pour les stations communiquant avec le protocole TCP/IP, un réseau virtuel pour les stations communiquant avec le protocole IPX, etc.

Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN. Par contre, elle est légèrement moins performante puisque les commutateurs sont obligés d'analyser des informations de niveau 3 pour fonctionner. Les VLAN par protocole sont surtout intéressant dans des environnements hétérogènes multi-protocoles (Novell Netware avec IPX, Unix avec TCP/IP, Macintosh avec Appletalk, etc.). La généralisation de TCP/IP leur a fait toutefois perdre de l'intérêt.

2.3 Les protocoles de transport des VLANs

Afin d'assurer le transport des VLANs, certains protocoles ont été mis en place :

2.3.1 La norme 802.1q

Ici, l'idée serait d'arriver à ce que certains ports du switch puissent être assignés à plusieurs VLANs, ce qui fera économiser du câble et aussi des ports sur le switch.

Le principe consiste à ajouter dans l'en-tête de la trame Ethernet un marqueur qui va identifier le VLAN. Il existe quelques solutions propriétaires pour réaliser ceci, mais le système s'est avéré tellement intéressant qu'une norme a été définie, il s'agit de la norme 802.1q. [12]

1) Description de la norme

Le tableau suivant illustre la modification de la trame Ethernet et l'ajout d'un champ sur 4 octets par la norme 802.1Q :

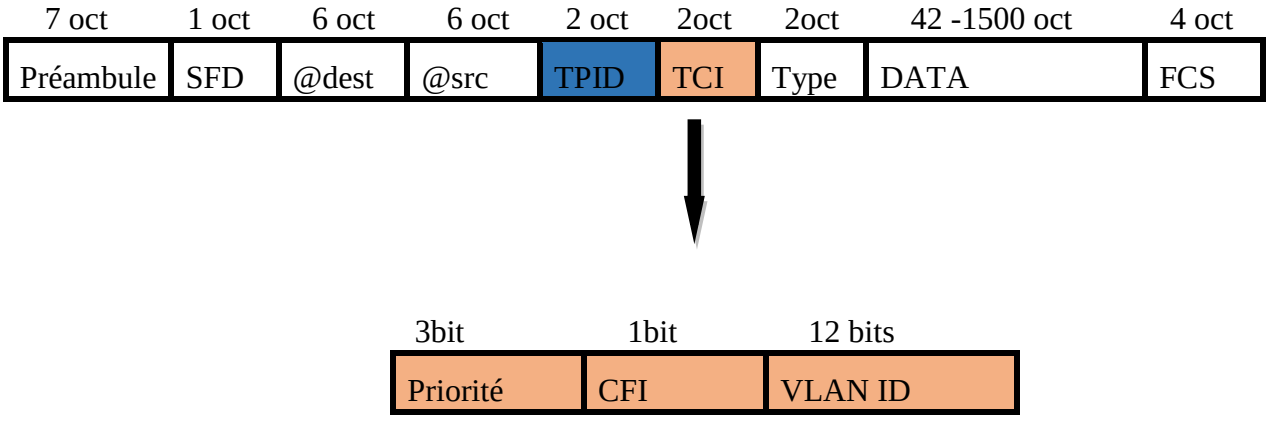

Tableau II.1: Extension de la trame Ethernet modifiée par la norme 802.1Q.

2) Tag Protocol Identifier (TPID)

C'est la partie qui définit le protocole de tag utilisé. Dans le cas du 802.1Q on trouvera comme valeur (en notation hexadécimale) : 0x8100.

3) Tag Control Information (TCI)

Cette partie se compose de trois champs :

a) User Priority : 3 bits utilisés pour coder 8 niveaux de priorité (de 0 à 7). On se sert de ces 8 niveaux pour fixer la priorité des trames d'un VLAN par rapport à d'autres

Exemple d'utilisation : on favorise un VLAN sur lequel on utilise la visioconférence (nécessitant beaucoup de bande passante) par rapport à un VLAN où l'on ne fait qu'envoyer et recevoir des mails.

b) Canonical Format Identifier(CFI) : Ce champ d'un bit assure la compatibilité entre adresses MAC Ethernet et Token Ring. Un commutateur Ethernet fixe cette valeur à 0 [12].

c) VLAN ID (VID) : C'est le champ d'identification du VLAN auquel appartient la trame par l'intermédiaire de ce champ de 12 bits, on peut coder 4094 VLAN (les valeurs 0 et FFF sont réservées). La valeur par défaut est 1.

<table>
<tr><td rowspan="2">2 octets

TPID

16 bits</td><td colspan="3">2 octets
TCI</td></tr>
<tr><td>USER Priority

5bits</td><td>CFI

1bit</td><td>VLAN ID

12bits</td></tr>
</table>

Tableau II.2 : Détails du champ 802.1Q

2.3.2 Le protocol ISL (Inter Switch Link Protocol)

Pour étendre les réseaux virtuels sur plus d'un commutateur, CISCO a mis au point son propre protocole ISL. Ce protocole achemine les informations d'appartenance aux réseaux virtuels. ISL représente en fait une structure de trame et un protocole qui, en plus de transport

des informations d'appartenance aux réseaux virtuels, permet à ces réseaux d'échanger des trames [19].

a) Présentation générale

Pour identifier les réseaux virtuels, ISL utilise un mécanisme de marquage explicite des paquets. Un commutateur qui utilise ce marquage encapsule la trame reçue dans un paquet dont l'en-tête contient un champ d'appartenance aux VLAN et l'adresse MAC de la trame, permettant d'acheminer le paquet vers le routeur et les commutateurs appropries.

Lorsqu'elle atteint le réseau destination, on supprime l'en-tête, et la trame est acheminée vers l'équipement récepteur.

b) Structure des trames ISL

Les trames ISL comprennent trois champs principaux :

- Un en-tête qui est constitué de plusieurs champs.
- Trame encapsulée dont la longueur est comprise entre 1 et 24575 octets.
- Champ CRC, ce champ qui est ajouté à la fin du paquet ISL, porte sur l'intégrité du paquet.

Le tableau II.3 ci-après illustre la structure d'une trame ISL :

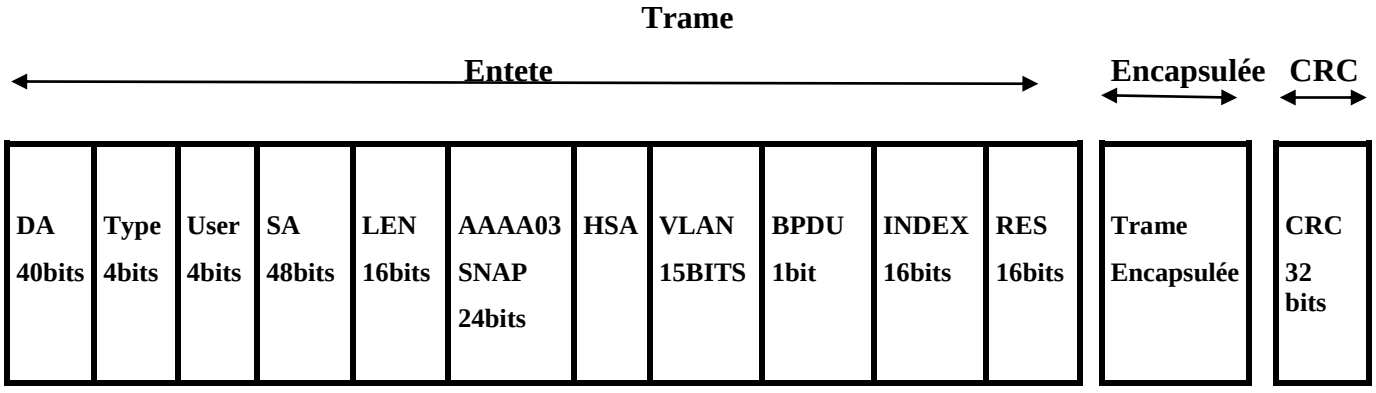

Tableau II.3 : structure de la trame ISL

2.3.3 La notion des trunks

Pour distribuer le réseau local virtuel on utilise des trunks. Un trunk est en fait la connexion physique sur laquelle transitent les trames de plusieurs VLANs. Ces trames sont identifiées par le VID afin d'arriver à bon port. On peut placer un trunk entre deux commutateurs, entre un commutateur et un hôte supportant le trunking et enfin entre un commutateur et un routeur pour effectuer un routage inter-VLAN. Il ne faut pas oublier que les VLANs transitant sur un même trunk se partagent la bande passante, c'est pourquoi il est

recommandé d'utiliser des connexions à débit important, comme du Gigabit Ethernet ou de la fibre optique dans le meilleur des cas.

Ce schéma ci-dessous (Figure II.6) nous illustre la liaison de trunk entre deux commutateurs :

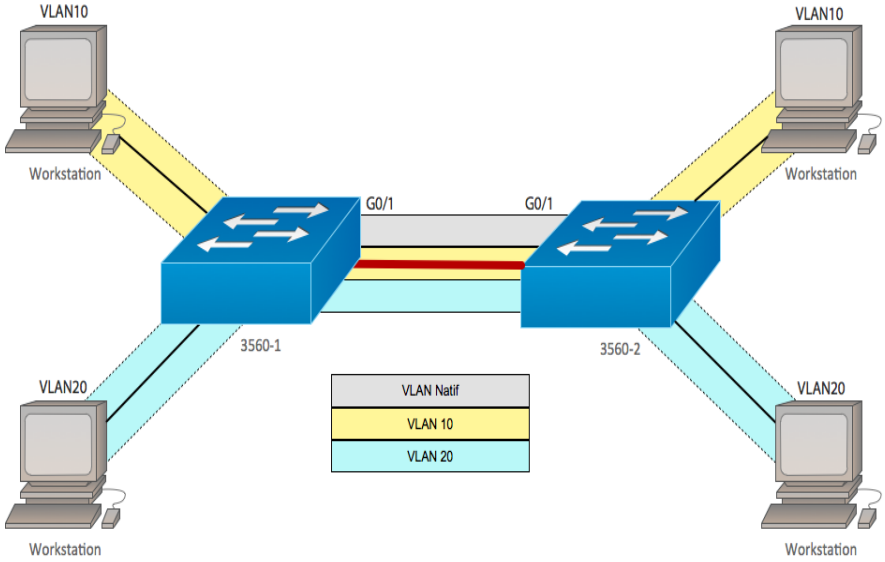

Figure II.6 : Utilisation du trunk entre deux commutateurs.

2.4 Quelques protocoles d'administration et de gestion des VLANs

Il est possible de configurer le 802.1q à la main pour permettre le transport des VLANs.

Pour cela, il faut configurer chaque port se trouvant sur le chemin d'un port tagué d'un VLAN à un autre. Il faut de plus répéter l'opération pour chaque lien défini.

On peut comprendre que le processus s'avère long et fastidieux. La norme prévoit donc des mécanismes pour taguer les ports automatiquement et administrer les VLAN d'une manière plus simple, plus abrégée et plus embryonnaire. Pour cela plusieurs protocoles ont été défini tels que le VTP, GVRP, DTP.

Dans ce qui suit, nous n'allons définir que le protocole VTP propriétaire CISCO, lequel nous allons utiliser par la suite dans le chapitre réalisation.

2.4.1 Le protocole VTP (VLAN Trunking Protocol)

Afin de ne pas redéfinir tous les VLANs existant sur chaque commutateur, CISCO a développé un protocole permettant un héritage de VLANs entre commutateurs. C'est le protocole VTP. Ce protocole est basé sur la norme 802.1q et exploite une architecture client-serveur avec la possibilité d'instancier plusieurs serveurs [12].

1. Comprendre le VTP (VLAN Trunking Protocol)

Un commutateur doit alors être déclare en serveur, on lui attribue également un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifie ou supprimé. Ainsi chaque commutateur client présent dans le domaine héritera automatiquement des nouveaux VLANs créent sur le commutateur serveur.

La mise en place d'un domaine VTP permet de centraliser la gestion des VLANs, ce qui peut s'avérer plus que plaisant dans un environnement abondamment commuté et comprenant de multiples VLANs.

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants :

a. Mode serveur, dans lequel le commutateur est chargé de diffuser la configuration aux commutateurs du domaine VTP.
b. Mode client VTP, dans lequel le commutateur applique la configuration émise par un commutateur en mode serveur.
c. Mode transparent, dans lequel le commutateur ne fait que diffuser, sans prendre en compte, la configuration du domaine VTP auquel il appartient.

2. Exemple d'utilisation des VTP

Pour comprendre le fonctionnement des VTP, nous allons l'illustrer dans cet exemple ci-dessous (Figure II.7**)**.

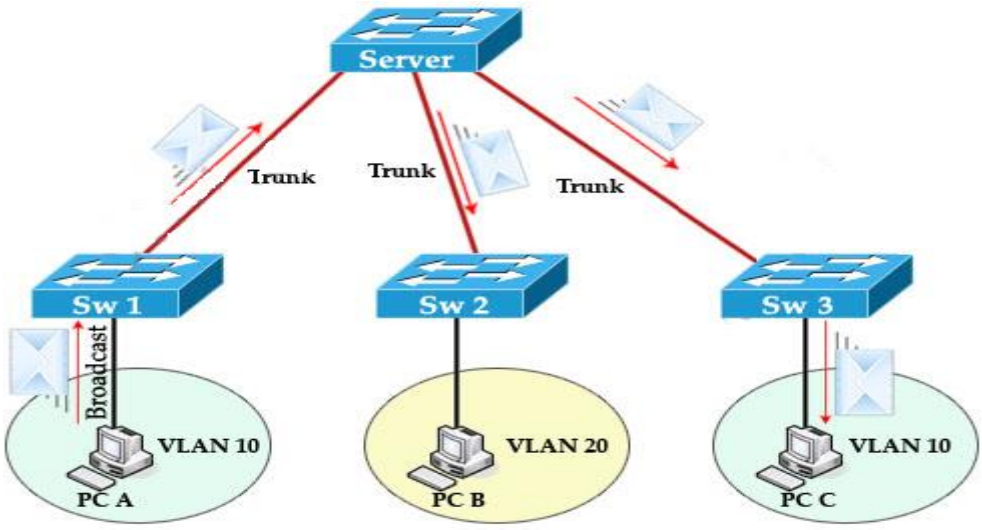

Figure II.7 : Fonctionnement du protocole VTP.

Les administrateurs peuvent changer les informations des VLAN sur les switchs fonctionnant en mode serveur uniquement. Une fois que les modifications sont appliquées, elles sont distribuées à tout le domaine VTP au travers des liens "trunk". En mode transparent, les modifications sont locales mais non distribuées. Les switchs en mode client appliquent automatiquement les changements reçus du domaine VTP.

Les configurations VTP successives du réseau ont un numéro de révision. Si le numéro de révision reçu par un switch client est plus grand que celui en cours, la nouvelle configuration est appliquée. Sinon, elle est ignorée. Quand un nouveau switch est ajouté au domaine VTP, le numéro de révision de celui-ci doit être réinitialisé pour éviter les conflits.

Conclusion

Nous avons vu tout au long de ce chapitre que la technologie des VLANs repose sur des concepts principaux et essentiels tels que la limitation des domaines de broadcast, la mobilité des utilisateurs et sans oublier le point important de notre but qu'est la sécurité.

En effet, grâce à cette technologie nous pouvons mettre à profit la technique de la commutation pour donner plus de flexibilité aux réseaux locaux tout en gardant une sécurité assez fiable et moins couteuse au sein de l'entreprise.

Toutes ces raisons nous ont motivées à proposer les VLANs comme solution pour sécuriser le réseau LAN de l'hôpital d'Amizour, mais avant tout, nous devons d'abord étudier l'architecture existante du réseau, afin de savoir comment organiser l'ensemble des services dans des réseaux virtuels, et tout ça sera aborder dans le chapitre suivant.

Chapitre 3 : Organisme d'accueil et Conception de l'Architecture LAN

Chapitre 3 : Organisme d'accueil et conception de l'architecture LAN

Introduction

Une bonne compréhension de l'environnement informatique aide à déterminer la portée du projet d'implémentation de la solution. Il est essentiel de disposer d'informations précises sur l'infrastructure réseau physique et les problèmes qui ont une incidence sur le fonctionnement du réseau. En effet, ces informations affectent une grande partie des décisions que nous allons prendre dans le choix de la solution et de son déploiement.

Nous allons donc décomposer ce chapitre en deux parties, la première sera consacrée à la présentation de l'hôpital d'Amizour, ainsi que l'architecture de son réseau.

Dans la deuxième partie nous allons concevoir l'architecture LAN qui nous servira pour la simulation tout en désignant les équipements et les interfaces que nous utiliserons.

Partie I : Organisme d'accueil

Nous allons donc commencer par une présentation de l'hôpital d'Amizour et de son parc informatique.

I.1 Présentation de l'hôpital

L'Etablissement public Hospitalier d'Amizour, baptisé « Hôpital BENMERAD EL MEKKI dont l'ouverture remonte au cours de l'année 1992 pour renforcer le secteur sanitaire d'Amizour.

Application du décret exécutif 07-140 de 19 mai 2007 portant création organisation et fonctionnement des EPH et des EPSP.

Implanté à 24 Km au sud du chef-lieu de la wilaya de Bejaia, sa capacité d'accueil est de 224 lits techniques, la population couverte s'élève à environ 160 000 habitants relevant des huit communes (Amizour, Barbacha, El Kseur, Smaoun, Benidjelil, Feraoun, Kendira et fenaia) ainsi que la population relevant des communes, des wilayas limitrophes (Sétif…..).

I.2 Historique

Le secteur sanitaire d'Amizour a été créé en 1981 suivant le décret n° :242/81 du : 05.09.1981 et a été rendu officiel selon le décret n° :254/85 du : 22.10.1985.

Le secteur sanitaire a assuré une couverture sanitaire de 03 DAIRA : Amizour, EL- Kseur et Barbacha qui regroupent huit (08) communes réparties comme suit :

1) **Daïra d'Amizour :**

- Commune d'Amizour
- Commune de Feraoun
- Commune de Smaoun
- Commune de Beni –Djellil

2) Daïra d'EL-Kseur :

- Commune d'EL-Kseur
- Commune de Toudja

3) Daïra de Barabcha :

- Commune de Barbacha
- Commune de Kendira

Le secteur sanitaire d'Amizour a fonctionné sans structure d'hospitalisation jusqu'en 1992 date de réception et de mise en service d'un hôpital d'une capacité de 240 lits.

I.3 Les différentes infrastructures du secteur sanitaire d'Amizour :

Le secteur sanitaire dispose des infrastructures suivantes :

- Un hôpital 240 Lits techniques (196 Lits organisés-arrêté N°57-04 DU 24.11.2004)
- Quatre (04) polycliniques (une polyclinique pour 39568 habitants)
- Six (06) centres de santé (soit un (01) centre pour 36379 habitants)
- Un (01) service d'épidémiologie et de médecine préventive (SEMEP) En 2007, le secteur est bien divisé en deux structures à savoir :

  - **Etablissement public hospitalier d'Amizour**
  - **Etablissement public de santé de proximité d'El-Kseur**

Conformément au décret n° : 07-140 du 19mai 2007 portant création, organisation et fonctionnement établissement public de sante de proximité

I.4 Mission et objectif de l'hôpital

L'établissement public hospitalier a pour mission la prise en charge de manière intégrée et hiérarchisée les besoins sanitaires de la population dans ce cadre, il est chargé de :

- D'assurer l'organisation et la programmation des soins curatifs de diagnostic.
- La prise en charge total des malades durant leurs hospitalisations.

L'E.P.H peut servir de terrain de formation médicale et paramédicale comme il contribue au perfectionnement et au recyclage des personnels de services.

I.5 Capacité de l'Etablissement

L'hôpital est composé d'un plateau technique et des services d'hospitalisation

I.5.1 Le Plateau technique

Le pavillon des urgences médico-chirurgicales (20 lits organisés) se compose de deux unités.

a. Unité d'accueil, tri, et mise en observation :

- partie réservée aux adultes : 07 lits
- partie réservée aux adultes : 03 lits

b. Réanimation médicale :

- unité d'hospitalisation : 05 lits

c. Le Bloc opératoire :

- 04 salles opératoires , dont 01 pour les urgences
- Une salle de réanimation chirurgicale : 05 lits

d. Un service d'imagerie médicale : avec deux salles de radiologies conventionnelles et d'une salle de scanner.

e. Un service de laboratoire d'analyse médicale.

f. Un service pharmacie.

g. Une banque de sang.

h. Un bureau des entrées.

I.5.2 Service d'hospitalisation : l'hôpital dispose de divers services d'hospitalisation :

- Pédiatrie
- Maternité –Gynécologie
- Médecine interne
- Chirurgie Générale
- Oncologie
- Réanimation médicale

Outre les services sus cités, l'hôpital dispose d'un service d'épidémiologie et d'un service de médecine du travail.

I.6 Organisation de l'EPH d'Amizour :

Comme tous les établissements public, l'E.P.H d'Amizour est doté : d'une direction, d'un secrétariat et de quatre sous directions comme suit :

- Sous-direction des ressources humaines.
- Sous-direction des finances et des moyens.
- Sous-direction des services sanitaires.
- Sous-direction de la maintenance des équipements médicaux et des équipements connexes.

I.6.1 Organigramme de l'établissement public Hospitalier D'Amizour (EPH)

Voici le schème général de l'EPH, dont chaque direction a pour but d'assurer le bon fonctionnement de chaque partie du groupe comme le montre la Figure III.1

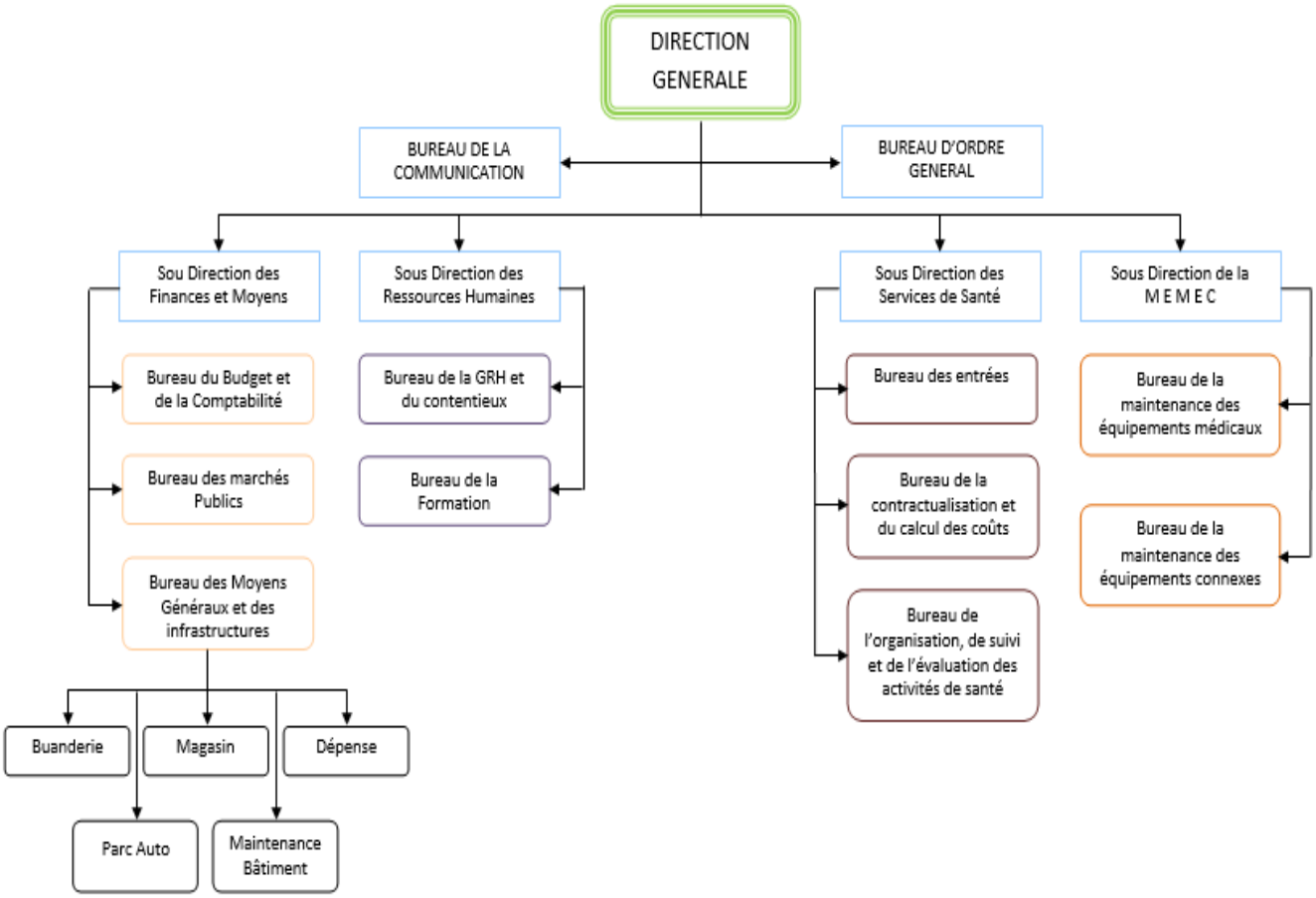

Figure III.1 : Organigramme de l'EPH

I.7 L'informatique dans l'hôpital

Vu le nombre important de patients à consulter et surtout pour faciliter la gestion de l'information les concernant, l'EPH dispose d'un réseau local câblé. Ce réseau informatique encore embryonnaire utilise un certain nombre de matériels et logiciels nécessaires à la bonne gestion de l'Hôpital.

I.7.1 Le parc informatique

L'EPH dispose d'un parc informatique composé de:

- Cinquante-deux (52) ordinateurs de bureau de marque HP équipés d'un dual-core, tous protégés par des onduleurs 500 VA de marque APC.

- Quatre (4) imprimantes matricielles et treize (13) imprimantes lasers de marque HP
- 5 switch d'accès de marque TP LINK.
- D'un modem-routeur de marque TP LINK.
- 2 serveurs de marque HP.

Il faut également noter la présence circonstancielle d'ordinateurs portables au sein du parc informatique de l'hôpital, apportés et utilisé par le personnel au sein de la structure.

Caractéristiques du Processeur	**Ram**	**Disque dur**	**Système d'exploitation**
2.4-3 GHz	2 GO	250-320 GO	Windows XP, Win7

Tableau III.1 : Caractéristiques des ordinateurs de l'EPH

I.7.2 Environnement serveur

L'EPH dispose en tout de deux serveurs:

- un serveur se trouvant au bureau des entrées, servant à héberger le logiciel patient partagé entre les différents services de l'hôpital, et le directeur.
- un autre serveur qui se situe au niveau du centre de calcul contenant le logiciel comptable.

I.7.3 Le matériel d'interconnexion

Les équipements d'interconnexion représentent le cœur du réseau dans une architecture.

S'ils sont mal dimensionnés, ils pourront avoir des effets négatifs sur le trafic du réseau, pouvant entrainer la détérioration de celui-ci. Dans notre cas d'étude, l'infrastructure du réseau de L'EPH étant embryonnaire, ne comporte qu'un commutateur (TP LINK) de 24 ports, 1 de 16 ports, et 3 de 8 ports pour l'interconnexion des différents clients et d'un modem routeur (TP-LINK) permettant l'accès à internet (Tableau III.2).

Equipement	**Marque**	**Nombre**	**Rôle**
Modem-Routeur	TP-LINK	1	Pour l'accès internet
Switch	TP-LINK	4	Pour interconnecter les ordinateurs

Tableau III.2 : les équipements d'interconnexion de l'EPH

I.7.4 Les applications

Les principaux systèmes d'exploitation utilisés par les machines au sein de l'EPH sont

Windows XP et Windows 7 pour les ordinateurs de bureau. Afin de suivre convenablement les patients au sein des différentes unités de 1'hôpital, un certain nombre de logiciels et de programmes sont utilisés, il s'agit:

- De l'application « Patient» utilisé par les médecins pour la saisie des informations concernant les patients et les différentes mesures à prendre en compte, cette application est utilisée par les différents services d'hospitalisation et du directeur.
- Une application appelée « COMPTABLE» est utilisé au niveau du centre de calcul permettant d'assurer la comptabilisation et ce pour établir les états financiers de l'hôpital.

I.7.5 Présentation du réseau

Dans le souci de faciliter le partage d'information entre les différentes unités de l'hôpital un réseau informatique local a été installé.

Un câblage filaire avec une topologie physique en étoile utilisant des câbles pour la liaison entre les ordinateurs de bureau et le Switch.

La plupart des ordinateurs de bureau fonctionnent en réseau avec une topologie étoile à travers le Switch qui est relié au modem routeur pour l'accès à internet.

I.7.6 Architecture du réseau

La Figure III.2 présente la topologie physique du réseau de l'EPH

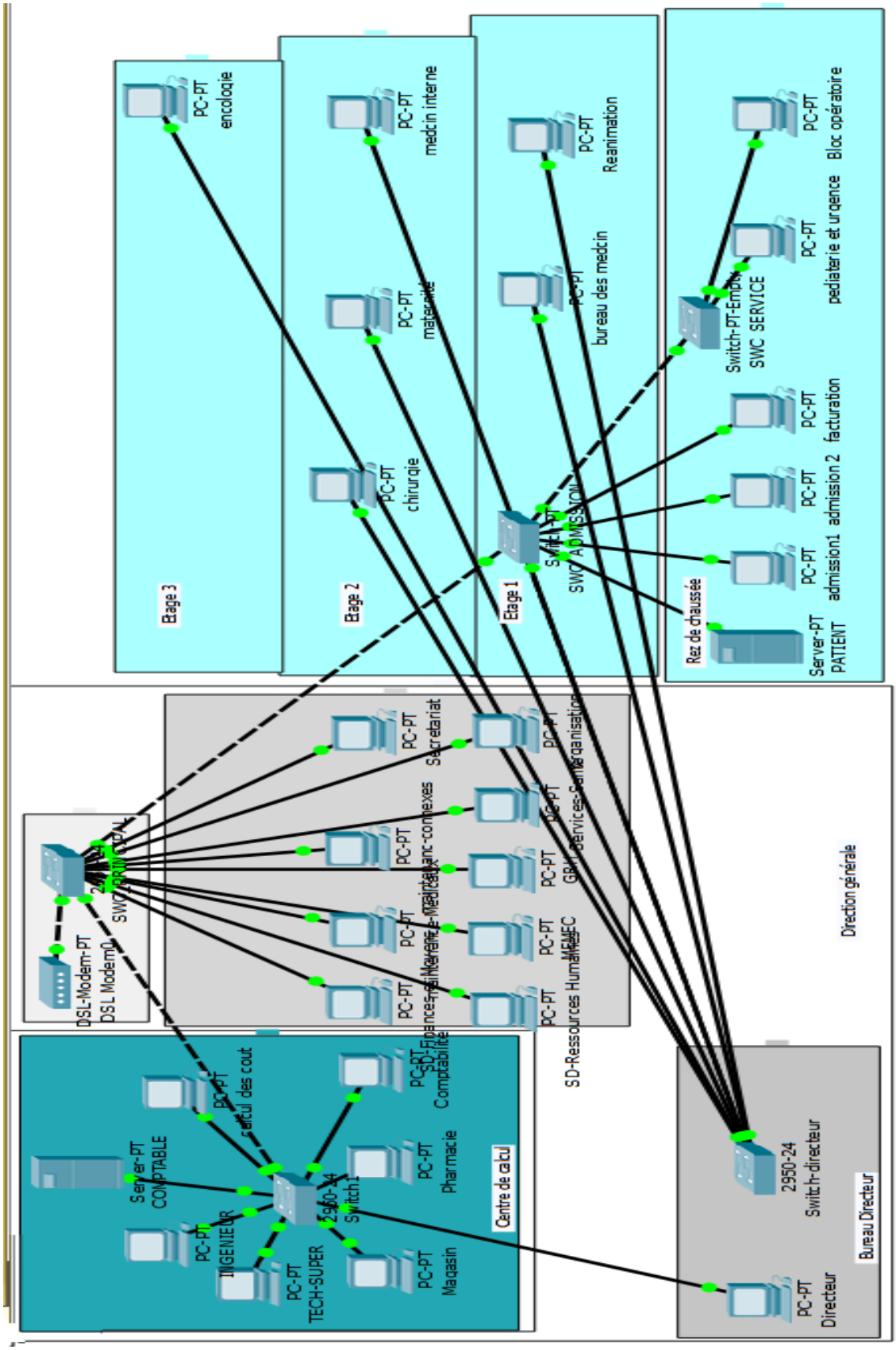

Figure III.2: Topologie physique du réseau de l'EPH

I.8 Problématique

L'étude du réseau de l'hôpital nous a permit de détérminer un nombre important de contraintes pouvant réduire ses performances, voir sa dégradation, nous avons :

- l'absence de segmentation du réseau en sous-réseau favorise l'action des utilisateurs pirates.
- L'absence de points d'acces wifi.
- L'allocaiton des adresses IP se fait de manière statique.
- L'absence d'un routeur.
- La non tolérance au pannes

Les questions principales que nous posons sont alors : comment filtrer les données circulant dans le réseau local ? Et comment pouvons-nous réduire les domaines de Broadcast ?

I.10 Spécification des besoins

Suite à l'étude critique de l'existant et aux échanges effectués avec le responsable informatique de l'EPH, plusieurs besoins ont été relevés, à savoir:

- Besoin de mettre en place des points d'accès Wi-Fi afin de couvrir toute la zone souhaité.
- Besoin de contrôler toute personne souhaitant se connecter au réseau Wi-Fi pour accéder à internet.
- Besoin de tolérance aux pannes.
- Besoin de segmenter le réseau câblé en plusieurs VLAN.
- Besoin de ajouter un commutateur de niveau 3 pour une meilleure gestion des Vlan.
- Besoin de mettre en place un serveur DHCP pour l'allocation dynamique des adresses IP.
- Besoin de mettre en place des listes de contrôles d'accès.
- La nécessité d'avoir un routeur pour de futures communications avec d'autres réseaux d'hôpitaux.

.

I.11 Solutions proposées

L'objectif de notre projet est de proposer des solutions afin de renforcer la politique de sécurité du réseau local pour cela :

Nous devons utiliser les VLAN afin de créer un ensemble logique isolé pour améliorer la sécurité du réseau local (LAN). C'est pour cela que nous découperons le réseau en plusieurs réseaux virtuels.

Il nous faudra également insérer des listes de contrôles d'accès dans le Switch-cœur afin d'offrir une couche de sécurité supplémentaire. En effet les ACL sont particulièrement adaptés pour autoriser ou refuser le trafic entrant et sortant de manière sélective.

Partie II : Conception des architectures

Nous allons maintenant passer à la conception de l'architecture que nous proposons.

II.1 Présentation général du modèle type

Notre modèle type se compose d'un réseau local (LAN) compose d'un routeur, un modem-routeur et un Switch-cœur, avec des Switchs d'accès.

Pour assurer la disponibilité et la continuité de fonctions, le routeur est lié avec le Switch-cœur et ce dernier avec tous les Switch d'accès.

Nous allons également mettre en place un serveur DHCP pour une affectation dynamique d'adresses IP, ainsi que des points d'accès Wifi.

II.2 Présentation des équipements utilisés pour la simulation

Les équipements réseau utilisées sont présentés dans le tableau qui suit :

Les équipements	**La marque et le type**
Switch Principal	Cisco Catalyst 3560
Switch d'accés	Cisco Catalyst 2950
Routeur	Cisco ISR 1841

Tableau III.3 : Présentation des équipements

II.3 Nomination des équipements et des VLANs

Nous allons nominer les équipements utilisés et les différents VLANs dont nous aurons besoin.

II.3.1 Nomination des équipements

Nous nominons les équipements par des noms significatifs pour faciliter la conception de l'architecture du réseau local. Les switch d'accès seront nominés selon leur emplacement par exemple: centre de calcul (SWC_CALCUL), bureau des admissions (SWC_ADMISSION).

Switch princpale	**Switch d'accès**	**Serveur**	**Routeur**
SWC_SERVEUR	SWC_SERVICE	SRV_DHCP	EPH_AMIZOUR
	SWC_ADMISSION	SRV_PATIENT	
	SWC_CALCUL	SRV_COMPTABLE	
	SWC_DG		
	SWC_DIRECTEUR		

Tableau III.4 : Les noms des équipements

II.3.2 Nomination des VLANs

Pour notre réseau nous avons choisie l'adresse 10.10.0.0/24 que nous allons utiliser pour la segmentation du réseau en VLANs par port (Tableau III.5).

Nom	**Numéro**	**Adresse IP**	**Masque Réseau**
VLAN_DG	VLAN 10	10.10.10.0/24	255.255.255.0
VLAN_CALCUL	VLAN 11	10.10.12.0/24	255.255.255.0
VLAN_ADMISSION	VLAN 12	10.10.12.0/24	255.255.255.0
VLAN_URGENCE	VLAN 13	10.10.13.0/24	255.255.255.0
VLAN_OPERAT	VLAN 14	10.10.14.0/24	255.255.255.0
VLAN_MATERN	VLAN 15	10.10.15.0/24	255.255.255.0
VLAN_BDM	VLAN 16	10.10.16.0/24	255.255.255.0
VLAN_REA	VLAN 17	10.10.17.0/24	225.255.255.0
VLAN_MI	VLAN 18	10.10.18.0/24	255.255.255.0
VLAN_CHIRURGIE	VLAN 19	10.10.19.0/24	255.255.255.0
VLAN_ENCOLOGIE	VLAN 20	10.10.20.0/24	255.255.255.0

VLAN_SRVDHCP	VLAN 21	10.10.21.0/24	255.255.255.0
VLAN_DIRECTEUR	VLAN 22	10.10.22.0/24	255.255.255.0
VLAN_COMPTABLE	VLAN 23	10.10.23.0/24	255.255.255.0
VLAN_SRVPATIENT	VLAN 24	10.10.24.0/24	255.255.255.0
VLAN_SRVCOMPT	VLAN 25	10.10.25.0/24	255.255.255.0

Tableau III.5 : Nomination des VLAN

II.3.3 Les VTP

Le protocole VTP assure la cohérence de la configuration VLAN en gérant l'ajout, la suppression et le changement de nom des réseaux locaux virtuels sur plusieurs commutateurs d'un réseau.

Le tableau III.6 ci-dessous montre la configuration du VTP :

Switch	**Mode VTP**
SWC_ PRINCIPAL	Serveur
SWC_SERVEUR	Client
SWC_DISTRIBUTION1	Client
SWC_DISTRUBTION2	Client
SWC_ADMISSION	Client
SWC_CALCUL	Client
SWC_DG	Client

Tableau III.6 : les modes VTP

II.4 Désignation des interfaces

Les interfaces sur les équipements sont indiquées dans le tableau suivant (Tableau III.7) :

Local Device	**Remote Device**	**Interface Local**	**Interface Remote**
SWC_PRINCPAL	SWC_SERVEUR	Fa0/21	Gig0/1
	SWC_DISTRIBUTION1	Fa0/24	
	SWC_DISTRIBUTION2	Fa0/23	
SWC_SERVEUR	SRV_DHCP	Fa0/1	/
	SRV_PATIENT	Fa0/2	
	SRV_COMPTABLE	Fa0/3	
SWC_DISTRIBUTION1	SWC_ADMISSION	Fa0/21	/
	SWC_CALCUL	Fa0/23	
	SWC_DG	Fa0/22	
SWC_DISTRIBUTION2	SWC_ADMISSION	Fa0/21	/
	SWC_CALCUL	Fa0/23	
	SWC_DG	Fa0/22	
SWC_ADMISSION	PC_ ADMISSION1	Fa0/1	/
	PC_ ADMISSION2	Fa0/2	
	PC_ FACTURATION	Fa0/3	
	PC_MATERNITE	Fa0/4	/
	PC_PEDIATERIE	Fa0/5	
	PC_BUREAU_MEDECIN	Fa0/6	
	PC_OPERATOIRE	Fa0/7	
	PC_REA	Fa0/8	
	PC_MEDECINE_INTERNE	Fa0/9	
	PC_CHIRURIGIE	Fa0/10	
	PC_ENCOLOGIE	Fa0/11	
SWC_CALCUL	PC_DIRECTEUR	Fa0/8	/
	PC_CALCUL-COÛTS	Fa0/7	
	PC_PHARMACIE	Fa0/1	
	PC_MAGASIN	Fa0/2	
	PC_COMPTABLE	Fa0/3	
	PC_INGENIEUR	Fa0/4	

	PC_TECH_SUPER	Fa0/6	
SWC_DG	PC_SD-Finances et Moyens	Fa0/3	/
	PC_MEMEC	Fa0/4	
	PC_GRH	Fa0/8	
	PC_Services-Santé	Fa0/9	
	PC_ORGANISATION	Fa0/10	
	PC_SD-Ressources Humaines	Fa0/11	
	PC_maintenance-connexes	Fa0/6	
	PC_maintenance-Médicaux	Fa0/5	
	PC_SECRETARIAT	Fa0/2	

Tableau III.7 : Désignation des interfaces

Conclusion

La première partie de ce chapitre nous a permis d'avoir une vue globale sur l'établissement publique hospitalier d'Amizour, nous avons éclairci notre thème en mettant en avant une problématique bien précise ce qui nous a conduit logiquement à la proposition d'une solution qui se résume principalement à l'insertion des ACL et une segmentation du réseau en VLANs.

La deuxième partie a été consacrée à la conception de l'architecture du réseau informatique où nous avons désigné, nominé les différents équipements, interfaces et les différents VLANs que nous utiliserons dans la phase de réalisation.

Chapitre 4 :

Réalisation

Chapitre 4 : Réalisation

Introduction

Dans ce chapitre, nous allons passer à la dernière étape qui est la réalisation. Cette phase est cruciale pour la mise en place de tout ce que nous avons vu et fait auparavant, nous implémenterons la solution précédemment proposée et conçu, pour ce faire nous commencerons par la présentation du simulateur utilisé, puis nous expliquerons en détail les différentes étapes suivies pour la réalisation de l'architecture LAN et la création des VLANs.

4.1 Présentation du simulateur « Cisco Packet Tracer »

Packet Tracer est un simulateur de matériel réseau Cisco .Cet outil est créé par Cisco Systems qui le fournit gratuitement aux centres de formation, étudiants et diplômés participants, ou ayant participé, aux programmes de formation Cisco (Cisco Networking Academy). Le but de Packet Tracer est d'offrir aux élèves et aux professeurs un outil permettant d'apprendre les principes du réseau, tout en acquérant des compétences aux technologies spécifiques de Cisco. Il peut être utilisé pour s'entraîner, se former, préparer les examens de certification Cisco, mais également pour de la simulation réseau.

Pour notre travail nous avons utilisé la version 6.3.

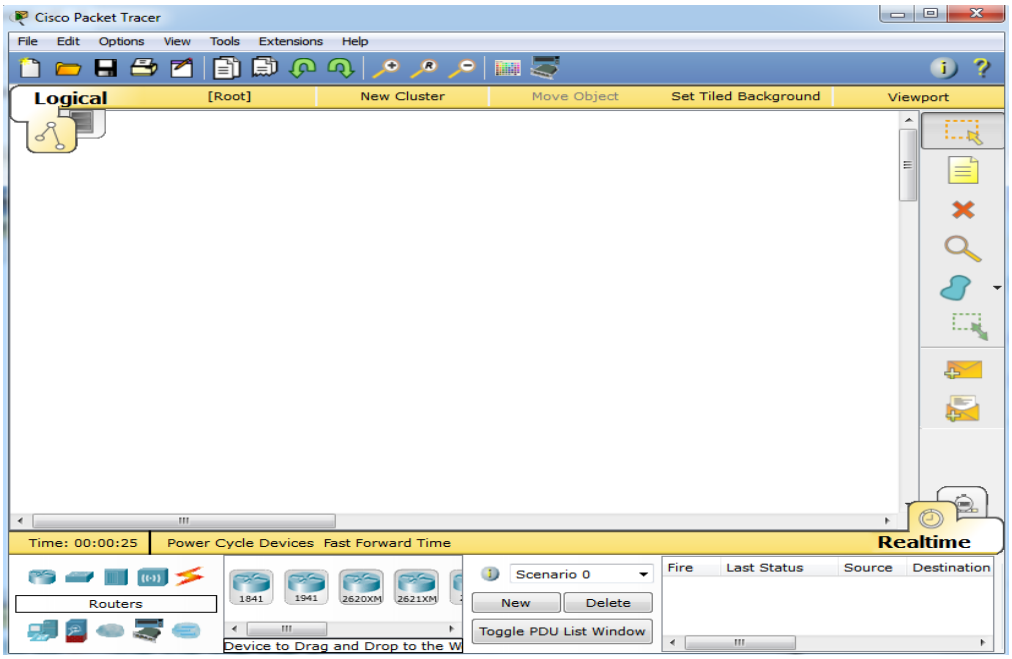

Figure IV.1 : Interface Packet Tracer

4.2 Configuration des équipements

Toutes les configurations des équipements du réseau seront réalisées au niveau de la CLI (Commande Langage Interface) (Figure IV.2). CLI est une interface de simulateur Cisco Packet Tracer qui permet la configuration des équipements du réseau à l'aide d'un langage de commandes.

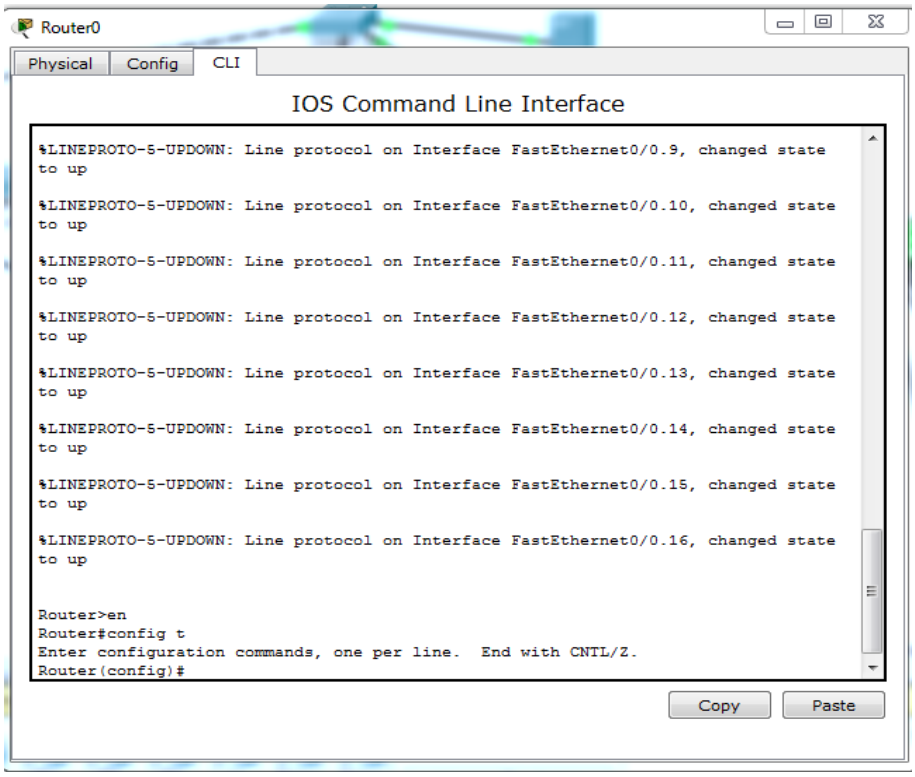

Figure IV.2 : interface CLI

Nous allons lancer des séries des configurations sur tous les équipements du réseau. Dans ce qui suit, tout en montrant des exemples de chaque configuration

4.2.1 Configuration des commutateurs

Nous allons commencer par la création des VLANs sur le switch principal, sachant qu'il y aura en tout 16 VLANs (10,11, 12, 13.., 25).

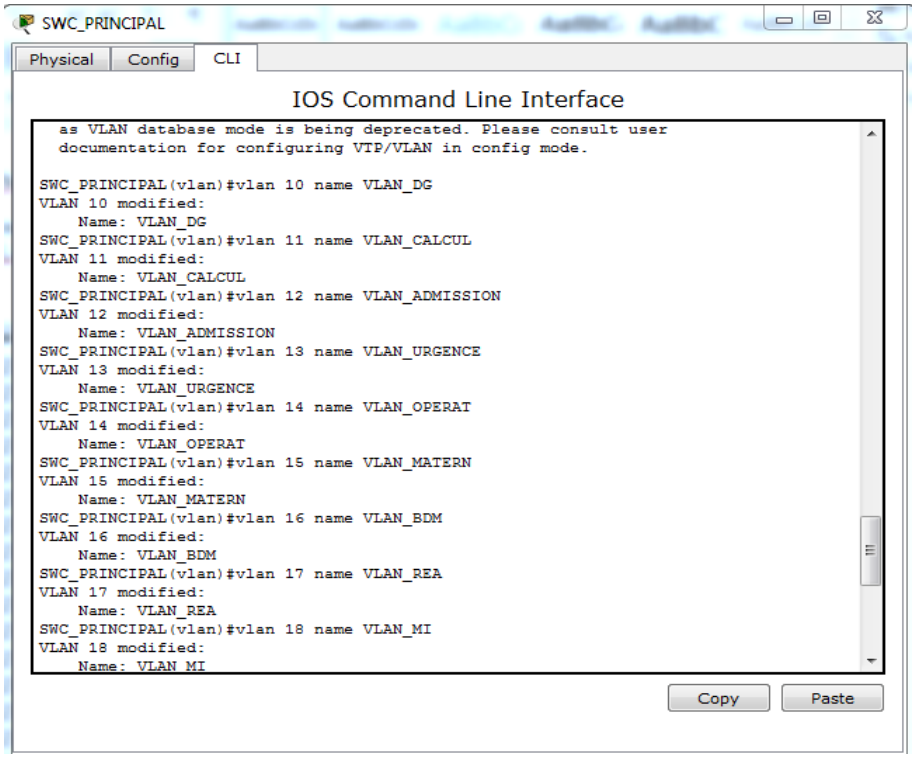

Figure IV.3 : Création des VLANs sur le switch principal

Ensuite nous allons suivre les étapes de configurations illustrées ci-dessous :

a) Configuration de Hostname : (Nomination des équipements sur « Cisco Packet Tracer »).

b) Configuration des mots de passe.

c) Configuration de VTP.

d) Configuration des VLANs.

e) Configuration des interfaces.

f) Configuration de Spanning-Tree.

g) Insertion des ACL.

h) Configuration du routage RIP et inter-VLAN.

a) Configuration des hostname

Cette configuration a pour but de renommer les commutateurs par des noms significatifs Nous prendrons comme exemple le switch d'accès du centre de calcul (Figure IV.4), sachant que c'est la même procédure pour les autres commutateurs.

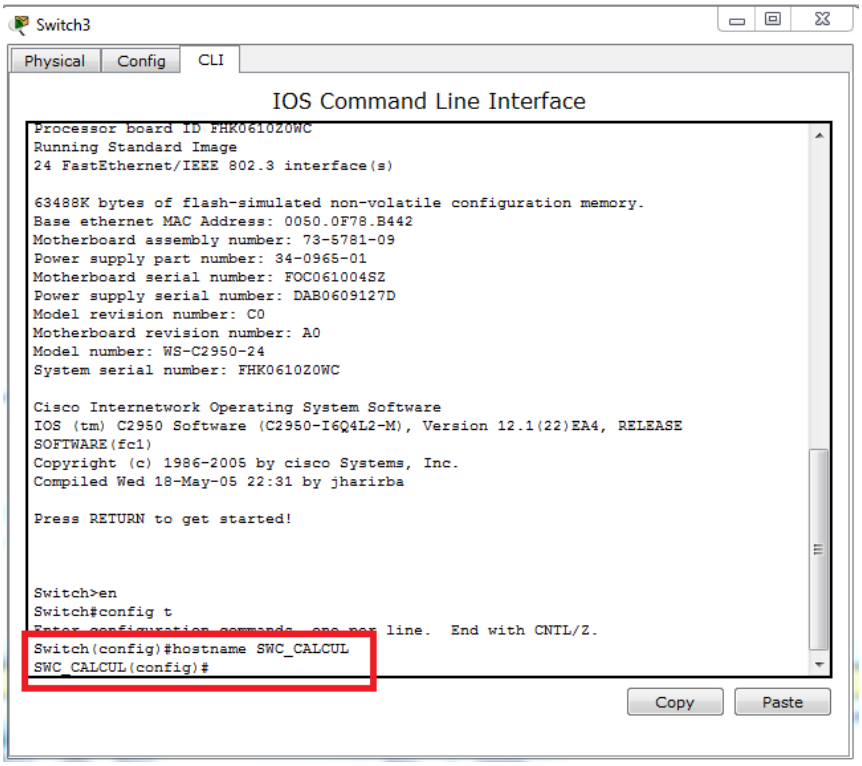

Figure IV.4 : Nomination d'un switch d'accès du centre de calcul

b) Configuration des mots de passe

Nous allons maintenant passer à la configuration des mots de passe.

- **Sécuriser l'accès à la ligne de console**

  Notre choix c'est porté sur « ephconsole » comme mot de passe via console, l'exemple que nous prendrons est le SWC_DG. La figure IV.5 montre les commandes de mise en place du mot de passe. La même chose sera faite pour les autres commutateurs.

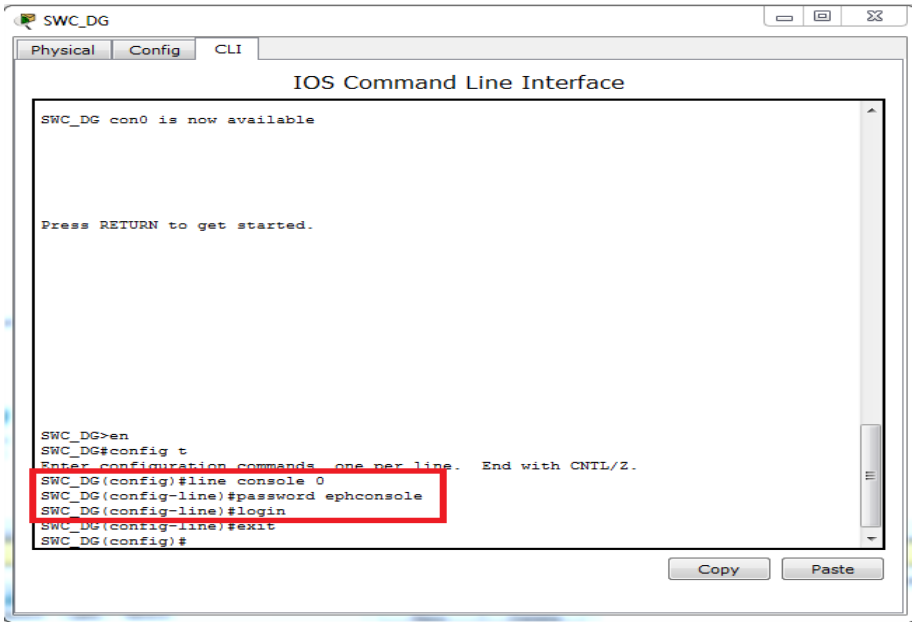

Figure IV.5 : Attribution du mot de passe console au SWC_DG

- **Sécuriser l'accès au mode privilégié**

  Pour sécuriser l'accès au mode privilégié, nous avons choisi le mot de passe ephsecret.

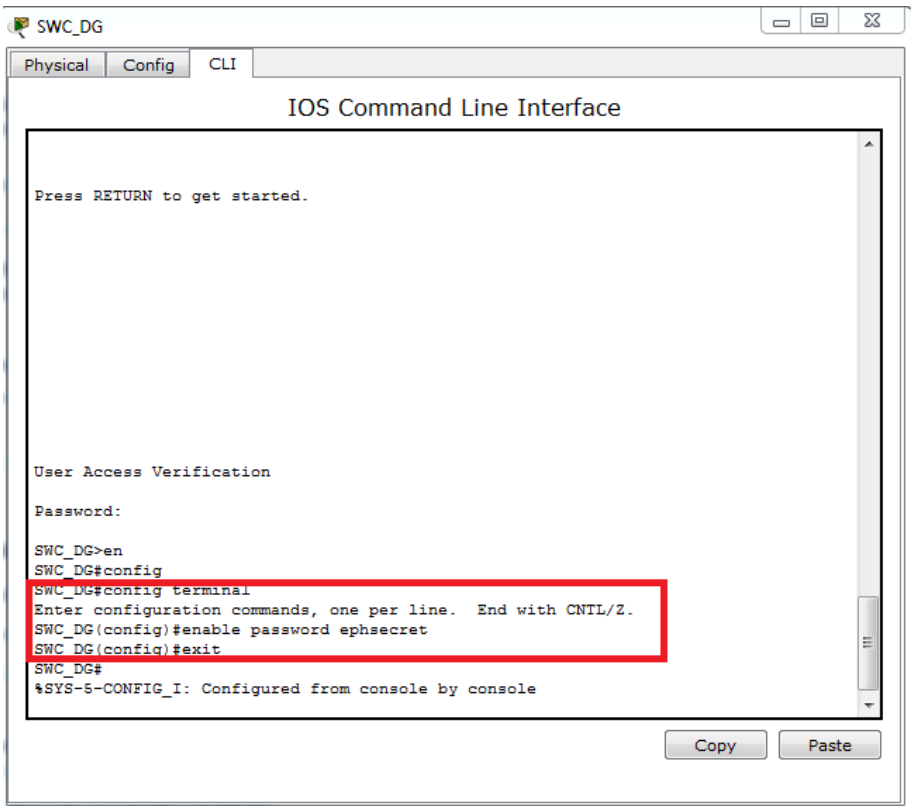

Figure IV.6 : Attribution du mot de passe pour le mode privilégié au SWC_DG

- **Configurez un mot de passe chiffré pour sécuriser l'accès au mode privilégié**

Le mot de passe d'activation (enable) doit être remplacé par le mot de passe secret chiffré à l'aide de la commande enable secret. Nous avons choisi ephsecret en tant que mot de passe secret actif.

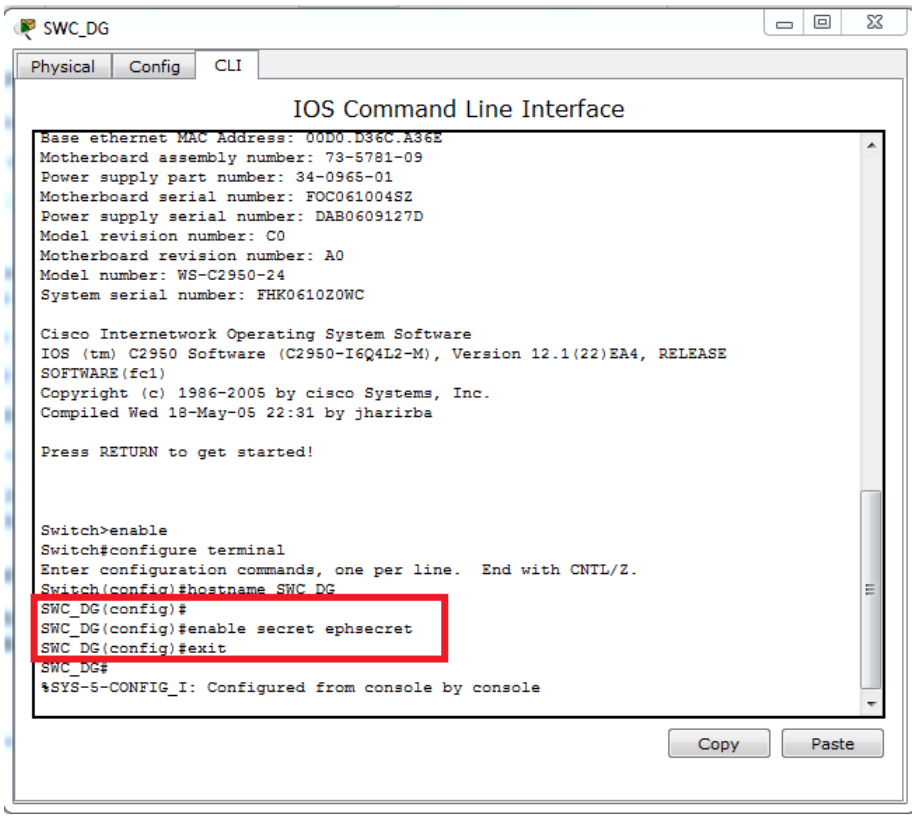

Figure IV.7 : Mot de passe secret

- **Chiffrer les mots de passe**

Le mot de passe secret actif (enable secret) a été chiffré, mais les mots de passe d'activation (enable**)** et de console sont toujours en clair. Nous allons maintenant chiffrer ces mots de passe en clair à l'aide de la commande service password-encryption.

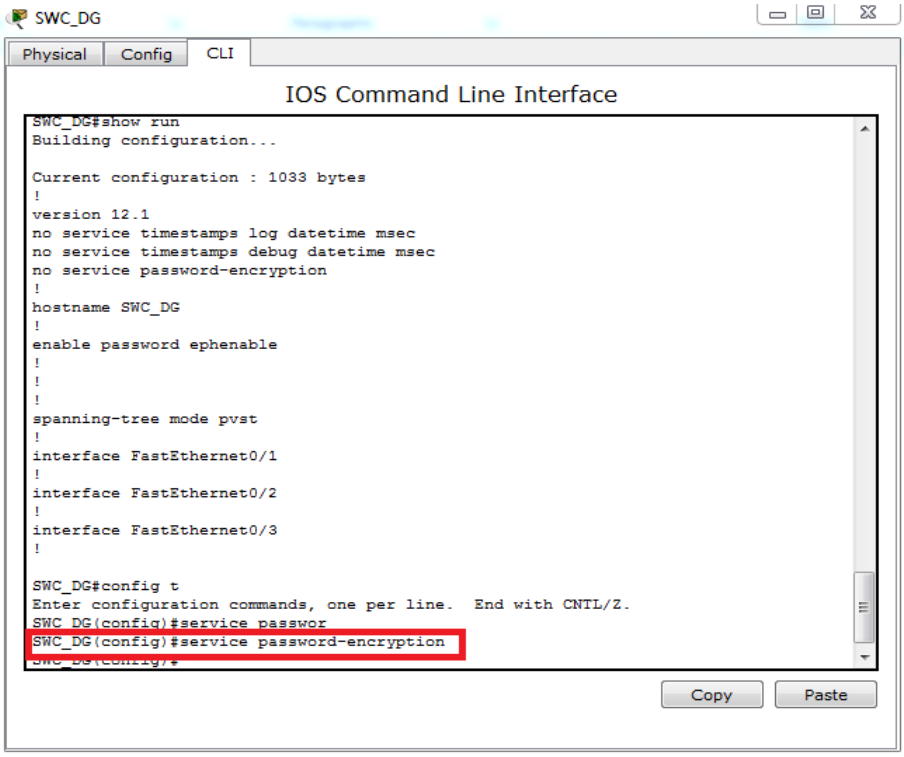

Figure IV.8 : Chiffrement du mot de passe

- **Sécuriser l'accès à distance avec SSH**

L'accès à distance via Telnet sur un équipement Cisco n'est pas sécurisé. Il est préférable d'utiliser le protocole SSH qui chiffre les informations afin d'apporter une couche de sécurité à la connexion à distance.

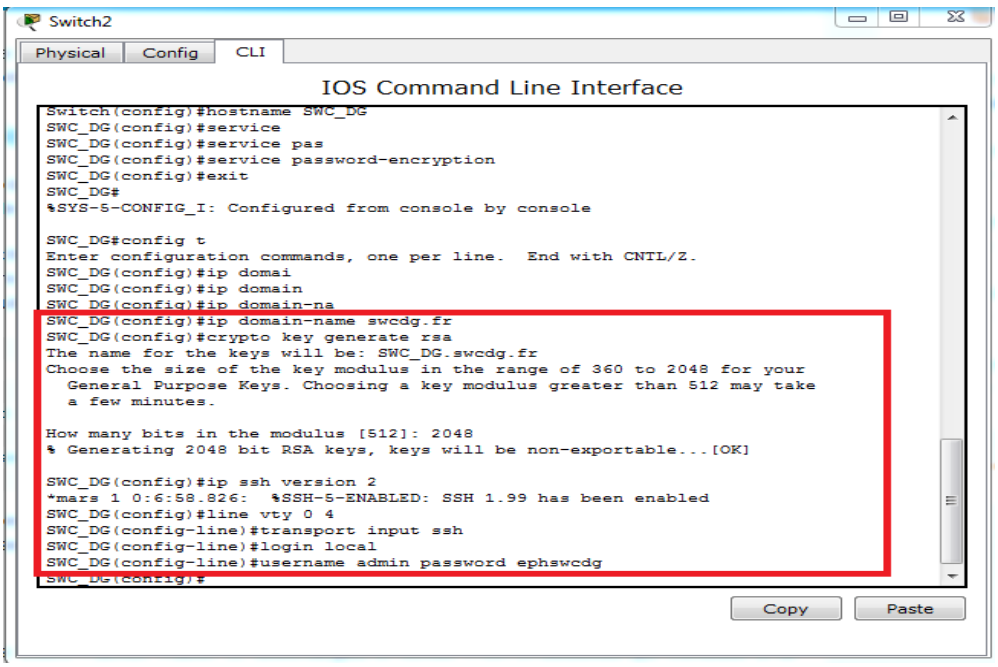

Figure IV.9: Sécuriser l'accès SSH sur un switch

c) Configuration du VTP

Maintenant nous allons configurer le protocole VTP, le switch principal sera configuré en mode serveur (Figure IV.10) et les switchs d'accès en mode client. Nous prendrons le switch admission comme exemple (Figure IV.11), la même chose sera appliquée aux autres commutateurs.

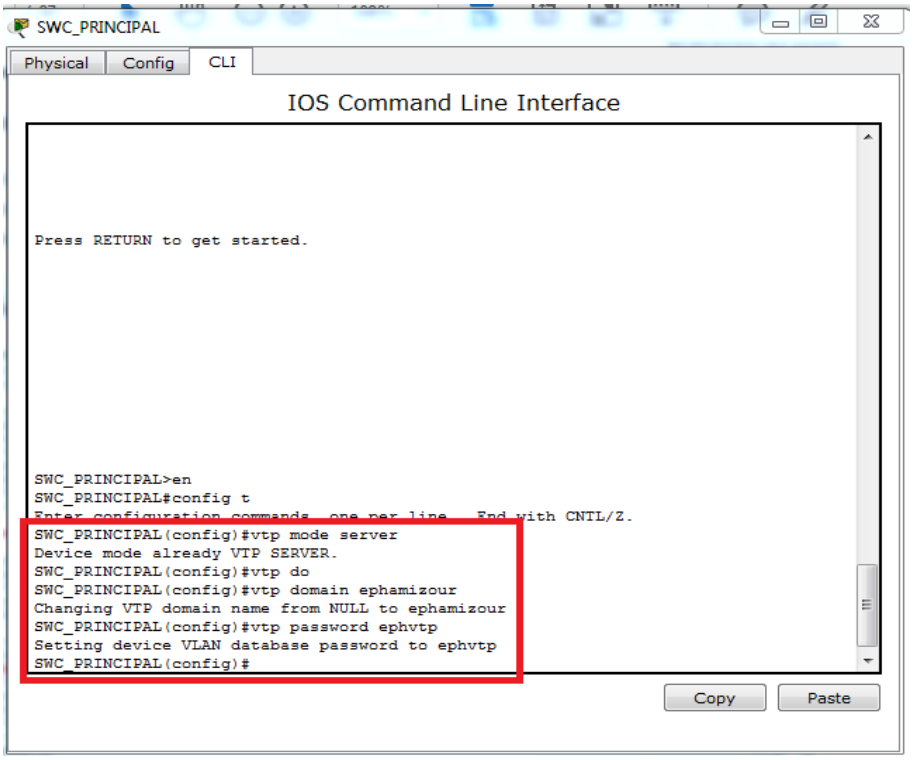

Figure IV.10 : VTP serveur

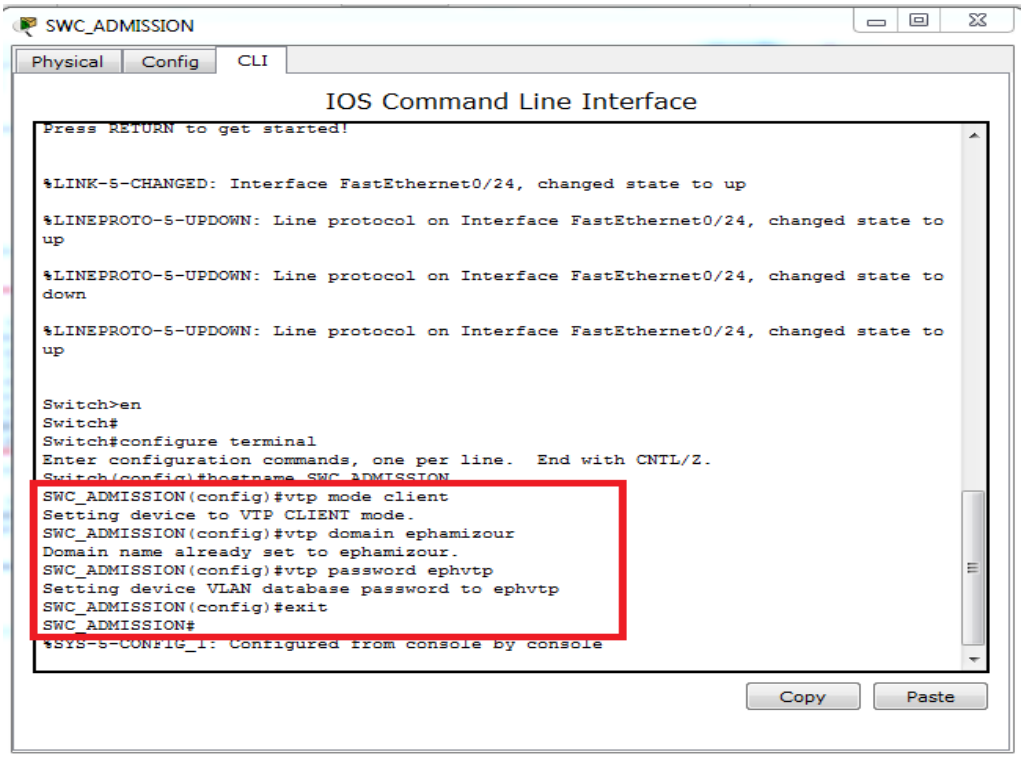

Figure IV.11: VTP client

d) Configuration des VLANs

Dans cette partie de configuration nous allons attribuer les adresses IP de passerelle pour chaque VLAN au niveau du Switch-cœur, nous allons également utiliser la commande « ip helper » pour donner l'adresse du serveur DHCP à chaque VLAN comme illustré dans la figure suivante.

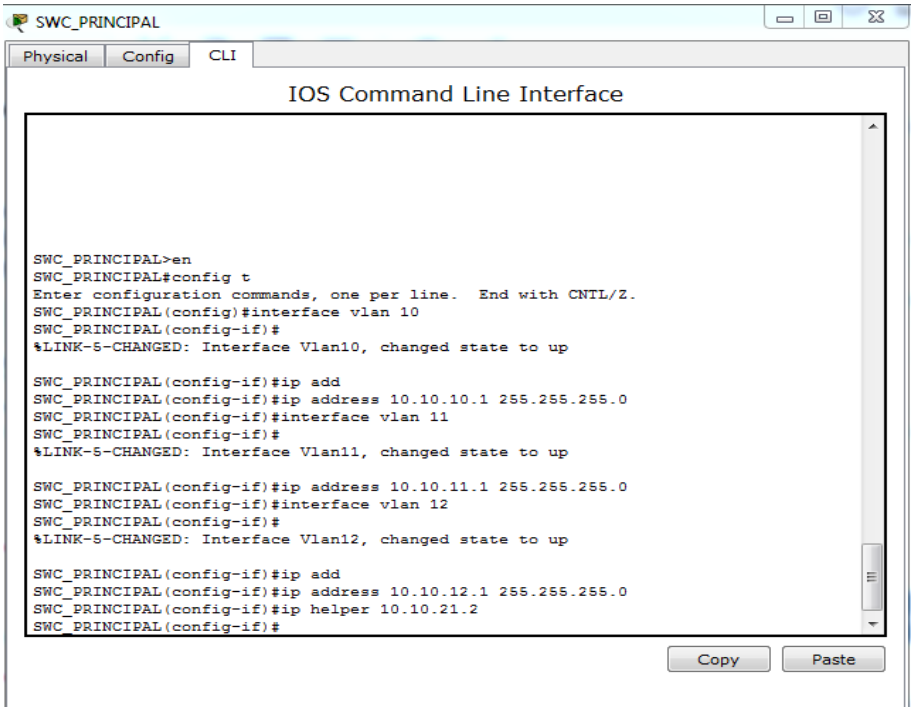

Figure IV.12 : Interfaces des VLANs au niveau de SWC_PRINCIPAL

e) Configuration des interfaces

Nous allons configurer les liaisons entre les commutateurs en mode trunk. Par contre les interfaces en mode accès se trouvent au niveau des liens entre les commutateurs d'accès et les PC.

Les figures suivantes illustrent les configurations faites.

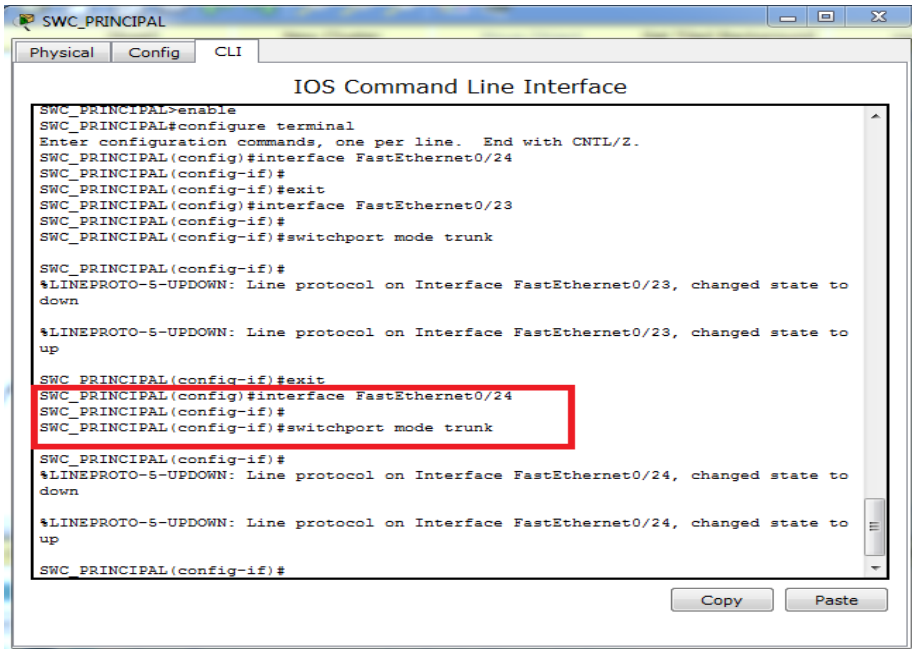

Figure IV.13 : Activation des liens trunk au niveau du switch principal

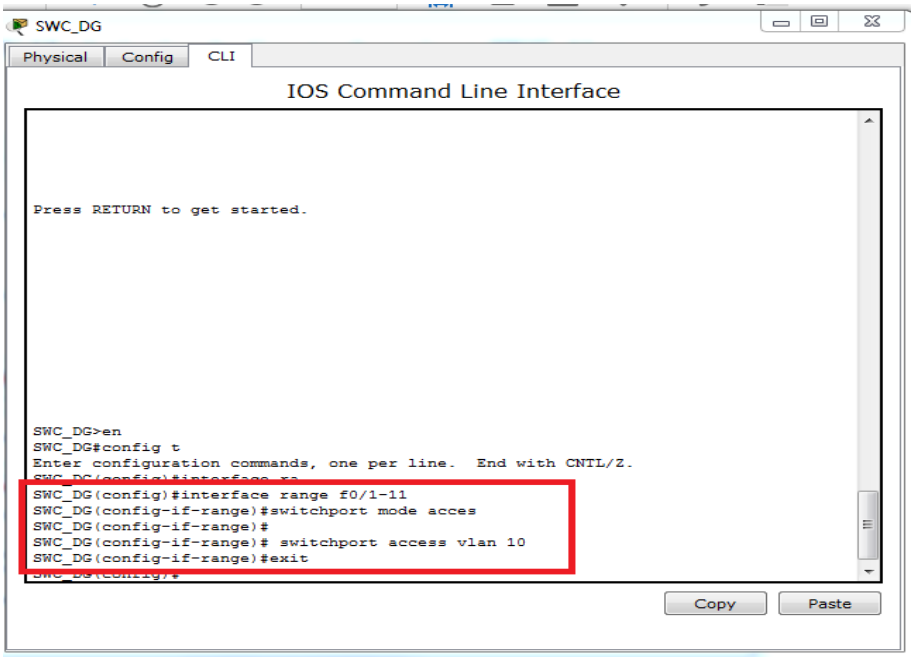

Figure IV.14 : Activation des liens Access au niveau du switch direction générale

f) Configuration de Spanning-Tree

Maintenant nous allons configurer le protocole Spanning-Tree pour définir le switch principal en tant que switch racine.

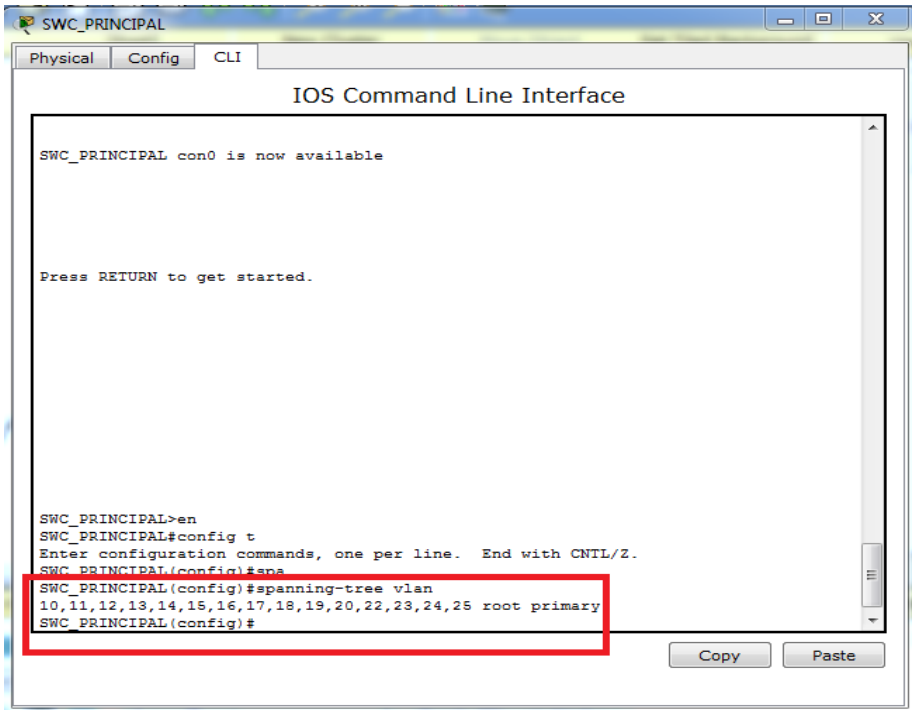

Figure IV.15 : Configuration de Spanning-Tree

g) Insertion des ACL

Nous allons maintenant utiliser les listes des contrôles d'accès afin de limiter la communication entre certains VLANs, nous avons pris comme exemple le VLAN 10 de la direction générale auquel nous avons bloqué la communication avec les autres VLANs comme le démontre la figure ci-dessous.

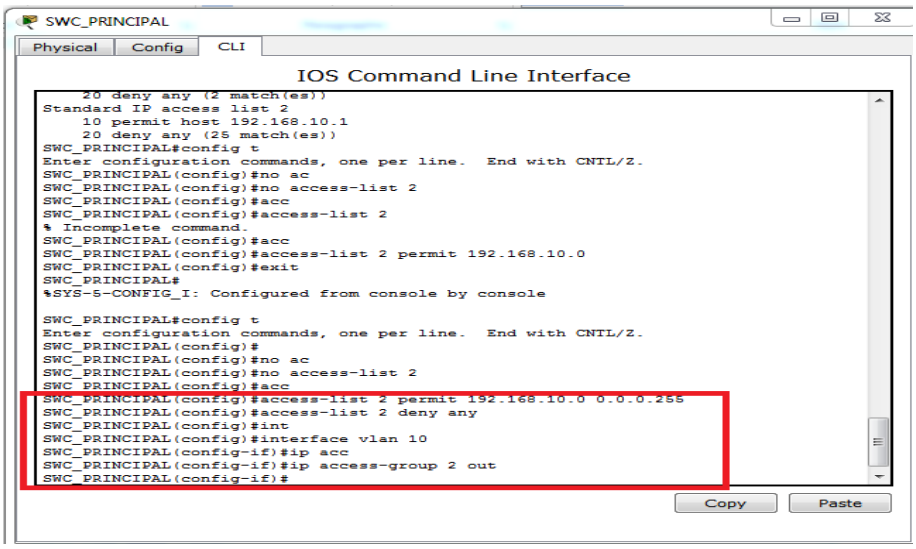

Figure IV.16 : ACL au niveau du VLAN de la direction générale

h) Configuration du routage RIP et inter-VLAN

Nous allons maintenant configurer le routage inter-VLAN avec la commande « ip routing », et le routage RIP au niveau du switch cœur, pour cela nous allons commencer par attribuer une adresse IP à l'interface GigabitEthernet0/1 laquelle est directement liée au routeur.

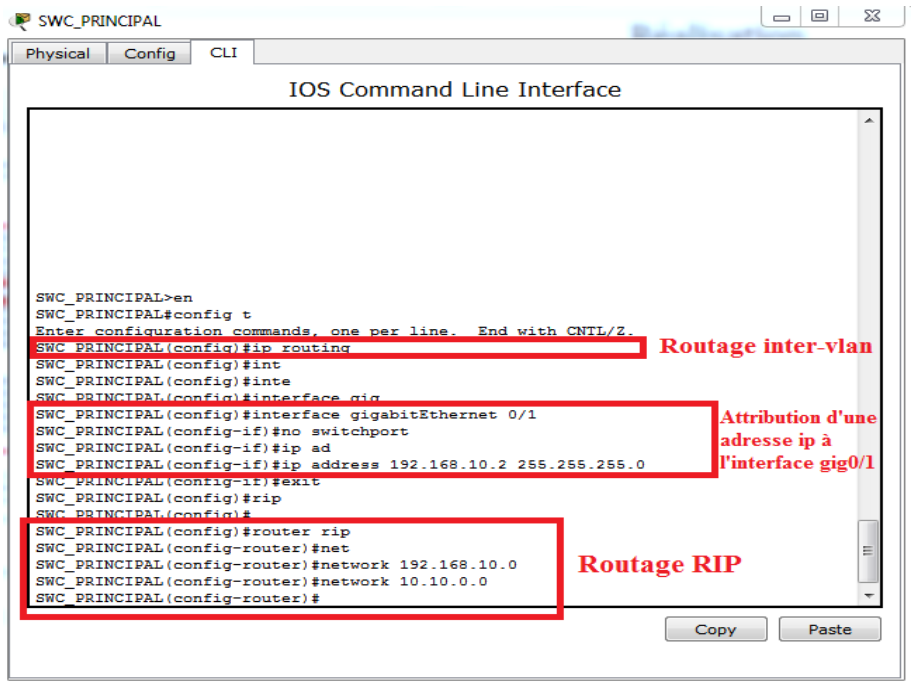

Figure IV.17 : Activation du routage inter-VlAN et RIP sur SWC_PRINCIPAL

4.2.1 Configuration du routeur

Pour la configuration des routeurs nous allons suivre les étapes de configurations suivantes :

a) Configuration de l'interface.

b) Configuration du routage RIP.

Les hostnames et les mots de passe sont configurés de la même façon que sur les commutateurs.

a) Configuration de l'interface

Dans cette étape nous allons attribuer une adresse IP à interface du routeur qui est directement liée avec le switch-cœur, et l'activer par la suite, comme la figure IV.18 l'illustre.

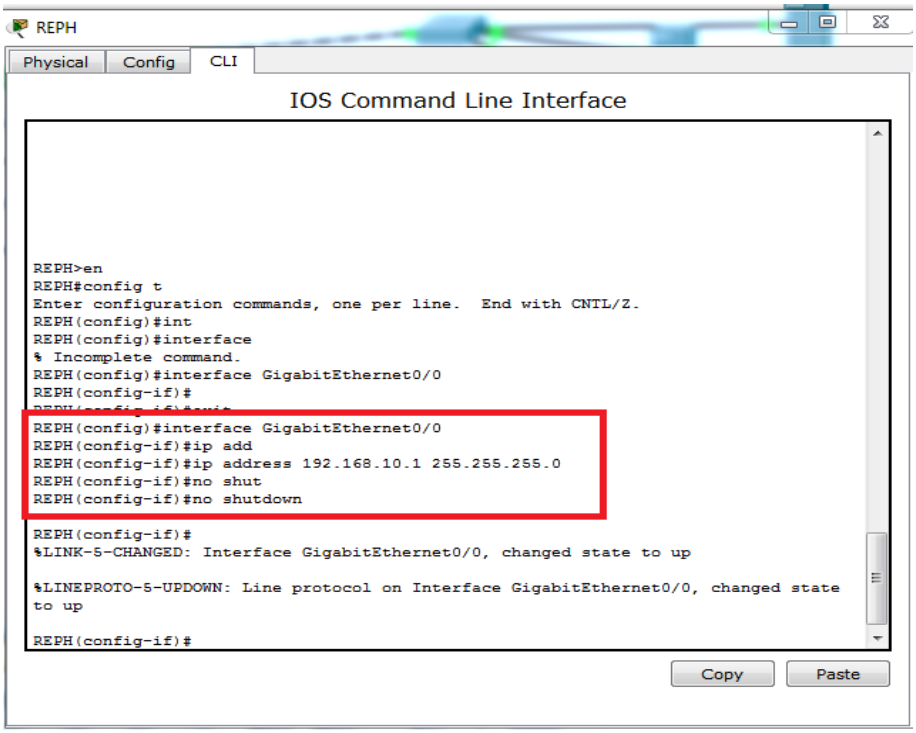

Figure IV.18 : Adressage et activation de l'interface au niveau du routeur

b) Configuration du routage RIP

Maintenant nous allons configurer le protocole de routage RIP au niveau du routeur, comme le montre la figure suivante.

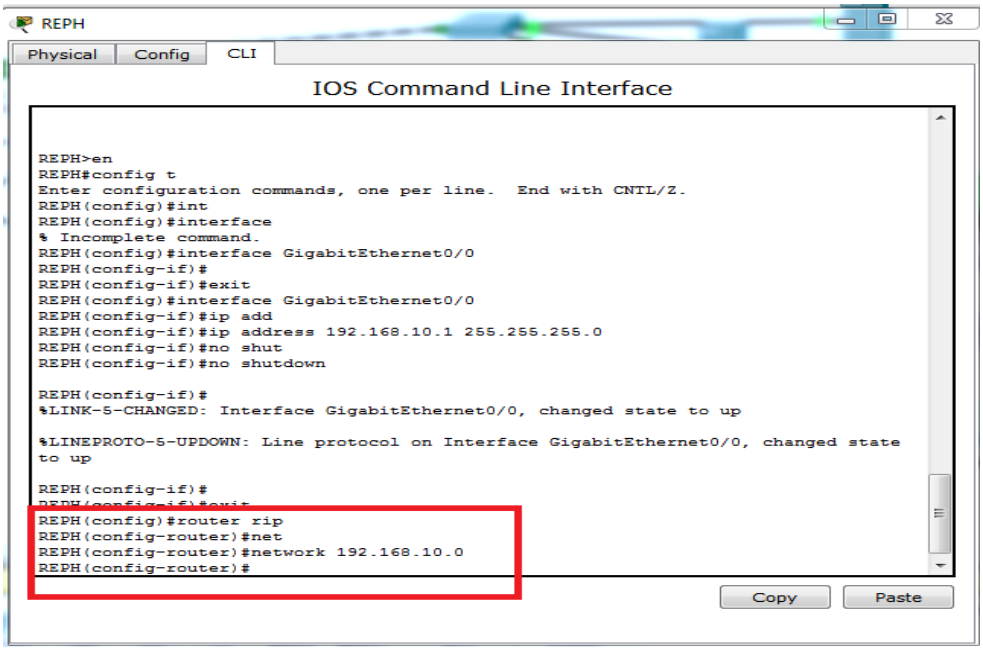

Figure IV.19: Configuration du protocole RIP sur le routeur

4.2.3 Configuration du serveur DHCP et les PC

Dans cette étape de configuration nous allons configurer le serveur DHCP et les PC pour une attribution automatique d'adresses IP.

a) Configuration DHCP

Pour configurer le serveur DHCP, nous devons créer des pools d'adresses qui comporteront les noms des VLANs tout en introduisant les gateway et le nombre maximum d'adresses, ensuite nous allons attribuer une adresse IP statique au serveur DHCP, les figures suivantes montrent les étapes de configuration.

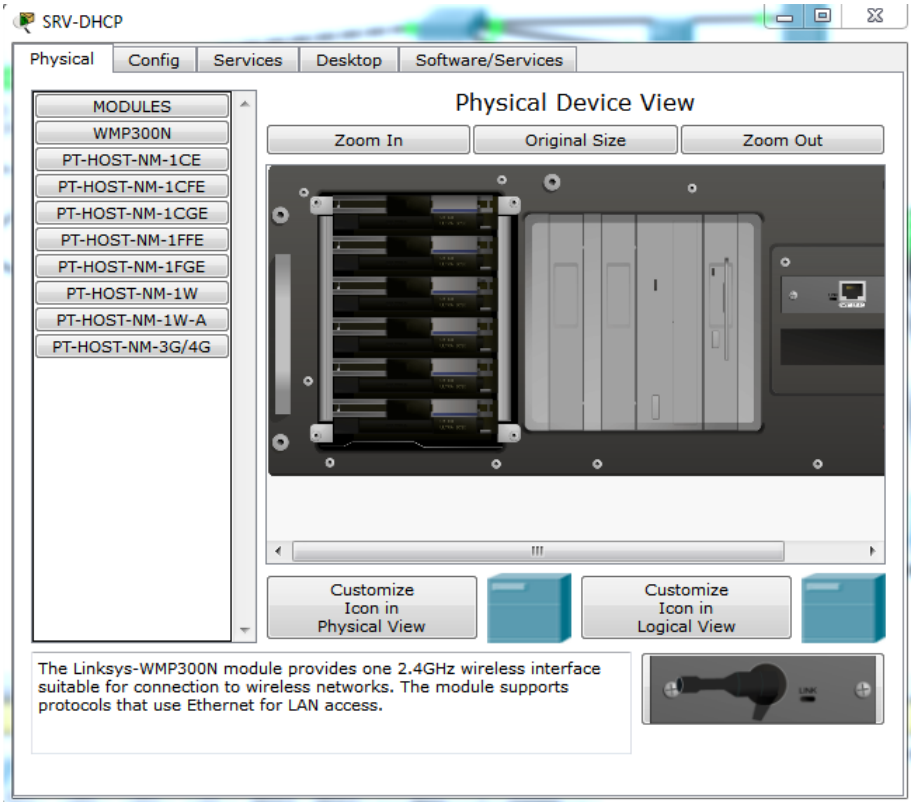

Figure IV.20 : l'interface principale du serveur DHCP

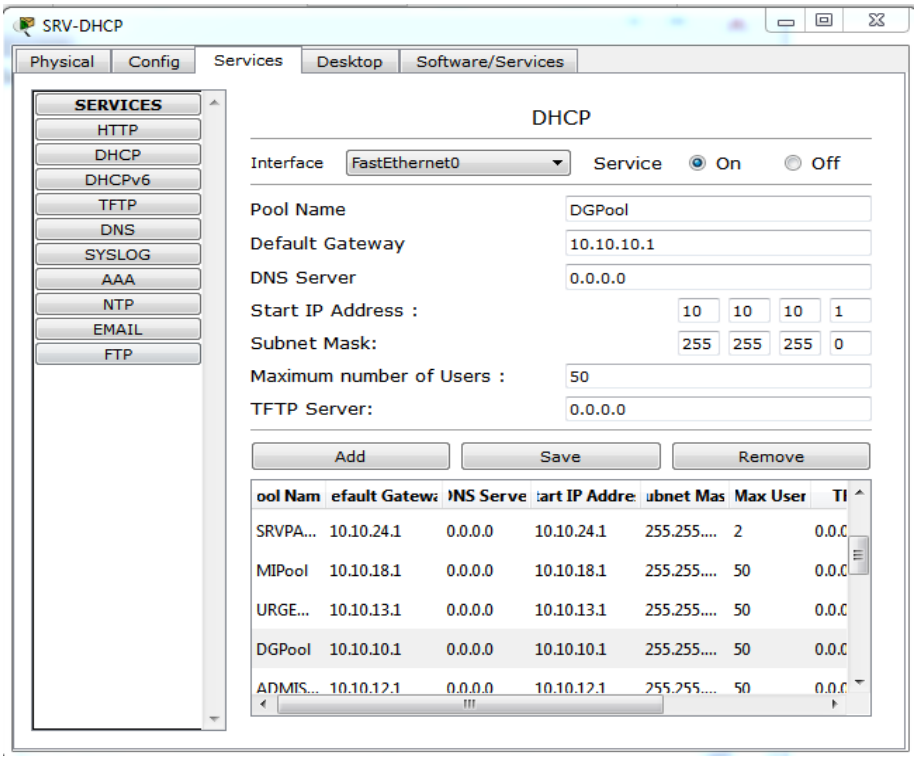

Figure IV.21 : Création des Pool d'adresses.

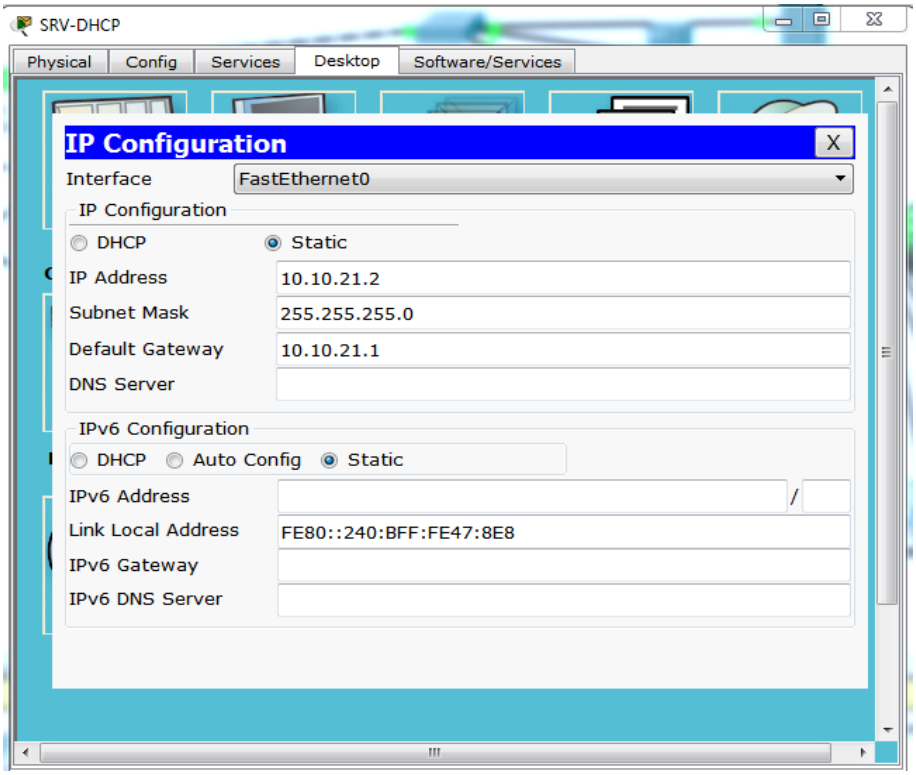

Figure IV.22: Attribution d'une adresse au serveur DHCP

L'attribution d'adresse IP aux autres serveurs se fait également de manière statique.

b) Configuration PC

La configuration des PC passe par l'attribution d'une adresse IP dynamiquement comme le montre la figure suivante.

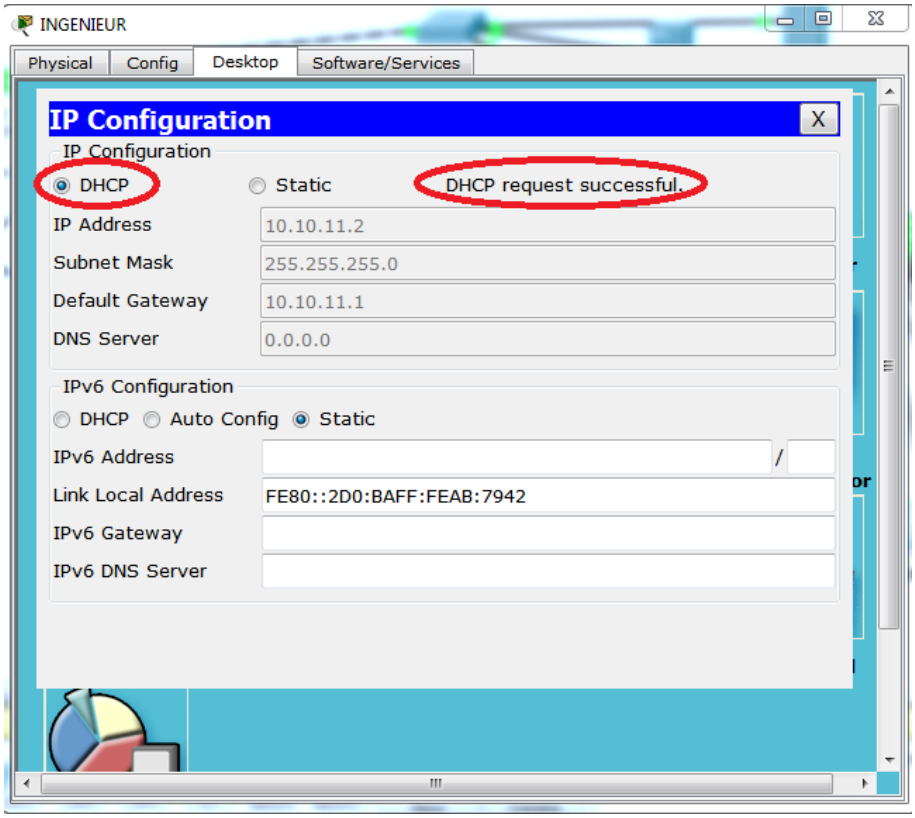

Figure IV.23 : Attribution dynamique d'une adresse à un PC

4.2.4 Tests et validation de la configuration

Dans cette partie nous allons vérifier la création des VLANs et les communications entre tous les équipements en utilisant la commande « Ping ». Ces tests sont faits entre équipements (PC, Switchs et routeurs), inter-VLANs, et intra-VLANs. Il est à noter que la commande Ping aide à vérifier la connectivité au niveau IP.

a) Test de création des VLANs

A l'aide de la commande « show vlan brief », nous pouvons voir les différents VLANs créés.

La figure IV.24 montre les VLANs crées au niveau du SWC-PRINCIPAL

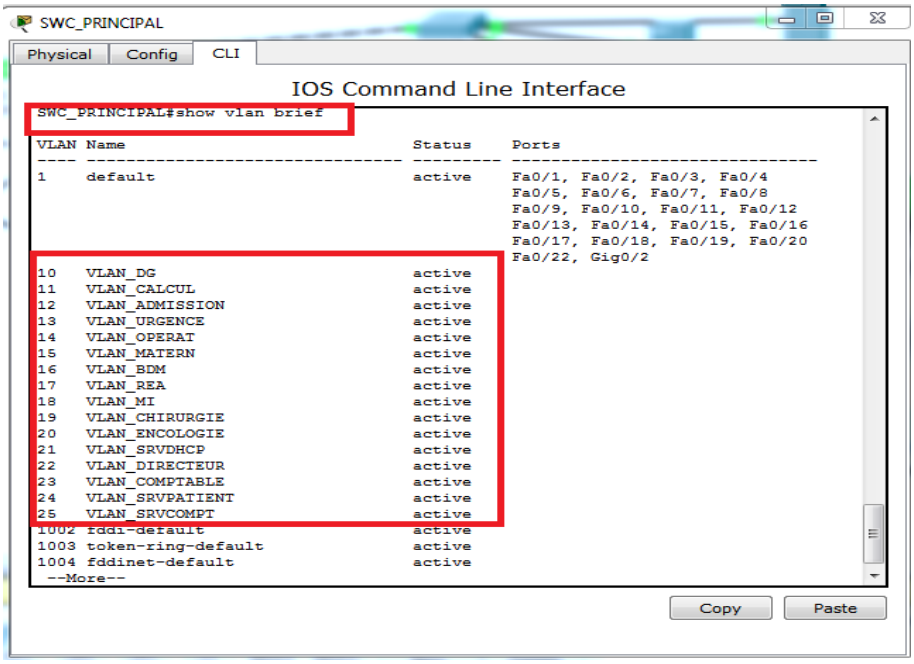

Figure IV.24: Test de création des VLANs

b) Test intra-VLAN

Ping réussi entre le PC_MEMEC (10.10.10.3) et le PC_SECRETARIAT (10.10.10.7) qui appartiennent au même VLAN (le VLAN DG)

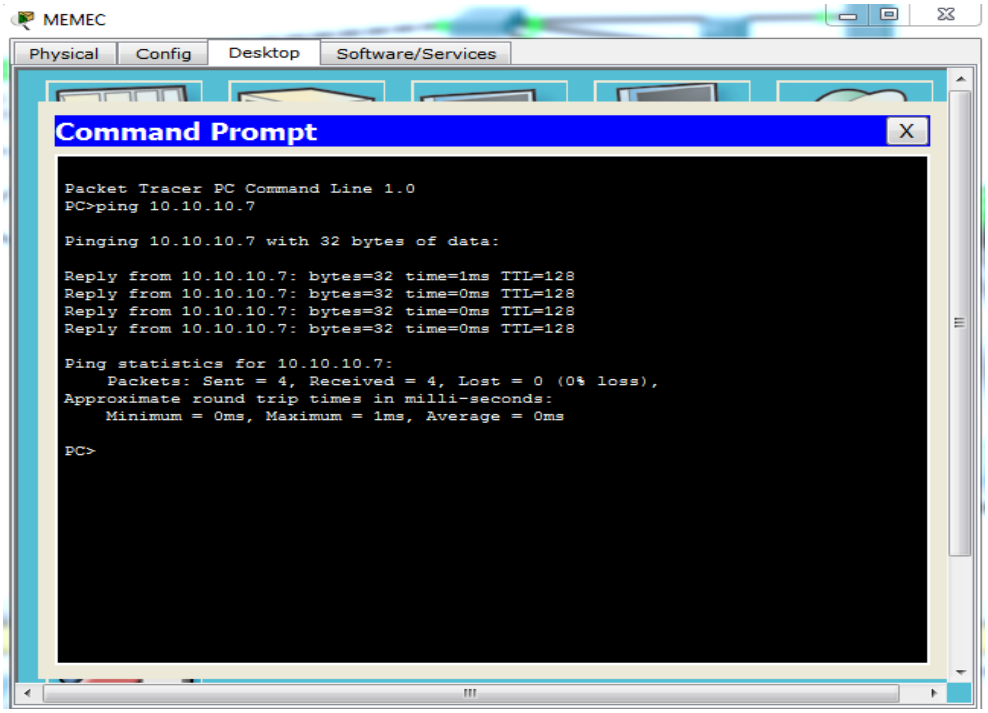

Figure IV.25 : Ping réussi entre PC_MEMEC et PC_SECRETARIAT

c) Test inter-VLAN

Nous allons maintenant illustrer deux exemples, dans le premier, nous ferons un test de communication entre le pc du VLAN directeur (10.10.22.2) et le serveur patient (10.10.24.2) (Figure IV.26) appartenant à un autre VLAN, sachant que le directeur doit pouvoir accéder au serveur utilisant le logiciel patient.

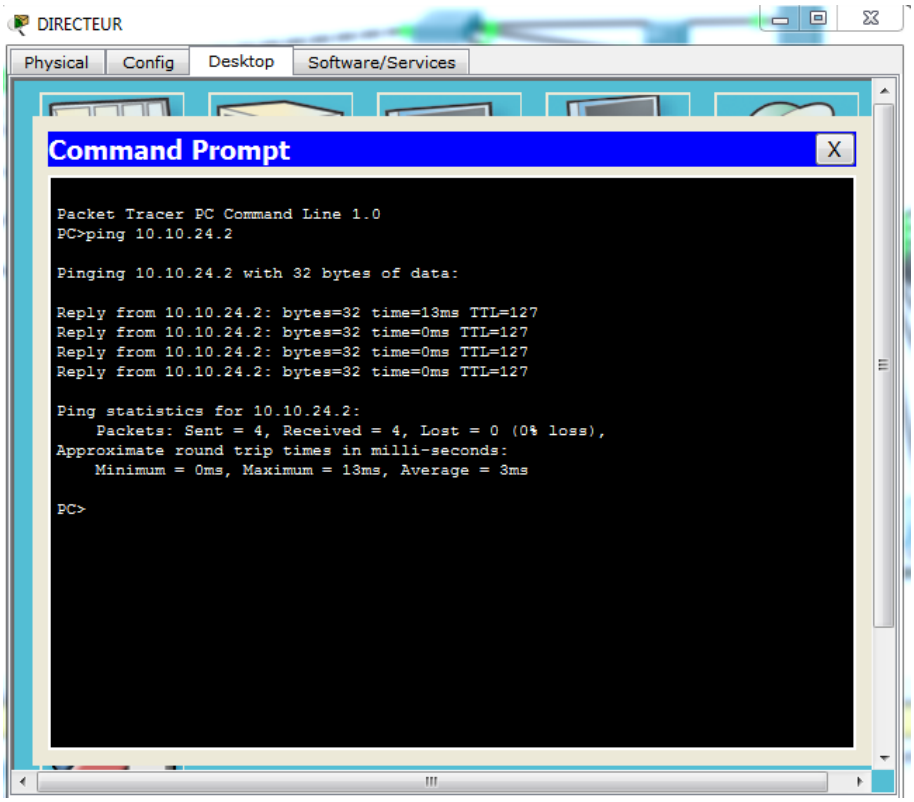

Figure IV.26 : Ping réussi entre le pc du directeur et le serveur patient

Par contre dans le deuxième exemple, nous allons démontrer que le PC_PHARMACIE (10.10.11.4) ne peut pas communiquer avec le serveur comptable (10.10.25.2) (Figure IV.27) car nous avons limité l'accès au serveur grâce à des ACL préalablement implémentées au niveau du Switch-cœur.

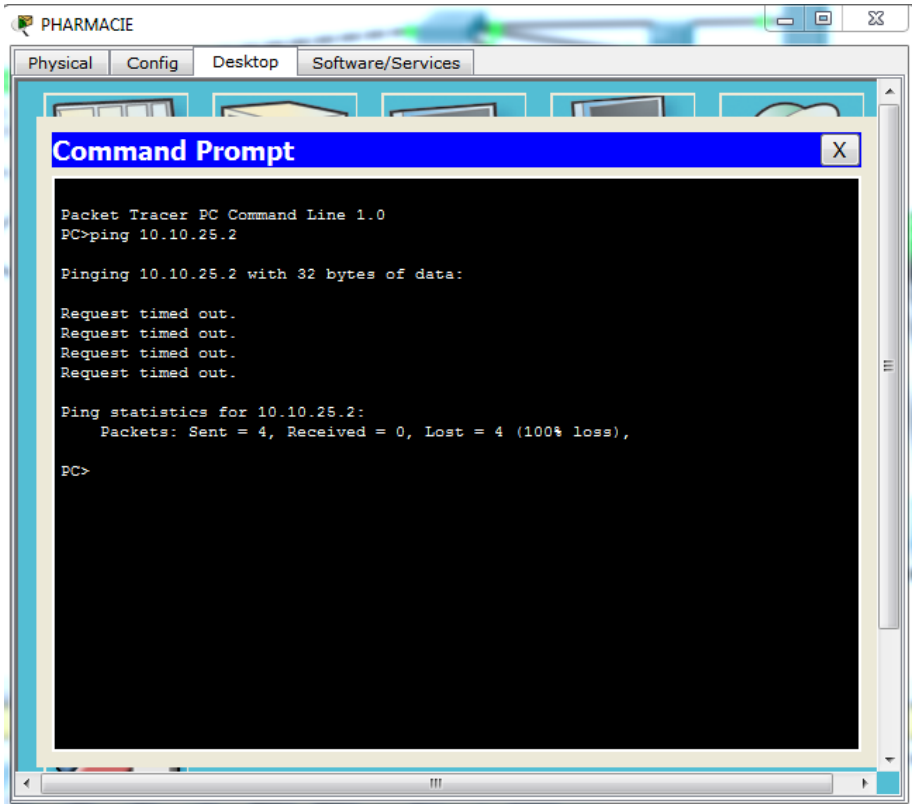

Figure IV.27 : Ping échoué entre le pc_pharmacie et serveur comptable

4.3 Configuration des points d'accès WIFI

Nous allons maintenant configurer les points d'accès Wifi, nous prendront pour exemple un point d'accès wifi (Figure IV.28) situé au centre de calcul et un laptop (Figure IV.29).

a) Configuration du point d'accès Wifi :

Nous allons d'abord configurer une clé wifi au niveau du point d'accès.

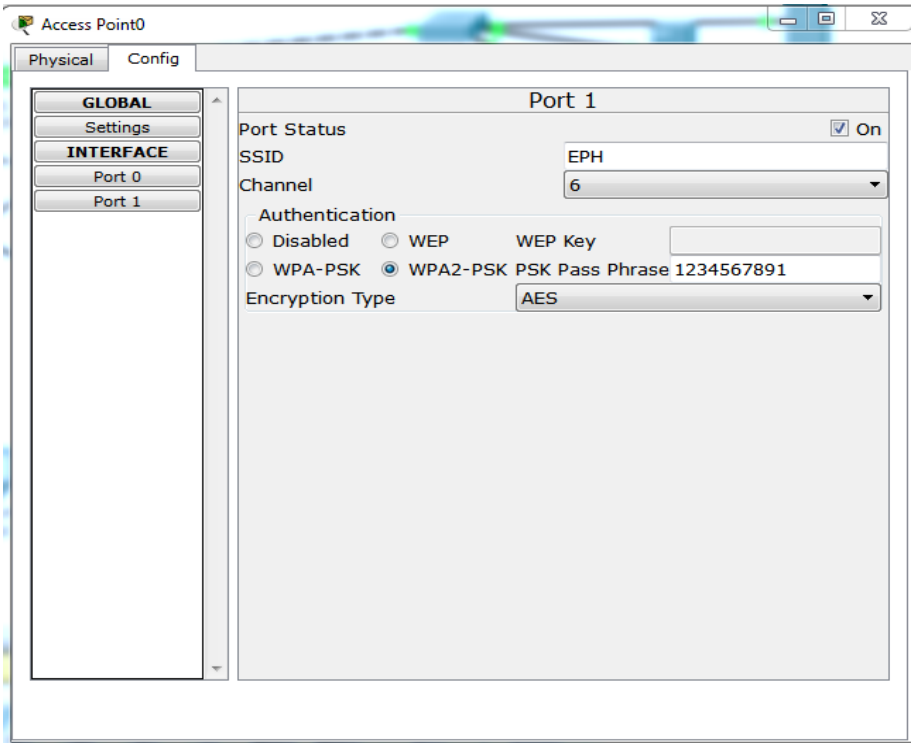

Figure IV.28 : Configuration du point d'accès wifi

b) Configuration du laptop

Nous allons maintenant insérer la même clé wifi au niveau du laptop (Figure IV.29), afin que ce dernier puisse se connecter au point d'accès wifi (Figure IV.30).

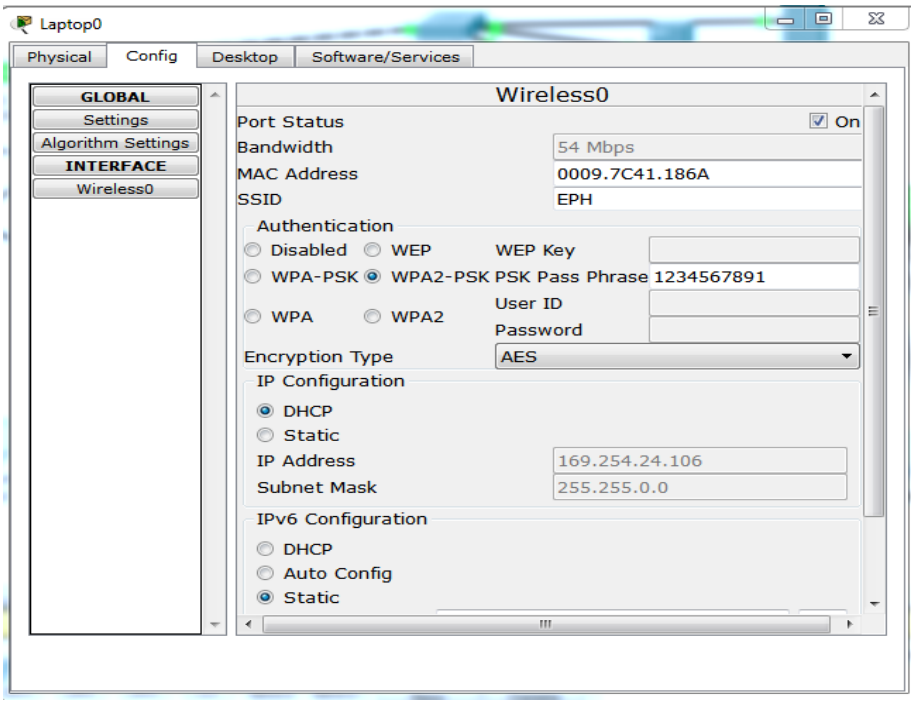

Figure IV.29 : Configuration wifi sur un laptop

Figure IV.30 : Connexion au point d'accès wifi réussie.

4.4 Architecture réalisée

La Figure IV.31 représente l'architecture réalisée.

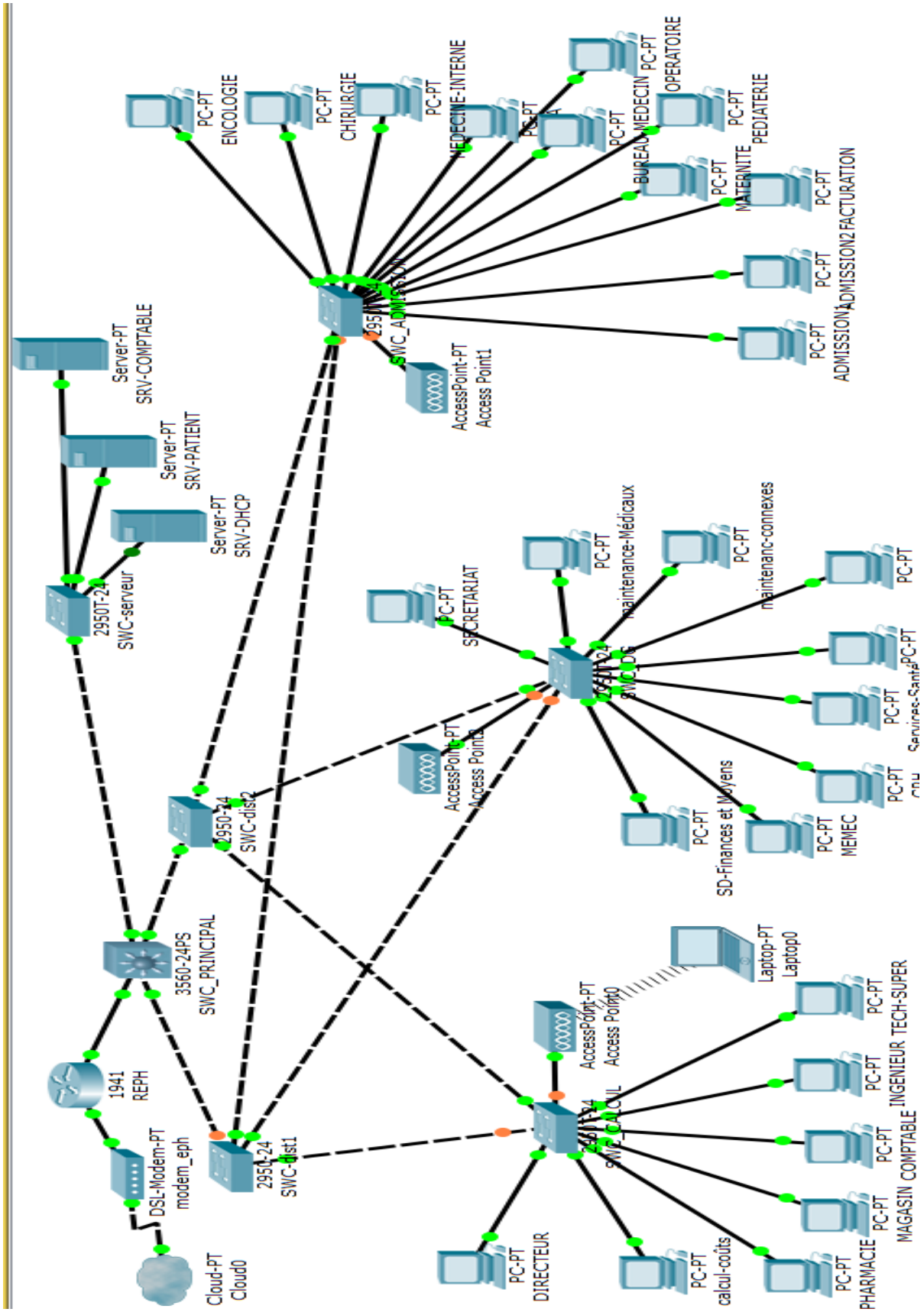

Figure IV.31: Architecture réalisée

Conclusion

Pour finaliser notre projet, nous avons commencé par introduire le simulateur Packet tracer, nous l'avons par la suite utilisé pour la configuration de notre architecture réseau, nous avons donc expliqué comment nous avons configuré les commutateurs (créations des VLANs, mots de passe, insertion des ACL, etc.) et le routeur, ensuite nous sommes passé à des tests de vérification, et nous avons fini par la configuration des points d'accès Wifi.

Conclusion générale

Nous avons essayé à travers ce mémoire d'apporter une solution pour sécuriser le réseau informatique de l'hôpital d'Amizour. Comme nous l'avons constaté, l'EPH est constituée de plusieurs services à savoir le service des admissions, la direction générale, pédiatrie, réanimation, etc. Alors nous avons opté pour une solution basée sur les réseaux virtuels en procédant à la segmentation logique du réseau local de l'hôpital afin d'améliorer sa sécurité.

En effet, nous avons présenté un travail divisé en deux grandes parties, à savoir l'approche théorique qui est subdivisée en deux chapitres : le premier a porté sur les généralités sur les réseaux et la sécurité informatique; le second quant à lui fut dédié aux VLANs où nous avons cité les raisons de leur utilisation ainsi que les différents types de VLAN existants. Ensuite, nous avons mis un accent sur la fameuse norme 802.1Q qui a été dédiée pour répondre à un besoin de normalisation sur le transport des VLANs ainsi qu'une présentation du protocole d'administration et de gestion des VLAN nommé VTP.

La deuxième partie a été consacrée à la finalisation du projet, laquelle est aussi subdivisé en deux chapitres dont le premier a porté sur une étude préalable de l'organisme dans laquelle nous avons présenté l'hôpital et exposé la problématique, laquelle après une critique de l'existant, nous avons solutionné par la segmentation du réseau local en plusieurs réseaux virtuels, et l'insertion des listes de contrôles d'accès afin de filtrer le trafic réseau, s'ensuit une présentation des différents équipements, interfaces et VLANs.

Le dernier chapitre quant à lui a été consacré à la réalisation où nous avons présenté l'outil de simulation Packet tracer ayant servi à l'élaboration du projet, tout en expliquant les configurations des différents équipements, et la création des VLAN, nous avons également procédé à une série de tests en envoyant des requêtes "pings" pour évaluer l'efficacité de notre solution.

Ce projet nous a permis d'acquérir une expérience personnelle et professionnelle très bénéfique. Ce fut une occasion pour notre groupe de se familiariser avec l'environnement du travail et de la vie professionnelle, d'élargir et d'approfondir nos connaissances sur l'administration des réseaux informatiques.

Bibliographie

[1] : G.DESGEORGE. La sécurité des réseaux ,3eme édition Dunod ,2012

[2] : G. PUJOLLE, Initiation aux réseaux, Édition eyrolles, 27 février 2014

[3] : JF.PILLOU, Fabrice LEMAINAQUE, Tout sur les réseaux et internet, 4eme édition dunod, 3 juin 2015.

[4] : JF.PILLOU, Tout sur les systèmes d'information, Paris Dunod 2006.

[5] : JA. BUCHMANN, introduction à la cryptographie, 2eme édition Dunod ,2006.

[6] : P.ATELEN, Réseaux informatique notion fondamental, 3eme édition ENI, janvier 2009.

[7] : S. GHERNAOUTI-HELIE, Sécurité informatique et réseaux, DUNOD, Paris, 2011.

[8] : T.LAMMEL, CCNA CISCO certified network associate study guide ,6éme edition, 2007.

Webliographie

[9] : https://aresu.dsi.cnrs.fr Vlan Dernier accès juin 2016.

[10] : http://cisco.goffinet.org Spanning-tree Dernier accès juin 2016.

[11] : http : //cms.ac-martinique.fr Généralité sur les vlan Dernier accès mai 2016.

[12] : http : //www-igm.univ-mlv.fr type de vlan Dernier accès juin 2016.

[13] : http://www.linux-france.org ACL Dernier accès juin 2016.

[14] : http://www.netalya.com Réseaux Dernier accès mai 2016.

[15] : http://www.packettracernetwork.com Packet tracer Dernier accès juin 2016.

[16] : http://reussirsonccna.fr Tout savoir sur les domaines de collision et diffusion Dernier accès juin 2016.

[17] : https://www.securiteinfo.com Sécurité Dernier accès juin 2016.

Résumé

Les réseaux virtuels ou VLANs ont révolutionné le concept de segmentation des réseaux, ils permettent de constituer autant de réseaux logiques que nous désirons sur une seule infrastructure afin d'améliorer sa sécurité.

L'objectif de notre travail consiste à implémenter une solution avec les réseaux virtuels afin de sécuriser le réseau LAN de l'hôpital d'Amizour, mais ce travail ne peut pas être réalisé sans faire une étude de l'architecture existante de l'EPH.

Sur le plan applicatif, nous avons choisi d'organiser les VLANspar service, lesquels nous avons créé sur un switch coeur, par la suite nous sommes passés à la configuration des listes de contrôle d'accès (ACL) afin de filtrer le trafic réseau.

Pour la simulation de notre architecture réseau, nous avons eu recours au simulateur de matériel réseau Cisco Packet Tracer, qui nous a permis de configurer les différents composants.

Mots clés: VLAN, LAN, ACL, Cisco Packet Tracer

Abstract:

The virtual Network or VLANs revolutionized the concept of the segmentation of the Network. They allow to constitute several logical Network that we desire on only one infrastructure in order to improve its safety.

The aim of our research consists in implementing a solution concerning the virtual Network so as to secure the local Network area LAN of "The Hospital of Amizour ". But this research cannot be accomplished without making a study on an existent architecture of that hospital.

On the plan of the application we have chosen to organize the VLAN via the service that we have founded in the Switch Layer three. Afterwards, we moved to the layout of the of the access controlled lists (ACL) in order to filter the Network Traffic.

For the simulation of our Network Architecture, we have had a recourse to simulator of the Network material "Cisco Packet Tracer" that has enables us to configure the different components.

Key Words: VLAN, LAN, ACL, Cisco Packet Tracer.