République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire De Fin d'Etude

En vue d'obtention du diplôme de master professionnel en informatique
spécialité : Adminstration et Sécurité des Réseaux Informatiques

Thème

La haute disponibilité des réseaux campus. Cas d'étude : Sonatrach

Réalisé par :
M^elle^ BOUBEKRI *Sara* et M^elle^ MEBARKI *Ryma* .

Soutenu le 28/06/2016 devant le jury composé de :

Président	**D^r^ A.BAADACHE**	**U. A/Mira Béjaïa.**
Examinateur	**M^r^ N.SALHI**	**U. A/Mira Béjaïa.**
Encadreur	**D^r^ A/M. BOUDRIES**	**U. A/Mira Béjaïa.**

Promotion 2015/2016

Dédicace

A cœur vaillant rien d'impossible, à conscience tranquille tout est accessible
Quand il y a la soif d'apprendre, tout vient à point à qui sait attendre

Je dédie ce travail :

A mon père : Aucune dédicace ne saurait exprimer l'amour, l'estime, le dévouement et le respect que j'ai toujours eu pour toi. Ce travail est le fruit de tes sacrifices que tu as consentis pour mon éducation et ma formation.

A ma très chère mère : Tu représentes pour moi le symbole de la bonté par excellence, la source de tendresse et l'exemple du dévouement qui n'a pas cessé de m'encourager et de prier pour moi.

A mes frères Walid et Massi que j'aime plus que tout.

A mes grands parents et à toute ma famille.

A ma binôme mais avant tout mon amie Sara.

A tous mes amis en particulier : Sarah et yacine (l'équipe Smartli), Mina, Sihem et Meriem.

Aux trois personnes qui ont toujours été la pour moi quand j'en avais le plus besoin : Sarah, Karim et Said, merci pour tout.

A la personne qui a su me redonner le sourire, à mon chéri Y.

A tous mes camarades de promotion.

Ryma

Dédicace

Je dédie ce travail :

A mon père, mon premier encadreur, depuis ma naissance ;

A ma très chère mère : quelle trouve ici l'hommage de ma gratitude qui, si grande quelle puisse être ne sera a la hauteur de ses sacrifices et ses prières pour moi ;

A mon frère nabil et ma sœur katia à qui je souhaite beaucoup de réussite et de bonheur ;

A ma très chère binôme ryma ceci est le fruit de notre travail

A tous mes amis et en particulier Mina, Sihem, Cecy, Karim, Said;

A mon chéri que dieu me le préserve ;

A toute ma famille en témoignage de mon profond respect ;

Enfin, A nos camarades de promotion qu'il trouve ici l'expression de mes sentiments les plus dévoués et mes vœux les plus sincères ;

Que dieu le tout puissant vous préserve tous et vous procure sagesse et bonheur.

Sara

Remerciements

Nous remercions avant toute chose dieu le tout puissant qui a guidé nos pas pour l'accomplissement de ce modeste travail.

Nous tenons aussi à remercier et à exprimer notre profonde gratitude à Dr « Boudries », notre promoteur de nous avoir fait confiance durant le projet.

Nous remercions notre encadreur de stage Mr « Souadi » pour le temps précieux qu'il nous a accordé.

Nous adressons aussi nos remerciements au président et aux membres du jury qui nous font honneur en acceptant de juger notre travail.

Notre reconnaissance s'adresse à nos familles qui ont su nous apporter, sans relâche, leurs soutiens durant toutes ces longues années d'études.

Enfin que tous ceux qui, de prés ou de loin ont contribué à l'aboutissement de ce travail soient assurés de nos profondes gratitudes.

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES ABRÉVIATIONS

CLI : Command Line Interface.
DHCP : Dynamic Host Configuration Protocol.
BID : Bridged Identity.
BPDU : Bridge Protocol Data Unit.
DRGB : Direction Régionale de Béjaia.
CD : Disque Compact.
DMZ : Demilitarized Zone.
DNS : Domain Name System.
DVD : Digital Versatile Disc.
EIGRP : Extended Interior Gateway Routing Protocol.
ENAC : Entreprise Nationale de Canalisations.
ENIP : Entreprise Nationale de la Pétrochimie.
HSRP : Hot Standby Routing Protocol.
HTTP : Hypertext Transfer Protocol.
IGRP : Intenior Gateway Routing Protocol.
IP : Internet Protocol.
ISO : Organisation Internationale de normalisation.
JPEG : Joint Photographic Experts Group.
LAN : Local Area Network.
MAC : Media Access Control.
MAN : Metropolitan Area Network.
NVRAM : Mémoire RAM Non Volatile.
OSI : Open System Interconnection.
OSPF : Open Shortest Path First. **PC :** Personel Computer.
RFC : Request For Comments (Ensemble de documents qui font référence auprés de la communité internet).
RIP : Routing Information Protocol.

RTC : Region Transport Centre.
SSG : Secure Services Gateways.
STA : Spannig Tree Algorithm.
STP : Spanning-Tree Protocol.
TCP : Transmission Control Protocol.
USB : Universal Serial Bus.
VLAN : Virtual Local Area Network.
VRRP : Virtual Router Redundancy Protocol.
VTP : VLAN Trunking Protocol.
WAN : Wide Area Network.

INTRODUCTION GÉNÉRALE

Le besoin d'échanger des données se faisait sentir juste après l'apparition des ordinateurs, puis l'homme eut l'idée de les relier entre eux, c'est là où apparait le concept des réseaux informatiques.

Dans toute entreprise la notion de réseaux sonne comme une évidence, chaque entreprise existante d'une certaine taille dispose en général d'un réseau informatique LAN ou WAN, qui lui permet d'effectuer le partage de ressources et de données. Vu l'importance des informations qui sont souvent véhiculées dans les réseaux, ceci requièrent une bonne gestion du réseau, une souplesse d'utilisation et un certain degré de sécurité. Ces derniers sont devenus des éléments clés de la continuité des systèmes d'information de l'entreprise quelques soient son activité, sa taille et sa répartition géographique.

SONATRACH ne cesse d'acquérir des nouvelles solutions qui assurent une haute disponibilité de son réseau. Notre stage au sein de la RTC nous a permis de découvrir le réseau et de mieux comprendre son fonctionnement. L'objectif principal de notre projet consiste à la configuration et la mise en place d'un réseau campus d'une entreprise, pour l'échange des informations entre l'ensemble des équipements de ce dernier.

Afin d'atteindre l'objectif sollicité, nous avons divisé notre mémoire en quatre principaux chapitres : D'abord le premier chapitre donne un aperçu sur les réseaux, ensuite le second chapitre porte sur la présentation de la RTC Sonatrach, cependant nous exposerons la problématique de notre travail et quelques eventuelles solutions. Dans le troisième chapitre, nous parlerons des réseaux campus et de la haute disponibilité tout en expliquant le concepts des VLANs et l'étude de quelques protocoles utilisés dans notre configuration. Enfin, dans le dernier chapitre nous présenterons la solution mise en place avec l'explication de la configuration des différents protocoles et les tests de validation pour nous assurer que notre objectif a bien été atteint.

CHAPITRE 1

GÉNÉRALITÉS SUR LES RÉSEAUX

1.1 Introduction

Afin de bien mener notre travail sur l'étude et l'optimisation d'un réseau local étendu, il est primordial de bien assimiler les notions de base sur les réseaux informatiques. A travers ce chapitre nous allons exposer quelques concepts théoriques sur les réseaux informatiques afin de mieux comprendre leur fonctionnement. De ce fait, toutes les notions nécessaires seront présentées.

1.2 Définition d'un réseau

Un réseau a pour fonction de transporter les données d'une machine terminale vers une autre machine terminale. Pour ce faire, une série d'équipements et de processus sont nécessaires, allant de l'environnement matériel, utilisant des câbles terrestres ou des ondes radio, jusqu'à l'environnement logiciel constitué de protocoles, c'est-à-dire de règles permettant de décider de la façon de traiter les données transportées.

1.3 Définition d'un réseau informatique

Un réseau informatique est un réseau dont chaque noeud est un système informatique autonome, ces noeuds sont reliés par des supports matériels et logiciels, et ont aussi la possibilité de communiquer entre eux directement ou indirectement. En pratique, deux ordinateurs suffisent pour constituer un réseau informatique [1].

Suivant l'éloignement entre ces équipements, on distingue les réseaux suivants [2] :

- **Le LAN (Local Area Network)**
  Un réseau local (LAN) est un réseau connectant des équipements informatiques, les uns très proches des autres, par exemple un ensemble d'équipements informatiques connectés et échangeant des informations au sein d'une salle, d'un appartement ou d'un immeuble forme un réseau LAN. Plusieurs bâtiments proches peuvent aussi constituer un réseau local.
- **Le MAN (Metropolitain Area Network)**
  Le réseau MAN interconnecte plusieurs LAN géographiquement proches (au maximum quelques dizaines de kilomètres). Le MAN aussi appelé réseau intermédiaire, permet de mettre en réseau des ordinateurs grâce à des antennes ou à des émetteurs dans un périmètre équivalent à une ville.
- **Le WAN (Wide Area Network)**
  Le réseau WAN est un réseau connectant des équipements informatiques à des grandes distances, les uns à la suite des autres. Plusieurs équipements informatiques connectés à partir de plusieurs points du globe peuvent former un réseau étendu.

1.4 Architecture des réseaux

On distingue généralement deux types d'architecture de réseaux bien différents, ayant tout de même des similitudes :

- **Les réseaux poste à poste (Peer to Peer/ égal à égal) :**
  Les réseaux poste à poste ne comportent en général que peu de postes, moins d'une dizaine de postes, parce que chaque utilisateur fait office d'administrateur de sa propre machine, il n'y a pas d'administrateur central, ni de super utilisateur, ni de hiérarchie entre les postes, ni entre les utilisateurs [3].
- **Les réseaux organisés autour de serveurs (client/serveur) :**
  Les réseaux client/serveur comportent, en général, plus de dix postes. La plupart des stations sont des "postes clients". C'est-à-dire des ordinateurs dont se servent les utilisateurs, les autres stations sont dédiées à une ou plusieurs tâches spécialisées, on dit alors qu'ils sont des serveurs [3].

Le type d'architecture de réseau à installer dépend des critères suivants [4] :

- Taille de l'entreprise.
- Niveau de sécurité nécessaire.
- Type d'activité.
- Niveau de compétence d'administration disponible.
- Volume du trafic sur le réseau, besoins des utilisateurs sur le réseau.

1.5 Topologie des réseaux

Nous avons deux types de topologies :

1.5.1 La topologie physique

La topologie physique est la façon dont les équipements (ordinateurs) sont reliés entre eux.

1.5.2 La topologie logique

La topologie logique est la façon dont transitent les informations.

Nous avons quatre types de topologies :

- **Réseau multipoint en bus :** Dans un réseau multipoint en bus (Figure 1.1), tous les noeuds sont reliés directement à la liaison centrale, laquelle est tirée entre les deux noeuds les plus éloignés [1].

- **Réseau multipoint en anneau :** Dans un réseau multipoint en anneau (Figure 1.1), tous les noeuds sont reliés directement à la liaison centrale, laquelle reboucle sur elle même, les communications sont monodirectionnelles [2].

- **Réseau point à point en étoile :** Dans un réseau point à point en étoile (Figure 1.1), tous les noeuds sont reliés à un noeud central (serveur, qui est une machine puissante ou appareillage dédié), le nombre de liaisons est ainsi minimal (N-1 liaisons pour N noeuds), mais le réseau est limité par les possibilités du noeud central [2].

- **Réseau point à point en arbre :** Un réseau point à point en arbre est un assemblage de réseau point à point en étoile [2] (Figure 1.1).

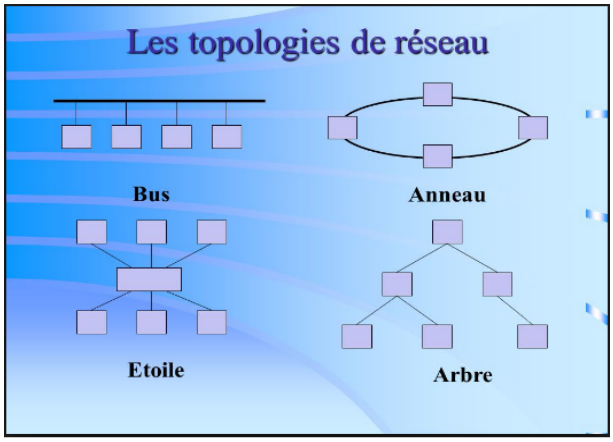

FIGURE 1.1 – Les différentes topologies des réseaux

1.6 Les modèles de réseaux

Nous avons deux types de réseaux :

1.6.1 Le modèle OSI

L'organisme ISO a défini en 1984 un modèle de référence, nommé Open System Interconnexion (OSI) [5] destiné à normaliser les échanges entre deux machines. Il définit ce que doit être une communication réseau complète. L'ensemble du processus est ainsi découpé en sept couches hiérarchiques [1] (Figure 1.2).

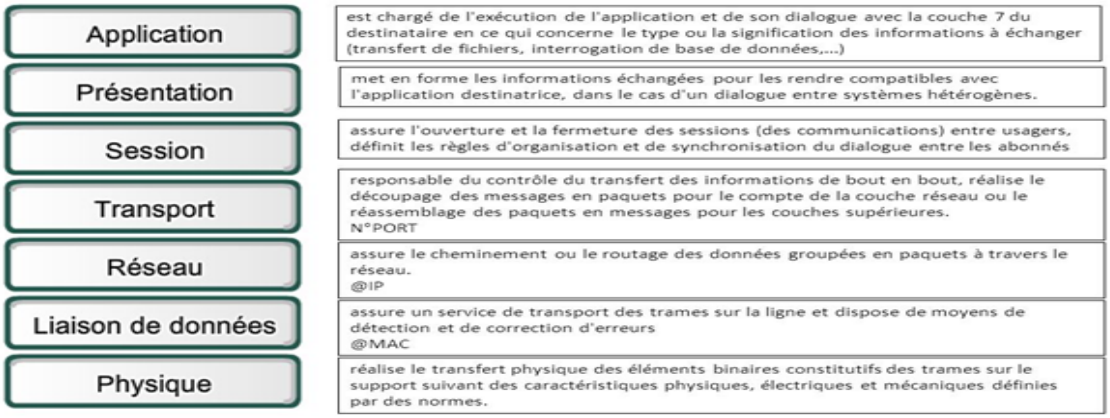

FIGURE 1.2 – Le modèle OSI

1.6.2 Le modèle TCP/IP (Transmission Control Protocol/Inernet Protocol)

Le protocole TCP/IP (Figure 1.3) est utilisé sur le réseau Internet pour transmettre des données entre deux machines (protocole de transport).

- Le TCP prend à sa charge l'ouverture et le contrôle de la liaison entre deux oridinateurs.
- Le protocole d'adressage IP assure le routage des paquets de données [1].

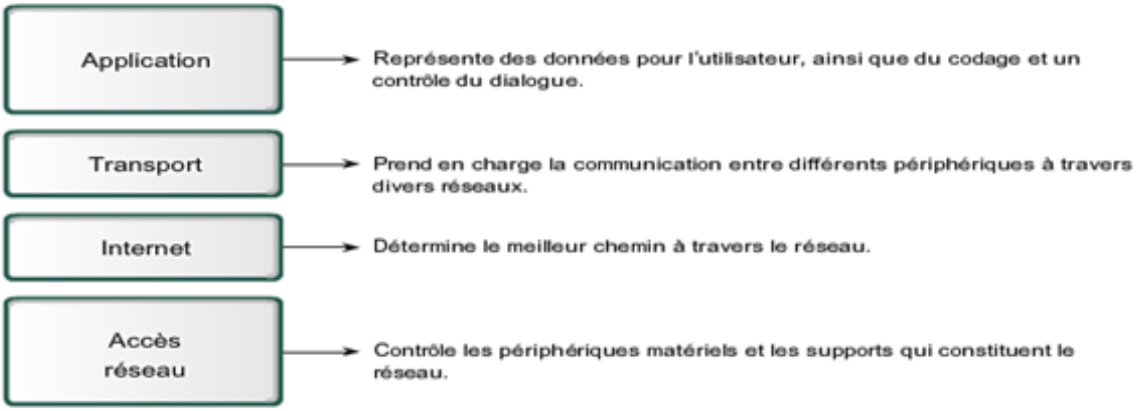

FIGURE 1.3 – Le modèle TCP/IP

1.7 Les équipements de base d'un réseau informatique

Nous avons plusieurs équipements, nous pouvons citer [6] :

1.7.1 Les unités hôtes

Les hôtes sont des unités directement connectées à un segment de réseau, nous pouvons les retrouver sous forme d'ordinateurs, de serveurs, de scanners ou d'imprimantes.

1.7.2 Les commutateurs (switchs)

Un commutateur est un équipement qui relie plusieurs câbles ou fibres dans un réseau informatique ou un réseau de télécommunication. Les commutateurs permettent de créer des circuits virtuels et de diriger les informations vers une destination précise sur le réseau. L'utilisation de switchs permet de sécuriser les informations transmises sur le réseau, à la différence des concentrateurs qui envoient les informations sur tous les ordinateurs, les switchs envoient les données uniquement aux destinataires qui doivent les recevoir. La commutation est un mode de transport de trame au sein d'un réseau informatique et de communication [7].

1.7.3 Les routeurs

Un routeur est un élément intermédiaire qui permet de relier deux réseaux. Il assure le routage des paquets d'une interface à une autre. Il opère au niveau de la troisième couche du modèle OSI (la couche réseau). La plupart des routeurs sont capables de déterminer automatiquement l'itinéraire le plus adapté entre le départ et la destination à l'aide des adresses, ce qui permet d'acheminer le paquet avec le meilleur itinéraire. Pour diriger les informations, le routeur doit comprendre le protocole utilisé, qui est un langage que les ordinateurs utilisent pour communiquer, comme par exemple : TCP/IP, TCP, IP [7].

1.8 Les protocoles de niveau 2

Cette couche correspond à la couche de liaison de données dans le modèle OSI. À ce niveau, on trouve par exemple les protocoles suivants :

1.8.1 Les virtual LAN (VLAN)

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français réseau local virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

1.8.1.1 Définition d'un VLAN

Un réseau local virtuel (VLAN) est un réseau local (LAN) distribué sur des équipements de niveau 2 du modèle OSI (couche liaison). Le domaine de diffusion se retrouve ainsi réparti sur ces mêmes équipements de niveau 2. Ainsi, tous les hôtes appartenant au même réseau local (domaine de diffusion) constituent un groupe logique indépendant de la topologie physique du réseau. Les VLAN ont été uniformisés conformément à la spécification IEEE 802.1Q. Il subsiste cependant des variantes d'implémentation d'un constructeur à l'autre [8].

1.8.1.2 Agrégation de VLAN

Une agrégation est une liaison point à point entre deux périphériques réseaux qui porte plusieurs VLANs à l'ensemble d'un réseau.
Une agrégation de VLAN n'appartient pas à un VLAN spécifique, mais constitue plutôt un conduit pour les VLANs entre les commutateurs et les routeurs [8].

1.8.2 Vlan Trunking Protocol (VTP)

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 [9].

1.8.2.1 Définition du VTP

Un commutateur doit être déclaré en serveur, on lui attribue également un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifié ou supprimé. Ainsi chaque commutateur client, présent dans le domaine, héritera automatiquement des nouveaux VLANs crées 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 [10].

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants [11] :

- **Le mode serveur**
  - L'information est stockée dans la NVRAM.
  - Il défini le nom de domaine VTP.
  - Il peut ajouter, modifier ou supprimer un VLAN.
  - Il stocke la liste des VLANs du domaine VTP.
- **Le mode client**
  - Il possède un nom de domaine.
  - Il stocke une liste de VLANs non modifiable.
- **Le mode transparent**
  - Il ne participe pas aux domaines VTP du réseau.
  - Il transmet les paquets VTP via ses liens trunk.
  - Il possède sa propre liste de VLANs qu'il est possible de modifier.

Si une des conditions suivantes n'est pas respectée, le domaine de VTP ne sera pas valide et l'information ne se propagera pas :

- Il faut assigner le même nom de domaine de VTP à chaque commutateur.
- L'option trunk pour l'interconnexion des commutateurs doit être activée [11].

Exemple (Figure 1.4)

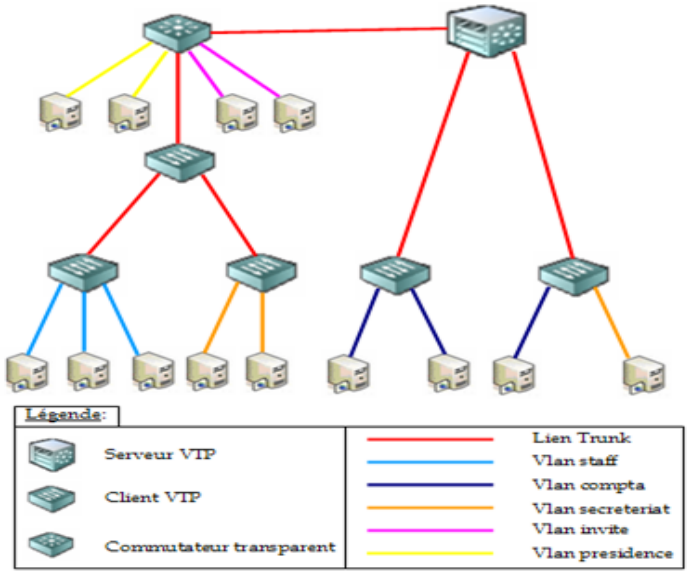

FIGURE 1.4 – Le protocole VTP

Le serveur diffuse la liste des VLANs. Les paquets VTP Advertisements sont identifiés par un numéro de révision. Le numéro de révision le plus élevé sera celui qui modifiera la base de données VLAN. Elle se propage sur les liens trunk.
Les commutateurs en mode transparents ont leur propre liste. Cette liste n'est pas diffusée sur le réseau mais les paquets VTP le sont [11].

1.8.2.2 Concept du VTP

Une trame mise en oeuvre dans le protocole VTP se compose d'un champ d'en-tête et d'un champ de message. Les informations VTP sont insérées dans le champ de données d'une trame Ethernet. La trame Ethernet est ensuite encapsulée comme trame d'agrégation 802.1Q. Chaque commutateur du domaine envoie régulièrement des annonces de chaque port d'agrégation vers une adresse de multidiffusion réservée. Ces annonces sont reçues par les commutateurs voisins, qui mettent à jour leur configuration VTP et VLAN selon le besoin [9]. La figure 1.5 illustre les mises en oeuvre par le protocole VTP :

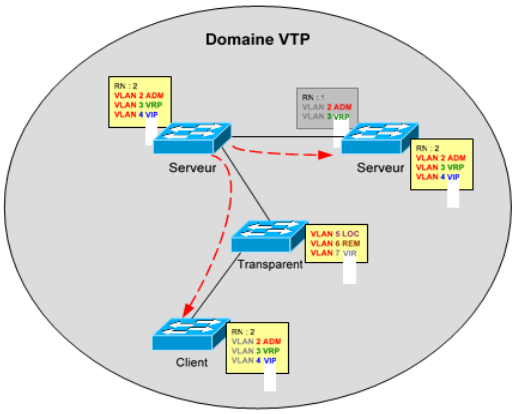

FIGURE 1.5 – Exemple du concept du protocole VTP

1.8.3 Le protocole STP (Spanning-Tree Protocol)

1.8.3.1 Définition du STP

Le protocole STP est un protocole de couche 2 qui fonctionne sur des ponts et des commutateurs. La spécification du protocole STP est IEEE 802.1. L'objectif principal de ce protocole est de vérifier qu'aucune boucle n'est créée lorsqu'il y'a des chemins redondants dans le réseau car ces dernières sont fatales [9].

1.8.3.2 Concept du protocole STP

Le protocole STP utilise l'Algorithme Spanning Tree (STA) pour déterminer quels ports de commutateurs doivent être configurés en état de blocage afin d'empêcher la formation de boucles sur un réseau. L'algorithme STA désigne un commutateur unique comme pont racine et il l'utilise comme point de référence pour le calcul de tous chemins. Tous les commutateurs associés au protocole STP échangent des trames BPDU pour identifier le commutateur doté de l'identificateur de pont (BID) le plus faible sur le réseau. Le commutateur doté de l'identificateur (ID) le plus faible devient automatiquement le pont racine pour calcul de l'algorithme STA. L'unité BPDU est la trame de message échangée par les commutateurs pour le protocole STP. Chaque trame BPDU contient un identificateur de pont qui identifie le commutateur ayant envoyé la trame BPDU. L'identificateur de pont contient une valeur de priorité, l'adresse MAC du commutateur émetteur et un ID système étendu facultatif. La valeur d'identificateur de pont la plus faible est déterminée par la combinaison de ces trois champs. Une fois que le pont racine a été déterminé, l'algorithme STA configure les ports des commutateurs dans des rôles de ports indépendants. Les rôles des ports décrivent le lien entre les ports et le pont racine de réseau et spécifient s'ils sont autorisés à acheminer le trafic [9].

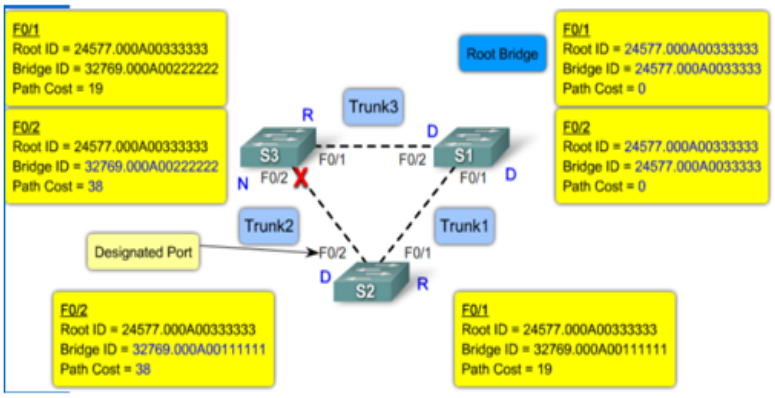

FIGURE 1.6 – Exemple du concept du protocole STP

1.9 Les protocoles de niveau 3

1.9.1 L'adressage IP

L'adresse IP est un numéro unique qui permet d'identifier chaque ordinateur connecté sur un réseau, ce numéro est réparti en 4 fois 8bits allant de 0 à 255 séparé par des points. On distingue deux partie dans une adresse IP, la partie réseau et la partie hôte. La première identifie le réseau sur le quel est connectée la machine et le deuxième identifie les machines connectées à ce réseau. Pour identifier ces deux parties, chaque adresse est liée à un masque de sous-réseau qui permet de définir sur quel réseau elle se trouve [12].

Les adresses IP sont séparées en plusieurs classes :

- Les adresses IP de classe A : 0 à 127
- Les adresses IP de classe B : 128 à 191
- Les adresses IP de classe C : 192 à 223
- Les adresses IP de classe D : 224 à 239
- Les adresses IP de classe E : 240 à 255

1.9.2 Adresse de diffusion

Une adresse de diffusion ("broadcast" en anglais) est une adresse permettant de désigner toutes les machines d'un réseau, elle est obtenue en plaçant tous les bits de la partie machine à un [12].

1.9.3 Adresse privée

Pour éviter les ambiguïtés avec les adresses de réseau et les adresses de diffusion, les adresses "tout à zéro" et "tout à un" sont déconseillées pour désigner des machines sur un réseau. Dans chaque classe d'adresses, certaines adresses réseaux sont réservées aux réseaux privés [12].

- Classe A : 10.0.0.0 à 10.255.255.255
- Classe B : 172.16.0.0 à 172.255.255.255
- Classe C : 192.168.0.0 à 192.255.255.255

1.9.4 Le routage

Le routage est un processus qui permet de sélectionner des chemins dans un réseau pour transmettre des données depuis un expéditeur jusqu'à un ou plusieurs destinataires, cette fonction emploie des algorithmes de routage et des tables de routage. Le principal périphérique de routage est le routeur, ce dernier utilise des adresses IP pour diriger les paquets d'un réseau à un autre et doit aussi maintenir sa table de routage à jour et connaître les changements effectués sur les autres appareils par lesquels il pourrait faire transiter le paquet. Il existe deux manières pour remplir et mettre à jour la table de routage, manuellement (routage statique) ou de façon dynamique [12].

1.9.4.1 Les types de routage

Il existe deux modes de routages bien distincts lorsque nous souhaitons aborder la mise en place d'un protocole de routage, il s'agit du routage statique et du routage dynamique [12] :

- **Le routage statique :** Dans le routage statique, les tables sont remplies manuellement par l'administrateur réseau. Il est utilisé sur des petits réseaux ou sur des réseaux d'extrémité. L'administrateur doit faire la gestion des routes de chaque unité de routage du réseau, les chemins statiques ne s'adaptent pas aux modifications des environnements réseaux, les informations sont mises à jour manuellement à chaque modification topologique de l'inter-réseau.
- **Le routage dynamique :** Avec le routage dynamique, les tables sont remplies automatiquement. On configure un protocole qui va se charger d'établir la topologie et de remplir les tables de routage. On utilise un protocole de routage dynamique sur des réseaux plus importants. Le routage dynamique permet également une modification automatique des tables de routage en cas de rupture d'un lien sur un routeur. Il permet également de choisir la meilleure route disponible pour aller d'un réseau à un autre.

1.9.4.2 Les protocoles de routage

Tous les protocoles de routage ont pour objectif de maintenir les tables de routage du réseau. Pour y parvenir, les protocoles diffusent des informations de routage aux autres systèmes du réseau afin de transmettre les modifications des tables de routage. Un protocole de routage sert à améliorer la vitesse de routage, à gagner du temps en évitant de devoir configurer manuellement toutes les routes sur chaque routeur, à améliorer la stabilité du réseau en choisissant à chaque fois la meilleure route [13].

Les protocoles de routage peuvent être classés en deux catégories :

- Les protocoles à vecteur de distance.
- Les protocoles à état de liens.

- **Les protocoles à vecteur de distance :** Un protocole de routage à vecteur de distance [14] est celui qui utilise un algorithme de routage qui additionne les distances pour trouver les meilleures routes (Bellman-Ford). Souvent, il envoie l'intégralité de la table de routage aux voisins. Il est sensible aux boucles de routage. Ce type de méthode compte le nombre de sauts qu'il y a entre deux endroits, et c'est en fonction de ce nombre de sauts, qu'il va choisir le chemin le plus court. Nous citerons RIP et IGRP :
  - **RIP :** signifie *Routing Information Protocol* (protocole d'information de routage), Il s'agit d'un protocole de type Vector Distance (Vecteur Distance), c'est-à-dire que chaque routeur communique aux autres routeurs la distance qui les sépare (le nombre de sauts qui les sépare). Ainsi, lorsqu'un routeur reçoit un de ces messages il incrémente cette distance de 1 et communique le message aux routeurs directement accessibles. Les routeurs peuvent donc conserver de cette façon la route optimale d'un message en stockant l'adresse du routeur suivant dans la table de routage de telle façon que le nombre de sauts pour atteindre un réseau soit minimal [14].
  - **IGRP :** signifie *Intenior Gateway Routing Protocol*, c'est un protocole propriétaire développé par Cisco Systems, plus robuste que le RIP et possédant moins de limitations. EIGRP *(Extended Interior Gateway Routing Protocol)* est une version évoluée.
- **Les protocoles à état de liens :** Un protocole de routage à état de liens [14] utilise un algorithme plus efficace (Dijkstra ou Shortest Path First). Les routeurs collectent l'ensemble des coûts des liens et construisent de leur point de vue l'arbre de tous les chemins. Les meilleures routes sont alors intégrées à la table de routage. L'avantage de tels algorithmes est d'offrir une convergence rapide sans boucles et à chemins multiple.

  Nous citerons OSPF :
  - **OSPF :** *(Open Shortest Path First)*, plus performant que RIP et commence donc à le remplacer petit à petit. Contrairement à RIP, ce protocole n'envoie pas aux routeurs adjacents le nombre de sauts qui les sépare, mais l'état de la liaison qui les sépare. De cette façon, chaque routeur est capable de dresser une carte de l'état du réseau et peut, par conséquent, choisir à tout moment la route la plus appropriée pour un message [14].

    De plus, ce protocole évite aux routeurs intermédiaires d'avoir à incrémenter le nombre de

sauts, ce qui se traduit par une information beaucoup moins abondante, ce qui permet d'avoir une meilleure bande passante utile qu'avec RIP.

1.10 Conclusion

Une bonne compréhension de l'ensemble des concepts de bases de son sujet, permettra d'avoir une idée claire sur les réseaux informatiques et d'aborder son thème, en s'appuyant ainsi, sur une étude d'état des lieux. Dans le chapitre suivant, nous présenterons l'organisme d'accueil.

CHAPITRE 2

PRÉSENTATION DE L'ORGANISME D'ACCEUIL

2.1 Introduction

L'étude de l'organisme d'accueil est une étape importante qui sert à représenter les contraintes sous lesquelles se réalisera notre projet. Dans ce chapitre, nous allons présenter l'entreprise SONATRACH, citer les différents départements qui la constituent et donner quelques informations qui nous seront utiles dans notre travail, tout en posant la problématique autours de laquelle tournera notre mémoire.

2.2 Présentation générale de l'organisme d'accueil

SONATRACH est un Groupe pétrolier et gazier intégré sur toute la chaine des hydrocarbures. Il détient en totalité ou en majorité absolue, plus de vingt entreprises importantes sur tous les métiers connexes à l'industrie pétrolière tel que le forage, le raffinage... Il possède aussi des participations significatives dans près de 50 entreprises implantées tant en Algérie qu'à l'étranger.

2.3 Historique et missions

L'entreprise "SONATRACH" (Société Nationale pour le Transport et la Commercialisation des Hydrocarbures) a été crée le 31 Décembre 1963 par le décret n°63/491, les statuts ont été modifiés par le décret n°66/292 du 22 Septembre 1966, et SONATRACH devient "Société nationale pour la recherche, la production, le transport, la transformation et la commercialisation des hydrocarbures", cela a conduit à une restructuration de l'entreprise dans le cadre d'un schéma directeur approuvé au début de l'année 1981 pour une meilleure efficacité organisationnelle et économique, de ces principes SONATRACH a donné naissance à 17 entreprises : (NAFTAL, ENIP, ENAC,...etc.)

Après sa restructuration en 1982, et sa réorganisation en 1985, SONATRACH s'est recentrée sur ses métiers de base que constituent les activités suivantes :

- Exploration et recherche.
- Exploration des gisements d'hydrocarbures.
- Le transport par canalisation.
- La liquéfaction et la transformation de GAZ.
- La commercialisation.

Pour la réalisation de ces objectifs, SONATRACH est divisé en cinq branches différentes représentées dans la figure 2.1 :

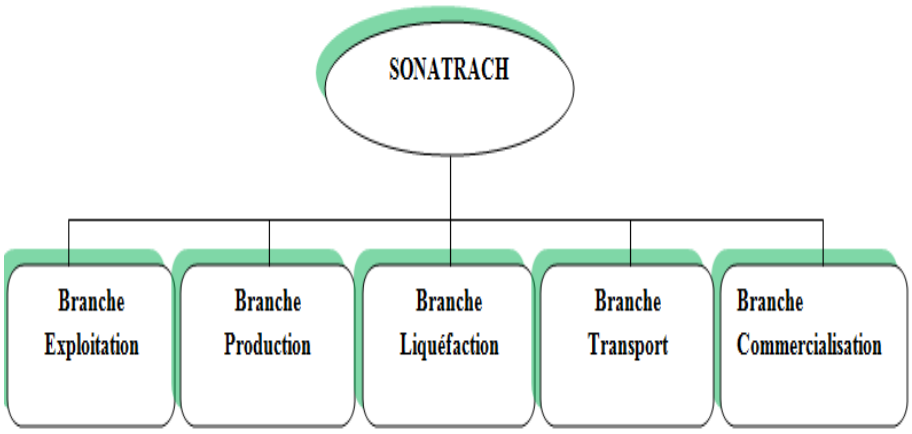

FIGURE 2.1 – Organigramme de la RTC

A travers cette transformation structurelle et fractionnelle, un schéma de groupes a évolué en constituant des branches d'activités autonomes et leurs filiations. De la branche (Activité de transport par canalisation), se trouve la Direction Régionale de Bejaia (DRGB) où s'est déroulé notre stage pratique.

2.4 Activités de la branche transport par canalisation (TRC)

L'activité de transport par canalisation (TRC) est en charge de l'acheminement des hydrocarbures pétroles brut, gaz et condensat vers les ports pétroliers, les zones de stockages et les pays d'exploitation. Les missions affectées à la branche transport par canalisation sont :

- La gestion et l'exploitation des ouvrages et canalisations de transport d'hydrocarbures.
- La coordination et le contrôle de l'exécution des programmes de transport arrêtés en fonction des impératifs de production et de commercialisation.
- La maintenance, l'entretien et la protection des ouvrages et canalisations.
- L'exécution des révisions générales, des machines tournantes et équipements.
- La gestion de l'interface transport des projets internationaux du groupe ou en partenariat.

La SONATRACH possède cinq directions régionales de transport des hydrocarbures :

- La direction régionale Est (Skikda).
- La direction régionale Centre (Béjaia).
- La direction régionale Ouest (Arzew).
- La direction régionale de Haoud-El-Hamra.
- La direction régionale d'Ain Amenas.

2.5 Présentation de la direction régionale de Bejaia (DRGB)

La DRGB est l'une des cinq directions chargée du transport, du stockage et de la livraison des hydrocarbures liquides et gazeux. Les hydrocarbures transportés à travers les canalisations gérées et exploitées par la DRGB sont :

- Le GAZ naturel.
- Le pétrole brut.
- Le condensat.

2.6 Structure de la DRGB

Nous illustrons les directions et sous-directions dans le diagramme de la figure 2.2 comme suit : la figure 2.3 représente l'organisation humaine du département informatique :

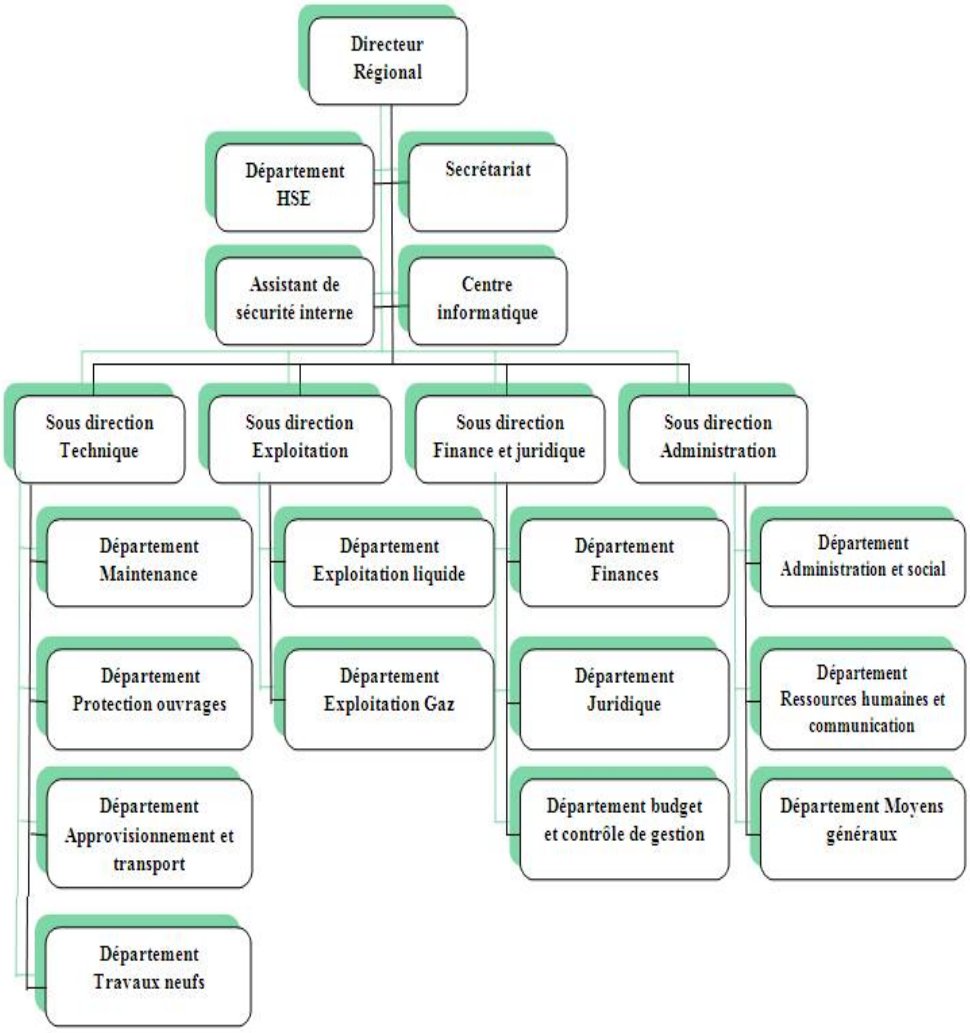

FIGURE 2.2 – Organigramme de la RTC

- **Direction régionale :** Elle est dirigée par un directeur régional aidé par des assistants et un secrétariat.
- **Secrétariat.**
- **Assistant de sûreté interne :** Sa mission est de protéger et de sauvegarder le patrimoine humain et matériel de la DRGB.
- **Centre informatique :** Il regroupe les moyens d'exploitation et de développement des applications informatiques pour l'ensemble des structures de la DRGB, ainsi que la gestion du réseau informatique interne.
- **Sous direction technique :** Elle a pour mission d'assurer la maintenance et la protection des ouvrages. Elle est organisée en quatre départements : département maintenance, département protection des ouvrages, département approvisionnement et transport et département des travaux neufs.
- **Sous direction Exploitation :** Elle est chargée de l'exploitation des installations de la région, et de maintenir le fonctionnement de trois ouvrages en effectuant des réparations en cas de fuite, de sabotage ou de panne pour les stations de pompage. Elle est composée de deux départements : le département exploitation liquide et le département exploitation gaz.
- **Sous direction Finances et Juridique :** Elle a pour mission d'effectuer la gestion financière, le budget et le contrôle de gestion et de prendre en charge les affaires juridiques de la DRGB. Elle est organisée en trois départements : département finances, département juridique, département budget et contrôle de gestion.
- **Sous direction Administration :** Elle a pour mission la gestion des ressources humaines et les moyens généraux. Elle est organisée en trois départements : département administration et social, département ressources humaines et communication et département moyens généraux.

– **Présentation du centre informatique :** Le centre informatique est chargé du développement et de l'exploitation des applications informatiques de gestion pour le compte de la direction régionale de Béjaia (DRGB) et des autres régions.

2.7 Organisation structurelle

L'organisation du centre ne cesse de subir des changements et l'évolution rapide de l'informatique pousse le centre à adopter des actions nouvelles à chaque fois afin de subvenir aux nouveaux besoins de l'entreprise.

Pour mener à bien sa mission, le centre informatique s'organise en trois services tels qu'ils sont schématisés dans la figure 2.3 :

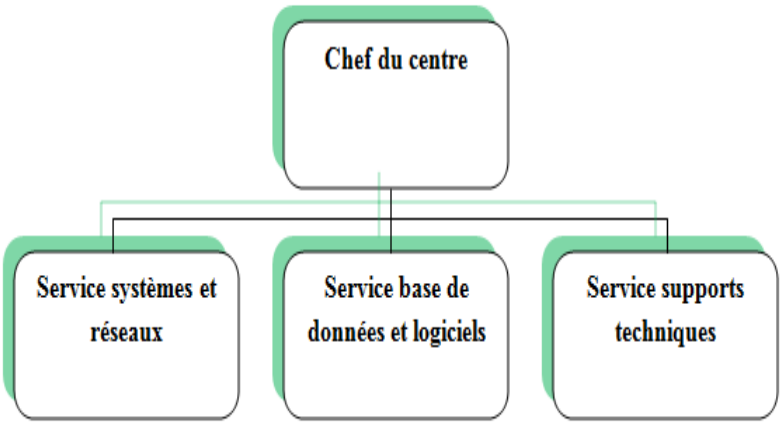

FIGURE 2.3 – Organigramme du centre informatique

2.8 Organisation fonctionnelle

Chaque service a sa propre fonction, nous allons définir et citer les différentes tâches de chacun ci-dessous :

2.8.1 Service systèmes et réseaux

- **Système :**
  - Choix des équipements informatiques et logiciels de base.
  - Mise en oeuvre des solutions matérielles et logicielles retenues.
  - Installation et configuration des systèmes.
  - Mise en oeuvre des nouvelles versions de logiciels.
- **Réseau :**
  - Assurer le bon fonctionnement et la fiabilité des communications.
  - Assurer l'administration du réseau et organiser l'évolution de sa structure.
  - Etude et choix de l'architecture du réseau à installer et la participation à sa mise en place.
  - Définition des droits d'accès à l'utilisation du réseau.
  - Assurer la surveillance permanente pour détecter les pannes.
  - Traitement des incidents survenant sur le réseau.

2.8.2 Service base de données et logiciels :

- **Base de données :**
  - Conception des bases de données, optimisation et suivi des données informatiques.
  - Installation, configuration et exploitation du système de gestion de bases de données et ses bases.
  - Mise en oeuvre et gestion des procédures de sécurité.
  - Gestion de la sauvegarde, la restauration et la migration des données.
- **Logiciels :**
  - Etude et conception des systèmes d'information.
  - Développement et maintenance des applications informatiques pour TRC.
  - Déploiement des applications et formation des utilisateurs.

2.8.3 Service supports techniques

- Assistance aux utilisateurs en cas de problèmes software et hardware.
- Installation des logiciels de gestion, technique et bureautique.
- Formation aux nouveaux produits installés.

2.9 Aspect réseau

Le réseau de la DRGB est constitué de deux parties connectées entre elle (le réseau de l'ancien bâtiment et le réseau du nouveau bâtiment). En effet, il a subit une extension après la construction du nouveau bâtiment.

2.9.1 Les commutateurs utilisés dans le réseau de la DRGB

Le réseau de la DRGB utilise deux types de commutateurs :

- **Les commutateurs intelligents :** En plus de leur fonction ils peuvent faire le routage. Dans le réseau de la DRGB, on trouve trois exemples de ce type qui sont :
  - Catalyst Cisco 6509 : La gamme Catalyst 6509 représentée sur la figure 2.4 offre des moyens pour soutenir la capacité de la bande passante du système et des capacités améliorées de gestion des câbles. Elle fournit également des flux d'air d'avant en arrière qui est optimisé pour les conceptions allée chaude et froide dans le centre de données co-localisées et les déploiements de services. En outre elle offre une protection exceptionnelle des investissements en soutenant plusieurs générations de produits sur le même châssis, réduisant ainsi les coûts totaux de propriété. Le cadre Cisco Catalyst 6509 supporte à la fois la gamme Cisco Catalyst 6500 Supervisor Engine 32 et Cisco Catalyst 6500 Series Supervisor Engine 720 familles, avec LAN associés, WAN, et des modules de services [15].

FIGURE 2.4 – Gamme Catalyst Cisco 6509

– Catalyst Cisco 3750 : La gamme Cisco Catalyst 3750 représentée dans la figure 2.5 est une ligne de commutateurs innovants qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables. Cette gamme de produits dispose de la technologie Cisco StackWise, interconnectant les commutateurs au sein d'une même pile à 32 Gbps qui permet de construire un système unique de commutation à haute disponibilité. En outre, elle est optimisée pour les déploiements Gigabit Ethernet haute densité et comprend un large éventail de commutateurs qui répondent aux exigences en matière d'accès, d'agrégation ou de connectivité dorsale pour de petits réseaux [16].

FIGURE 2.5 – Gamme Catalyst Cisco 3750

– Catalyst Cisco 3550 : C'est une gamme de commutateurs CISCO empilables, il fournit une haute disponibilité et des fonctionnalités avancées de qualité de service et de la sécurité afin d'améliorer l'exploitation de réseau (Figure 2.6) [16].

FIGURE 2.6 – Gamme Catalyst Cisco 3550

- **Les commutateurs non intelligents :** Ce type de commutateurs ne permet pas de faire le routage. Le réseau de la DRGB contient le type suivant :
  – Catalyst 2950 : Le Cisco Catalyst 2950 Séries Switch est une configuration fixe, empilable commutateur autonome qui fournit un accès rapide à vitesse filaire Ethernet et Gigabit Ethernet. Le Catalyst 2950 représenté sur la figure 2.7 dispose de deux ensembles distincts de fonctionnalités du logiciel et une gamme de configuration pour permettre aux petits environnements, de taille moyenne et les succursales d'entreprise et industriels à choisir la bonne combinaison pour la périphérie du réseau [17].

FIGURE 2.7 – Gamme Catalyst Cisco 2950

2.10 Aspect sécurité

- **Serveur antivirus :** Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de programme modifiant ou supprimant des fichiers, que ce soit des documents infectés de l'utilisateur ou des fichiers nécessaires au bon fonctionnement de l'ordinateur. Un antivirus vérifie les fichiers et courriers électroniques, les secteurs de boot (pour détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clés USB, CD, DVD etc), les données qui transitent sur les éventuels réseaux (dont Internet) etc [18].
- **Serveur filtrage Web :** Permet d'interdire l'accès à des sites au contenu répréhensible ou plus simplement de bloquer les bannières publicitaires. Les règles de filtrage sont mises à jour automatiquement dans l'établissement à partir d'une base de données. Les sites filtrés sont classés par catégories (adultes, piratages, publicités) modifiables, ainsi c'est l'établissement qui maîtrise sa politique de filtrage [19].
- **Serveur reporting :** C'est un outil complet et de rapport facile à utiliser qui permet d'évaluer l'utilisation de l'Internet par des employés de l'entreprise, identifier tous les problèmes possibles avec accès à l'Internet ou à la consommation de la bande passante réseau en générant des rapports détaillés, des résumés ou des graphiques. Il est utilisé pour montrer comment la connexion Internet est utilisée et pour affiner les stratégies de filtrage afin de maximiser les ressources du réseau [19].
- **Firewall juniper ssg 550 :** Représente une nouvelle classe de dispositif de sécurité construite à cet effet qui offre un parfait mélange de haute performance, de sécurité et de connectivité LAN/WAN pour les déploiements de bureau régional et de leurs branches. Avec un réseau éprouvé et la protection au niveau application, le SSG 550 peut être mis en oeuvre comme dispositif de sécurité autonome pour arrêter les vers, les logiciels espions, cheval de trois, les logiciels malveillants et autres attaques émergentes (Figure 2.8) [20].

FIGURE 2.8 – Firewall Juniper ssg 550

Firewall juniper ssg 550 représenté dans la figure 2.8 contient un ensemble de règles structurées en trois zones qui se présentent comme suit :

- **La zone strust :** C'est la zone la plus confiante, car elle autorise le trafic sortant et interdit le trafic entrant et c'est pour cela que la RTC lui a confiée son réseau LAN.
- **La zone untrust :** C'est une zone qui autorise de trafic entrant et interdit le trafic sortant.
- **La DMZ (Demilitarized Zone) :** C'est une zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet derrière le par-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (DNS, HTTP, DHCP). Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise et, pour certains, depuis le réseau externe. Le but est ainsi d'éviter toute connexion directe au réseau interne.

2.11 Problématique

Après avoir analysé l'état actuel du système de réseau de l'entreprise, nous avons soulevé les problématiques suivantes :

- Une architecture hiérarchique avec une mauvaise répartition des équipements informatiques (switchs...).
- Une architecture hiérarchique qui a besoin d'une optimisation au niveau de la haute disponibilité.
- Répartition des vlans en mode end to end (non local).

2.12 Propositions

Afin de répondre aux différentes problématiques, nous avons suggéré un ensemble de propositions et solutions pouvant remédier aux différentes lacunes soulevées durant notre stage :

- La redondance matérielle au niveau de la couche Core afin de remédier aux pannes.
- Proposer une vision pour la distribution des VLANs en mode local.

2.13 Objectifs

Les configurations que nous nous apprêtons à réaliser doivent exploiter les différents procédés liés à un réseau campus LAN (Cisco), afin d'optimiser le réseau existant, le futur système doit répondre aux critères suivants :

- Utilisation de la haute disponibilité dans le but d'optimiser la durée d'exécution en temps réel.
- Utilisation des VLANs en mode local au niveau des sous-réseaux.

2.14 Conclusion

Dans ce chapitre, nous avons appris à mieux comprendre la structure et l'organisation du réseau de la RTC de Béjaia, et d'étudier notre problématique afin de proposer les solutions adéquates et les objectifs à atteindre.

CHAPITRE 3

LA HAUTE DISPONIBILITÉ DES RÉSEAUX CAMPUS

3.1 Introduction

Après avoir présenté l'organisme de l'entreprise et les différents problèmes pèsant sur leur réseau, nous allons à présent dans ce chapitre élaborer une étude descriptible des solutions proposées, ainsi qu'une argumentation du choix de ces dernières qui seront implémentées en illustrant les avantages et les atouts de chaque solution qui nous ont poussés à les choisir.

3.2 Structure des réseaux campus

Un modèle de conception de réseau hiérarchique rend le problème complexe de la conception du réseau en petits problèmes plus faciles à gérer. Chaque niveau dans la hiérarchie répond à un ensemble de problèmes différents. Cela aide le concepteur à optimiser le matériel et le logiciel réseau. Cisco propose une hiérarchie à trois niveaux comme approche privilégiée pour la conception du réseau. Dans ce modèle, les dispositifs de réseau et de liaisons sont regroupés en fonction de trois couches.

Les modèles en couches sont utiles car la conception du réseau devient modulaire, ce qui facilite l'évolutivité et les performances. Les dispositifs de chaque couche ont des fonctions similaires et bien définies, cela permet aux administrateurs d'ajouter facilement, remplacer et supprimer des composants individuels du réseau. C'est ce type de flexibilité et d'adaptabilité qui rend la conception de réseau hiérarchique hautement évolutive pour une architecture idéale elle doit répondre à un certain nombre d'objectifs comme [21] :

- **La redondance au niveau des couches principales et de distribution garantit la disponibilité de chemins d'accès :** Exemple, Des commutateurs de couche d'accès sont connectés à deux commutateurs de couche de distribution différents, afin de garantir une redondance du chemin d'accès. Lorsque l'un des commutateurs de la couche de distribution devient inopérant, le commutateur de couche d'accès peut basculer vers l'autre commutateur de couche de distribution. En outre, des commutateurs de couche de distribution sont connectés à deux commutateurs

de couche coeur de réseau minimum pour garantir la disponibilité du chemin d'accès en cas de défaillance d'un commutateur principal. La seule couche où la redondance est limitée est la couche d'accès. En général, les périphériques de noeud d'extrémité, tels que les ordinateurs, les imprimantes et les téléphones sur IP, n'offrent pas la possibilité de se connecter à plusieurs commutateurs de couche d'accès pour la redondance. En cas d'échec d'un commutateur de couche d'accès, seuls les périphériques connectés à celui-ci sont affectés par la panne. Le reste du réseau peut continuer de fonctionner normalement.

- **L'évolutivité :** Les réseaux créés selon le modèle hiérarchique peuvent connaitre une croissance plus forte, sans effet négatif sur le contrôle et la facilité de gestion, parce que les fonctionnalités sont localisées et qu'il est plus facile de détecter les problèmes éventuels. Les réseaux téléphoniques publics commutés sont un exemple de réseau hiérarchique à très grande échelle.
- **La facilité de mise en oeuvre :** Puisqu'un modèle hiérarchique attribue des fonctionnalités précises à chaque couche, la mise en oeuvre du réseau s'en trouve facilitée.
- **La facilité de dépannage :** Les fonctions de chaque couche étant clairement définies, il devient plus facile d'isoler les problèmes qui peuvent survenir sur le réseau. Il est également plus facile de segmenter temporairement le réseau pour réduire l'étendue d'un problème.
- **La prévisibilité :** Il est relativement facile de prévoir le comportement d'un réseau utilisant des couches fonctionnelles. La planification de la capacité de croissance du réseau s'en trouve considérablement simplifiée, tout comme la modèlisation des performances du réseau à des fins d'analyse.
- **La prise en charge de protocoles :** La combinaison d'applications et de protocoles actuels et futurs est beaucoup plus facile sur des réseaux créés selon un modèle hiérarchique, en raison de l'organisation logique de l'infrastructure sous-jacente.
- **La facilité de gestion :** tous les avantages énumérés ci-dessus rendent le réseau plus facile à gérer [22].

– **Les différentes couches des réseaux Campus :** Avant l'architecture réseau était composée de la manière suivante : Les principaux services placés au centre du réseau avec des switchs niveau 2 qui assurent le transport entre les utilisateurs et les ressources. Maintenant, l'architecture réseau recommandée est en 3 couches (Figure [10]) :

  - **Core layer (la couche coeur) :** Cette couche est nécessaire pour assurer l'évolutivité des réseaux campus elle va s'occuper de switcher le trafic vers le bon service, de la manière la plus rapide qui soit. La couche coeur du réseau est essentielle à l'inter connectivité entre les périphériques de la couche distribution. Par conséquent, il est important qu'elle bénéficie d'une disponibilité et d'une redondance élevée. La zone principale peut également se connecter à des ressources Internet.

- **Distribution layer (la couche distribution) :** La couche distribution est située entre la couche d'accès et la couche coeur, elle permet de différencier le noyau du reste du réseau. Le but de cette couche est de fournir la sécurité et la définition des limites en utilisant des listes d'accès et autres filtres pour limiter ce qui entre dans le noyau. Par conséquent, cette couche définit la politique du réseau. Une politique est une approche de traitement de certains types de trafics, y compris ce qui suit [23] :
  - La segmentation du réseau en plusieurs domaines de diffusion en utilisant les VLANs.
  - La translation entre les différents types de média comme Ethernet et Token ring.
  - L'agrégation des routes.
  - Le routage entre les VLANs.
  - Mise à jour du routage.

  Les points importants à considérer au niveau de cette couche sont la disponibilité, l'équilibre des charges et la qualité de services.

  Les mécanismes utilisés par cette couche sont :
  - Caractéristiques de STP.
  - Routage de couche 3.
  - HSRP.
- **Access layer (la couche accès) :** La couche accès sert d'interface avec les périphériques finaux, tels que les ordinateurs, les imprimantes et les téléphones sur IP, afin de fournir un accès au reste du réseau. La couche accès peut inclure des routeurs, des commutateurs, des ponts, des concentrateurs et des points d'accès sans fil. Le rôle principal de la couche accès est de fournir un moyen de connecter des périphériques au réseau, ainsi que de contrôler les périphériques qui sont autorisés à communiquer sur le réseau, cette couche permet aussi de définir le domaine de collision, d'authentifier les accès des utilisateurs au réseau, d'offrir des liens redondants vers la couche Distribution Layer et enfin d'offrir des services intelligents comme la découverte automatique des adresses IP.

  Les mécanismes utilisés par la couche d'accès sont :
  - Protocoles de niveau 2.
  - STP (Spanning Tree Protocol).
  - Services réseaux intelligents (qualité de service, classification et contrôle du trafic, contrôle des accès, alimentation en ligne, VLAN voix suppression de diffusion, agrégation de liens (trunking)).
  - VLANs privés.

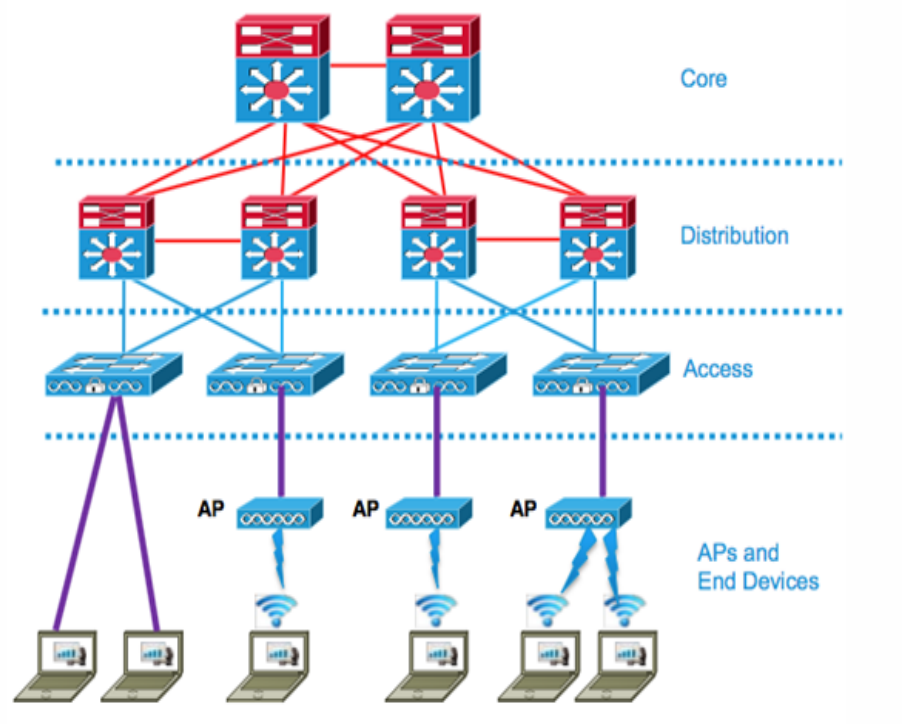

FIGURE 3.1 – Exemple d'une architecture hiérarchique

3.3 La haute disponibilité et l'équilibre des charges

3.3.1 Définition de la haute disponibilité

La haute disponibilité est un terme souvent utilisé en informatique, à propos d'architecture de système ou d'un service pour désigner le fait que cette architecture ou ce service a un taux de disponibilité convenable, cette dernière concerne de plus en plus d'entreprises comme de particuliers. On appelle haute disponibilité (high avaiability) toutes les dispositions visant à garantir la disponibilité d'un service, c'est-à-dire assurer le bon fonctionnement de ce dernier [24].

3.3.2 Définition de l'équilibre des charges

L'équilibre des charges est une fonctionnalité standard du logiciel du routeur de Cisco IOS, et est disponible à travers toutes les plateformes de routeur. Il est inhérent au processus de transfert dans le routeur et est automatiquement activé si la table de routage a plusieurs chemins vers une destination. Il est basé sur des protocoles de routage standards, tels que le Protocole d'informations de routage (RIP), (EIGRP) et (OSPF) ou dérivé de mécanismes de transfert de paquets et de routes configurées statiquement.Tels que ces quelques protocoles que nous allons définir ci-dessous, Il permet à un routeur d'utiliser plusieurs chemins vers une destination lors du transfert de paquets [20].

3.3.3 Protocoles de mise en place de la haute disponibilité et de l'équilibre des charges

Nous citerons deux différents protocoles :

3.3.3.1 Le protocole HSRP (Hot Standby Routing Protocol)

HSRP est un protocole propriétaire Cisco qui a pour fonction d'accroitre la haute disponibilité dans un réseau par une tolérance aux pannes. Cela se fait par la mise en commun du fonctionnement de plusieurs routeurs physiques (au minimum deux) qui, de manière automatique, assurerons la relève entre eux, c'est-à-dire d'un routeur à un autre.

Plus précisément, la technologie HSRP permettra au routeurs situés dans un même groupe que l'on nomme "standby group" de former un routeur virtuel qui sera l'unique passerelle des hôtes du réseau local. En se cachant derrière ce routeur virtuel aux yeux des hôtes, les routeurs garantissent en effet qu'il y est toujours un routeur qui assure le travail de l'ensemble du groupe. Un routeur dans ce groupe est donc désigné comme "actif" et ce sera lui qui fera passer les requêtes d'un réseau à un autre.

Pendant que le routeur actif travaille, il envoie également des messages aux autres routeurs indiquant qu'il est toujours "vivant" et opérationnel. Si le routeur principal (élu actif) vient de tomber, il sera automatiquement remplacé par un routeur qui était alors jusqu'à présent "passif" et lui aussi membre du groupe HSRP. Aux yeux des utilisateurs toutefois, cette réélection et ce changement de passerelle sera totalement invisible car ils auront toujours pour unique passerelle le routeur virtuel que forment les routeurs membres du groupe HSRP. Le routeur virtuel aura donc toujours la même IP et adresse MAC aux yeux des hôtes du réseau même si en réalité il y a un changement du chemin par lequel transitent les paquets [25].

3.3.3.2 Le protocole VRRP (Virtual Router Redundancy Protocol)

VRRP est un protocole semblable au protocole HSRP plus normalisé, il est implémenté sur les routeurs d'autres marques que Cisco. Ce protocole est un protocole d'élection qui attribue de façon dynamique les responsabilités d'un routeur virtuel à l'un des routeurs VRRP présents dans le LAN. VRRP fournit un ou plusieurs routeurs secondaires pour un routeur configuré statiquement sur le LAN.

Le routeur maître est associé à l'adresse IP virtuelle du groupe. C'est lui qui va répondre aux requêtes des clients sur cette adresse IP. Un ou plusieurs routeurs de secours pourront reprendre le rôle du maitre en cas de défaillance de celui-ci.

Après avoir défini les réseaux campus et la haute disponibilité dans ces réseaux, nous allons à présent parler des trafics entre les VLANs dans les réseaux campus [26].

3.4 Trafic entre-VLAN

Le trafic entre VLAN est assuré par un équipement de niveau 3. En effet pour que les machines puissent communiquer d'un VLAN à un autre, il est nécessaire de passer par un routeur ou bien un switch multifonction en subdivisant logiquement l'interface liée au commutateur en sous interfaces virtuelles, tel que, chaque sous interface à créer est liée au nombre de VLANs existants, elles fournissent une solution pour le routage entre les différents VLANs.

Le concept d'agrégation ou bien le trunk qui utilise la norme IEEE.802.1Q pour l'identification des trames est indispensable, il consiste à regrouper plusieurs liaisons virtuelles en une liaison physique unique, la fonction d'un trunk est de transporter les informations des VLANs entre plusieurs commutateurs interconnectés et donc d'étendre la portée des VLANs à un ensemble de commutateurs.

Les interfaces entre les commutateurs distribution et les commutateurs d'accès, doivent être toutes configurées en mode Trunk, afin qu'elles puissent transporter les informations des différents VLANs (Figure 3.2)[27] :

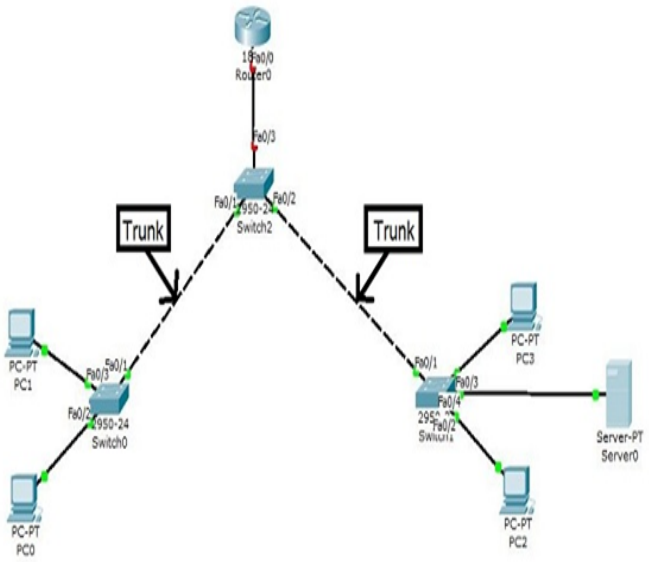

FIGURE 3.2 – Les liens Trunk

3.5 Conclusion

Dans ce chapitre nous avons défini le trafic entre VLANs ainsi que les réseaux campus ,la haute disponibilité et l'équilibre des charges de ces réseaux. Pour le chapitre suivant, il consistera à une démonstration de l'implémentation de notre projet.

CHAPITRE 4

RÉALISATION

4.1 Introduction

Ce présent chapitre consistera à mettre en oeuvre les solution proposées pour la réalisation de notre projet, en exposant les différentes configurations nécessaires à implémenter sur le LAN. Ces configurations entourent entre la configuration des VLANs, VTP, STP et HSRP en se basant sur le simulateur Cisco packet tracer. Pour présenter les configurations que nous avons réalisées, nous nous sommes servies des captures d'écran qui illustrent les étapes de la configuration afin d'éclaircir chaque composant de cette dernière et son fonctionnement. Enfin, des tests de validation pour confirmer le bon fonctionnement du réseau seront réalisés.

4.2 Présentation du simulateur Cisco "Packet Tracer"

Packet Tracer est un logiciel développé par CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc...[28].

4.3 Segmentation des VLANs

L'organisation réseau se fera en le segmentant à l'aide des VLANs. Chaque section du réseau représente un VLAN. Par conséquent, il y'aura naissance de 8 VLANs à savoir :

- Direction.
- Informatique.
- HSE.
- Sureté interne.
- Sous direction exploitation.
- Sous direction technique.
- Sous direction administrative.
- Sous direction finance et juridique.

4.4 Plan d'adressage

L'adresse du réseau est 192.168.0.0/24 avec une possibilité de création de 255 sous-réseaux, avec un masque 255.255.255.0

L'adressage du réseau local et de toutes les stations, se basera sur une adresse privée et c'est à partir de cette dernière que l'affectation des adresses IP pour l'ensemble des équipements et des VLANs va être accomplie. Les machines affiliées à un VLAN, vont prendre toute les adresses IP d'une même adresses sous-réseau.

Le tableau suivant montre le plan d'adressage des VLANs.

Nom VLAN	VLAN-id	Adresse sous-réseau
Dirction	10	192.168.10.0/24
Informatique	20	192.168.20.0/24
HSE	30	192.168.30.0/24
Sureté Interne	40	192.168.40.0/24
S.Dirction Exploitation	50	192.168.50.0/24
S.Dirction Technique	60	192.168.60.0/24
S.Dirction Administrative	70	192.168.70.0/24
S.Dirction Finance et Juridique	80	192.168.80.0/24

TABLE 4.1 – Plan d'adressage des VLANs

4.5 Présentation de l'architecture réseau avant la configuration

La figure 4.1 illustre l'architecture réseau que nous allons réaliser sous le simulateur packet tracer :

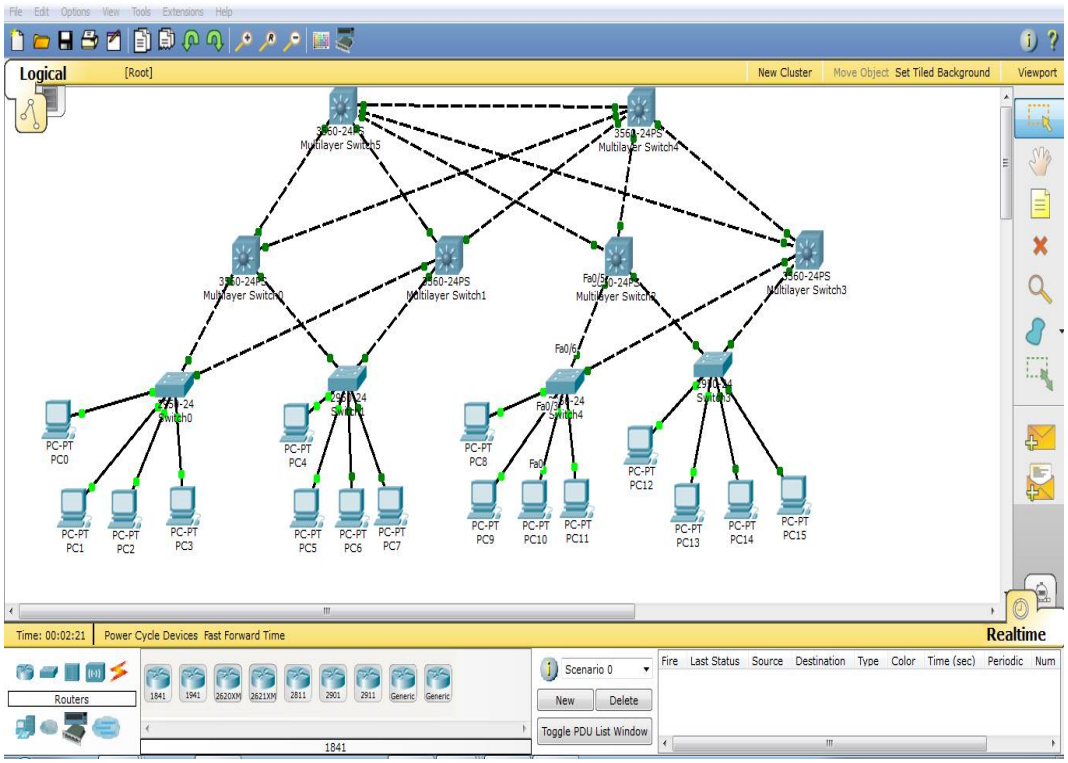

FIGURE 4.1 – Présentation de l'architecture

4.6 Interface commande de Packet Tracer

Toutes les configurations des équipements du réseau seront réalisées au niveau de CLI (Command Line Interface) (Figure 4.2). CLI est une interface de simulateur Packet Tracer qui permet la configu-

ration des équipements du réseau à l'aide d'un langage de commandes, c'est-à-dire que c'est à partir des commandes introduites par l'utilisateur du logiciel que la configuration est réalisée.

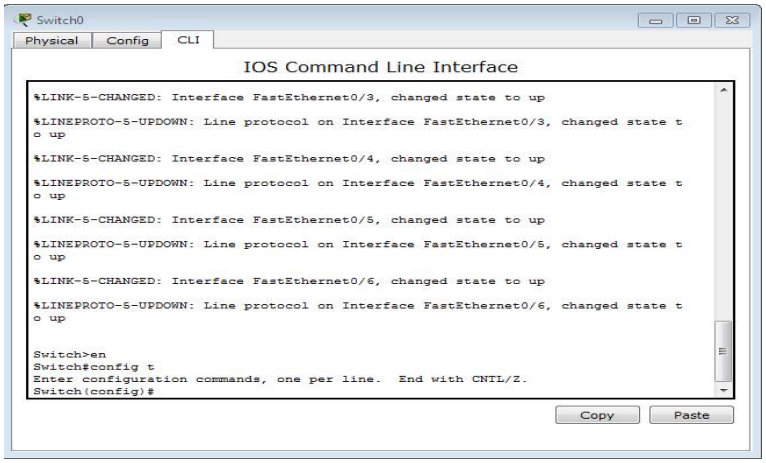

FIGURE 4.2 – Interface CLI

4.7 Configuration des équipements

La configuration des équipements du réseau sera au niveau des commutateurs de niveau 2 et niveau 3 constituant le réseau local des stations En effet, une série de configurations a été réalisée à travers ces équipements, en montrant un exemple de chaque configuration.

4.7.1 Sécuriser l'accès aux périphériques

Il faut savoir qu'IOS (International Standardization Organization) utilise des modes organisés hiérarchiquement pour faciliter la protection des périphériques. Dans le cadre de ce dispositif de sécurité, IOS peut accepter plusieurs mots de passe, ce qui nous permet d'établir différents privilèges d'accès aux périphériques (Figure 4.3).

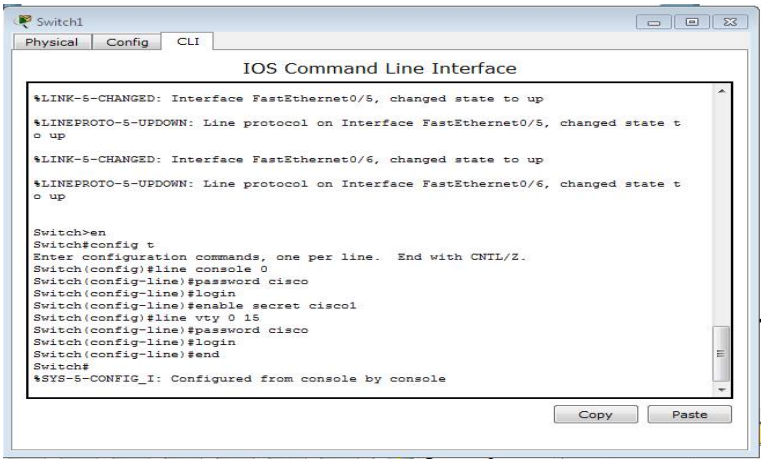

FIGURE 4.3 – Configuration de mot de passe

4.7.2 Configuration du protocole VTP

L'ensemble des commutateurs coeur de LAN seront configurés comme des serveurs -VTP. Donc, ce sont eux qui gèrent l'administration de l'ensemble des VLANs. Un nom de domaine est attribué. La figure 4.4 représente la configuration du serveur VTP au niveau du switch multifonctions.

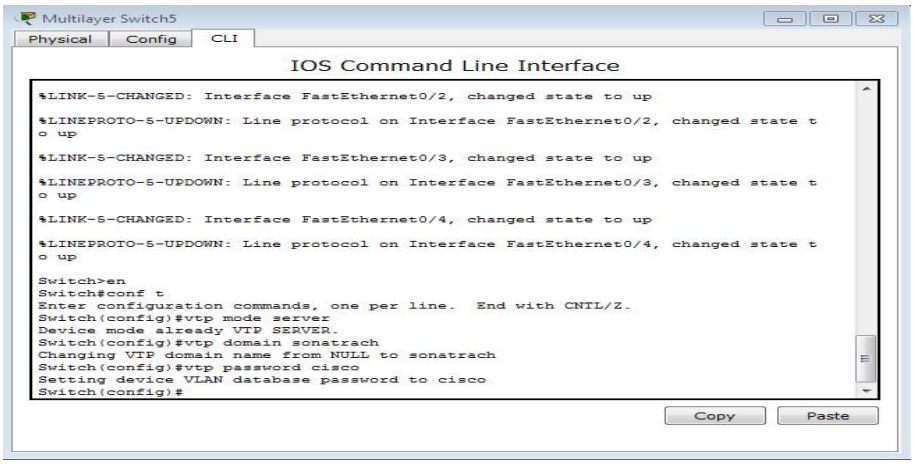

FIGURE 4.4 – Configuration du VTP-Server

La configuration des clients-VTP sera au niveau de tous les commutateurs Accès (Figure 4.5).

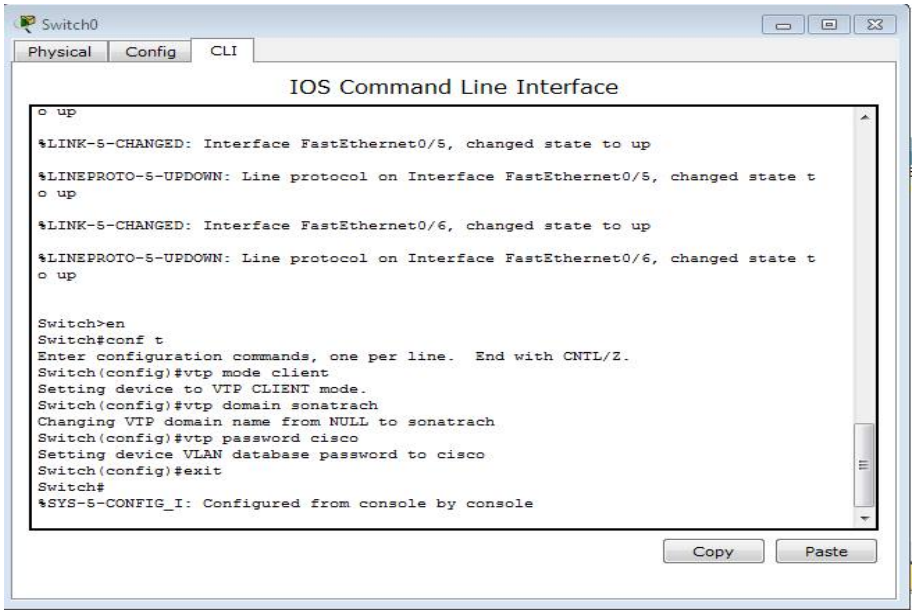

FIGURE 4.5 – Configuration du VTP-Client

4.7.3 Création des VLANs

La création des VLANs est faite au niveau des commutateurs multifonctions (server VTP) comme le montre la figure 4.6 :

FIGURE 4.6 – Création des VLANs sur le serveur VTP

4.7.4 Configuration des liens trunk

Les interfaces des équipements d'interconnexion à configurer en mode trunk, existent toutes entre l'ensemble des commutateurs Accès et le commutateur coeur. Les commandes suivantes nous permettent d'associer un port à un VLAN en mode trunk en s'aidant de la commande "range" qui pourra réunir toutes les interfaces en une seule fois (Figure 4.7) :

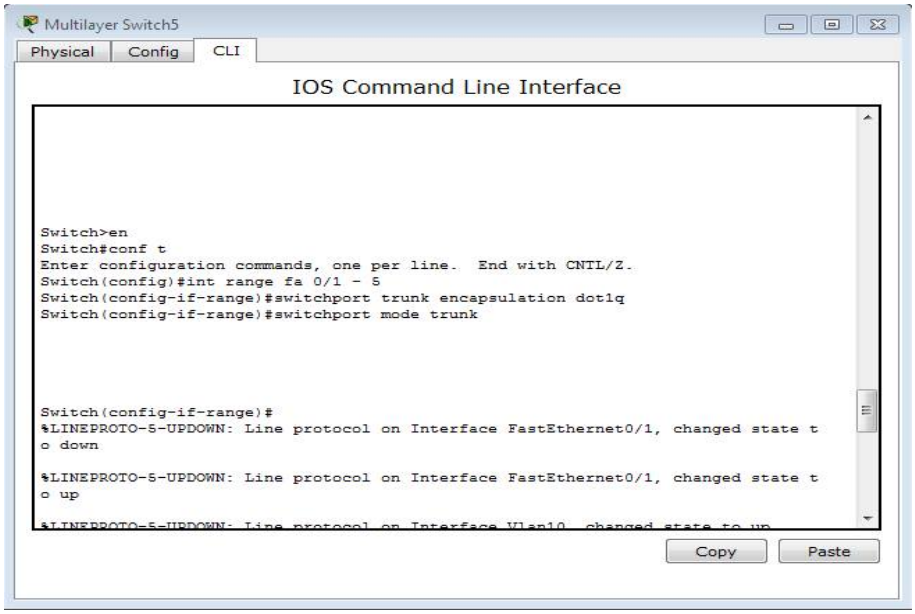

FIGURE 4.7 – Configuration des liens trunk

4.7.5 Attribution des ports de commutateurs au VLANs

C'est au niveau de chaque commutateur Accès que les ports vont être assignés aux différents VLANs existants. En effet, chaque port d'un commutateur appartiendra à un VLAN donné. Les commandes suivantes nous permettent d'associer un port à un VLAN en mode Accès (Figure 4.8) :

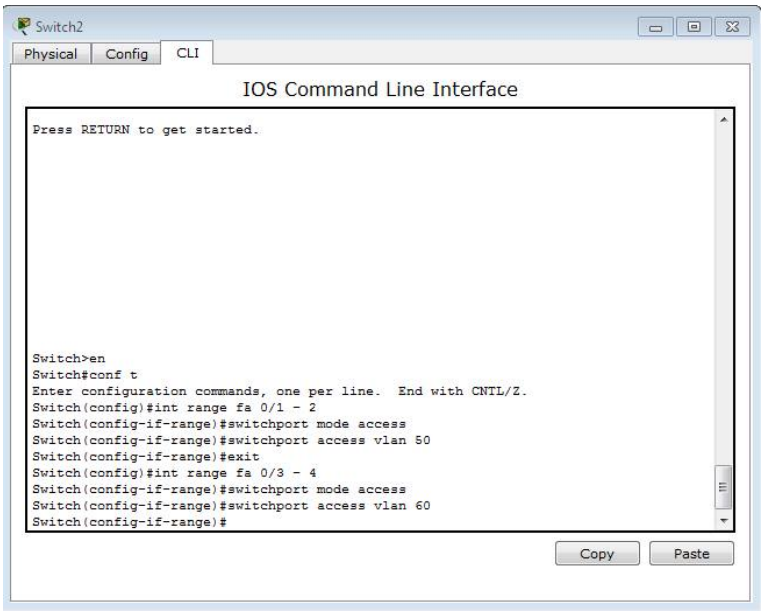

FIGURE 4.8 – Attribution des ports au VLANs

Apres avoir configuré les interfaces VLANs Il faut ensuite activer la fonction de routage (Figure 4.9) :

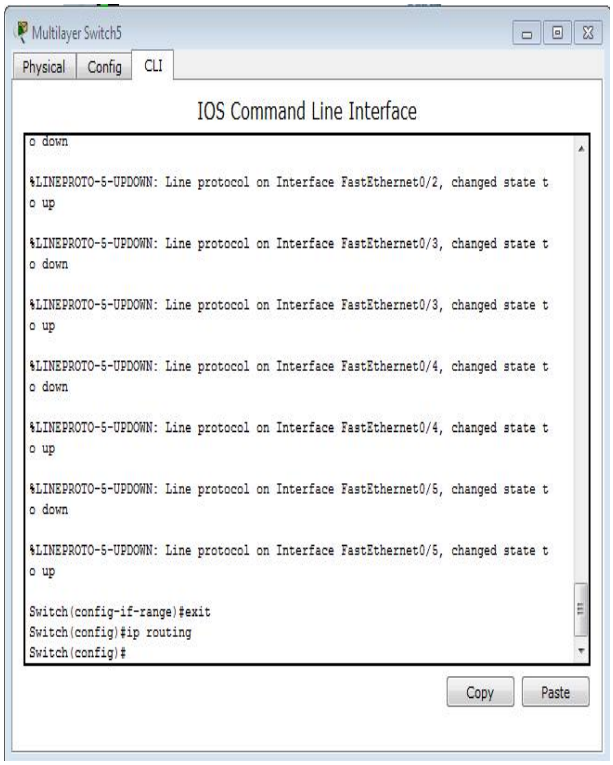

FIGURE 4.9 – Routage inter VLAN

4.7.6 Configuration du DHCP

Afin de simplifier à l'administrateur la gestion et l'attribution des adresses IP, on utilise le protocole DHCP qui permet de configurer les paramètres réseaux clients, au lieu de les configurer sur chaque ordinateur client. La figure 4.10 illustre les commandes qui nous permettent de configurer ce protocole au niveau du serveur (Figure 4.10) :

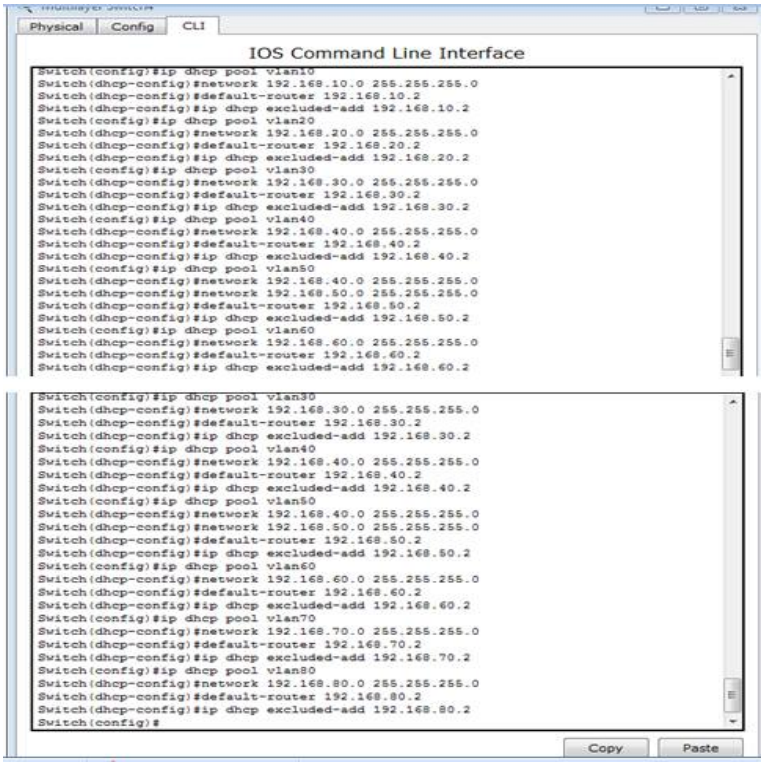

FIGURE 4.10 – Configuration du DHCP

Apres la configuration DHCP du serveur, à présent nous allons configurer les PC (Figure 4.11) :

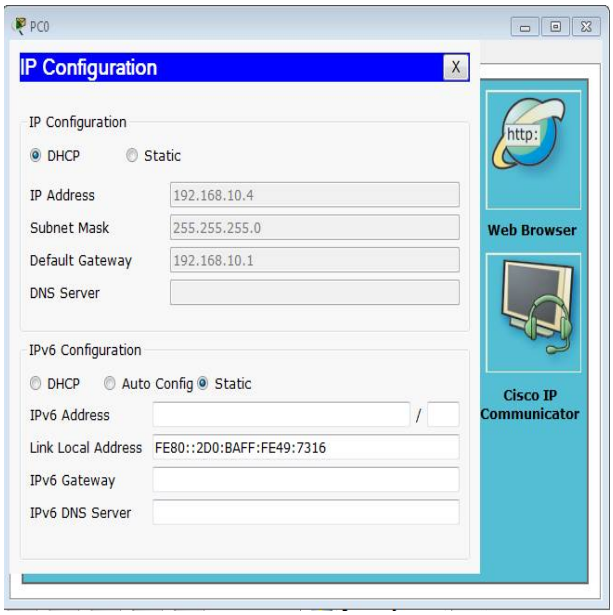

FIGURE 4.11 – Configuration du DHCP sur les PC

4.7.7 Configuration du STP

La figure 4.12 illustre les commandes qui nous permettent de configurer le protocole STP, et ainsi affecter un root primaire ou secondaire à un VLAN.

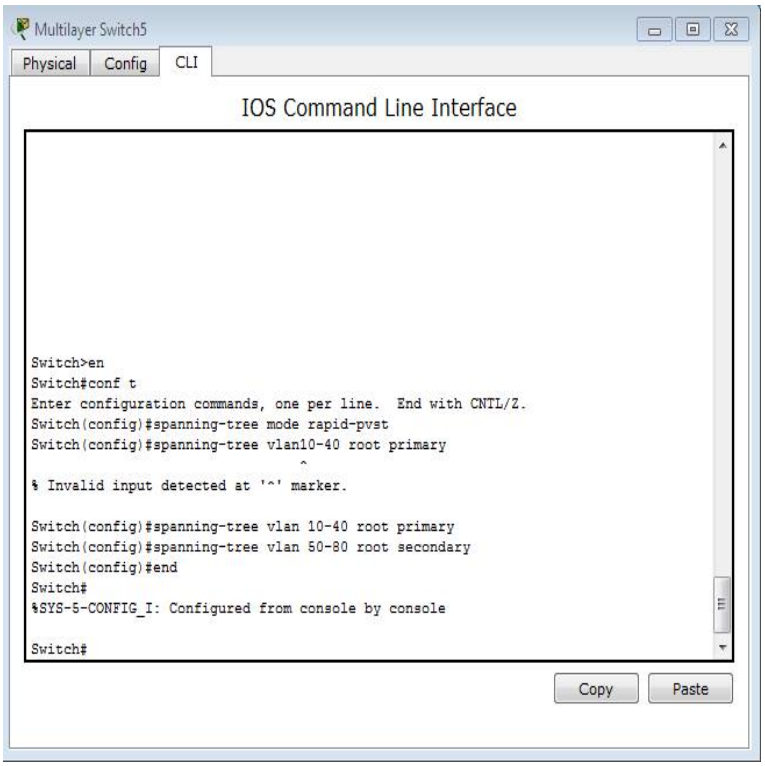

FIGURE 4.12 – Configuration du STP

4.7.8 Configuration de la haute disponibilité

La configuration de la haute disponibilité s'effectue au niveau des switchs multifonctions. Nous utilisons deux sortes de configuration HSRP : La première lorsqu'un VLAN est prioritaire, la deuxième lorsqu'il est secondaire. La figure 4.13 montre les VLANs prioritaires par rapport aux VLANs secondaires sur l'un des switchs multifonctions, et sur l'autre les priorités des VLANs seront renversées.

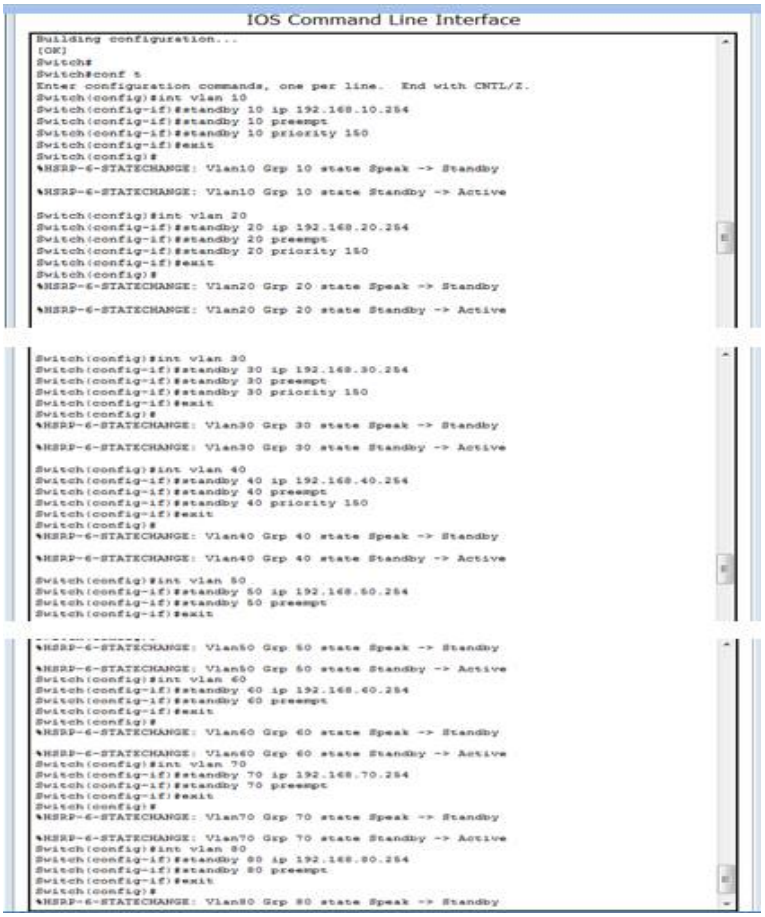

FIGURE 4.13 – Configuration du HSRP

4.8 Vérification et tests de validation

4.8.1 Vérification

Dans cette partie nous avons vérifié la configuration de tous les équipements à l'aide des commandes de vérification.

4.8.1.1 Contrôle de la bonne configuration du protocole VTP

- Contrôle du VTP server en utilisant la commande "show vtp statu" sur le switch Multilayer (Figure 4.14) :

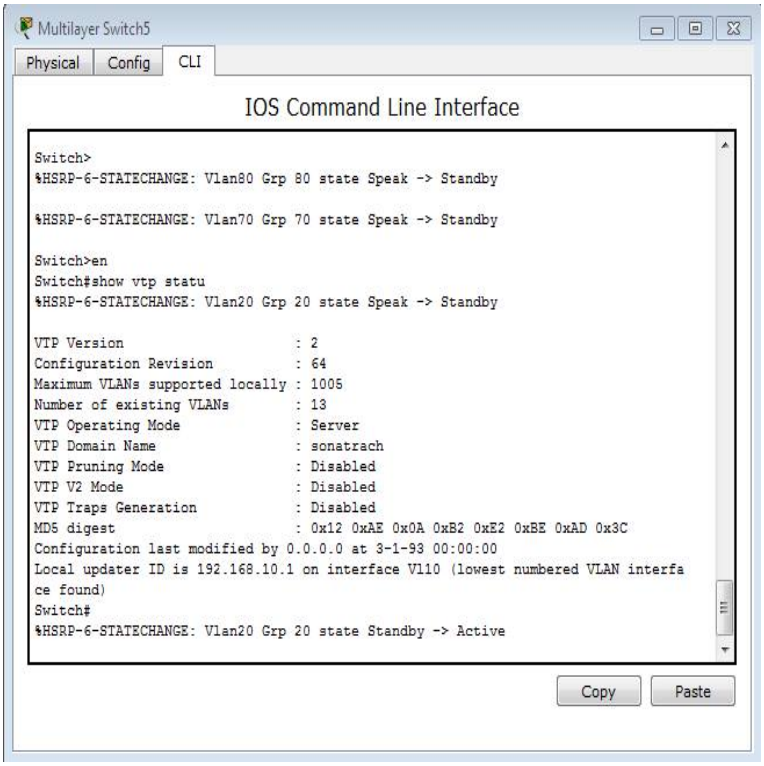

FIGURE 4.14 – Test VTP server

- Contrôle du VTP client en utilisant la commande "show vtp statu" sur le switch0 (Figure 4.15) :

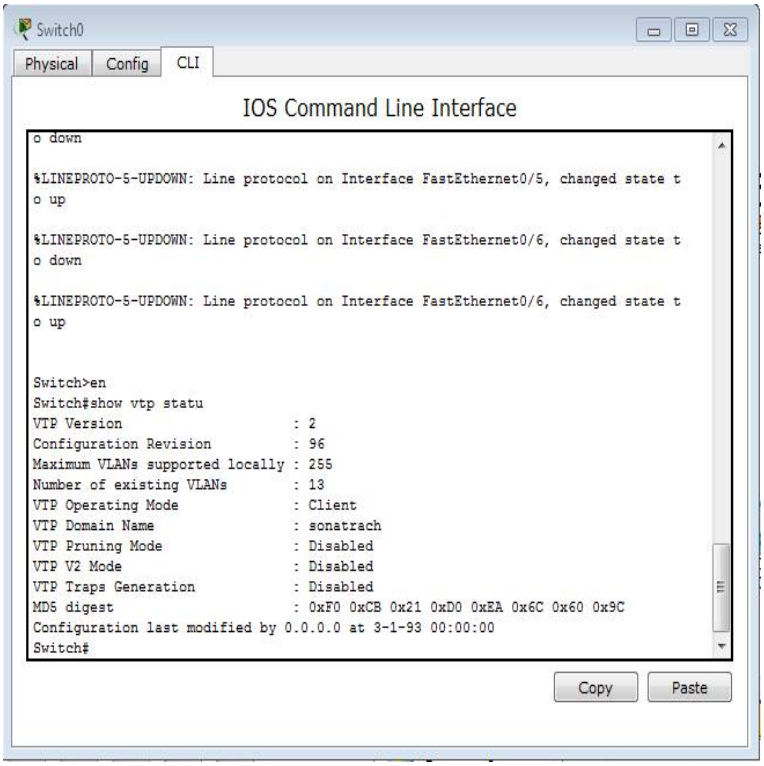

FIGURE 4.15 – Test VTP client

4.8.1.2 Contrôle des réseaux locaux virtuels créés sur le switch server s'ils ont bien été distribués sur les switchs clients

Apres avoir créé les VTP nous allons passer à la vérification de la distribution des VLANs dans les switchs clients, nous nous sommes servies de la commande "show vlan brief" (Figure 4.16) :

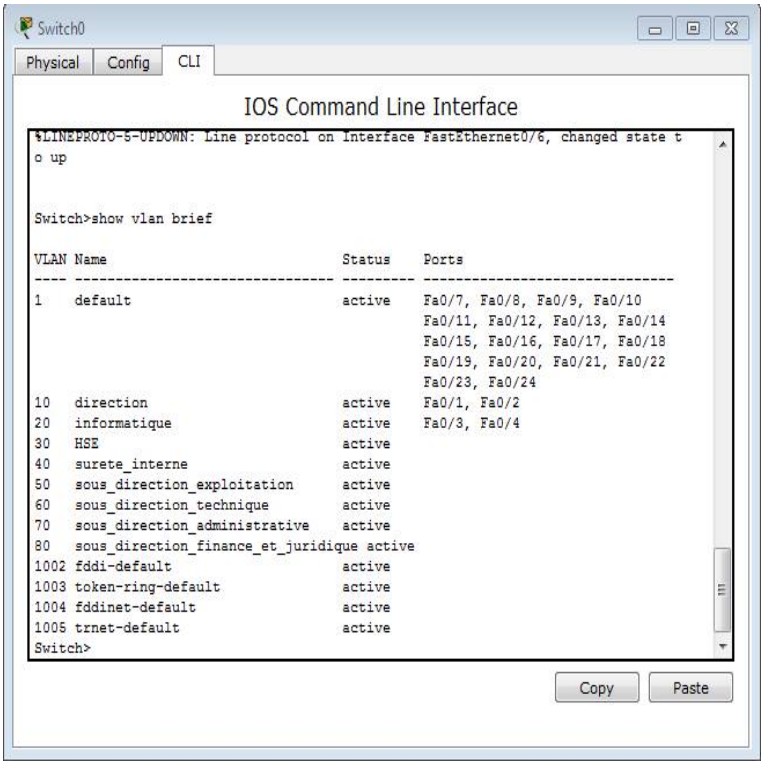

FIGURE 4.16 – VLANs distribués sur le switch0 Client

4.8.1.3 Vérification routage inter VLAN

A l'aide de la commande "show IP interface brief", on peut voir l'attribution des adresses IP sur les VLANs (Figure 4.17) :

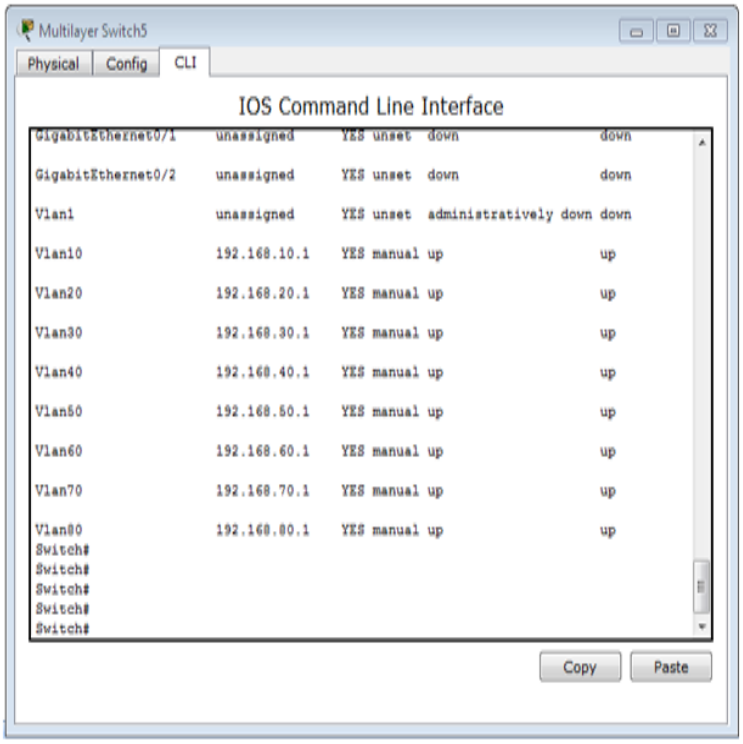

FIGURE 4.17 – Attribution des adresses IP sur les VLANs

4.8.1.4 Vérification de la distribution des adresses IP sur le serveur DHCP

Il est possible de vérifier que chaque poste a bien récupéré une adresse DHCP à l'aide de la commande "show ip dhcp binding" (Figure 4.18) :

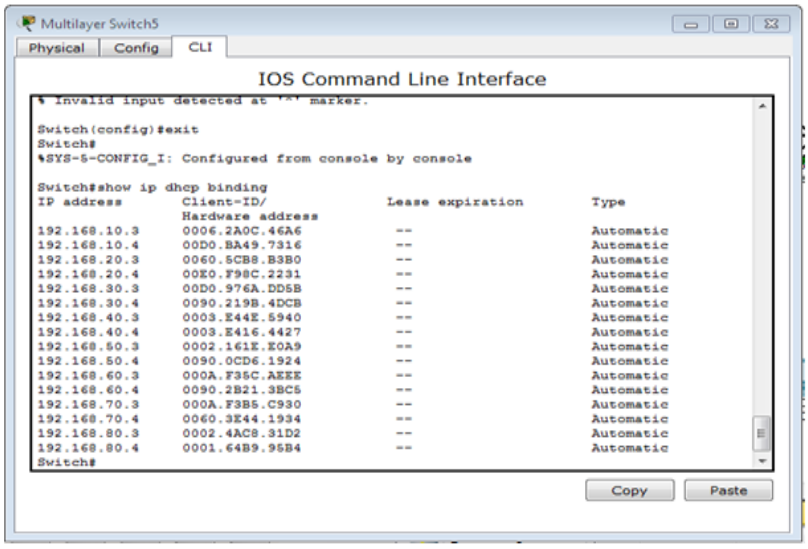

FIGURE 4.18 – Attribution des adresses IP sur le serveur DHCP

4.8.1.5 Vérification des adresses IP des PC attribuées par le DHCP

La figure 4.19 montre l'attribution des adresses IP par le DHCP.

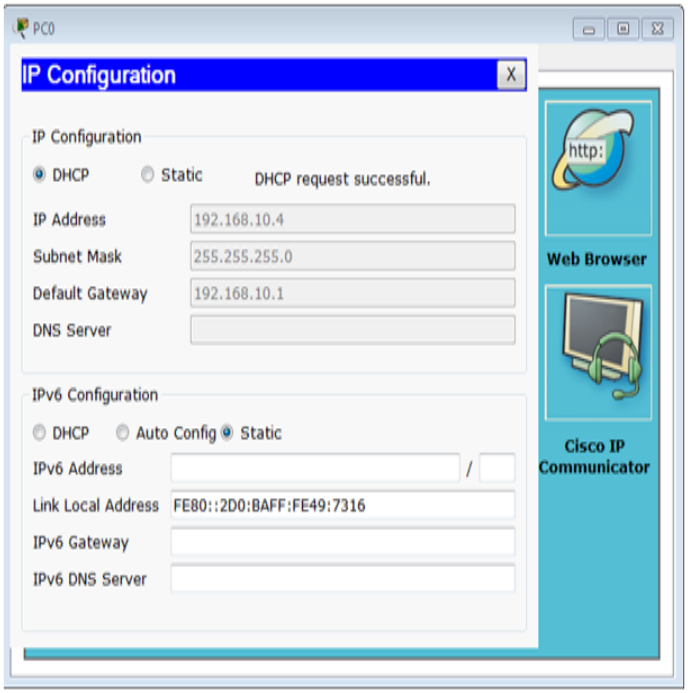

FIGURE 4.19 – Attribution des adresses IP par le serveur DHCP

4.8.1.6 Vérification du HSRP

Nous utilisons la commande "show standby brief" en mode privilégié pour vérifier l'état de HSRP, cette commande nous indique quel switch est actif et qui est en attente, sachant que nous avons utilisé l'équilibre des charges.

Sur le switch multilayer5, nous avons vlan 10, vlan 20, vlan 30 et vlan 40 actifs et le reste sont en standby (Figure 4.20) :

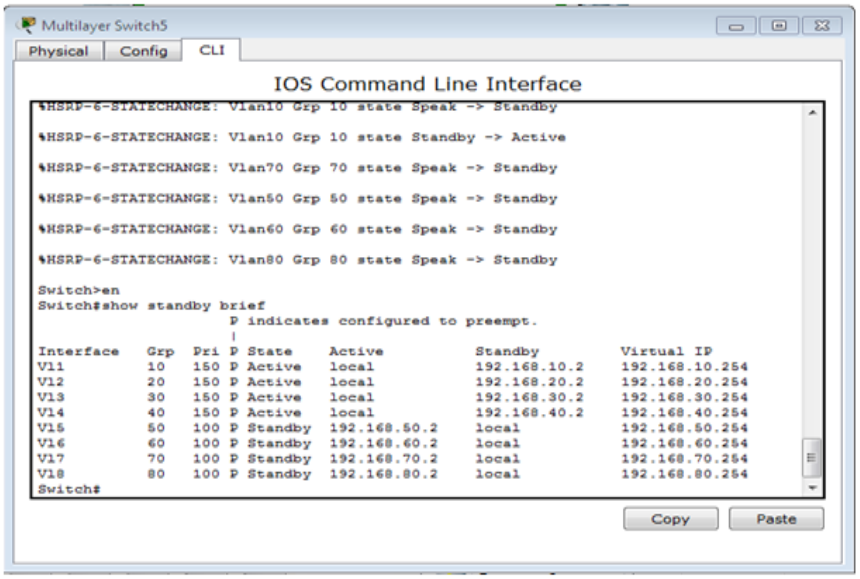

FIGURE 4.20 – configuration HSRP pour le switch multilayer5

Sur le switch multilayer4, nous avons vlan 50, vlan 60, vlan 70 et vlan 80 actifs et le reste sont en standby (Figure 4.21) :

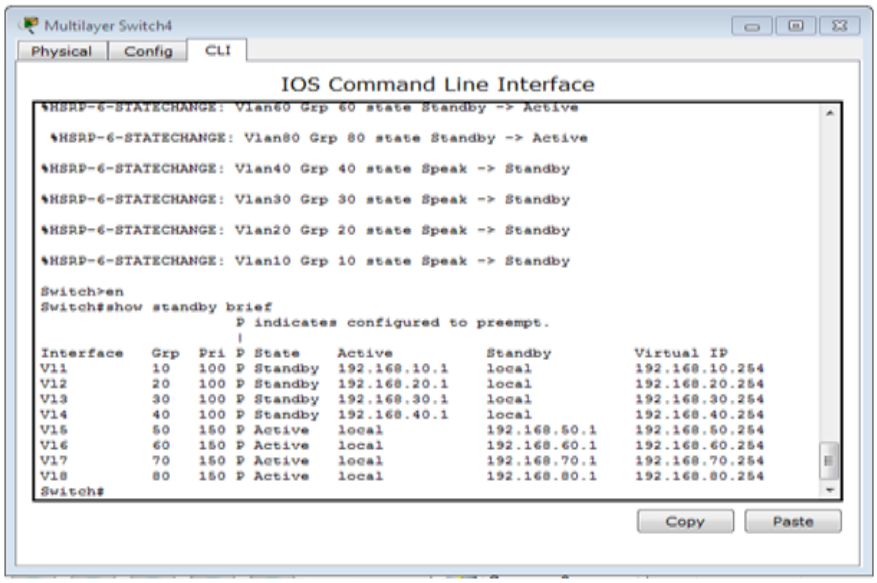

FIGURE 4.21 – configuration HSRP pour le switch multilayer4

4.8.2 Test de validation

Dans cette partie, l'ensemble des tests de validation consiste à vérifier l'accessibilité de l'ensemble des équipements en utilisant la commande "Ping" qui teste la réponse d'un équipement sur le réseau. Donc, si un équipement veut communiquer avec un autre, le Ping permet d'envoyer des paquets au destinataire. Si l'équipement récepteur reçoit ces paquets donc la communication est réussie.

4.8.2.1 Vérification de la communication entre les équipements d'interconnexion

On teste les communications inter-switchs et entre switch et switch multifonctions.
Exemple : Test réussi entre le switch multilayer et le switch d'accès (Figure 4.22) :

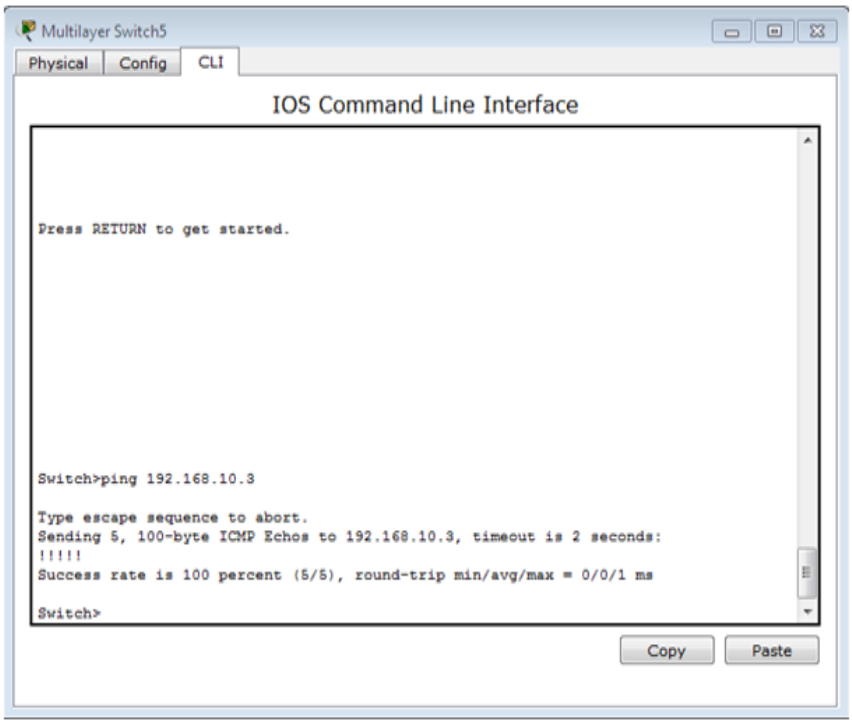

FIGURE 4.22 – test entre le switch multilayer et le switch d'accès

4.8.2.2 Vérification de la communication entre les PC

- **Test entre pc VLANs différents sur un même commutateur :** A ce stade, vérifiant l'accessibilité des différents équipements dans un même réseau mais dans deux VLANs distincts à partir du PC7. (192.168.40.3) en asseyant d'accéder au PC6 (192.168.30.4). La figure 4.23 illustre le succès du test effectué entre les différents VLANs sur un même commutateur.

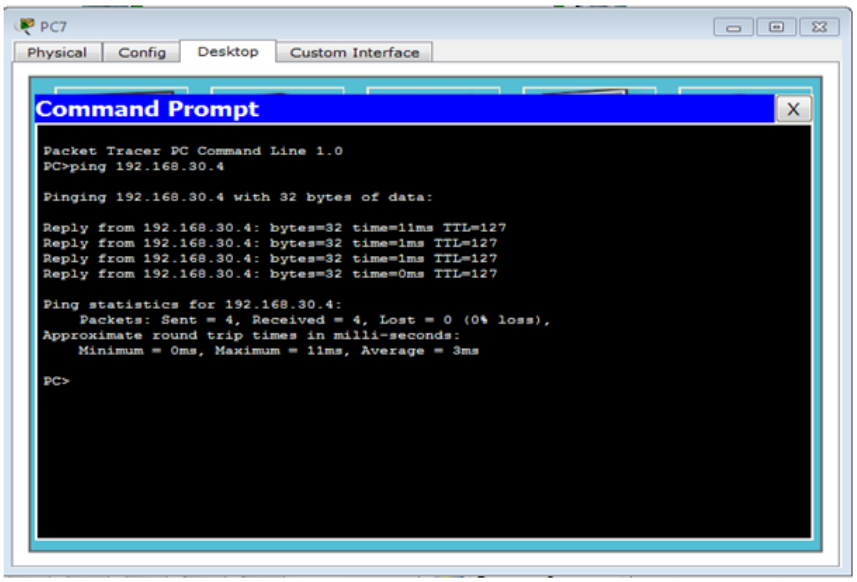

FIGURE 4.23 – Test entre PC VLANs différents

- **Test entre PC de VLAN et commutateur distincts :** Vérifions l'accessibilité des équipements du même VLAN situés dans un réseau local commun. Depuis le PC9(192.168.50.3), essayons d'accéder au PC12 (192.168.70.3) tel que, les deux se trouvent dans des VLANs et des commutateurs Accès différents (Figure 4.24) :

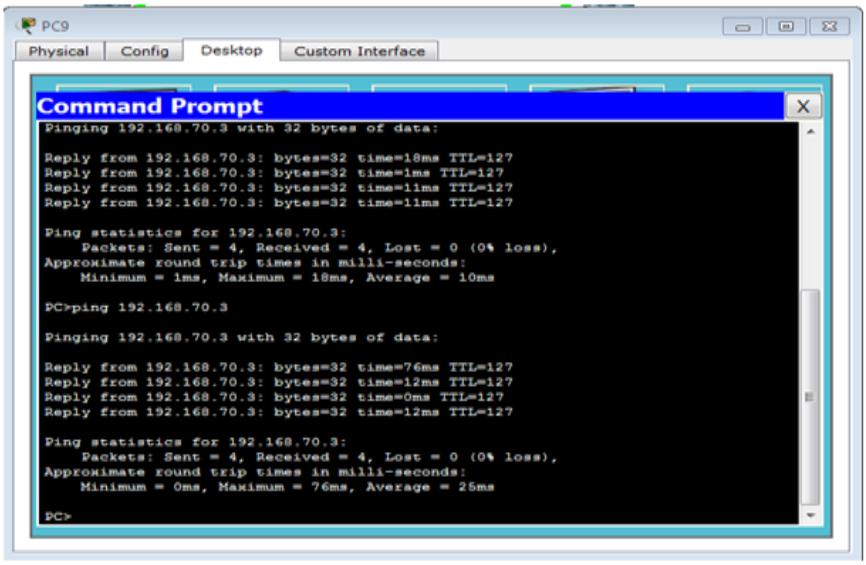

FIGURE 4.24 – Test entre PC de VLAN et commutateur distincts

4.8.2.3 Vérification de la haute disponibilité

Dans ce cas de figure nous testons la connectivité lorsque l'un des switchs coeur est défectueux, nous allons éteindre les interfaces du switch multilayer5 à l'aide de la commande "shutdown" (Figure 4.25) :

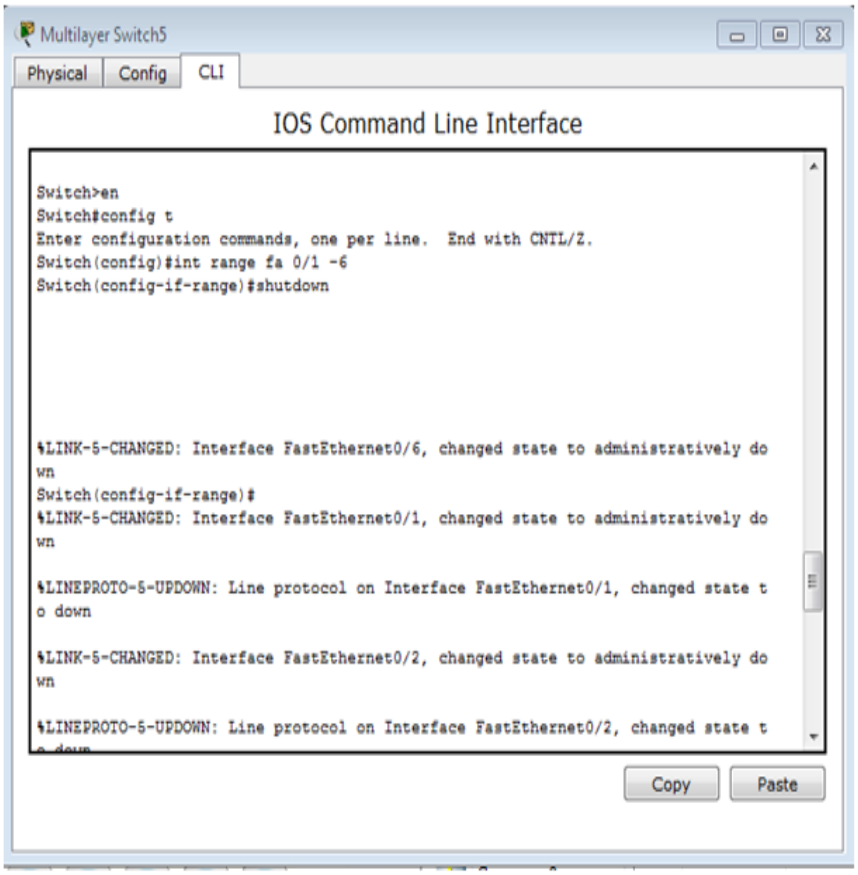

FIGURE 4.25 – Eteindre les interfaces de l'un des switchs coeur

Après avoir éteint le switch multilayer5 on teste à nouveau la connectivité :

- **Test entre pc différents VLANs sur un même commutateur quand le switch prioritaire est en panne :** A ce stade, vérifions l'accessibilité des différents équipements dans un même réseau mais dans deux VLANs distincts à partir du PC15 (192.168.80.4) en asseyant d'accéder au PC12(192.168.70.3), tout en sachant que le switch multilayer5 et en panne. La figure 4.26 illustre le succès du test effectué entre les différents VLANs sur un même commutateur.

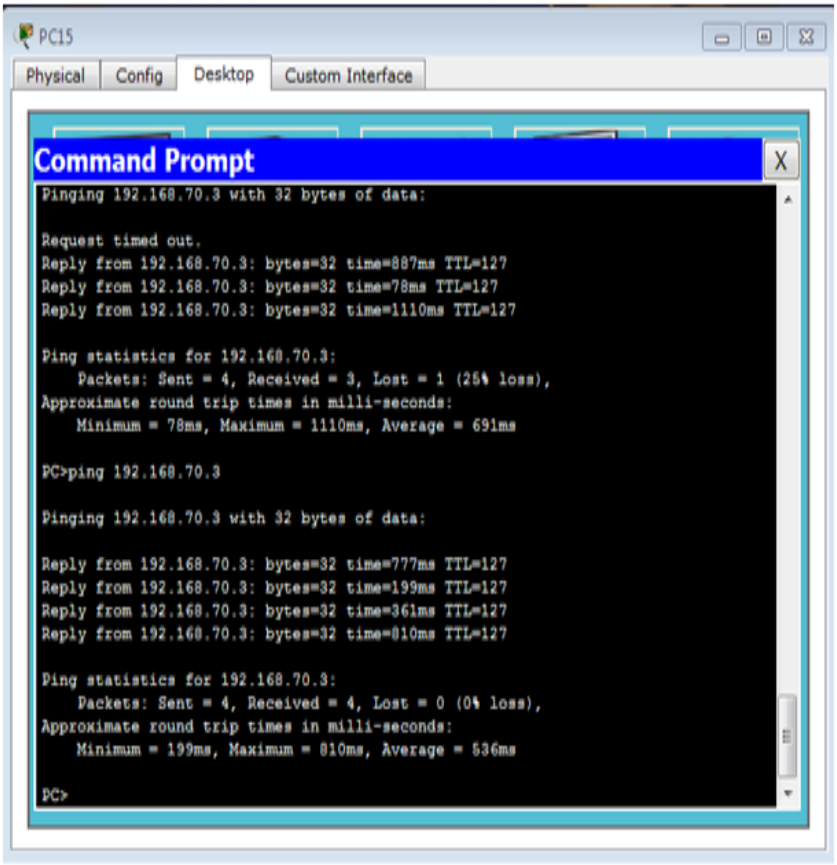

FIGURE 4.26 – Test entre les machine des différents Vlans et d'un même commutateur lorsque l'un des switchs coeur est défectueux.

- **Test entre pc différents VLANs et sur deux commutateur différents quand le switch prioritaire est en panne :** Dans ce cas de figure on teste la connectivité entre les PC et les commutateurs distincts lorsque le switch coeur est défectueux. A partir du PC2(192.168.20.3) appartenant au vlan 20 essayons d'accéder au PC4(192.168.30.4) qui appartient au vlan 30 (Figure 4.27) :

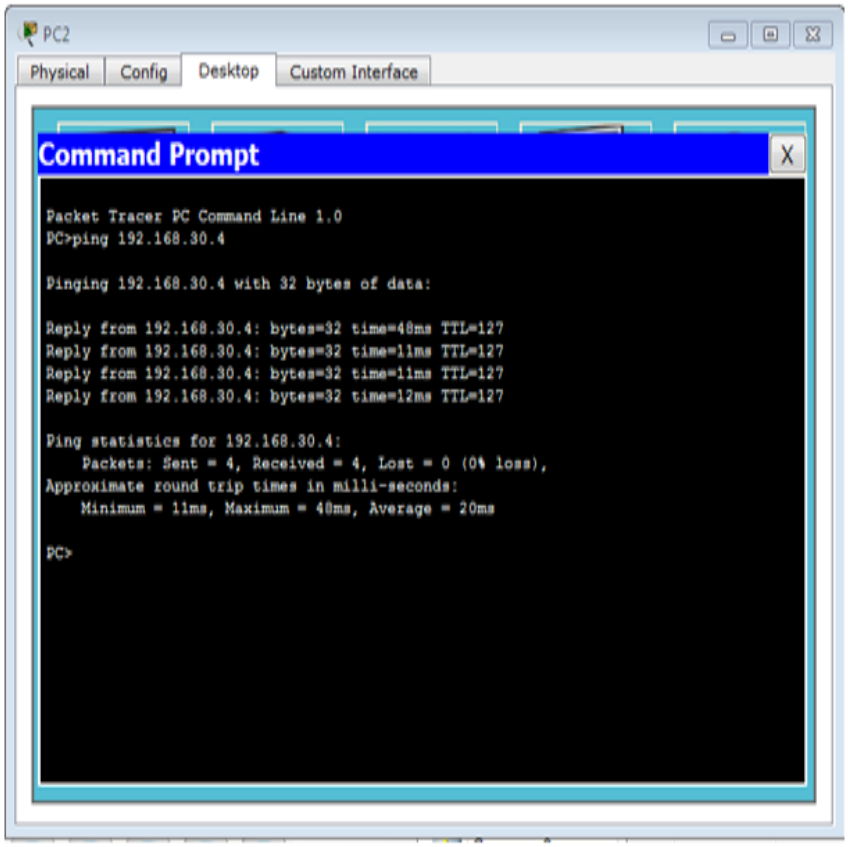

FIGURE 4.27 – Test entre pc différents VLANs et sur deux commutateur différents lorsque l'un des switchs coeur est défectueux.

4.9 Conclusion

Après avoir présenté une brève description de l'environnement de développement de réseau local, nous avons mis l'accent sur la présentation de quelques interfaces, qui porte sur l'ensemble des configurations, la mise en place du réseau LAN que nous avons réalisé, puis nous avons effectué un ensemble de tests de validation afin de prouver l'efficacité du réseau.

CONCLUSION GÉNÉRALE

L'objectif de notre travail était de mettre en oeuvre une solution réseau augmentant le taux de disponibilité en assurant un réseau fiable en terme de matériel tout en permettant une gestion facile aux administrateurs. Ce projet nous a permis de mettre en pratique les connaissances acquises durant la période de notre stage pratique au sein de la SONATRACH de Bejaia (RTC).

Pour mettre en oeuvre ce projet, nous avons acquis les connaissances nécessaires à la création d'un réseau d'entreprise efficace et extensible. Nous avons approfondi les fonctionnalités des commutateurs de niveau 2 et multi-niveaux tels que les VLANs, les trunks, le routage inter-VLAN, l'agrégation des ports, le Spanning Tree ainsi que la haute disponibilité.

Afin d'accomplir notre travail et d'aboutir au résultat escompté, nous avons choisi le simulateur Packet Tracer pour les différents avantages qu'il présente, en premier lieu la mise en évidence avec une grande exactitude de l'architecture du système à réaliser en précisant les différents composants, ainsi que la simplicité et la clarté des matériels dont on aura besoin, ce qui facilite considérablement la configuration sur Packet Tracer.

Ce projet nous a permis de faire une forte expérience fructueuse quia améliorée nos connaissances et nos compétences dans le domaine des réseaux d'entreprise "gestions et administrations" pour nous à l'avenir.

Tout travail n'est pas parfait, nous suggérons les perspectives suivantes :

- Proposer une vision pour la distribution des VLANs en mode local.
- Utiliser le protocole GLBP, qui non seulement permet de gérer la gestion de passerelles redondantes, mais en plus il permet d'équilibrer le trafic entre elles, là ou HSRP et VRRP se contentent d'en utiliser une et de laisser les autres en standby.

BIBLIOGRAPHIE

[1] : Réseaux informatiques, modèle OSI, protocole TCP/IP 58pages 20/05/2010.

[2] : Etude sur le déploiement d'un réseau informatique administré par Windows 2008 serveur avec une optimisation du QOS dans une entreprise publique par Yannick MUKOLE MPALUNGUNU institut supérieur d'informatique programmation et d'analyse 2010.

[3] : Https ://www.ladissertation.com/Sciences-et-Technologies/Informatique-Internet/Reseaux-Informatiques-81608.html, consulté le 20 Avril 2016.

[4] : Le réseau informatique dans la chaine de production d'une société de presse par germain AFFRO Essan 2010.

[5] : MODÈLES OSI ET TCP/IP VALET G. novembre 2010.

[6] : Http ://www.mongosukulu.com/index.php/en/contenu/informatique-et-reseaux/reseaux-informatiques/63-les-equipements-reseaux-informatiques, consulté le 19 Mai 2016.

[7] : PUJOLLE E. "Réseau TCP/IP" ENI éditions, 2009.

[8] : CHAMILLARD G. , ROHAUT S., "création, configuration et gestion d'un réseau local d'entreprise" , ENI édition, 2013.

[9] : VAUCAMPS A. , "cisco CCNA", ENI édition, 2010.

[10] : Le grand livre de sécuritéinfo, http :// www.sécuritéinfo.com, consulté le 23 Mars 2016.

[11] : SURZUR A. , DEFRANCE G. "la technologie des VLANs" 2000.

[12] : MONTAGIER J-L., "réseau d'entreprise par la pratique", EYROLLES éditions, 2007.

[13] : ATELIN philippe, Réseaux informatiques : notions fondamentales, 3eme Edition, ENI Editions, 2006.

[14] : PUJOLLE Guy, les Réseaux : les réseaux IP , 6eme Edition, Eyrolles, 2008.

[15] : http ://www.cisco.com/c/en/us/products/switches/catalyst-6509-neb-a-switch/index.html, consulté le 10 Avril 2016.

[16] : http ://www.cisco.com/web/offer/emear/dg20/CPQRG-110813-PDF.pdf, consulté le 30 Mars 2016.

[17] : http ://www.cisco.com/c/en/us/products/switches/catalyst-2950-series-switches/index.html, consulté le 02 Juin 2016.

[18] : http ://www.f-secure.com/fr-BE/web/home-be/anti-virus, consulté le 02 Juin 2016.

[19] : http ://www.websence.com/content/Regional/France/WebFilter.aspx, consulté le 10 Juin 2016.

[20] : http ://www.iss.net/support/, consulté le 11 Juin 2016.

[21] : BACHAR S. , HAGGAR bachar-salim.haggar@univ-reims.fr M2 Pro STIC-Info - INFO0912 Conception de réseaux de campus Lundi 12 octombre 2009.

[22] : Http ://www.coursnet.com/2015/01/les-avantages-de-reseau-hierarchique.html, consulté le 15 Juin 2016.

[23] : Déploiement de réseaux de campus session1.8 cisco systems in USA, consulté le 15 Juin 2016.

[24] : Http ://www.uptimeinstitute.com/professional-services/professional-services-tier-certification, consulté le 13 Juin 2016.

[25] : Http ://www.it-connect.fr/mise-en-place-du-protocole-hsrp, consulté le 04 Juin 2016./

[26] : Http ://docs.oracle.com/cd/E26919-01/html/E25864/gkfkc.html, consulté le 06 Juin 2016.

[27] : BELKHIRI B., "proposition et mise en oeuvre d'une solution de segmentation et de routage du réseau LAN étendu de la RTC Bejaia (région transport centre) Sonatrach Bejaia", mémoire de fin de cycle, promotion 2012.

[28] : IUT Nice Côte d'Azur Année 2012/2013 Réseaux LPSIL ADMIN

Résumé :

Ce document s'inscrit dans le cadre de notre projet de fin d'études pour l'obtention du diplôme de master en Informatique, spécialité Administration et Sécurité des Réseaux à l'université ABDERRAHMANE Mira de Béjaia. Il décrit notre travail durant notre stage au sein de la RTC Sonatrach.

L'objectif de la présente étude consiste à présenter un design d'une solution de haute disponibilité et d'équilibre des charges au niveau des réseaux campus en utilisant le protocole HSRP , cette solution consiste à mettre en place une redondance dans le réseau. A l'aide du simulateur Packet Tracer, une architecture hiérarchique interconnectant différent VLANs est proposée assurant ainsi la haute disponibilité afin de faciliter la communication entre les stations.

Mots clés : réseaux campus, haute disponibilité, VLAN's, HSRP.

Abstract:

This document registers as part of our project of the end of studies for the getting of the certificate of master in Computer science, speciality Administration and Security of Networks in the university ABDERRAHMANE Mira Béjaia. He describes our work during our internship within RTC SONATRACH.

The aim of this work is to introduce a design of a solution of high availability and of balance of expenses at the level of networks campus using HSRP protocol, this solution consists in setting a redundancy up in network. Using the simulator Packet Tracer, a hierarchic architecture interconnecting different VLANS is proposed so assuring the high availability to make communication easier between stations.

Keys words: networks campus, high availability, VLAN's, HSRP.