République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira de Béjaia

Faculté des Sciences Exactes

Département d'Informatique

MÉMOIRE DE FIN DE CYCLE

En vue de l'obtention du diplôme de Master en Informatique

Option : *Administration et Sécurité des Réseaux*

Thème

Sécurité des mises à jour des protocoles de routage dans les réseaux de moyenne dimension : étude et configuration cas d'étude SONATRACH

Réalisé par :

M^{elle} BOURENANE Nadjet

M^{elle} KARA Siham

Soutenu le 29 Juin 2016 devant le jury composé de :

Président	Dr	BAADACHE Abderhmane .
Examinateur	Dr	ALOUI Abdelouhabe .
Promoteur	Mr	AISSANI Sofiane .

Promotion : 2015/2016

Remerciements

Tout d'abord, nous remercions Dieu le tout-puissant qui nous a donné le courage, la force et la volonté pour mener ce travail.

Un grand merci pour nos familles, surtout nos parents qui nous ont épaulés, soutenus et suivis tout au long de ce projet.

A nos chères amis qui ont toujours été présents et fidèles.

A nos encadreurs ***Mr. AISSANI SOFIANE*** *à l'université et* ***Mr MADI KEMAL****et* ***CHELOUAH DJAMEL*** *à la RTC pour tout le temps qu'il nous ont consacré, pour leurs précieux conseils et pour toute leur aide et leur appui durant la réalisation de ce travail.*

Aussi à tous les enseignants et employés du département Informatique à qui on doit notre avancement.

Enfin, nous tenons aussi à remercier également tous les membres du jury pour avoir accepté d'évaluer notre travail.

Dédicaces

Je Dédie ce modeste travail : A Mes très chers parents ;
A Mes deux frères Farouk et Iles ;
A Mes deux sœur Sabrina et Nawal ;
A Mes cousins :Hamide,Hossine,Amine,Hani,Fateh ;
A Mes cousines :Farida,Hayatte,Fatiha,Tiziri ;
A Mon Oncle Abdelmadjid ;
A Mes tantes :Ghania, Salima et leurs enfants
Anissa,Aida,Meriem,Katia,Souhil,Kherdine,Nessrine ;
A Mes grands parents ;
A Mon fiancé Bachir et à toute sa famille ;
A Ma binôme ;
A Mes amies ;
A Tous ceux que j'aime.
Bournane Nadjet

Dédicaces

A mes parents : rien au monde ne pourra compenser les sacrifices qu'ils avaient consentis pour mon éducation, ma formation et mon bien être. Que dieu les protège, les gardes, leur prête longues vies et bonne santé.

A ma jumelle NAIMA que j'aime ;

A mes sœurs pour leur soutien, et sourtout l'ange de la famille Amira-Sara ;

A mon neveu que j'aime beaucoup Mehdi-Amine et ma nièce ANAIS ;

A mes oncles et tantes ;

A tous mes cousines et cousins ;

A toute ma famille ;

A mon fiancé Khodir et à tout ça famille ;

A ma binôme ;

A mes amies ;

A Tous ceux que j'aime.

KARA SIHAM

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

ACL	**A**ccess **C**ontrôle **L**ist
AES	**A**devanced **E**ncryption **S**tandard
CFI	**C**anonical **F**ormat **I**dentifier
CISCO	**C**omputer **I**nformation **S**ystem **C**ompany
CLI	**C**ommande **L**angage **I**nterface
CPU	**C**entral **P**rocessing **U**nit
DES	**D**nified **E**rocess **S**nit
DoS	**D**enial **O**f **S**ervice
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
DRGB	**D**irection de **R**égionale de **T**ransport de **B**ejaïa
DTE	**D**ata de **T**erminal **E**quimement
FTP	**F**ile de **T**ransfer De **P**rotocol
HSRP	**H**ot **S**tandby **R**outing De **P**rotocol
HTTP	**H**yper **T**ext **T**ransfer **P**rotocol
IEEE	**I**nstitute of **E**lectrics and **E**lectronics **E**ngeneers
IP	**I**nternet **P**rotocol
ISl	**I**nter **S**witch **L**ink
ISO	**I**nternational **S**tandardization **O**rganization
LAN	**L**ocal **A**rea **N**etwork
LSA	**L**ink **S**tate **A**dvertisement
LSDB	**L**ink **S**tate **D**ata **B**ase
MAN	**M**etropolitan **A**rea **N**etwork
MD5	**M**essage **D**igest **5**
OSI	**O**pen **S**ystems **I**nterconnexion
OSPF	**O**pen **S**hortest **P**ath **F**irst

PC	**P**ersonal **C**omputer
RIP	**R**outing **I**nformation **P**rotocol
RTC	**R**égion **T**ransport **C**entre
RSA	**R**ivest **S**hamir **A**dleman
SHA	**S**ecure **H**ash **A**lgorithm
SI	**S**écurité **I**nformatique
SGBD	**S**ystème **G**estion **B**ase **D**onnées
STP	**S**panning **T**ree **P**rotocol
TCI	**T**ag **C**ontrol **I**nformation
TCP	**T**ransmission **C**ontrol **P**rotocol
TPID	**T**ag **P**rotocol ID
TRC	**T**ransport Par **C**analisation
UDP	**U**ser **D**atagram **P**rotocol **N**rotocol
VID	**V**lan ID
VLAN	**V**irtual **L**ocal **A**rea **N**etwork
VTP	**V**LAN **T**runking **P**rotocol
WAN	**W**ide **A**rea **N**etwork

Introduction générale

L'évolution technologique de ces quinze dernières années a conduit à la possibilité de construire des systèmes informatiques de plus en plus sophistiqués et de moins en moins encombrants. Pour permettre d'équiper le maximum de points d'utilisation et constituer, pour tout employé d'une entreprise, d'une administration, et donc d'un établissement d'enseignement, l'outil indispensable améliorant son efficacité et par la suite sa productivité. Ces nouveaux systèmes offrent de nombreuses et précieuses possibilités, ils résolvent des problèmes de gestion ; aident à saisir et à mettre en forme des textes ; stockent localement des informations textuelles, graphiques ou numériques, vocales dans des fichiers d'où ils permettent de les extraire pour les retraiter, les afficher, les imprimer ou les transmettre vers un autre système ou utilisateur.

Un réseau informatique est un ensemble cohérent de matériels et de logiciels pour faire communiquer des équipements informatiques. Ces matériels communiquent entre eux grâce à un protocole. Un protocole est un ensemble de règles structurées selon lesquels deux entités différentes peuvent communiquer sans aucune ambiguïté. L'objectif d'une telle communication est de pouvoir partager des informations et des ressources matérielles.

Durant la période de notre stage, nous avons travaillé sur un réseau local : cas de l'entreprise SONATRACH. Nous avons étudié la façon avec laquelle SONATRACH utilise son réseau informatique, qui lui permet une meilleure circulation de l'information.

Afin d'atteindre les objectifs cités, nous avons organisé ce travail en quatre chapitre : Dans le premier chapitre qui s'intitule présentation de l'organisme d'accueil, nous établissons une description générale de l'entreprise SONATRACH et du centre informatique ou nous avons effectué notre stage.

Le deuxième chapitre consacré essentiellement pour présenter les notions fondamentales telque VLAN et quelques notions de base sur la sécurité des réseaux informatique qui nous servirons dans la partie pratique.

Le troisième chapitre est consacré à expliquer les concepts des VLANs et l'étude des protocoles VTP, STP, HSRP et DHCP que nous configurons.

Enfin,le dernier chapitre qui est la partie planification et réalisation, contient toutes les configurations appliquées, ainsi que les tests de validation pour vérifier si vraiment les objectifs ont été atteints.

Nous avons présenté à la fin une conclusion générale décrivant les points essentiels développés dans ce mémoire ainsi que les différents acquis théoriques et pratiques.

Chapitre 1

Présentation de l'organisme d'accueil

1.1 Introduction

Dans ce chapitre on s'intéresse à la présentation dans le détail de l'infrastructure réseau sécurité informatique et système de la région transport centre de Béjaïa, ainsi nous étudions l'organisation de ces services, c'est-à-dire, de découvrir les différents équipements informatiques que ça soit matériels, logiciels, ou système qui gérant le bon fonctionnement de cette entreprise.

1.2 Présentation de l'organisme d'accueil

1.2.1 Présentation de SONATRACH

Afin d'assurer le contrôle et la gestion du secteur naissant dans les années 1950 des hydrocarbures, une Direction de l'Energie et des Carburants ont été mises en place en Algérie. Des indicateurs significatifs d'une évolution peu probable du secteur des hydrocarbures ont été constatés. Pour un pays tel que l'Algérie, qui sortait de la guerre d'indépendance, une telle situation ne pouvait nullement convenir à sa stratégie de développement. Pour cela, l'Etat algérien se dota d'un instrument permettant la mise en œuvre d'une politique énergétique en créant le 31-12-1963 par décret n° 63 / 491 la société nationale pour le transport et la canalisation d'hydrocarbures. Cette société a changé de statuts le 22-07-1966 décrets n° 66/292, pour devenir " SONATRACH " Société Nationale chargée de la recherche, la production,

la transformation et la commercialisation des hydrocarbures. La volonté de l'Algérie de récupérer ses richesses naturelles et d'assurer pleinement le contrôle de leur exploitation, amena à nationaliser la production des hydrocarbures le 24/02/1971 par la signature d'une ordonnance, définissant le cadre d'activité des sociétés étrangères en Algérie. Grâce à cette nationalisation, l'entreprise SONATRACH est passée d'une petite entreprise de 33 agents en 1963 à un effectif de 103000 employés la fin des années 1980, et qui compte aujourd'hui 120 000 employés.

1.2.2 Les Activités principales de SONATRACH

Le but recherché par la restructuration et réorganisation est la décentralisation des pouvoirs. SONATRACH exerce ses activités dans quatre principaux domaines à savoir :

• **Activité amont** :recouvre les métiers de recherche, d'exploration, de développement et de production des hydrocarbures ;

• **Activité transport** :assure l'acheminement des différents hydrocarbures par canalisation ;

• **Activité aval** :a en charge le développement et l'exploitation des complexes hydrocarbures (liquéfaction, raffinerie,...) ;

• **Activité commercialisation** :a pour mission l'élaboration et l'application de la stratégie commerciales de SONATRACH sur le marché national et international.

1.2.3 Organigramme

Pour la réalisation de ces objectifs, SONATRACH est divisé en cinq branches différentes représentées par l'organigramme suivant :

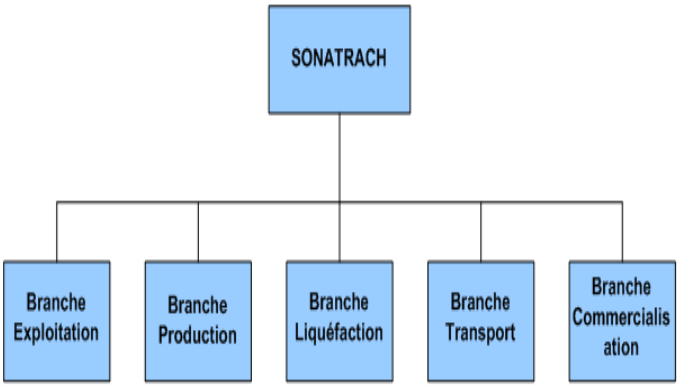

FIG. 1.1 – Les branches de SONATRACH

1.2.4 Présentation 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 :

• **L**a gestion et l'exploitation des ouvrages et canalisations de transport d'hydrocarbures ;

• **L**a coordination et le contrôle de l'exécution des programmes de transport arrêtés en fonction des impératifs de production et de commercialisation ;

• **L**a maintenance, l'entretien et la protection des ouvrages et canalisation ;

• **L**'exécution des révisions générales, des machines tournantes et équipements ;

• **L**a conduite des études, la réalisation et la gestion des projets de développement des ouvrages et canalisations ;

• **L**es installations de pompage et de stockage pour répondre aux besoins de SONATRACH dans les meilleures conditions d'économie, de qualité, de sécurité et de respect de l'environnement ;

• **G**ère l'interface transport des projets internationaux du groupe ou en partenariat.

La SONATRACH possède cinq directions régionales de transport des hydrocarbures :

- **L**a direction régionale Est Skikda(RTE) ;
- **L**a direction régionale Centre Bejaïa(RTC) ;
- **L**a direction régionale Ouest Arzew (RTO) ;
- **L**a direction régionale de Haoud-EL-Hamra (RTH) ;
- **L**a direction régionale d'Ain Amenas (RTI) ;
- **G**azoduc Espagne/Maroc (GEM) ;
- **G**azoduc Tunisie/Italie (GPDF).

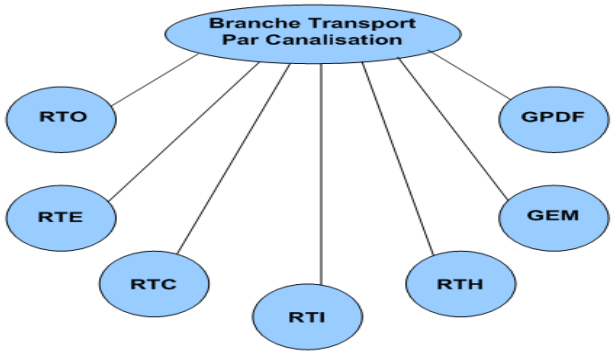

FIG. 1.2 – Branche transport par canalisation

1.2.5 Présentation de la direction régionale de transport de Bejaïa (DRGB)

La direction régionale de transport de Bejaia (DRGB) est l'une des cinq directions régionales de transport des hydrocarbures de la SONATRACH (TRC). Elle a pour mission de transporter, stocker et livrer les hydrocarbures liquides et gazeux.

1.2.6 Structure de la DRGB

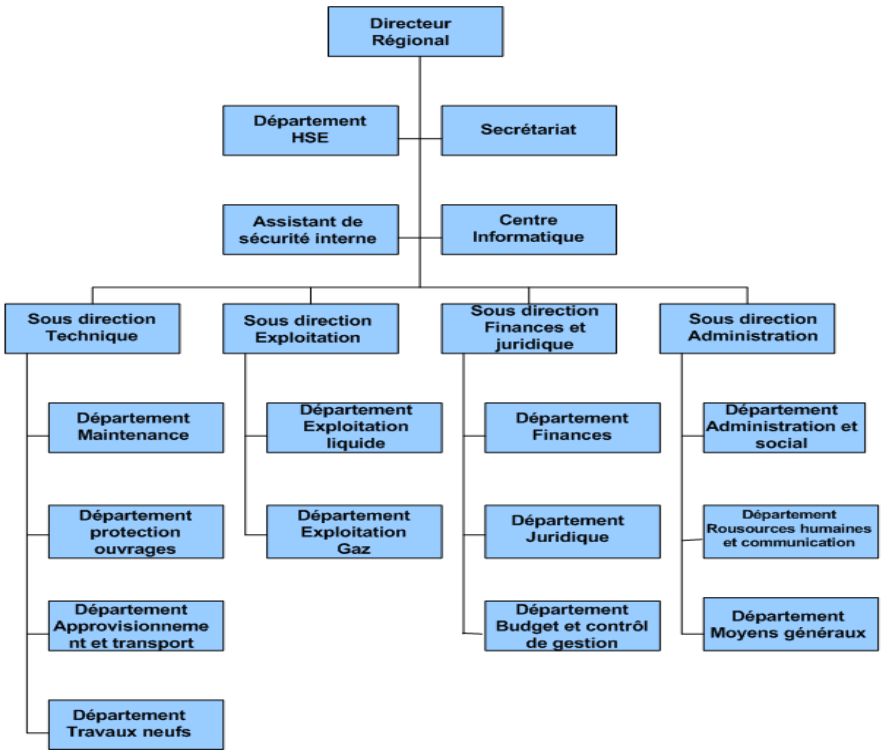

FIG. 1.3 – Organisation de la direction régionale de Béjaïa

1.3 Présentation de la structure concernée par l'étude

1.3.1 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 Béjaïa (DRGB) et des autres régions.

1.3.2 Organigramme du centre informatique

Le centre informatique s'organise en trois services tels qu'ils sont schématisés dans la figure suivante :

1.3.3 Organigramme

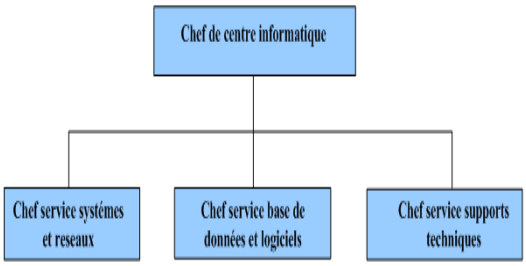

FIG. 1.4 – Organigramme du centre informatique

1.3.4 Rôle de chaque service

1.Service systèmes et réseaux :

Système

• **c**hoix des équipements informatiques et logiciels de base ;

• **M**ettre en œuvre les solutions matériels et logiciels retenues ;

• **I**nstallation et configuration des systèmes ;

• **O**rientation des travaux de l'équipe de développement par une bonne utilisation des ressources de l'ordinateur ;

• **M**ise en œuvre de nouvelles versions de logiciels.

Réseau

• **A**ssure le bon fonctionnement, la fiabilité des communications, l'administration du réseau et organise l'évolution de sa structure ;

• **C**onduire l'étude pour le choix de l'architecture du réseau à installer ;

• **P**articipe à la mise en place des réseaux ;

• **D**éfinit les droits d'accès pour l'utilisation du réseau ;

• **A**ssure la surveillance permanente pour détecter et prévenir les pannes ;

• **T**raitement des disfonctionnements et incidents survenant sur le réseau .

2.Service base de données et logiciel :

Base de données

• **C**onçoit les bases de données et assure l'optimisation et le suivi de la gestion des données informatiques ;

• **I**nstaller, configurer et exploiter le SGBD et ses bases ;

• **M**ise en œuvre et gestion des procédures de sécurité (accès, intégrité) ;

• **G**érer la sauvegarde, la restauration et la migration des données ;

• **A**ssure la cohérence et la qualité des données introduites par les utilisateurs.

Logiciels

• **E**tude et conception des systèmes d'information ;

• **D**éveloppement et maintenance des applications informatiques pour TRC ;

• **D**éploiement des applications et formations des utilisateurs.

3.Service supports techniques :

• **C**onçoit les bases de données et assure l'optimisation et le suivi de la gestion des données informatiques ;

• **A**ssistance aux utilisateurs en cas de problèmes software et hardware ;

• **I**nstallation des logiciels de gestion, technique et bureautique ;

• **F**ormation aux nouveaux produits installés.

1.4 conclusion

Dans ce chapitre nous avons présenté l'entreprise SONATRACH de Bejaia (RTC) dans la quelle nous avons suivi notre stage pratique. Ce dernier, nous a permis d'acquérir de nouvelles connaissances dans la mise en place et l'administration des réseaux d'entreprise.

Chapitre 2

Notions théoriques sur les réseaux et la sécurité

2.1 Introduction

Dans ce chapitre, nous allons focaliser notre étude essentiellement sur l'explication des principes fondamentaux sur lesquels se fondent les réseaux informatiques en particulier les réseaux locaux LAN et VLAN. Pour expliquer l'intérêt des réseaux LANs, savoir que signifie le réseau informatique est préalablement nécessaire, et les différents risques possibles, afin de déterminer nos besoins matériels et logiciels de sécurité.

Généralités sur les réseaux

2.2 Définition d'un réseau informatique

Le terme générique d'un réseau est ensemble d'objets interconnectes les uns avec les autres. Il permet de faire circuler des éléments de ses objets. Cependant un réseau informatique est un ensemble d'ordinateurs relies entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numérique (des valeurs binaire). [1]

2.2.1 Objectifs des réseaux informatiques

Un réseau informatique peut servir plusieurs buts distincts :

- **L**e partage de ressources(fichier,application,connexion à internet,etc.) ;

- **L**a communication entre personnes (courier électronique,discusion en direct,etc.) ;
- **L**a communication entre processus(entre des ordinateurs) ;
- **L**es jeux vidéo multi-joueures.

2.3 Classification des réseaux

Trois grandes catégories de réseaux en fonction de la distance maximale reliant deux points :[2]

2.3.1 Les réseaux LAN (Local Area Network)

Un réseau LAN est définit comme un ensemble de périphériques appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répondue étant Ethernet), il couvre une distance qui est inférieur à 1 km.

2.3.2 Les réseaux WAN (Wide Area Network)

Un WAN permet l'interconnexion de réseaux locaux et métropolitains à l'échelle d'une région, d'une ville, d'un pays ou de la planète. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles. Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau (le routage des informations). Ils couvrent une distance qui est supérieur 10 km.

2.3.3 Les réseaux MAN (Métropolitain Area Network)

Le réseau interconnecte plusieurs (minimum deux) LANs à travers de grandes distances géographiques (au maximum quelques dizaines de km) à des débits importants. Un MAN est formé de commutateur ou de routeurs interconnectés par des liens hauts débits (généralement en fibre optique), ils couvrent une distance qui est entre 1 km et 10 km.[3]

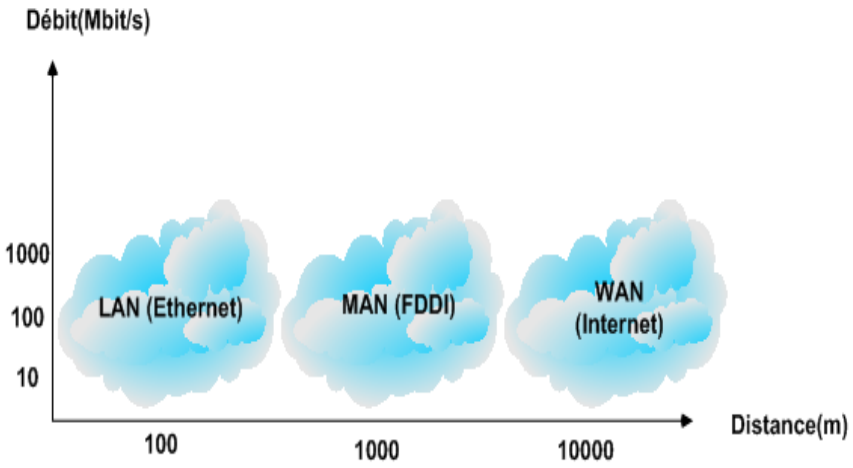

FIG. 2.1 – les différents types des réseaux

2.4 Modèle de références OSI (Open Systems Interconnexion)

Le modéle OSI sert de référence pour mieux comprendre la communication réseau, ce modèle décrit les modifications qui peuvent être apportées à un message depuis sa création jusqu'à sa transmission sur le support physique.

Le modèle OSI est constitué de sept couches. À chaque couche est associée une fonction bien précise, l'information traverse ces couches, chacune y apporte sa particularité ces couches sont les suivantes : [4]

- **La couche 1 (physique)**

Elle définit les caractéristiques du matériel nécessaire pour mettre en œuvre le signal de transmission (protocole Ethernet), comme des tensions, des fréquences, la description d'une prise. . . ;

- **La couche 2 (liaison de données)**

Elle effectue le travail de transmission des données d'une machine à une autre (protocole Ethernet) ;

• **La couche 3 (réseau)**

Cette couche fournit les moyens de communication et détermine la fonction de routage qui achemine le transfert des paquets d'une extrémité à une autre. Elle gère l'adressage de transmission des données entre l'émetteur et le récepteur ;

• **La couche 4 (transport)**

Elle garantie que le destinataire obtient exactement l'information qui lui a été envoyée. Cette couche met par exemple en œuvre des règles de renvoi de l'information en cas d'erreur de réception (protocole TCP/IP) ;

• **La couche 5 (session)**

- Organise et synchronise les échanges entre tâches distantes.
- Gère et ferme les sessions de communication entre les applications ;

• **La couche 6 (présentation)**

Elle est responsable de la présentation sous un format (une syntaxe) lisible par l'application. Par exemple :

- Passage de code ASCII au code VIDEOTEXE ;
-Compression décompression des données.

• **La couche 7 (application)**

Elle est constituée des programmes d'application ou services, qui se servent du réseau. Ils ne sont pas forcément accessibles à l'utilisateur car ils peuvent être réservés à un usage d'administration (protocole http).

2.5 Le modèle TCP/IP

Contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation mais il est inspiré du modèle OSI. Il reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre.
Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application. [5] [6]

Les différant couches du modèle TCP/IP sont les suivantes :

- **Hôte -réseau :** Spécifie la forme sous les données doivent être acheminées quel que soit le type de réseau utilisé. [1]

- **Internet :** La couche inter-réseaux a pour rôle de transmettre les données à travers une série de réseaux physiques différents qui relient un hôte source avec un hôte destination. Les protocoles de routage sont étroitement associés à ce niveau. IP est le protocole routé de base sur l'Internet.[7]

- **Transport :** La couche transport prend en charge la gestion de connexion, le contrôle de flux, la retransmission des données perdues et d'autres modes de gestion des flux. Les protocoles TCP et UDP sont dédiés à ces fonctions de transport.[7]

- **Application :** Elle contient tous les protocoles de haut niveau qu'un utilisateur souhaite avoir à sa disposition tels que Telnet (utilisateur permettant l'utilisation de programmes sur des machines distantes via un réseau), FTP (File Transfer Protocol), http (Hyper Text Transfer Protocol) et d'autre. [7]

Le schéma ci-dessous (Figure2.2) nous montre la différence entre ces deux modèles :

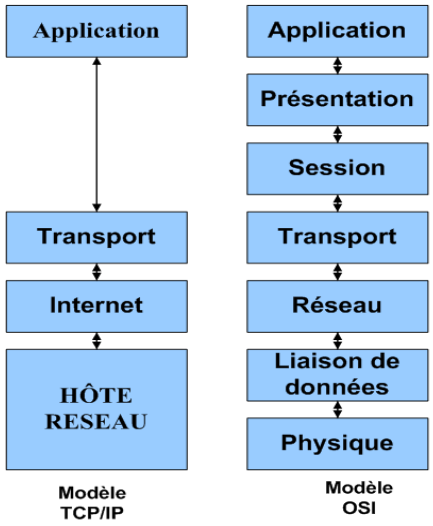

FIG. 2.2 – la différence entre le modéle OSI et TCP/IP

2.6 Le routage

C'est est la fonction qui s'occupe de diriger les donnes réseaux a travers différents segments jusqu'au prochain point de route. Cette fonction emploi des algorithmes de routage. Le périphérique de routage est le routeur .Il utilise les adresses IP pour diriger correctement les paquets d'un réseau ou segment a un autre .Il doit maintenir sa table de routage à jour et connaitre les changements effectués sur les autres appareils par lesquels il pourrait faire transiter le paquet.[8]

2.6.1 Définition d'une route

Un route c'est le chemin existe entre deux extrémités (source et destination) à travers laquelle les paquets sont envoyés.

2.6.2 Les types de routes

Il existe trois routes qui sont :[8]

2.6.2.1 Le routage statique

Le routage statique est un principe de routage programmé par l'administrateur de réseau afin de déterminer le chemin que doit empreinte un paquet pour atteindre sa destination. L'administrateur doit faire la gestion des routes de chaque unité de routage de réseau, les chemins statiques ne s'adaptent pas aux modifications des environnements réseaux.

Le routage statique présente plusieurs avantages et inconvénients :[9]

2.6.2.2 Avantages du routage statique

• **Économie de bande passante**

Étant donné qu'aucune information ne transite entre les routeurs pour qu'ils se tiennent à jour, la bande passante n'est pas encombrée avec des messages d'information et de routage.

• **Sécurité**

Contrairement aux protocoles de routage dynamique que nous allons voir plus bas, le routage statique ne diffuse pas d'information sur le réseau puisque les informations de routage sont directement saisies de manière définitive dans la configuration par l'administrateur.

• **Connaissance du chemin à l'avance**

L'administrateur ayant configuré l'ensemble de la topologie saura exactement par où passent les paquets pour aller d'un réseau à un autre, cela peut donc faciliter la compréhension d'un incident sur le réseau lors des transmissions de paquets.

2.6.2.3 Inconvénient du routage statique

• **L**a configuration de réseaux de taille importante peut devenir assez longue et complexe, il faut en effet connaitre l'intégralité de la topologie pour saisir les informations de manière exhaustive et correcte pour que les réseaux communiquent entre eux. Cela peut devenir une source d'erreur et de complexité supplémentaire quand la taille du réseau grandit.

A chaque fois que le réseau évolue, il faut que chaque routeur soit au courant de l'évolution par une mise à jour manuelle par l'administrateur qui doit modifier les routes selon l'évolution.[10]

2.6.3 Le routage dynamique

Ce procédé se base sur l'ajout des réseaux distants à la table de routage à l'aide d'un protocole de routage dynamique (RIP, OSPF,...).Après la découverte initiale du réseau, ces derniers mettent à jour et gèrent les réseaux dans leurs table de routage sans nécessiter l'intervention de l'administrateur réseau. [11]

Le routage dynamique présente aussi des avantages et des inconvénients.[12]

2.6.4 Avantages du routage dynamique

• **U**ne maintenance réduite par l'automatisation des échanges et des décisions de routage ;

• **U**ne modularité et une flexibilité accrue, il est plus facile de faire évoluer le réseau avec un réseau qui se met à jour automatiquement ;

• **S**a performance et sa mise en place ne dépendent pas de la taille du réseau .

2.6.5 Inconvénient du routage dynamique

• **I**l peut être plus compliqué à mettre en place lors de son initialisation ;

• **I**l consomme de la bande passante de par les messages que les routeurs s'envoient périodiquement sur le réseau ;

• **L**a diffusion automatique de message sur le réseau peut constituer un problème de sécurité car un attaquant peut obtenir des informations sur la topologie du réseau simplement en écoutant et en lisant ces messages d'information du protocole de routage et même en créer afin de se faire passer pour un membre du réseau.

2.6.6 Routage par default

La route par défaut est la route qui sera utilisée lorsqu'aucune route spécifique pour aller vers la destination spécifique n'aura été trouvée. [13]

2.7 L'interconnexion d'un réseau local

Des matériels sont donc utilises pour interconnecter les réseaux entre aux. Ils permettent également de segmenter les réseaux de taille important, en domaine plus

petite.

Les éléments d'nterconnexion sont :[14]

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

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

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.

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

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

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

Adaptateur : Un adaptateur (adapter) sont destines à être insères dans un poste de travail ou un serveur afin de les connecter à un système de câblage.

Lorsqu'il s'agit de deux réseaux de même type, il suffit de faire passer les trames de l'un sur l'autre. Dans le cas contraire, c'est-à-dire lorsque les deux réseaux utilisent des protocoles différents, il est indispensable de procéder à une conversion de protocole avant de transférer les trames. Ainsi, les équipements à mettre en œuvre sont différents selon la configuration face à laquelle on se trouve.

Généralité sur la sécurité

La sécurité des réseaux informatiques est nécessaire pour protéger le réseau d'une enterprise et de se prémunir contre tout type d'attaques pouvant perturber le réseau. La sécurité informatique (SI) est l'ensemble des moyens (méthodes, techniques et Outils) mises en ouvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles. Elle à pour objectif d'assurer les propriétés suivantes :[16]

La confidentialité :Assurer que l'information ne soit divulguée ou révélée qu'aux personnes autorisées.

L'authentification :C'est la propriété qui assure que seules les entités autorisées ont accès au système.

L'intégrité :Assurer que l'information contenue dans les objets ne soit ni altérée, ni détruite de manière non autorisée.

La disponibilité :L'accès par un sujet autorise aux ressources et informations du système doit être toujours possible.

Non répudiation :C'est la propriété qui assure la preuve de l'authenticité d'un acte c'est-à-dire que l'auteur d'un acte ne peut ensuite dénier l'avoir effectué.

2.8 Outils de la sécurité

2.8.1 Cryptographie

La cryptographier est la science qui utilise les concepts mathématique pour cryptage (chiffrement) et le décryptage (déchiffrement) des données. Elle permet ainsi de stocker des informations confidentielles ou de transmettre sur des réseaux non sécurisés (tel que l'internet), afin qu'aucune personne autre que le destinataire ne puisse les lire.

Alors que la cryptographier consiste à sécuriser les donner, la cryptanalyse est

l'étude des informations cryptées, afin de découvrir le secret. La cryptanalyse classique implique une combinaison intéressante de résonnement analytique, d'application d'outils mathématique, de recherche de modèle, de patience, de détermination et de chance. Ces cryptanalyses sont également appelés des pirates. La cryptographier est divisées en deux axes majeurs : [17]

- **Cryptographie symétrique**

Une même clé est utilisée pour crypter et décrypter le message, très efficace et assez économe en ressources CPU cette technique pose le problème de la distribution des clés dans un réseau étendu (exemple DES, triple DES ou le récent AES). [[18]

- **Cryptographie asymétrique**

Chaque utilisateur dispose d'un jeu unique de clés, dont l'une est privée (secrète) et l'autre publique (exemple RSA). Pour recevoir des documents protégés, le détenteur d'un jeu de clés envoie sa clé publique à ses interlocuteurs, qui l'utilisent pour chiffrer les données avant de les lui envoyer. Seul le destinataire et détenteur des clés peut lire les informations en associant sa clé privée à sa clé publique. Cette technique nécessite des clés plus longues pour une sécurité équivalente.

2.9 Fonctions de hachage

Ce type de fonction est très utilisé en cryptographie, principalement dans le but de réduire la taille des données à traiter par la fonction de cryptage. En effet, la caractéristique principale d'une fonction de hachage est de produire un haché des données, c'est-à-dire un condensé de ces données. Ce condensé est de taille fixe, dont la valeur diffère suivant la fonction utilisée (MD5, SHA). [19] [20]

2.10 Signature numérique

Les signatures numérique permettent à la personne qui reçoit une information de contrôle l'authenticité de son origine, et également de vérifier que l'information en question est intacte.

Ainsi, les signatures numériques des systèmes à des clés publiques permettent l'authentification et le contrôle d'intégrité des données. Le principe de la signature consiste à appliquer une fonction mathématique sur portion de message, cette

fonction mathématique s'appelle fonction de hachage et le résultat appelé code de hachage, ce code de hachage est ensuite crypté avec les clés privées de l'émetteur et rajouter au message ensuite le destinataire décrypte le code grâce à la clé publique puis il compare ce code qu'il calcule grâce au message reçus.

Le destinataire sait aussi que le message provient de l'émetteur, puisque seul le dernier possède la clé privée qui a crypté le code. [21]

2.11 VLAN

Un VLAN (Virtual Local Area Network ou Virtual LAN) est un réseau local regroupant un ensemble des machines utilisant la technologie Ethernet pour regrouper les éléments du réseau (utilisateurs, périphériques, etc.) selon des critères logiques (fonction, partage de ressources, appartenance à un département, etc.), sans se heurter à des contraintes physiques (dispersion des ordinateurs, câblage informatique inapproprié, etc.). [22]

2.11.1 Topologie de VLAN

On distingue généralement trois [22] techniques pour construire des VLANs, en fonction de leurs méthodes de travail, nous pouvons les associer à une couche particulière du modèle OSI.

- **VLAN de niveau 1 ou VLAN par port**

On affecte chaque port des commutateurs à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par sa connexion à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN.

Si on déplace physiquement une station il faut désaffecter son port du Vlan puis affecter le nouveau port de connexion de la station au bon VLAN. Si on déplace logiquement une station (on veut la changer de VLAN) il faut modifier l'affectation du port au VLAN.

• **VLAN de niveau 2 ou VLAN MAC**

On affecte chaque adresse MAC à un VLAN. L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC. En fait il s'agit, à partir de l'association MAC/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLANs en fonction de l'adresse MAC de l'hôte qui émet sur ce port.

L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation des machines portables). Si on veut changer de VLAN il faut modifier l'association MAC / VLAN.

• **VLAN de niveau 3 ou VLAN d'adresses réseaux**

On affecte une adresse de niveau 3 à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par l'adresse de niveau 3 ou supérieur qu'elle contient(le commutateur doit donc accéder à ces informations). En fait, il s'agit à partir de l'association adresse niveau 3 VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLANs.

Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLANs en accédant aux informations de couche 3. Ceci est un fonctionnement moins rapide que le VLAN de niveau 2. Quand on utilise le protocole IP on parle souvent de VLAN par sous-réseau.

2.12 Pare-feu (firewall) ou garde-barriére

Un firewall (pare-feu ou garde barrière) est un dispositif de contrôle d'accès de réseau, conçu pour refuser tout le trafic n'est pas explicitement permis. Deux mécanismes sont utilisés : La première consiste à interdire le trafic, et le deuxième à l'autoriser. Il à une fonction différente de celle d'un routeur, qui es un dispositif de réseau destiné à acheminer le trafic aussi rapidement que possible. Donc un routeur peut être un pare-feu. Effectivement, un routeur est destiné à acheminer tout le trafic aussi vite que possible, il est configuré pour refuser un certain type de trafic. Alors le pare-feu fournit généralement un niveau de configuration plus riche. Ils peuvent être configurés pour autoriser le trafic en fonction du service, de l'adresse IP de la source ou de la destination ou de l'ID de utilisateur à l'origine de la requête. Les pare-feu

peuvent aussi être configurés pour enregistrer tout le trafic. Ils peuvent aussi une fonction de gestion centralisée de la sécurité.

En bref un firewall est un ordinateur (et un programme) qui filtre ce qui passe d'un réseau à un autre. [23]

La figure ci-dessus présente l'architecture classique d'un firewall

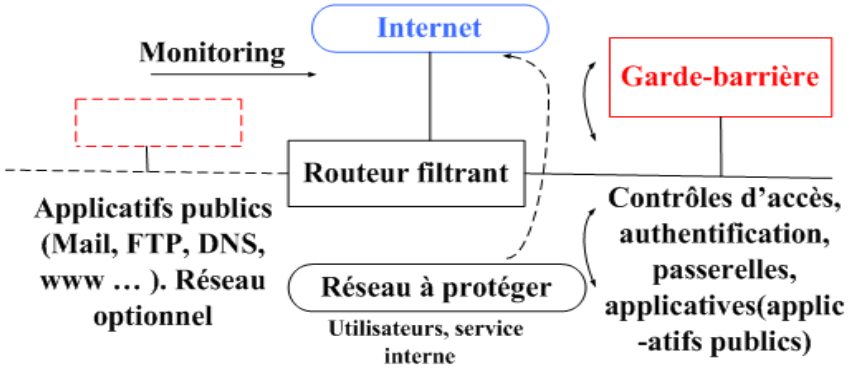

FIG. 2.3 – Architecture classique d'un pare-feu

• **Types de firewall**

Il existe deux types de pare-feu : le pare-feu de niveau application et le pare-feu de niveau réseau. Bien que relavant de concepts différents, ils peuvent tous deux assurer les fonctions de sécurité nécessaire pour bloquer le trafic non autorisé.[23]

2.13 conclusion

Ce chapitre nous a permis d'avoir une bonne compréhension des concepts de base et d'éclaircir les différentes idées du réseau LAN, nous avons vu le modèle de référence OSI et le modèle TCP/IP, ses différentes couches et les éléments physiques qui le constitue, Ainsi la sécurité des mises a jours des protocoles de routage RIP, OSPF, ensuite nous avons énuméré les attaques visant chacun de ces protocoles.

Chapitre 3

Etude de quelques protocoles

3.1 Introduction

Les réseaux informatiques rencontrent souvent divers problèmes, à titre d'exemple : la complexité de la configuration des VLANs et le risque des boucles de routage. Par ailleurs, la configuration des protocoles VTP (Virtual Trunking Protocol), et STP (Spanning Tree Protocol) permettent de surpasser les deux problèmes cités ci-dessus.

A travers ce chapitre, nous allons aborder l'étude des protocoles VTP, STP, HSRP et le service DHCP dans le cadre des VLANs.

Les protocoles de routage

3.2 Protocole de routage à vecteur de distance (RIP)

La technologie de vecteur de distance veut dire que les routes sont annoncées en tant que vecteurs de distance et de direction. La distance est définie en termes de mesure, comme le nombre de sauts, et la direction est le routeur de tronçon suivant ou l'interface de sortie. Parmi les protocoles de routage à vecteur de distance, on compte RIP V1, RIP V2 , OSPF.

Un routeur utilisant un protocole de routage à vecteur de distance ne connait pas le chemin complet vers un réseau de destination. Le routeur ne connait que les éléments suivants :[24]

• **L**a direction ou l'interface dans laquelle les paquets doivent être transmis ;

• **L**a distance le séparant du réseau de destination.

Pour mieux comprendre la technologie à vecteur de distance, nous étudierons le fonctionnement des protocoles RIP et OSPF.[24]

3.2.1 Protocole RIP (Routing Information Protocol)

Le protocole RIP, est un protocole à vecteur de distance qui utilise le nombre de sauts comme métrique. S'il existe plusieurs chemins vers une destination, le protocole RIP sélectionne celui qui comporte le moins de saut.

Ce protocole est limité à 15 sauts, un réseau situé à une distance de plus de 15 sauts il ne peut pas fournis de route pour ce réseau. Les routeurs échangent les informations de routage via des messages de mise à jour qui sont diffusés toutes les 30 secondes. S'il le routeur ne reçoit aucun information de routage de l'un de ces routeurs adjacents pendent 180 secondes (Time out), il mettra à l'infini (le métrique=16) les entrées ayant comme, le protocole RIP enlève toutes les entrées n'y a toujours aucune mise à jour après 240 secondes, le protocole RIP enlève toutes les entrées dans la table de routage correspondant au routeur qui ne répond pas.

3.2.1.1 Fonctionnement du protocole RIP

Le protocole de routage RIP fait partie des protocoles de routage interne basé sur les algorithmes à vecteur de distance. Ces algorithmes utilisent l'algorithme de Bellman-Ford. Il permet à chaque routeur de communiquer aux autres routeurs la métrique, lorsqu'un routeur reçoit un de ces messages, il incrémente cette distance de 1 et transfère le message aux routeurs directement accessibles.

Une route est composée de :[25]

• **L**'adresse du réseau destinataire ;

• **L**'adresse du routeur pour atteindre le réseau de destination (next hop) ;

• **L**a métrique qui représente le nombre de routeur à traversé pour atteindre le réseau de destination.

En réception, le routeur compare les routes reçues avec les siennes et met sa propre table à jour si :

• **U**ne route reçue est meilleure ;

• **U**ne route reçue est nouvelle.

3.3 Protocole de routage à état de lien (OSPF)

L'algorithme de routage à vecteur de distance peut conduire à des boucles qui ralentissent sa convergence. Cela est dû au fait que les routeurs ont une connaissance partielle de la topologie du réseau.

Pour éviter la production des boucles dans un protocole de routage à état des liaisons ou(link states), il faut que chaque routeur ait une connaissance complète de la topologie du réseau. L'algorithme Dejikstra permet d'obtenir cette connaissance en inondant périodiquement le réseau avec des paquets contenant une information sur l'état des liens du réseau (LSA : Link State Advertisement), ce qui permet à chaque routeur de construire la topologie complète du réseau. Ensuite chaque routeur exécute en local l'algorithme de Dejikstra pour le calcul des plus courts chemins vers toutes les destinations.

Les routeurs communiquent entre eux par les LSAs qui décrivent leurs liens. Un LSA contient l'adresse du routeur, l'adresse de ses voisins et le coût de chaque liaison aves ses voisins. Lorsqu'un routeur reçoit un LSA, il l'enregistre dans une LSA Data Base, et l'envoie à chaque interface autre que celle par la quelle il est arrivé. [26]

3.3.1 Protocol OSPF (Open Shortest Path First)

Le protocole OSPF est un protocole permettant d'établir les tables de routages pour des routeurs se trouvant dans un domaine administratif de l'internet.

On parle de routage intra-domaine (ou interne) par opposition à du routage inter-domaine (ou externe) possédant d'autres contraintes. Il fait partie des protocoles dit à état de liens (Links State).[27]

3.3.1.1 Fonctionnement du protocole OSPF

Dans le protocole OSPF, établit des relations d'adjacence avec ses voisins immédiats en envoyant des messages hello à intervalle régulier. Chaque routeur communique ensuite la liste des réseaux auxquels il est directement connecté par des messages LSA (Link-State Advertisements) propagés de poche en poche à tous les routeurs du réseau.

L'ensemble des LSA forme la base de données des liens Link-State Data base

(LSDB), qui est identique pour tous les routeurs participants. Chaque routeur utilise ensuite l'algorithme de Dejikstra, Shotest Path First, pour déterminer la route la plus courte vers chacun des réseaux de la base commune. Chaque réseau établit donc sa table de routage à partir de la LSDB.[26]

La figure ci-dessus illustre le format de message OSPF :

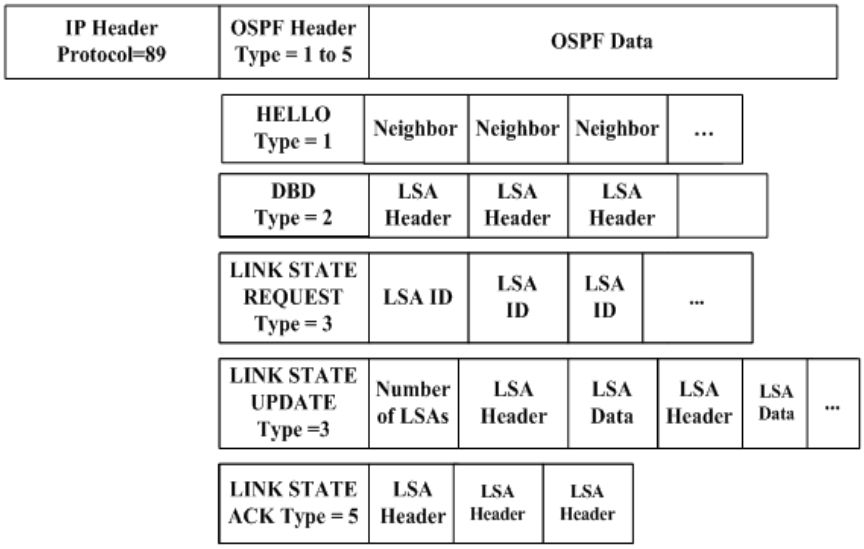

Fig. 3.1 – Le format de message OSPF

3.4 Problèmes des protocoles de routage

L'objectif des protocoles de routage est de maintenir les tables de routage du réseau dans un état intègre et cohérent, mais qui n'ont pas été conçus d'une manière sécurisée. Eventuellement, par le biais de diverses attaques, d'injecter, de modifier ou d'impacter d'une manière ou d'une autre un processus de routage.

Toute attaque ou perturbation du routage peut impacter directement la disponibilité du réseau et de ses services. Parmi les obstacles que rencontrent les protocoles de routage sont [28] :

• **Boucles de routage**

Les protocoles de routage ont des mécanismes pour assurer la cheminement sans boucle. Mais les mesures donnent des évidences que ces boucles existent parfois dans le transfert des paquets inter-domaine. La cause exacte de cet effet est peu claire. Il croit que le délai de propagation des messages de routage cause de moments ou il y a des contradictions de routage entre les routeurs.[28]

• **Croissance de la table de routage**

Le nombre des préfixes (adresses de réseau) annoncés sur l'internet augmente si rapidement cela provoque une surcharge dans la table de routage. Cela cause l'instabilité rejeter les nouveaux chemins, interrompe les sessions d'échanges de route, ou redémarrer le routeur. [26]

• **Mauvaises configuration**

Les erreurs de configuration de routage peuvent perturber ou interrompe la connectivité d'internet, ces dernières sont nombreuses. La mauvaise configuration est effectivement dangereuse car elle permet aux attaquants de causer à la fois le déni d'accès (blackholing) dans un réseau et le déni de service (DoS) dans un autre réseau. [25]

3.5 Attaque visant RIP

Les attaques possibles pour RIP sont :[28]

• **Insertion de fausse route pour rediriger le trafic ou empoisonner la table de routage :**

L'attaquant qui connaît bien la topologie du réseau peut injecter des messages pour forcer un routeur à utiliser un chemin particulier afin de renifler les données. Il peut aussi empoisonner la table de routage par de fausses routes pour causer l'instabilité.

• **Déni de service DoS contre le port 520 UDP :**

L'inondation du port 520 est possible lorsque l'attaquant veut interrompre les échanges de route entre les routeurs.

3.6 Attaque visant OSPF

OSPF nécessite beaucoup de ressources pour effectuer les calculs de meilleur chemin. Cela permet à l'attaquant de causer l'instabilité en déclenchant périodiquement de faux changements. Pour réduire les échanges de routage, OSPF propose une structure hiérarchique qui permet de choisir un routeur principal. L'attaquant peut exploiter ce mécanisme d'élection pour devenir le routeur principal et modifier les routes sont :[28]

• **Tentatives pour être élu comme routeur principal :**

L'attaquant peut établir un faux routeur de haute et forces les routeurs à réélire le routeur principal (par un Dos vers le routeur principal courant). Après avoir gagné l'élection, l'attaquant peut modifier les informations de routage comme ce qu'il veut.

• **Insertion de fausse route :**

L'attaquant peut effectuer un Dos en mettant une grande valeur de séquence ou en envoyant de faux messages LSAs qui forcent les routeurs OSPF à renvoyer les LSAs afin de saturer les ressources. Il peut aussi injecter un faux chemin avec le numéro de séquence maximal, ce qui ne permet pas au routeur d'origine de ce chemin de corriger le problème.

Les protocoles de sécurité

3.7 VTP (Virtual Trunking Protocol)

L'une des principales difficultés d'un réseau qui utilise les réseaux VLANs réside dans la maintenance de la configuration VLAN à travers les différents commutateurs utilisés, sans point central de configuration et de maintenance des informations VLANs. L'administrateur réseau doit configurer les VLANs sur chaque commutateur séparément ce qui consomme du temps et prolonge les délais de dysfonctionnement de réseau en cas de pannes. De ce fait, pour résoudre ce problème, CISCO a proposé le protocole de liaison VTP. [29]

3.7.1 Concept d'agrégation

Une agrégation est une connexion physique et logique entre deux commutateurs par lesquels le trafic réseau est acheminé. Il s'agit d'un canal de transmission simple entre deux points. Ces points sont généralement des centres de commutation. Dans le contexte d'un environnement de commutation VLAN, une agrégation de VLAN est une liaison point-à-point physique ou logique qui prend en charge plusieurs VLAN. L'objectif d'une agrégation de VLAN est d'économiser des ports lors de la création d'une liaison entre deux unités contenant des VLANs La figure 3.2 illustre deux VLAN répartis sur deux commutateurs (Sa et Sb). Chaque commutateur utilise deux liaisons physiques, de sorte que chaque port transporte le trafic d'un VLAN unique. Il s'agit de la méthode la plus simple de mise en œuvre d'une communication VLAN entre commutateurs, mais elle n'offre pas une évolutivité suffisante. [30]

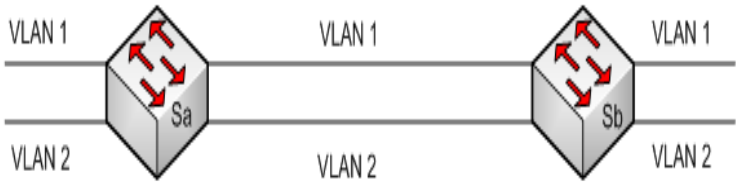

FIG. 3.2 – Mise en œuvre de communication sans le concept d'agrégation

L'ajout d'un troisième VLAN nécessite l'utilisation de deux ports additionnels, un pour chaque commutateur connecté. Cette configuration est également inefficace en termes de partage de charges. De plus, le trafic sur certains VLAN peut ne pas

justifier une liaison dédiée. Le concept d'agrégation de VLAN consiste à regrouper plusieurs liaisons virtuelles sur une liaison physique unique en permettant la transmission du trafic de plusieurs VLAN sur un câble unique entre les commutateurs (figure 3.3). [30]

FIG. 3.3 – Mise en œuvre de communication avec le concept d'agrégation

3.7.2 protocole VTP

Le rôle de VTP est de maintenir la cohérence de la configuration VLAN sur un domaine d'administration réseau commun. VTP est un protocole de messagerie qui utilise les trames d'agrégation de couche 2 pour gérer l'ajout, la suppression et l'attribution de nouveaux noms aux VLAN sur un domaine unique. De plus, VTP autorise les chargements centralisés qui sont communiqués à tous les autres commutateurs de réseau. Les messages VTP sont encapsulés dans des trames de protocoles Cisco ISL (figure 3.4) ou IEEE 802.1Q (figure 3.5), puis transmis sur des liens multi-VLAN autres unités. Dans les trames IEEE 802.1Q, un champ sur 4 octets est ajouté pour étiqueter les trames. Les deux formats transportent l'ID du VLAN. Alors que les ports de commutateur sont normalement à un seul VLAN, les ports multi-VLAN transportent, par défaut les trames de tous les VLAN. [30]

• **Structure des trames ISL**

Les trames ISL comprennent trois champs principaux :[31]

1.Un en-tête qui est constituée de plusieurs champs par exemple Type, User, Index.. ;

2.Trame encapsulé dont la longueur est comprise entre 1 et 24575 octets ;

3.Champ CRC, ce champ qui est ajoutée à la fin du paquet ISL, porte sur l'intégrité du paquet.

La figure ci-après illustre la structure d'une trame ISL :

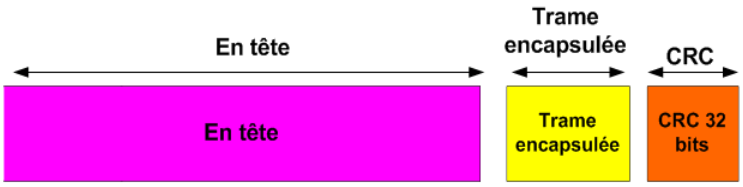

FIG. 3.4 – Format de Trame ISL.

• **Description de la norme**

La figure suivante illustre de la trame Ethernet.[32]

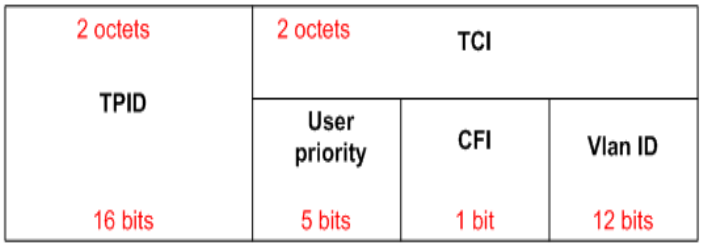

FIG. 3.5 – Détails du champ 802.1Q

1.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.

2.Tag Control Information (TCI)

Cette partie se compose de trois champs :[32]

• **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 on l'on ne fait qu'envoyer et recevoir des mails).

• **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 .

• **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.

3.7.2.1 Fonctionnement de VTP

Un commutateur doit alors être déclare en serveur, on lui attribut 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 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.

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants :[33]

• **Mode serveur**

Dans lequel le commutateur est chargé de diffuser la configuration aux commutateurs du domaine VTP.

• **Mode client VTP**

Dans lequel le commutateur applique la configuration émise par un commutateur en mode serveur

• **Mode transparent**

Dans lequel le commutateur ne fait que diffuser, sans prendre en compte, la configuration du domaine VTP auquel il appartient.

3.8 Le protocol STP (Spanning -Tree)

Le protocole Spanning-Tree est un protocole de couche 2 (liaison de données) conçu pour les switchs et les bridges. La spécification de STP est définie dans le document IEEE802.1Q [41]. Sa principale fonction est de s'assurer qu'il n'y a pas de boucles dans un contexte de liaisons redondantes entre des matériels de couche 2. STP détecte et désactive des boucles de réseau et fournit un mécanisme de liens de backup. Il permet de faire en sorte que des matériels compatibles avec le standard ne fournissent qu'un seul chemin entre deux stations d'extrémité. [33]

La figure 3.5 illustre un exemple de réseau avec une boucle :

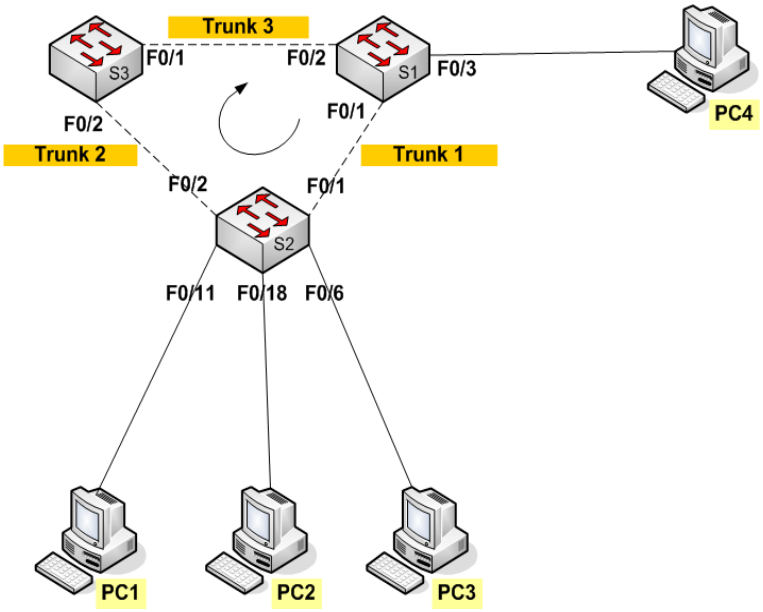

FIG. 3.6 – Réseau avec une boucle

Les ports qui génèrent des boucles sont automatiquement désactivés par le protocole Spanning-Tree (figure 3.6).

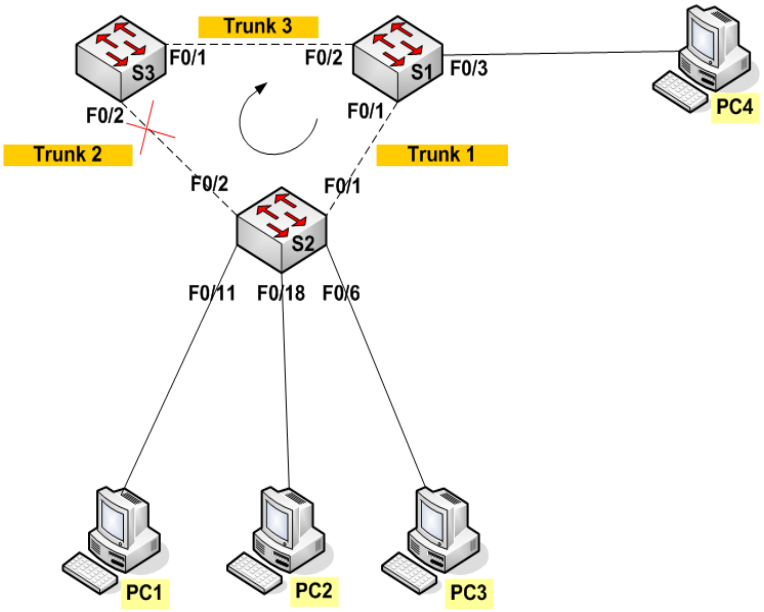

FIG. 3.7 – Désactivation d'un port avec le STP

3.8.1 Bridge Protocol Data Unit (BPDU)

Chaque commutateur a une adresse MAC et un numéro de priorité, la concaténation de ces deux nombre constitue l'identification du Bridge (BID). Les BIDs et autres informations du protocole Spanning Tree Protocol sont transportées dans des unités de trames de données spéciales nommées BPDU.

Les BPDUs sont échangés régulièrement (toutes les 2 secondes) et permettent aux ponts de garder une trace des changements sur le réseau afin d'activer ou de désactiver les ports requis. Quand un pont ou un bridge est raccordé au réseau, il ne va pas immédiatement commencer à transférer des donner Il va commencer par envoyer des BPDUs afin de déterminer la topologie du réseau.

Les BPDUs contiennent des informations de configuration sur le commutateur en train de transmettre des trames et ses ports, y compris le commutateur et l'adresse MAC du port, la priorité de commutateur, la priorité de port et le coût du port. Chaque configuration BPDU contient les informations suivantes :[33]

- l'identifiant du pont émetteur ;

- **l**'identifiant du port d'émission ;
- **l**'identifiant du pont que l'émetteur considère comme "Root-Bridge " ;
- **l**e coût pour joindre le Root-Bridge par rapport au port émetteur.

3.8.2 Topologie de STP

Afin d'établir une topologie, le processus Spaning-Tree effectue les étapes suivantes : [33]

- **Désignation d'un pont racine (Root-Bridge)**

Pour qu'un commutateur soit défini comme racine, les commutateurs (où le protocole STP est activé), vont s'échanger des trames BPDUs (Bridge Protocol Data Unit) afin de trouver quel pont a un BID le plus faible du réseau. Une fois trouvé, le commutateur ayant le plus faible BID devient un pont racine. Si le BID est le même pour les différents commutateurs, alors la comparaison se fera au niveau de l'adresse MAC.

- **Désignation des ports racines (Root-Port)**

Un port racine est un port qui sera utilisé pour transmettre les données. Chaque commutateur doit avoir un seul port racine qui sera désigné après le calcule de la distance la plus courte (où le coût le plus bas) vers le pont racine.

- **Désignation des ports désignés et non désignés**

Un port désigné est un port qui transfère le trafic au pont racine. Afin de définir les ports désignés et non désignés, les ports qui ne sont pas utilisés sont encore une fois analysés. C'est-à-dire, chaque commutateur va envoyer des trames BPDU et les BID les plus faibles seront les ports désignés et les plus forts seront les non désignés. Les non désignés vont donc permettre de ne pas avoir de boucles et la seule autorisation est celle des trames BPDU qui vont permettre au cas où un lien devient indisponible de reconfigurer un autre chemin (d'où l redondance).

La figure suivante présente un exemple d'un réseau après la configuration du protocole Spanning-Tree :

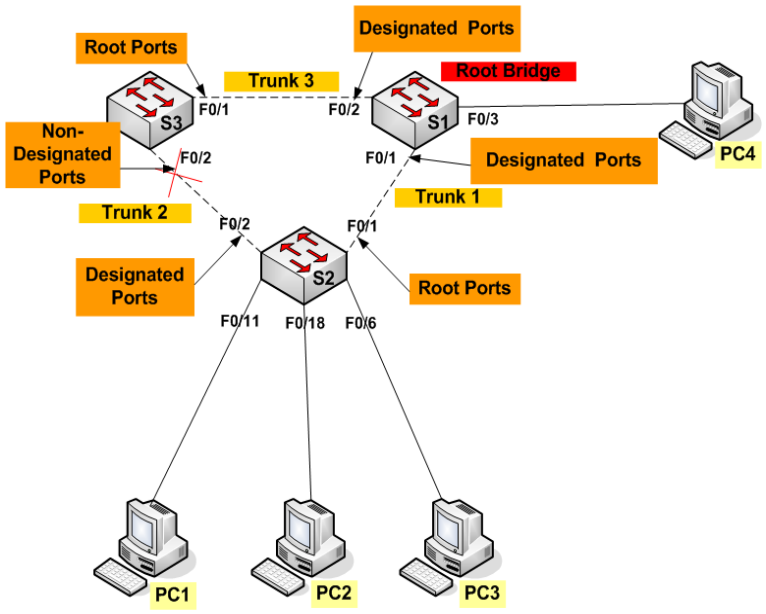

FIG. 3.8 – Gestion des ports par le protocole STP

3.9 Protocole HSRP

HSRP ou " Hot Standby Routing Protocol " est un protocole propriétaire Cisco qui a pour fonction d'accroitre la haute disponibilité dans un réseau par une tolérance aux pannes. [34]

3.9.1 Fonctionnement HSRP

HSRP est un protocole propriétaire crée par Cisco et très utilisé aujourd'hui dans nos LAN.

En pratique, HSRP permet :[34][35]

Qu'un routeur de secours (ou spare) prenne immédiatement, de façon transparente, le relais dès qu'un problème physique apparaît.

En partageant une seule même adresse IP et MAC, plusieurs routeurs peuvent être considérés comme un seul routeur Virtuel. Les membres du groupe de ce routeur virtuel sont capables de s'échanger des messages d'état et des informations.

Un routeur physique peut donc être responsable du routage et un autre en redondance.

Si le routeur, que nous appellerons primaire, a un problème, le routeur secondaire prendra sa place automatiquement. Les paquets continueront de transiter de façon transparente car les 2 routeurs partagent les mêmes adresses IP et MAC.

Un groupe de routeur va négocier au sein d'un même groupe HSRP (ou standby group), un routeur primaire (Active router), élu au moyen d'une priorité, pour transmettre les paquets envoyés au routeur virtuel.

Un autre routeur, le routeur secondaire (Standby router), sera élu lui aussi afin de remplacer le routeur primaire en cas de problème. Le secondaire assumera donc la tâche de transmettre les paquets à la place du primaire en cas de défaillance.

Le processus d'élection se déroule pendant la mise en place des liens, une fois ce processus terminé, seul le routeur primaire (Active) va envoyer des messages multicast en UDP périodiques HSRP aux autres afin de minimiser le trafic réseau.

Si ces messages ne sont plus reçus par le routeur secondaire (Standby), c'est que le routeur primaire à un problème et le secondaire devient donc Actif. L'élection se fait un peu à la manière de spanning-tree, en prenant en compte une priorité. Cette priorité est composée d'un paramètre " priority " compris entre 1 et 255 (255 étant le plus prioritaire) et de l'adresse IP de l'interface.

A priorités statiques égales, la plus haute adresse IP sera élue. Plusieurs groupes HSRP peuvent exister au sein d'un même routeur sans que cela ne pose problème. Seuls les routeurs du même numéro de groupe s'échangeront les messages HSRP.

3.10 Le protocole DHCP

DHCP signifie Dynamic Host Configuration Protocol. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau d'obtenir dynamiquement (c'est-à-dire sans intervention particulière) sa configuration (principalement, sa configuration réseau). Vous n'avez qu'à spécifier à l'ordinateur de se trouver une adresse IP tout seul par DHCP. Le but principal étant la simplification de l'administration d'un réseau.

Le protocole DHCP sert principalement à distribuer des adresses IP sur un réseau, mais il a été conçu au départ comme complément au protocole BOOTP (Bootstrap Protocol) qui est utilisé par exemple lorsque l'on installe une machine à travers un réseau (BOOTP est utilisé en étroite collaboration avec un serveur TFTP sur lequel le client va trouver les fichiers à charger et à copier sur le disque dur). Un serveur DHCP peut renvoyer des paramètres BOOTP(Bootstrap Protocol)ou de configuration propres à un hôte donné.[36]

3.10.1 Fonctionnement du protocole DHCP

Il faut dans un premier temps un serveur DHCP qui distribue des adresses IP. Cette machine va servir de base pour toutes les requêtes DHCP, aussi elle doit avoir une adresse IP fixe.

Dans un réseau, on peut donc n'avoir qu'une seule machine avec adresse IP fixe, le serveur DHCP.

Le mécanisme de base de la communication est BOOTP (avec trame UDP). Quand une machine est démarrée, elle n'a aucune information sur sa configuration réseau, et surtout, l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP. Pour faire ça, la technique utilisée est le broadcast : pour trouver et dialoguer avec un serveur DHCP, la machine va simplement émettre un paquet spécial de broadcast (broadcast sur 255.255.255.255 avec d'autres informations comme le type de requête, les ports de connexion...) sur le réseau local. Lorsque le serveur DHCP recevra le paquet de broadcast, il renverra un autre paquet de broadcast contenant toutes les informations requises pour le client.[36]

3.11 Conclusion

Ce chapitre comprend deux parties, dont nous avons essayé de clarifier, d'une part les protocoles de routage RIP, et OSPF, les attaques visant chacun de ces protocoles et d'autre part les protocoles de sécurité VTP, STP, DHCP, et HSRP, leur configuration au sein de réseau informatique, cette étude nous facilitera la tâche de configuration pour entamer directement la simulation du réseau de l'entreprise SONATRACH avec le simulateur Packet Tracer, qui sera l'objet de chapitre suivant.

Chapitre 4

Planification et Réalisation

4.1 Introduction

Dans le but d'illustrer et de compléter ce qui a été traité dans la partie théorique de notre mémoire, plus exactement dans deuxième et troisième chapitres, nous faisons une simulation de réseau informatique de l'entreprise SONATRACH, en commençant par une étude de l'existant puis en configurant sur ce dernier les protocoles présentés dans le deuxième chapitre nous appliquons la sécurité des mises à jour de routage sur ces protocoles.

Dans ce chapitre, nous présentons le logiciel utilisé et l'environnement de travail ainsi que les différentes configurations utilisées, enfin nous donnerons les résultats obtenus de la configuration. .

4.2 Système d'exploitation pour l'interconnexion de réseaux (IOS)

IOS est l'architecture logicielle qui est incorporée dans tous les routeurs CISCO .ce système est muni d'une interface en ligne de commandes, propres aux équipements de CISCO Systems. [3]

4.2.1 Rôle du système d'exploitation(IOS)

Un routeur ou un commutateur ne peut pas fonctionner sans système d'exploitation, l'IOS est une technologie centrale qui s'étend pratiquement tous les produits CISCO.son fonctionnement peut varier les unités d'interconnexion de réseaux sur

lesquelles il utilisé. L'IOS fournit les services réseau suivants [37] :

- Fonctions de routage et de commutation de base ;
- Accès faible et sécurisé aux ressources en réseau ;
- Evolutivité du réseau.

Pour accéder aux services fournis par IOS, en utilisant généralement une interface de ligne de commande (ILC).les fonctions accessible à travers ILC selon la version de CISCO IOS et le type du périphérique.[38]

4.2.2 Configuration de base d'un routeur CISCO

La configuration de base d'un routeur CISCO se fait en générale via porte console. Ce dernier, sur un routeur, est configuré comme une interface DTE (Data Terminal Equipement).les lignes de configuration d'un routeur apparaît dans la figure ci-dessus

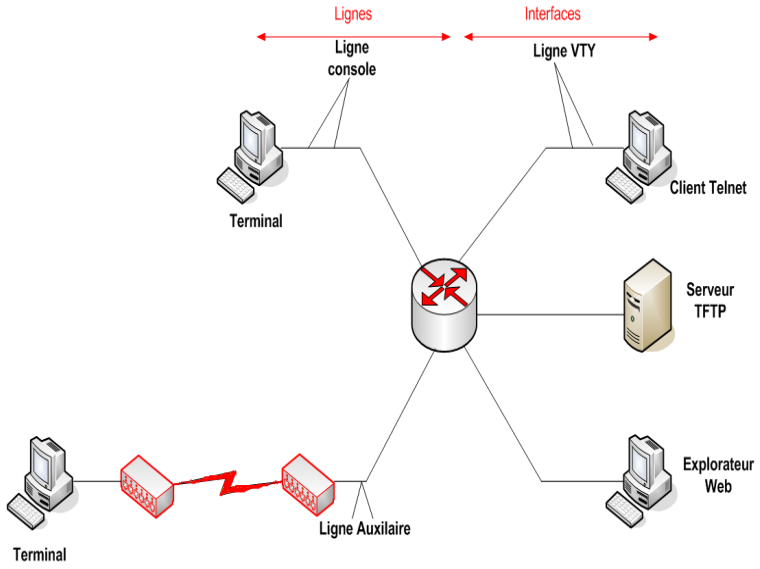

FIG. 4.1 – Lignes configuration routeur.

Un routeur peut être configuré à partir des sources externes suivantes :

-Ligne console : accès primaire, à utiliser si aucun autre accès de configuration n'est disponible.

-Ligne auxiliaire : accès à distance via une liaison RTC et modems interposés.

-Ligne(s) VTP : accès via un client Telnet.

• **Configuration du nom d'hôte IOS :**

Pour configurer un nom d'hôte IOS en utilisant les commandes suivantes :

-Router ♯ line console 0 pour accéder au mode de configuration globale.

-Router (config) ♯ hostname R1 : pour entrer le nom d'hôte.

-R1 (config) ♯ exit : pour quitter le mode de configuration globale.

• **Configuration des interfaces du routeur**

-R1 ♯ config t : Passez en mode de configuration globale.

-R1 (config) ♯ interface Serial0/0 : passez au mode de configuration d'interface en indiquant le type et le numéro d'interface.

-R1 (config-if) ♯ ip address 192.168.2.1 255.255.255.0 : Configurez l'adresse IP et le masque de sous-réseau.

• **Enregistrer les modifications apportées à un routeur**

R1 ♯ copy running-config startup-config : enregistre les modifications.

• **Vérifier des informations renvoyées par les commandes show**

R1♯ show running-config : Cette commande affiche la configuration en cours stockée dans la mémoire vive.

R1♯ show ip interface brief : Cette commande affiche des informations sommaires sur la configuration d'interface, notamment l'adresse IP et l'état de l'interface.

R1♯ show interfaces : Cette commande affiche tous les paramètres et toutes les statistiques de configuration d'interface.

• **Redémarage du routeur**

la commande **reload** (rechargement) permet de redémarrer le routeur sans configuration.

• **Vérifier les informations de routage**

R1♯show ip route : Cette commande affiche la table de routage actuellement utilisée par l'IOS pour choisir le meilleur chemin à emprunter afin d'atteindre les réseaux de destination.

R1♯show ip interface brief : Cette commande affiche des informations sommaires sur la configuration d'interface, notamment l'adresse IP et l'état de l'interface.

• **Commande de configuration des protocoles de routage dynamique**

Pour configurer les protocoles de routage, en utilisant les commandes suivantes :

Configuration de RIP V2

Les commandes liées à la configuration du protocole RIP sont :

R1 (config)♯router rip : permet d'activer le protocole RIP.

R1 (config-router)♯version : la version de RIP.

R1 (config-router)♯network adresse réseau : une fois le protocole RIP est activé on peut déclarer les réseaux directement connectés.

R1 (config)♯no router RIP : pour désactiver RIP.

• **Configuration de protocole OSPF**

Les commandes utilisées pour la configuration du protocole OSPF sont :

R1 (config)♯router OSPF id-processus : pour activer le routage OSPF.

R1 (config-router)♯ network @-IP-réseau masque-générique : adresse du routeur et le masque générique .

Area id-zone : pour indiquer les réseaux IP, le paramètre area indique le numéro de la zone.

• **Commande de route statique**

R1 (config)♯ip route adresse-réseau-distant masque-de-réseau @ IP du-routeur : permet la configurer une route statique.

R1 (config)♯ip route 0.0.0.0 0.0.0.0 @ IP du-routeur-de-saut-suivant : pour créer une route statique par défaut.

• **Configuration du protocole STP**

Les commandes suivantes nous permettent de configurer le Protocol STP en mode serveur :

Switch♯config terminal

Switch (config)♯Spanning-Tree mode rapide pvst

Switch (config)♯exit

• **Configuration du Protocol VTP**

Il existe deux mode : mode client et le mode serveur.

On utilise les commandes ci-dessous de configurer le Protocol VTP sur un switch :

Switch ♯configure terminal.

Switch (config)♯ vtp domain nom-domaine.
Switch (config)♯vtp mode server/client.
Switch (config)♯ mode version id-version.
Switch (config)♯ exit.

• **Configuration d'HSRP**

Voici la liste des commandes permettant d'implémenter et maîtriser le protocole HSRP :[39]

La commande **"standby priority xxx"** définit une priorité au routeur. Celui qui possédera la plus grande valeur sera élus actif. Si la configuration du routeur ne stipule pas la priorité, alors la valeur par défaut de 100 sera appliquée.

La commande **"standby preempt"** permet d'accélérer le processus d'élection.

La commande **"standby ip xxx.xxx.xxx.xxx"** indique l'adresse IP virtuelle partagée entre les deux routeurs.

4.3 Présentation "packet tracer"

CISCO propose des outils de simulation des réseaux de simulation et capture de trafique nommé le packet tracer [40]

Le logiciel Packet Tracer est un simulateur de réseau qui permet de configurer les différents composants d'un réseau informatique sans avoir à utiliser les appareils réels la figure 4.2 illustre la fenêtre principale du simulateur.

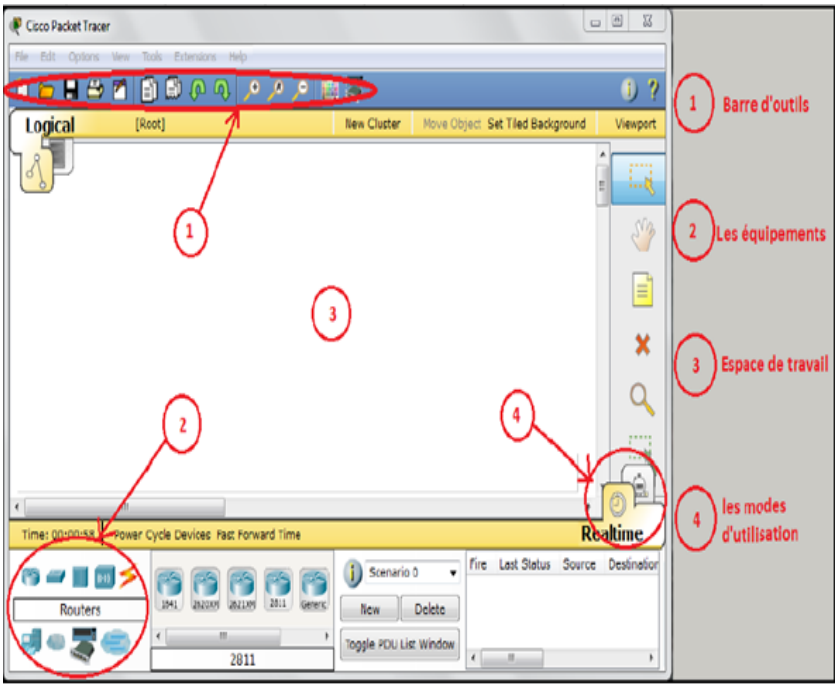

FIG. 4.2 – Cisco Packet Tracer

Les différents types d'appareils disponibles dans la boîte à outils de la zone 2 sont les suivants :

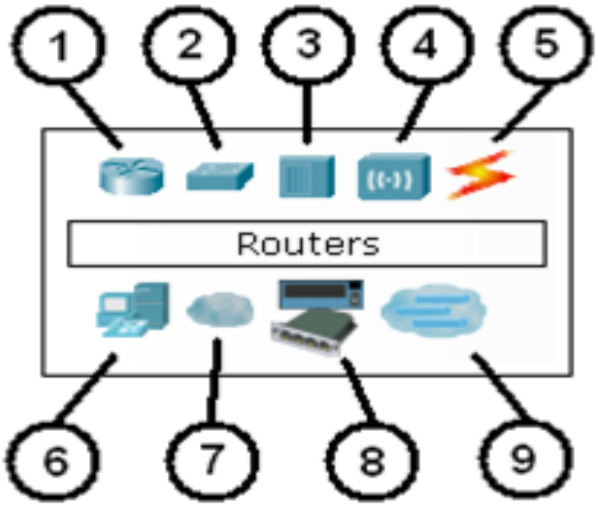

FIG. 4.3 – les différents types d'appareils

1. Les routeurs ;
2. Les commutateurs (switches) ;
3. Les concentrateurs (hubs) ;
4. Les bornes sans fil (wifi) ;
5. Les connexions ;
6. Les ordinateurs ;
7. Les réseaux étendus (wan) ;
8. Des appareils divers ;
9. Les connexions multi-usage.

4.4 Les VLANs du réseau de l'entreprise de sonatrach et leur 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 stations, se basera sur une adresse privée. Les machines affiliées à un VLAN, vont prendre toutes les adresses IP d'une même adresse sous-réseau. Les VLANs du réseau sounatrach sont : informatique, serveur, direction, HSE,LAN, wifi, salle.

Le tableau suivant présente les différents VLANs de l'entreprise de sounatrach.

Vlan	**Description**	**Adresse IP**	**Passerelle**
1	Par défaut	192.168.1.250/24	- - - -
10	Direction	192.168.10.0 /24	192.168.10.254 /24
20	Informatique	192.168.20.0 /24	192.168.20.254 /24
30	HSE	192.168.30.0 /24	192.168.30.254 /24
40	serveur	192.168.40.0 /24	192.168.40.254 /24
50	Salle	192.168.50.0 /24	192.168.50.254 /24
60	Manager	192.168.60.0 /24	192.168.60.254 /24
70	Les serveurs base de données	192.168.70.0 /24	192.168.70.254 /24

TAB. 4.1 – Plan d'adressage des VLANs

4.5 Structure générale du réseau de l'entreprise de SONATRACH

La figure suivant illustre la topologie physique de l'entreprise captée sous le simulateur packet Tracer.

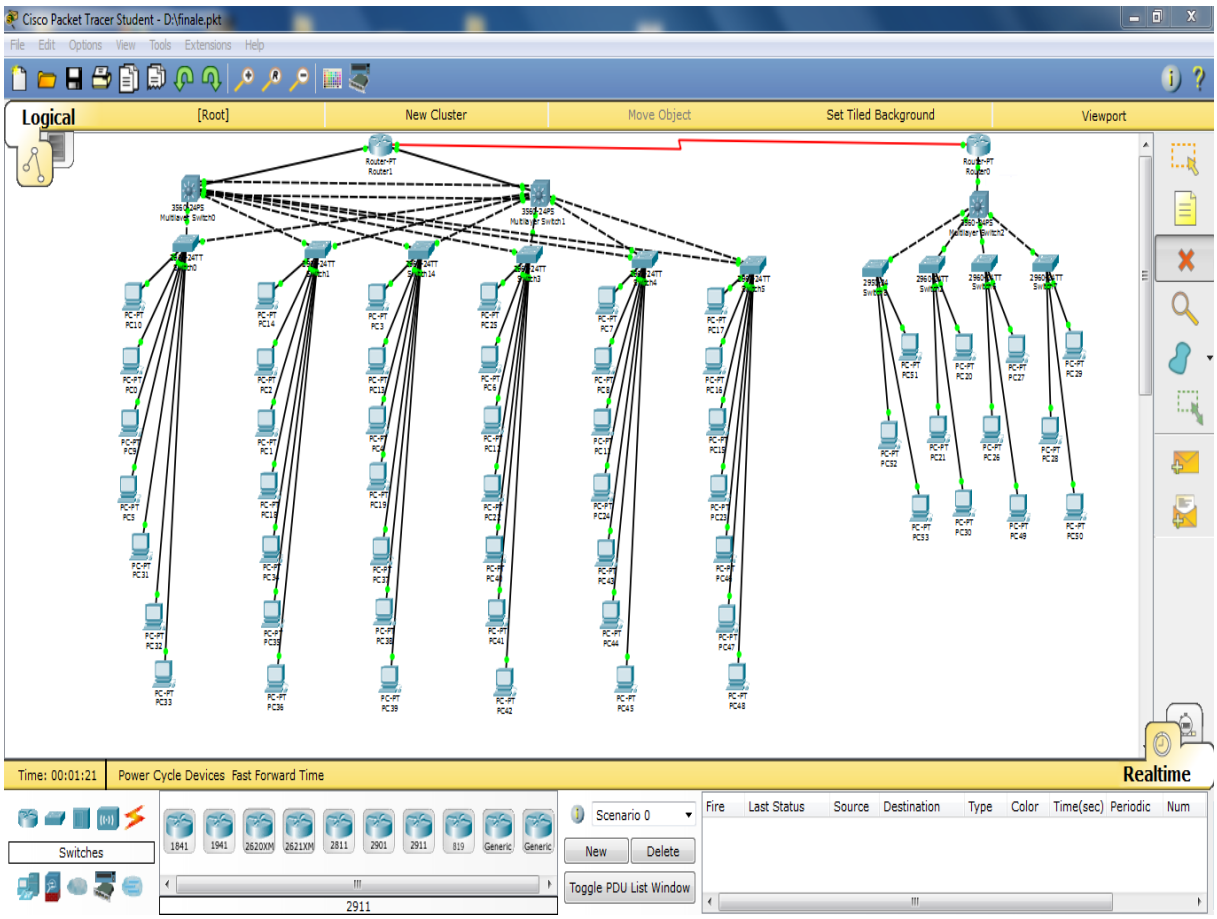

FIG. 4.4 – Structure générale de l'entreprise

4.6 Configuration des équipements

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

4.6.1 Sécuriser l'accès aux périphériques

Il faut s'avoir qu'IOS 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 différent privilèges d'accès au périphérique.

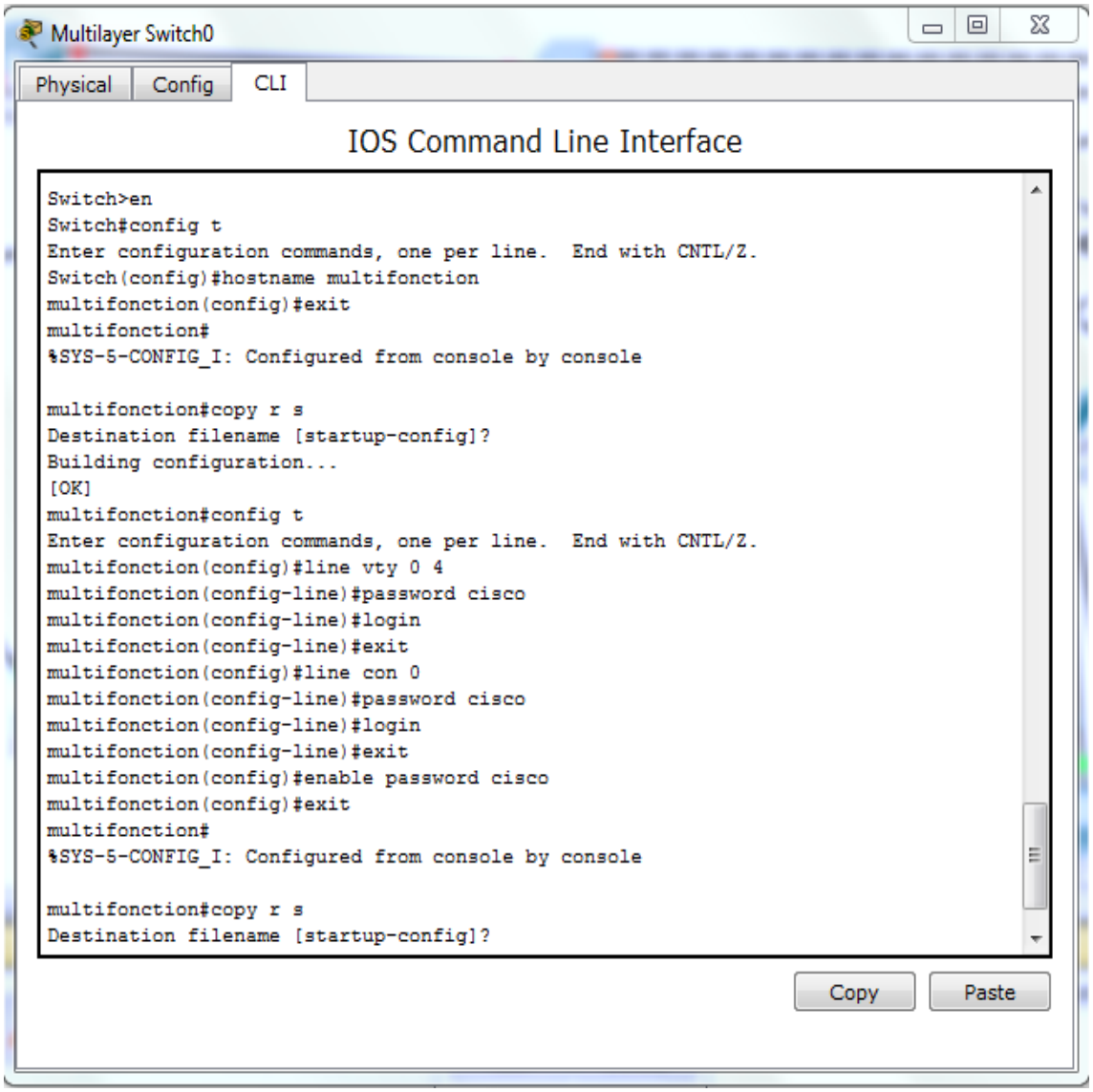

Fig. 4.5 – Configuration de mot de passe

La figure 4.6 permet de chiffrer le mot de passe

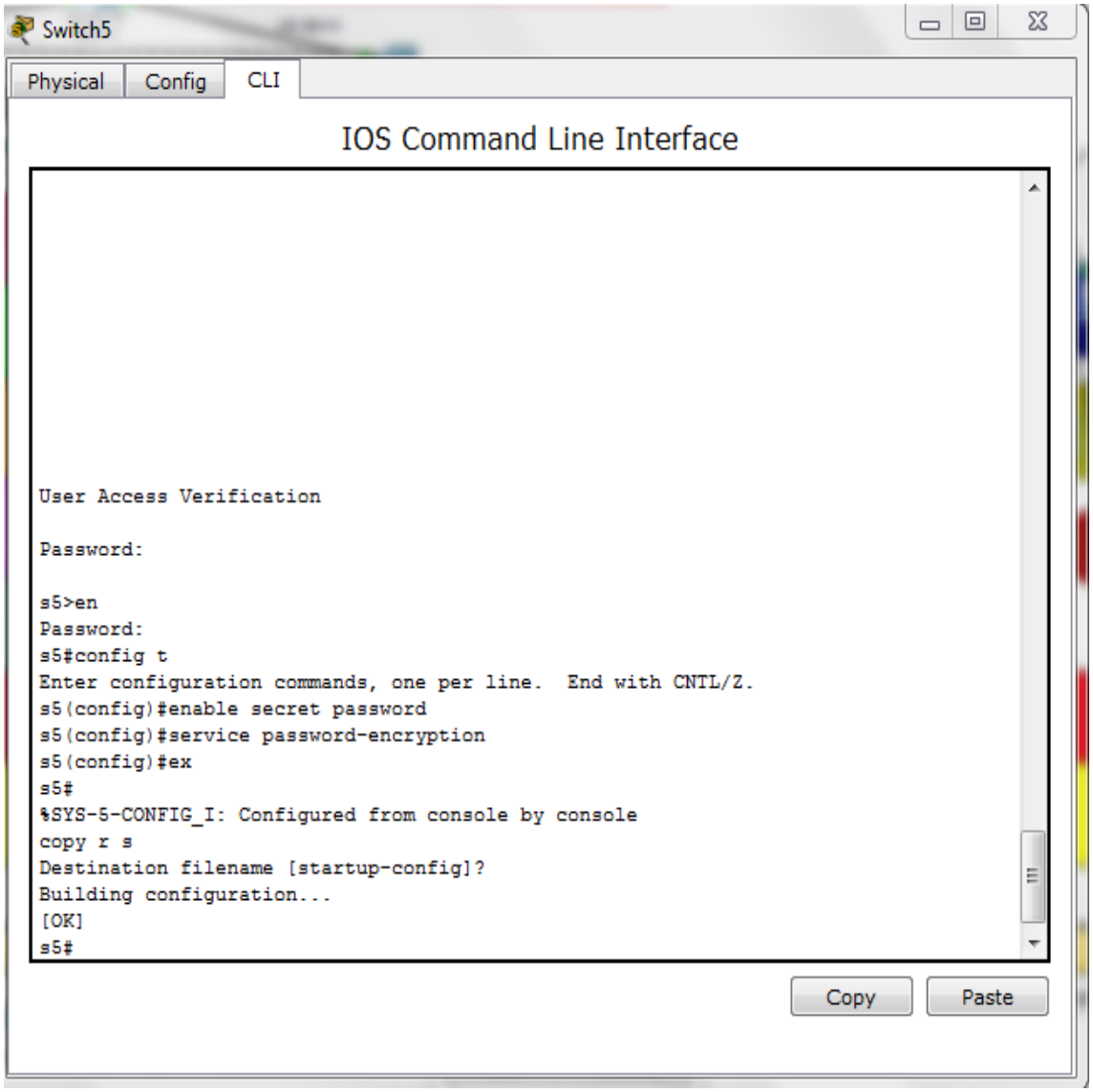

Fig. 4.6 – Crypter le mot de passe

4.6.2 Configuration des VLANs

La configuration des VLANs est faite au niveau des commutateurs dans le réseau, comme la montre la figure ci-dessus :

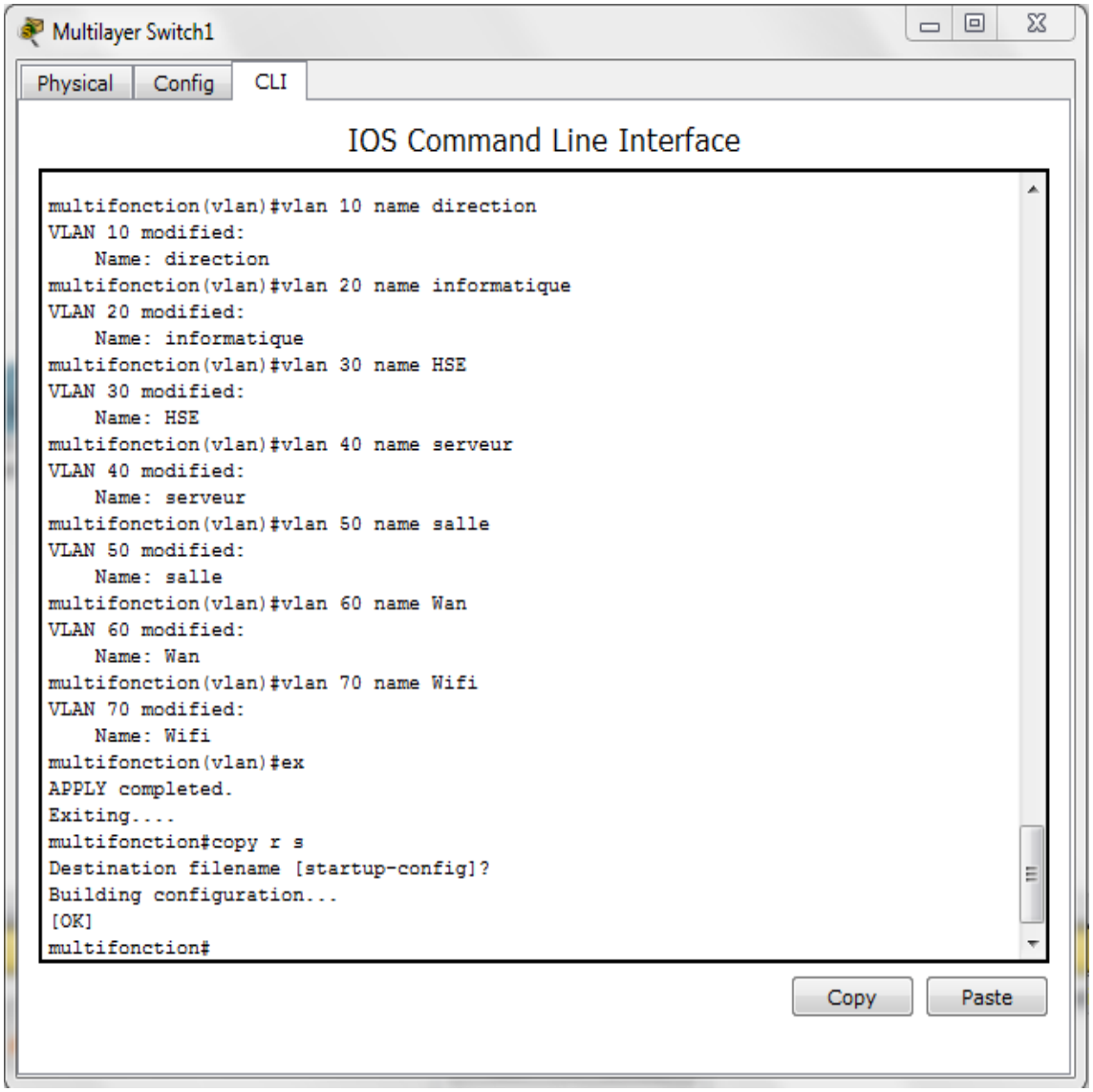

FIG. 4.7 – Création des VLANs

Il existe deux modes d'association d'un port au VLAN

• **Mode accès**

Les commandes suivantes nous permettent d'associer les ports au VLANs en mode Accès :

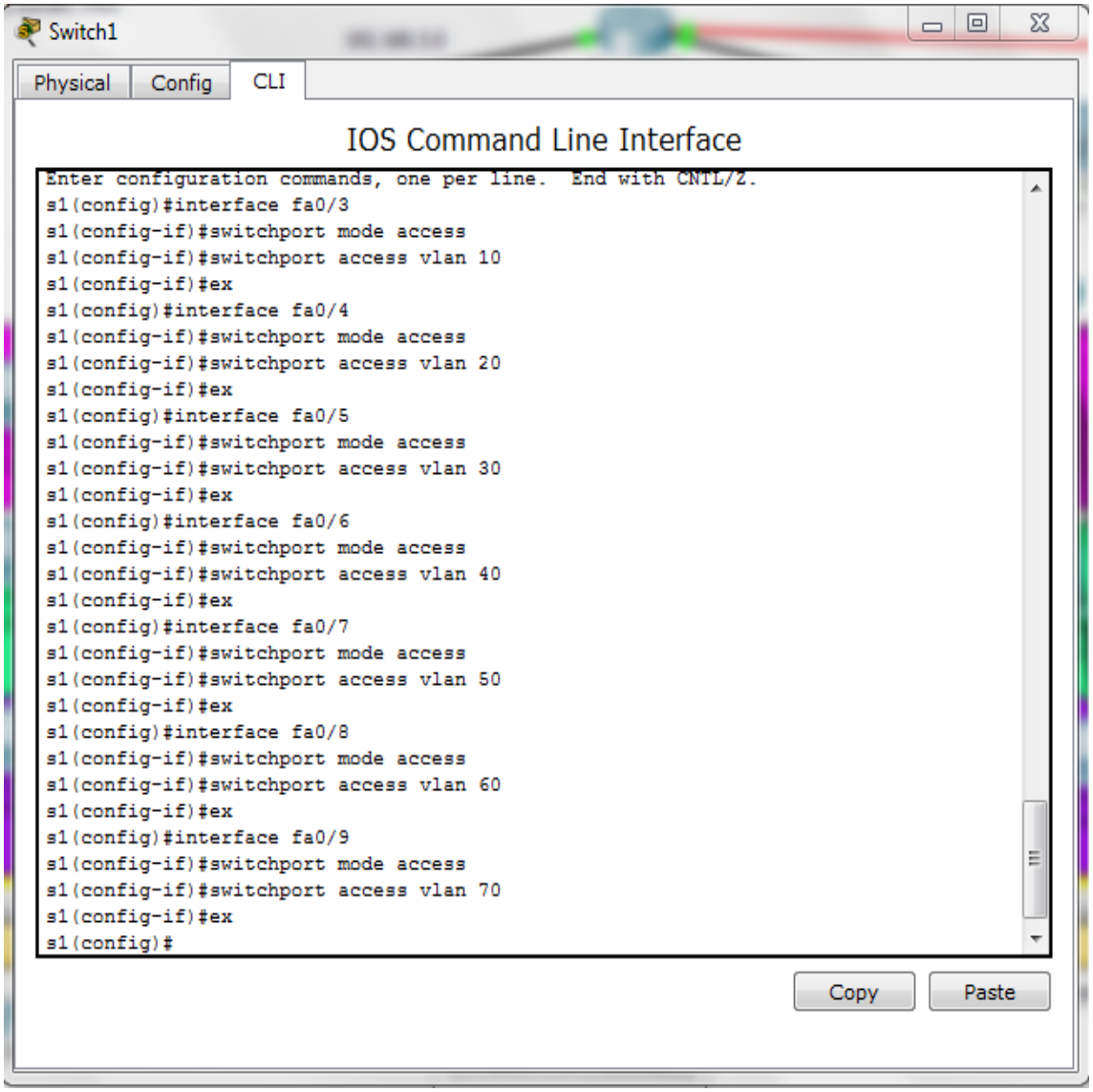

FIG. 4.8 – Attribution des ports aux VLANs

- **Mode Trunk**

Les interfaces des équipements d'interconnexion à configurer en mode trunk, existent toutes entre l'ensemble des commutateurs Accès et le commutateur multi-fonction.

Les commandes suivantes nous permettent d'associer les ports au VLANs en mode trunk :

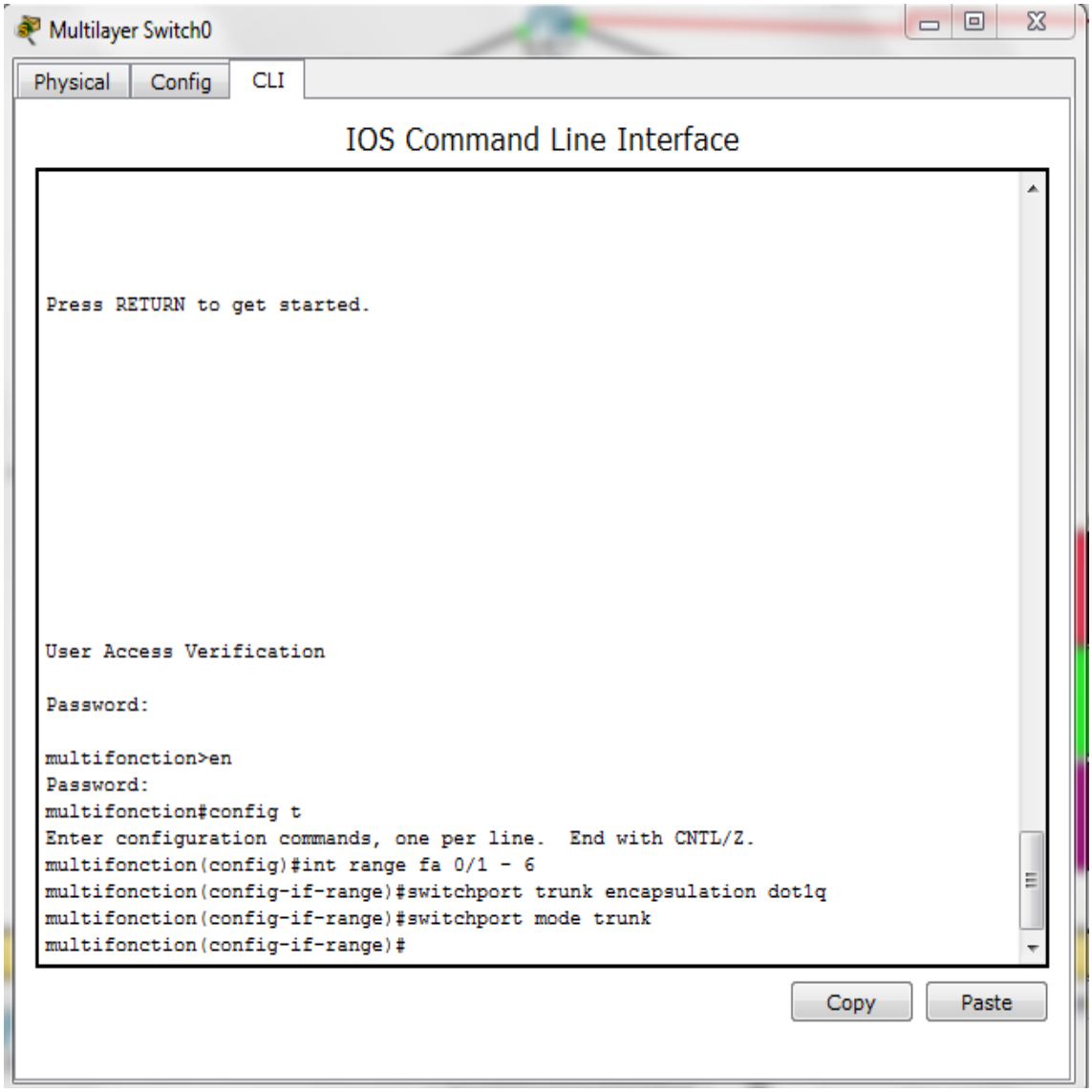

Fig. 4.9 – Configuration des liens Trunk

A travers ces étapes, nous avons réalisé une partie important de la configuration d'un réseau local intégrant des VLANs, voici l'architecture simulée du réseau de la RTC obtenue illustré dans la figure suivant :

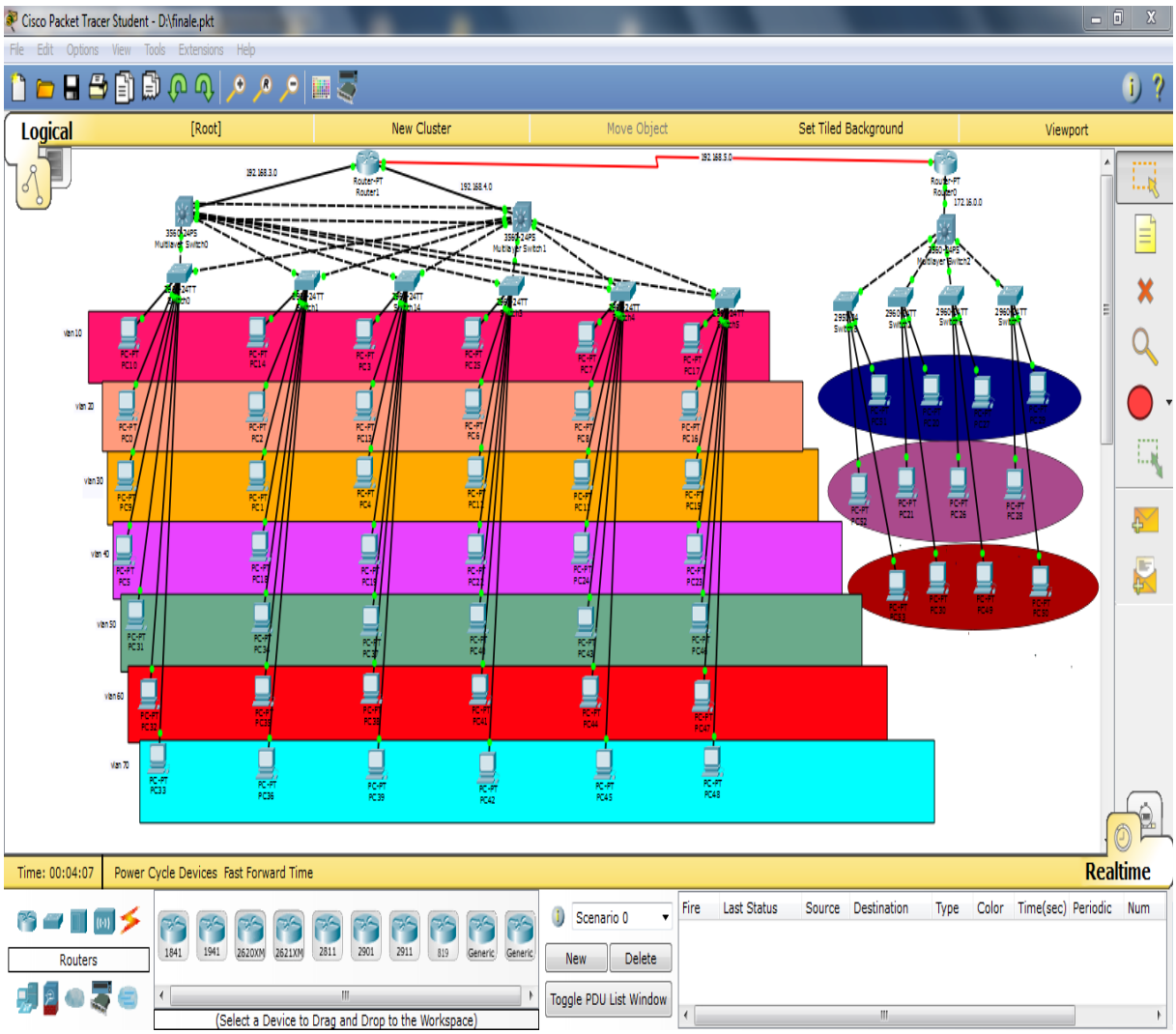

FIG. 4.10 – Architecture simulée du réseau de la RTC

4.6.3 Configuration du Protocole VTP

L'ensemble des commutateurs multifonction 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 ci-dessus représente la configuration du serveur VTP au niveau des Switchs multifonctions.

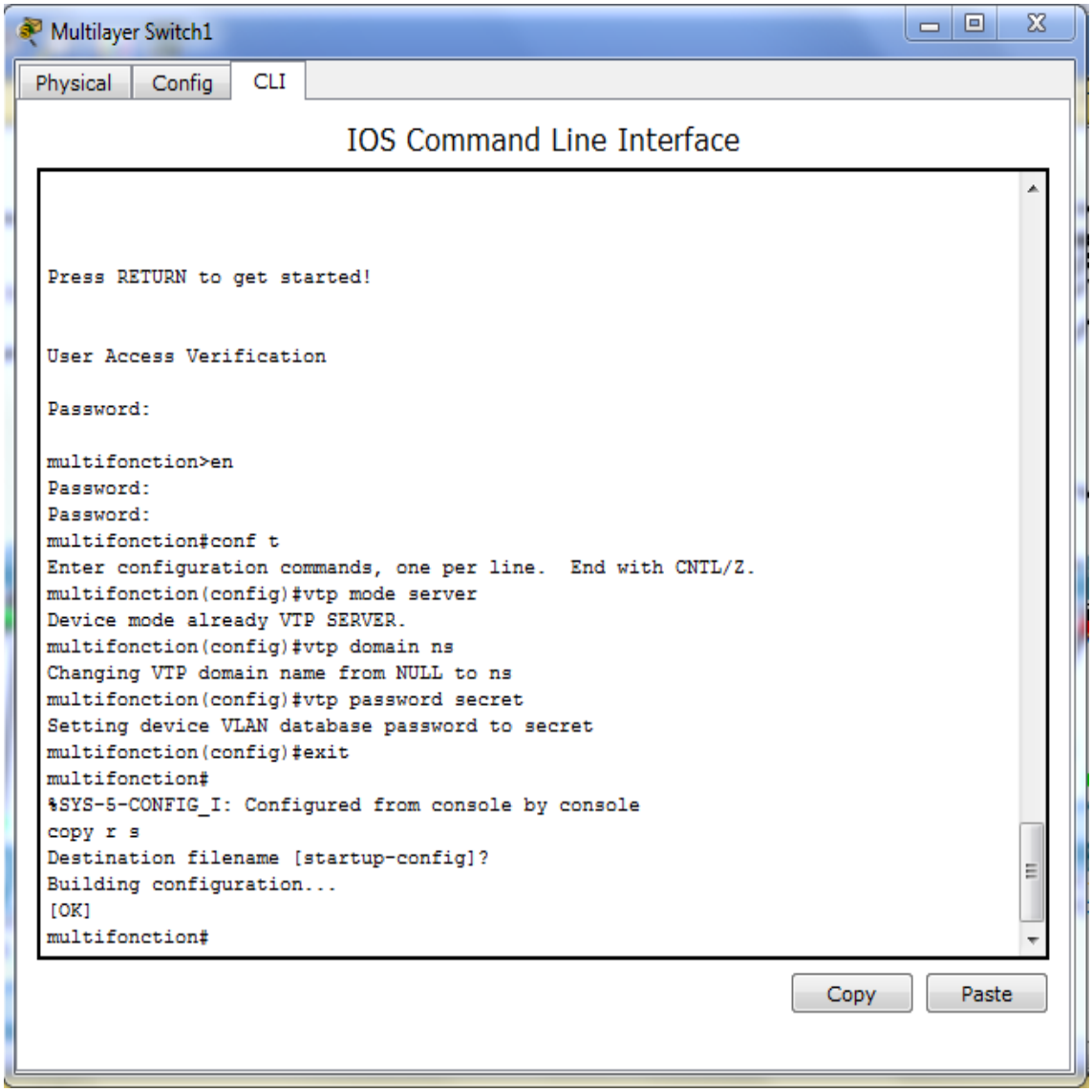

FIG. 4.11 – Configuration des VTP-serveur

Par ailleurs, la configuration des clients-VTP sera au niveau de tous les commutateurs Accès.

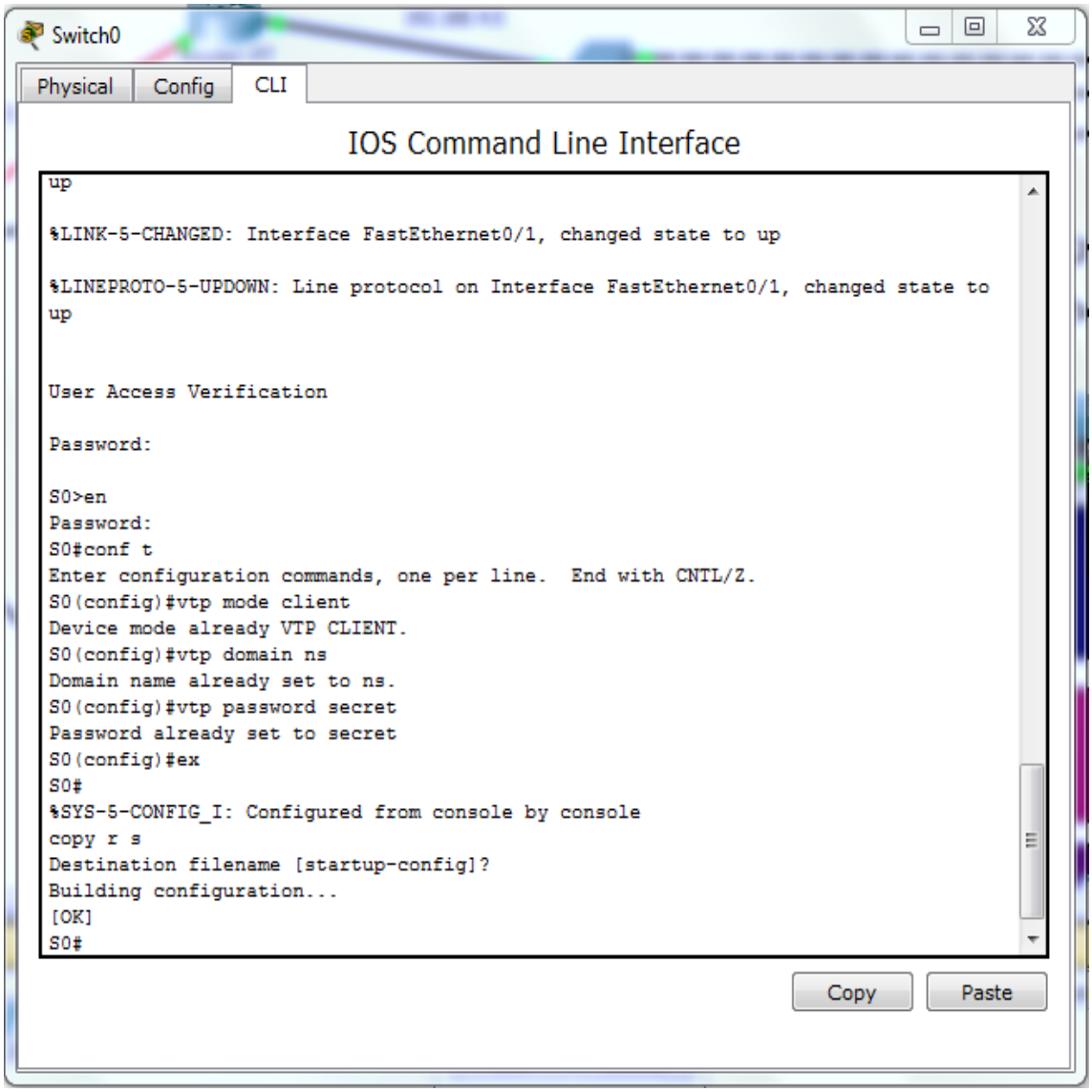

Fig. 4.12 – Configuration des VTP-client

4.6.4 Configuration de STP

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

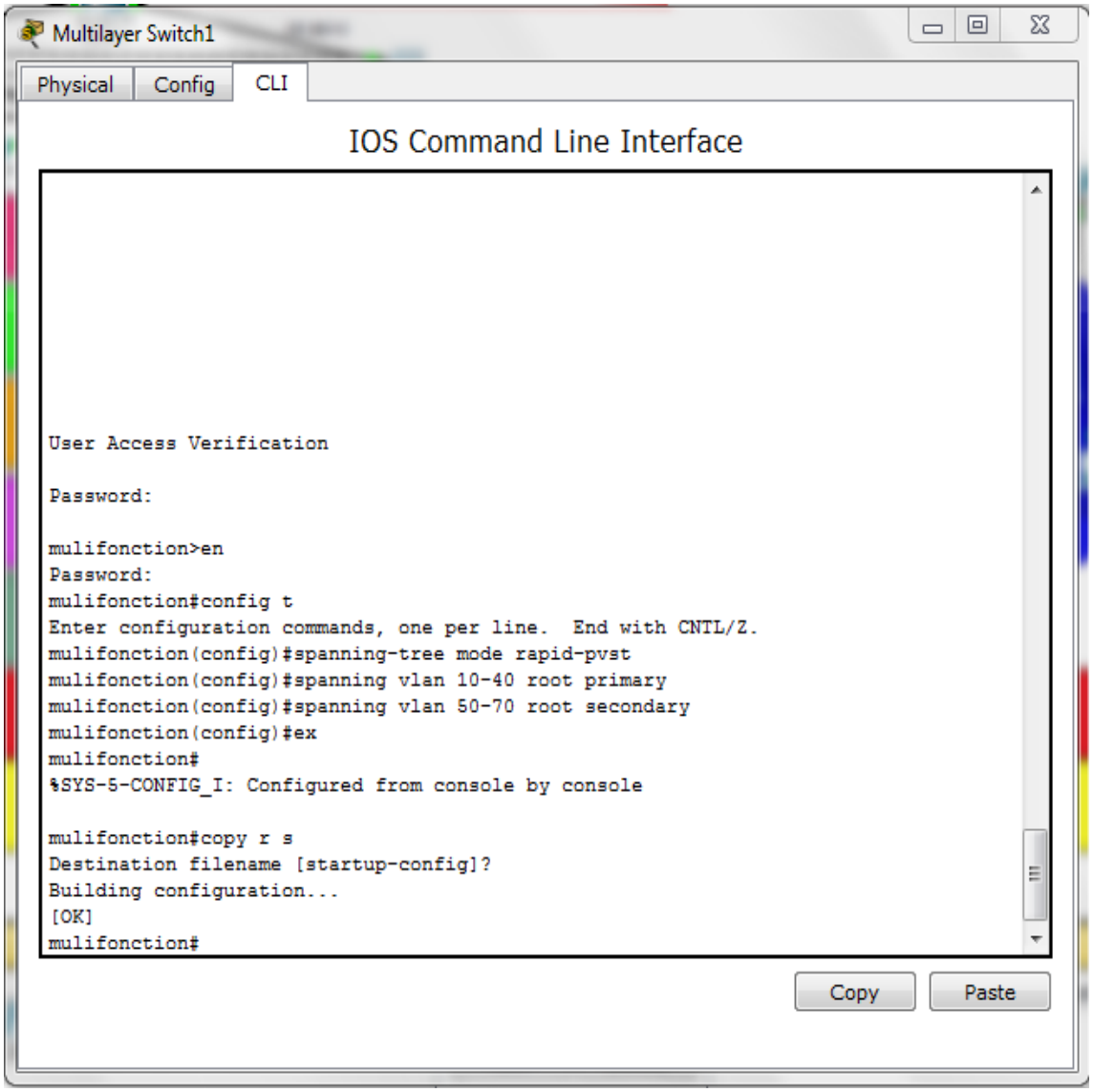

Fig. 4.13 – Configuration du STP

4.6.5 Configuration DHCP

Pour simplifier à l'administrateur la gestion et l'attribution des adresses IP, on utilise le protocole DHCP qui permet de configurer les paramètres réseaux client, au lieu de les configurer sur chaque ordinateur client.

La figure 4.13 illustre les commandes qui nous permettent de configurer ce protocole :

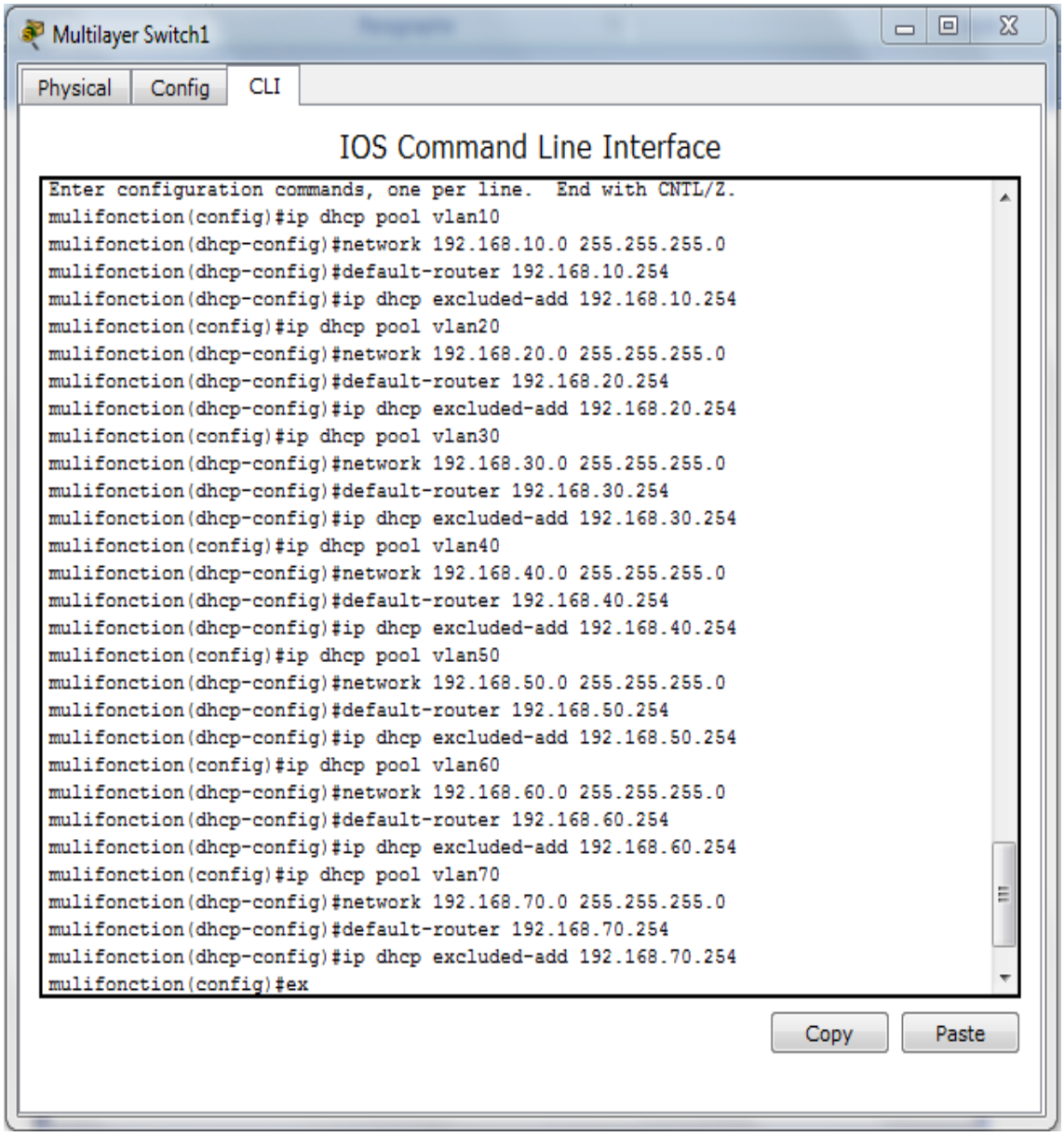

Fig. 4.14 – Configuration DHCP

4.6.6 Configuration HSRP

La figure ci-dessous montre les VLANs prioritaires par rapport aux VLANs secondaire sur l'un des Switchs multifonctions, et sur l'autre les priorités des VLANs seront renversées.

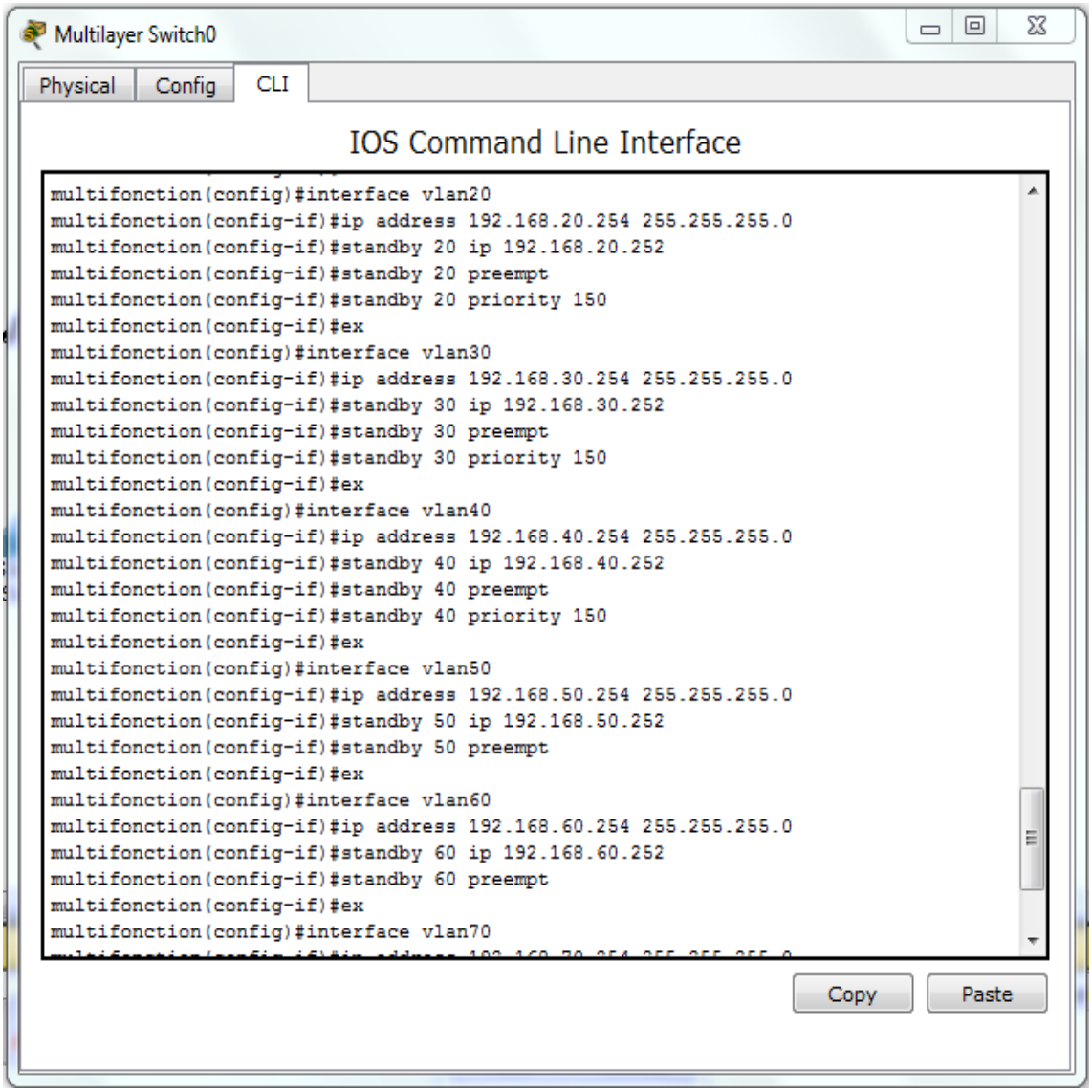

FIG. 4.15 – Configuration de HSRP

La figure 4.15 illustre le réseau local que nous avons réalisé dans le simulateur packet Tracer après la configuration des deux Switchs multifonction :

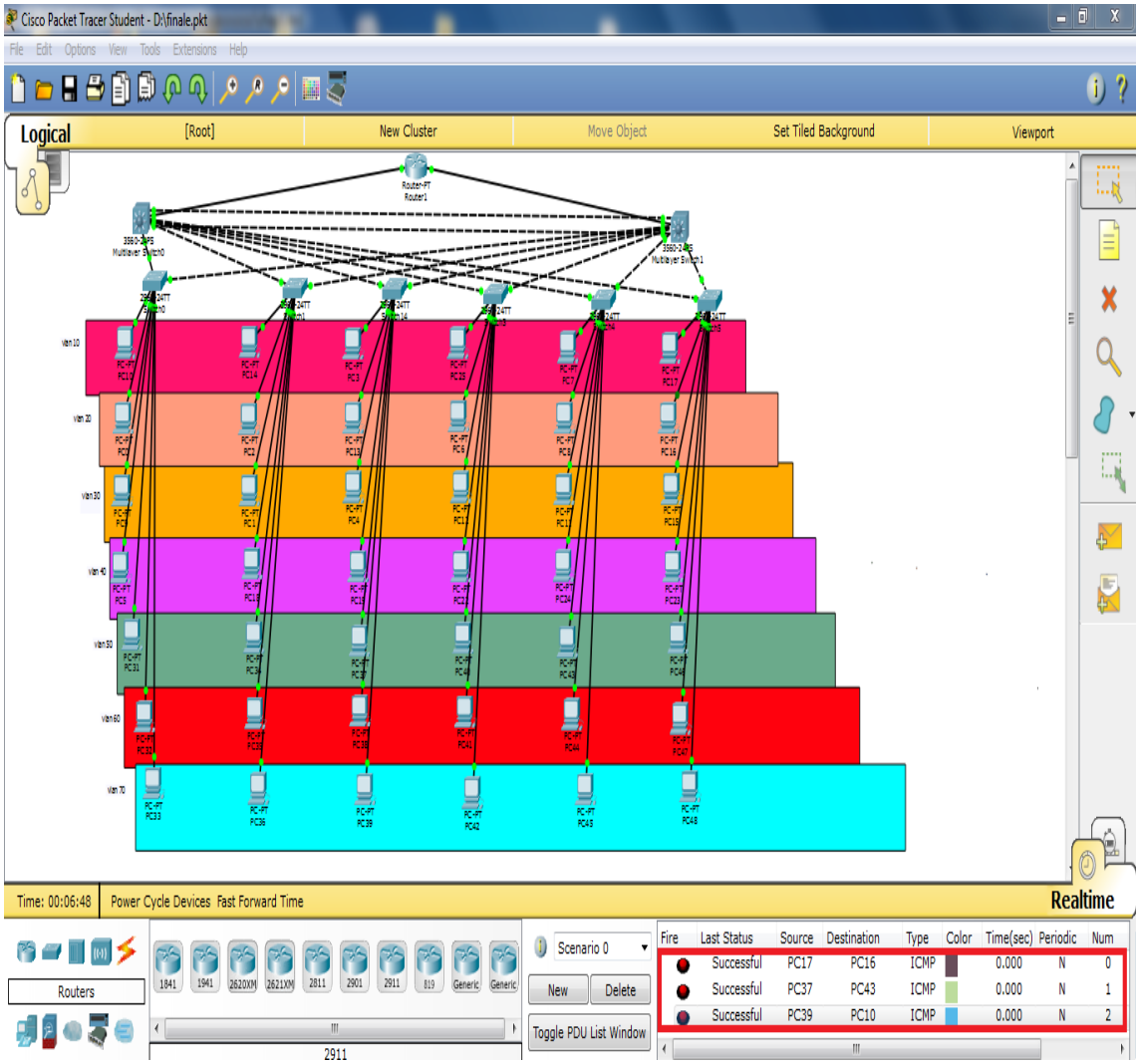

FIG. 4.16 – Réseau local après la configuration

4.6.7 Configuration RIP

L'implémentation de protocole RIP se fera au niveau de tous les routeurs et les Switchs multifonction.

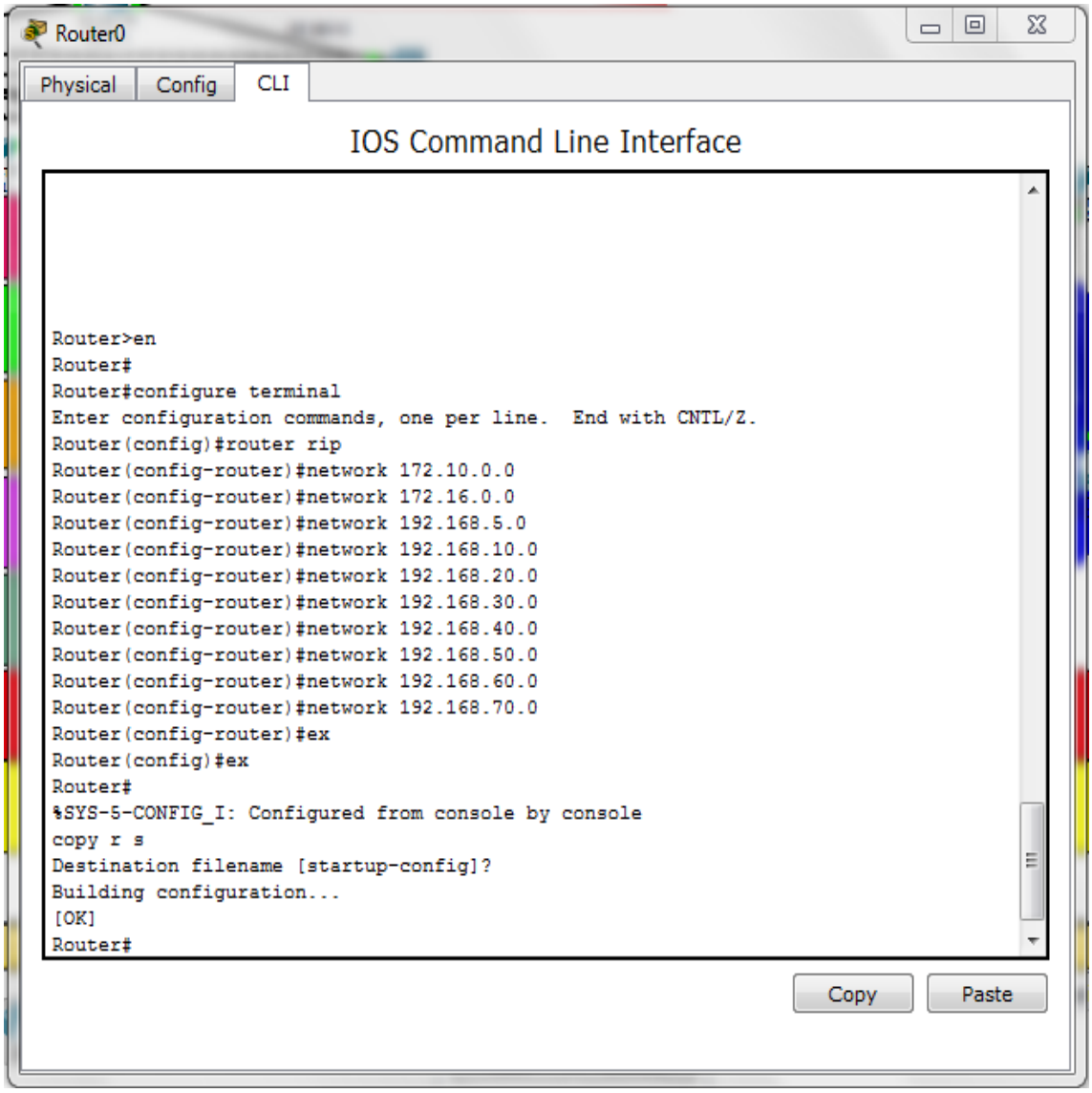

Fig. 4.17 – Configuration RIP au niveau du routeur

4.6.8 Configuration OSPF

La figure 4.18 permet la mise en place le protocole OSPF .

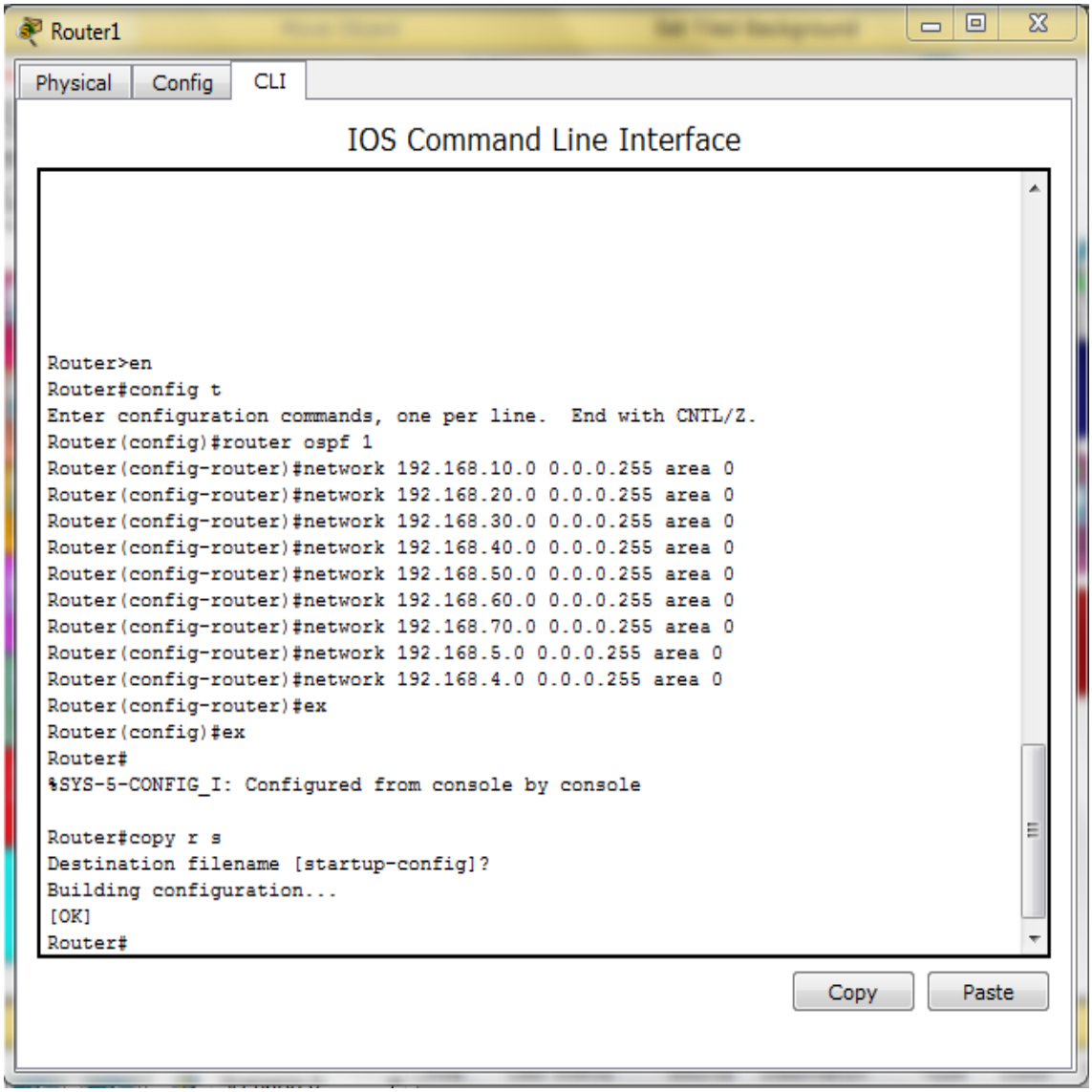

FIG. 4.18 – Configuration ospf

La figure ci-dessus montre la connexion du réseau que nous avons réalisé avec le réseau d'une autre station à l'aide du protocole de routage RIP.

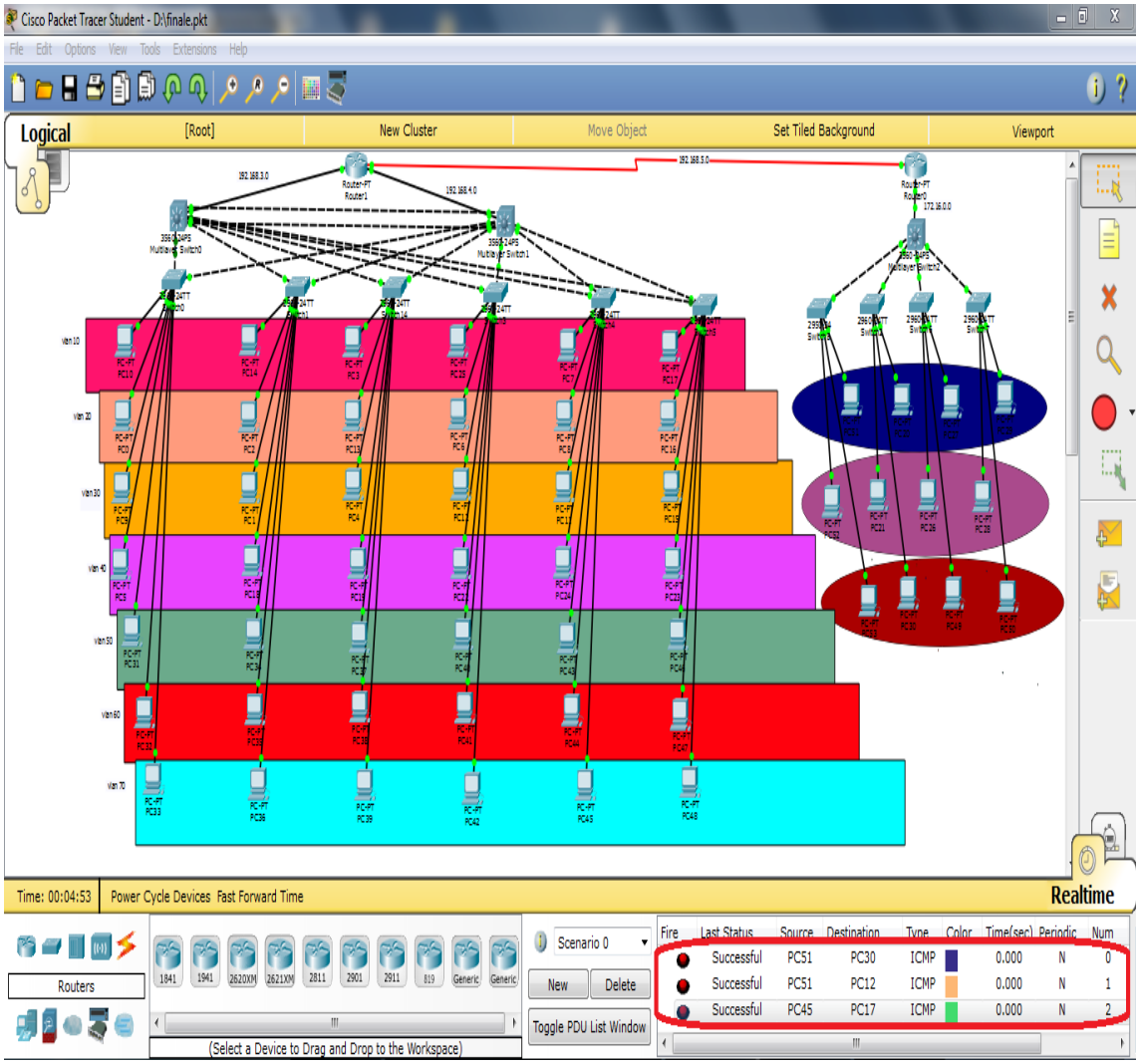

FIG. 4.19 – L'interconnexion de différents réseaux locaux

4.6.9 Liste de contrôle d'accès " Access Contrôle List "

✓Les listes de contrôle d'accès permettent de contrôler le trafic entrant et le trafic sortant d'un réseau. Ce contrôle est aussi simple qu'autoriser ou refuser les hôtes ou les adresses du réseau.

✓Une liste de contrôle d'accès est un scripte de configuration de routeur contrôlant l'autorisation " permit " ou le refus " deny " de passage des paquets.

✓Les listes de contrôle d'accès sont souvent utilisées dans les routeurs pare-feu entre le réseau interne et le réseau externe.

✓Pour les listes de contrôle d'accès entrant, les paquets entrant sont traités avant d'être routés vers l'interface de sortie.

✓Pour les listes de contrôle d'accès sortant, les paquets entrants sont traités après être routés vers l'interface de sortie.

La figure 4.19 illustre la configuration des ACLS

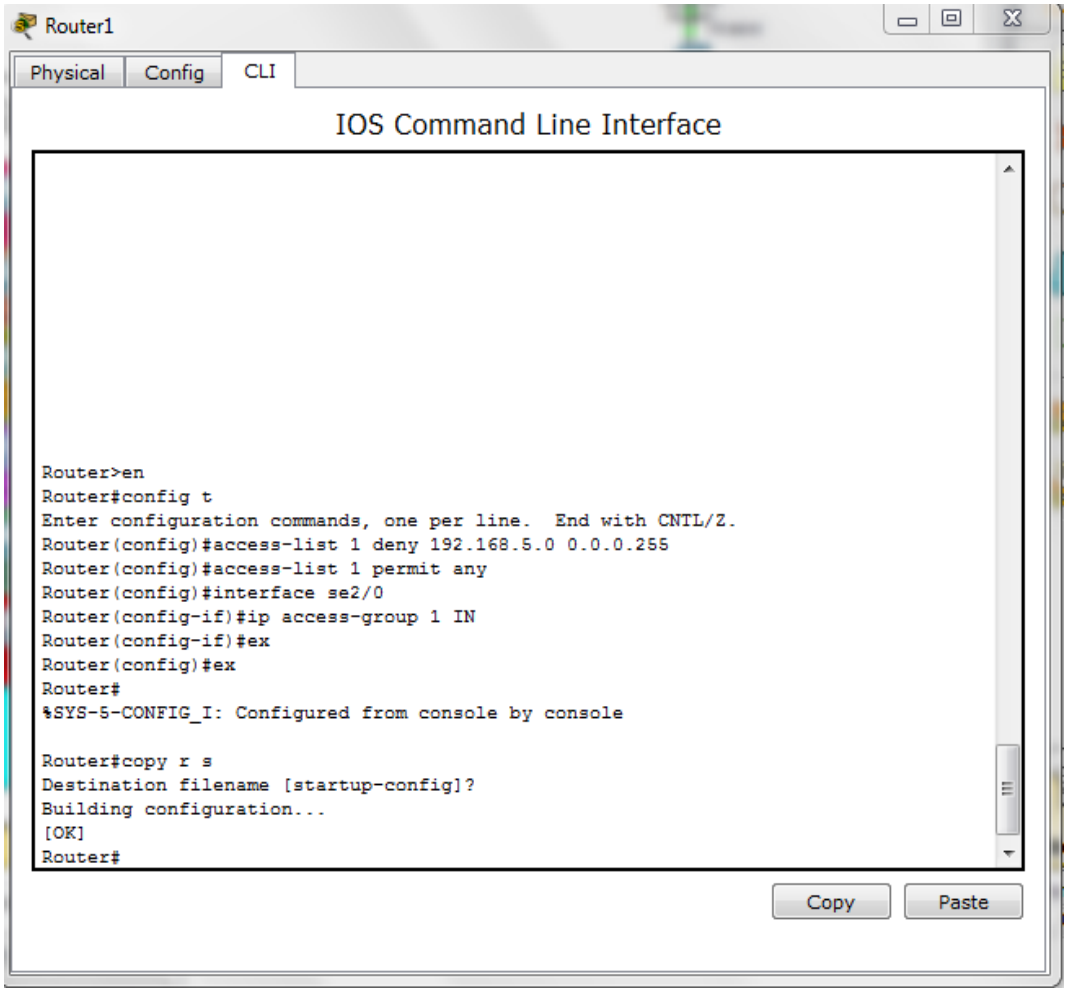

Fig. 4.20 – configuration d'un ACL

4.7 Vérification et tests de validation

4.7.1 Vérification

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

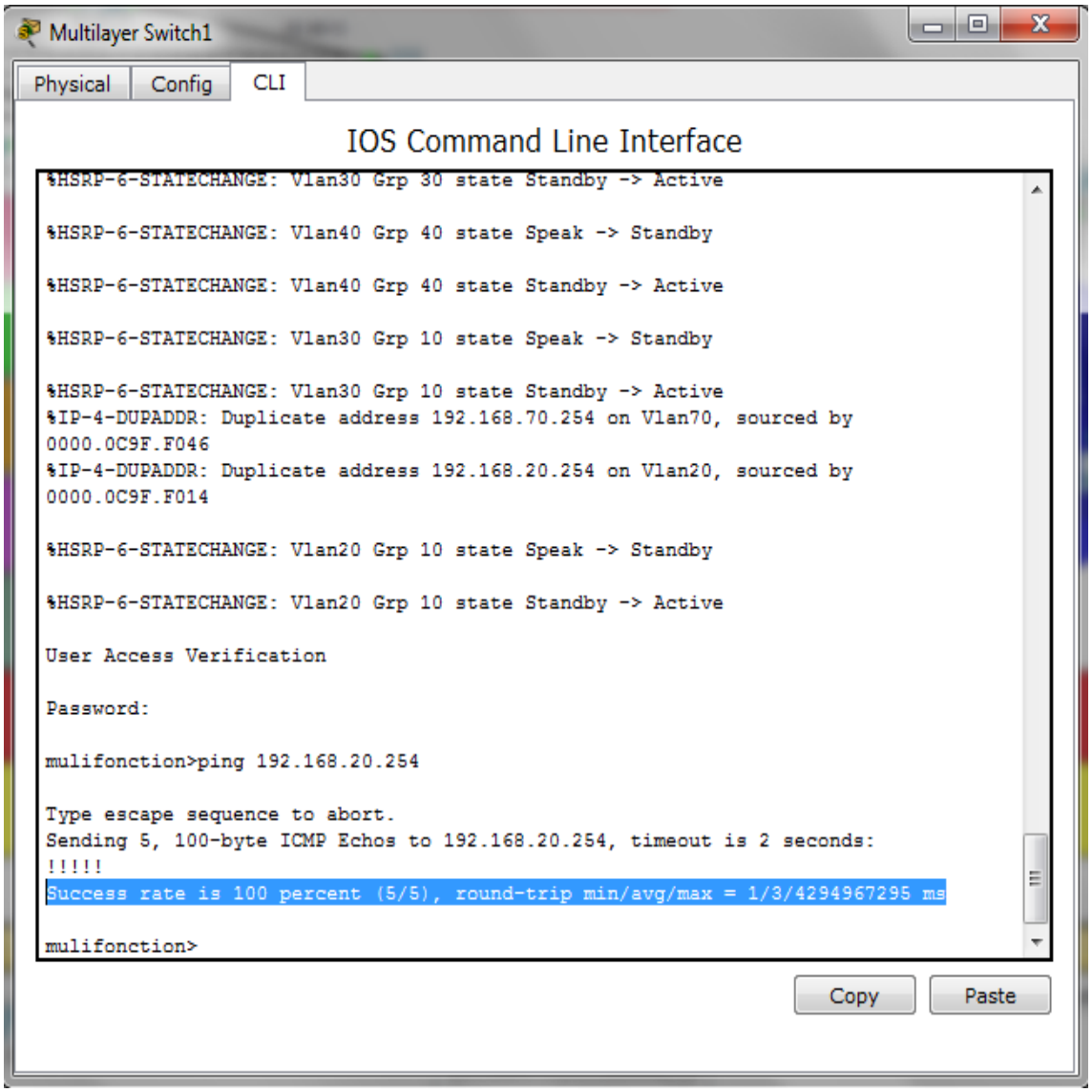

FIG. 4.21 – Test entre le Switch Accès et multifonction

• **Vérification de routage Inter-Vlan**

La commande "show ip interface brief", permet de voir les switchs virtuelle interface (SVI) comme le montre la figure suivant :

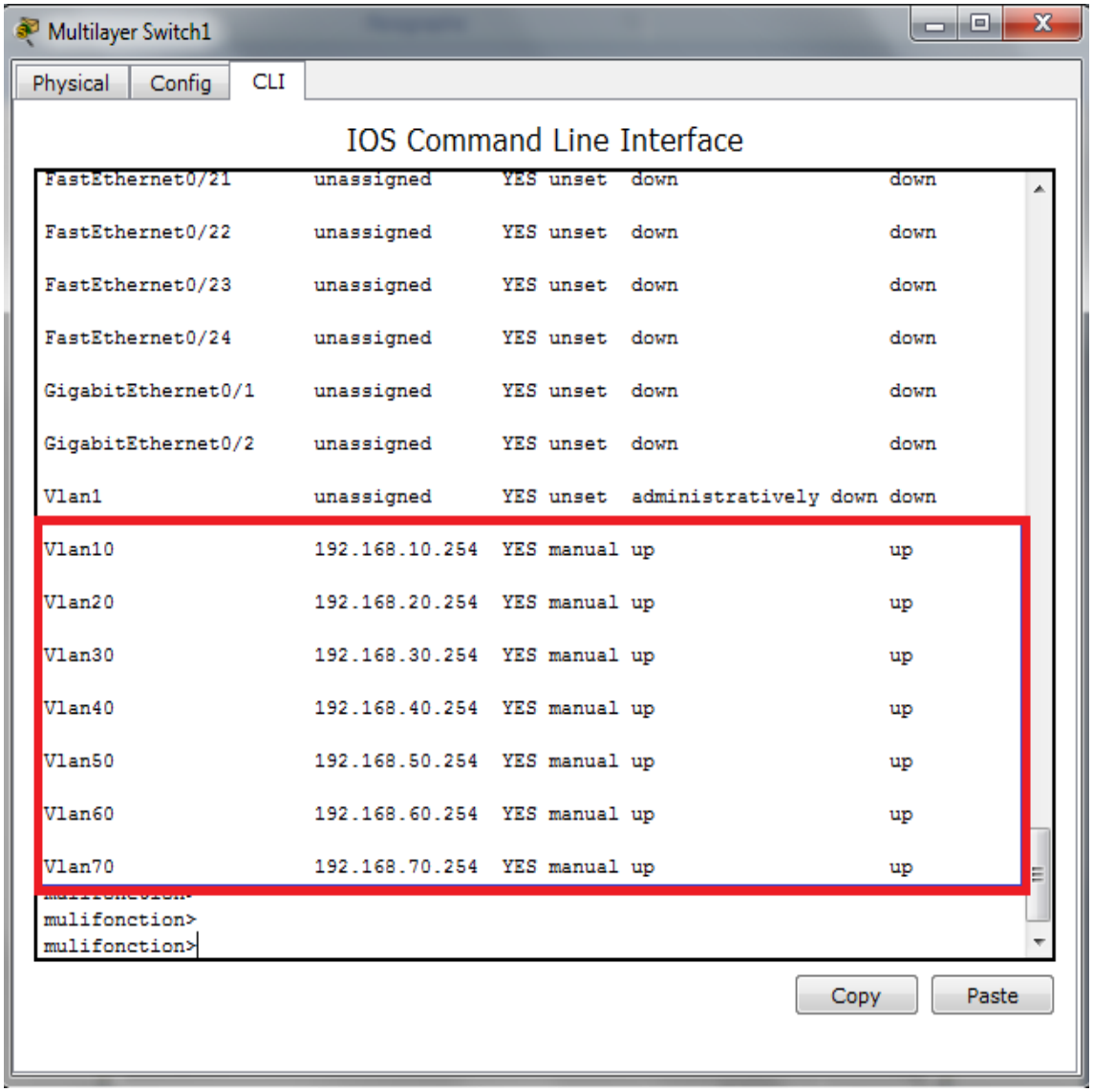

FIG. 4.22 – Switch Virtual Interface

• **Vérification de la distribution des adresses IP avec DHCP**

A l'aide de la commande " show ip DHCP binding" on à vérifier que chaque poste à bien récupère une adresse DHCP.

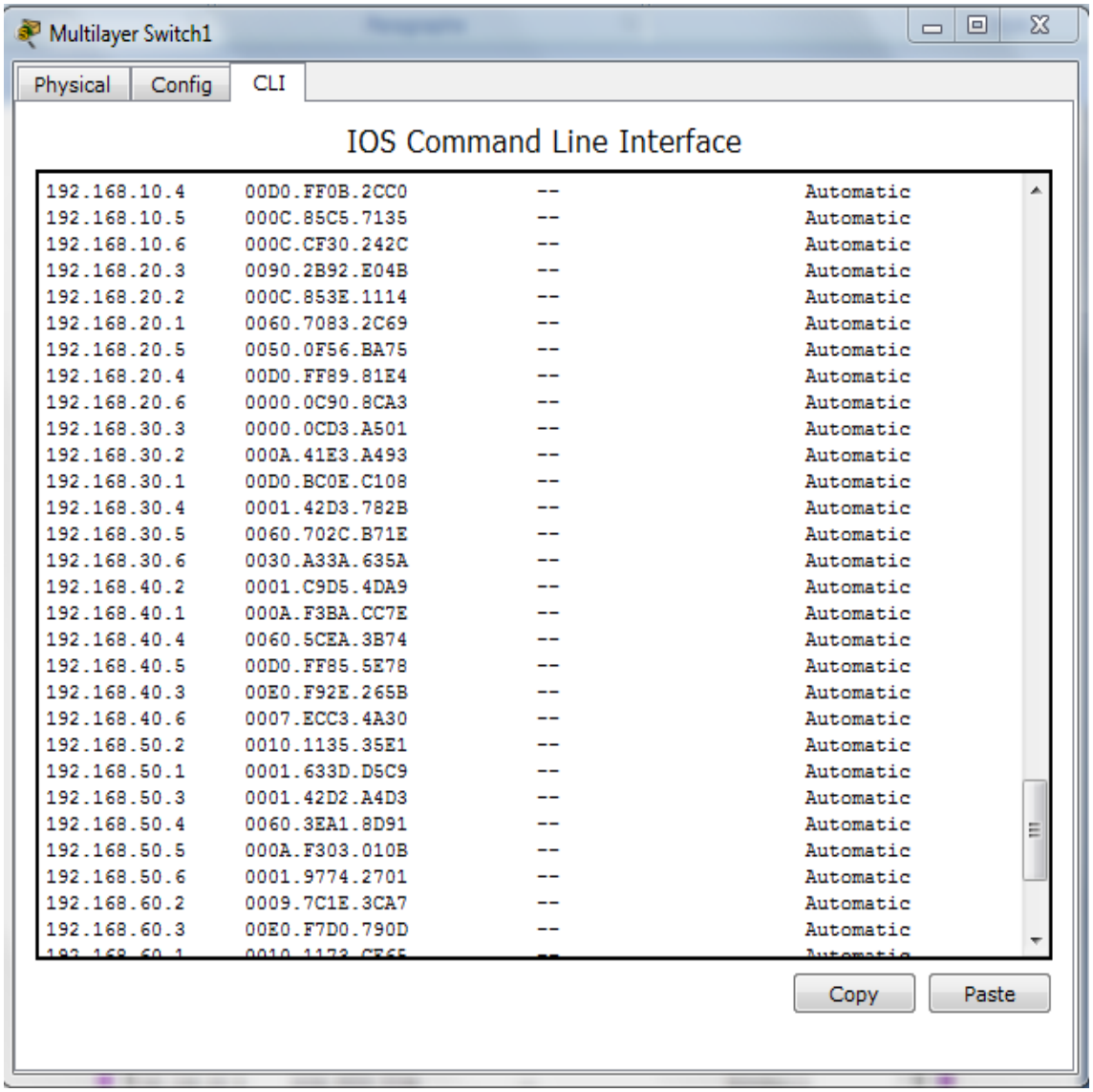

FIG. 4.23 – L'attribution des adresses IP

• **Vérification de HSRP**

La commande "show standby brief" nous indique quel switch est actif et qui est en attente comme le montre la figure suivant :

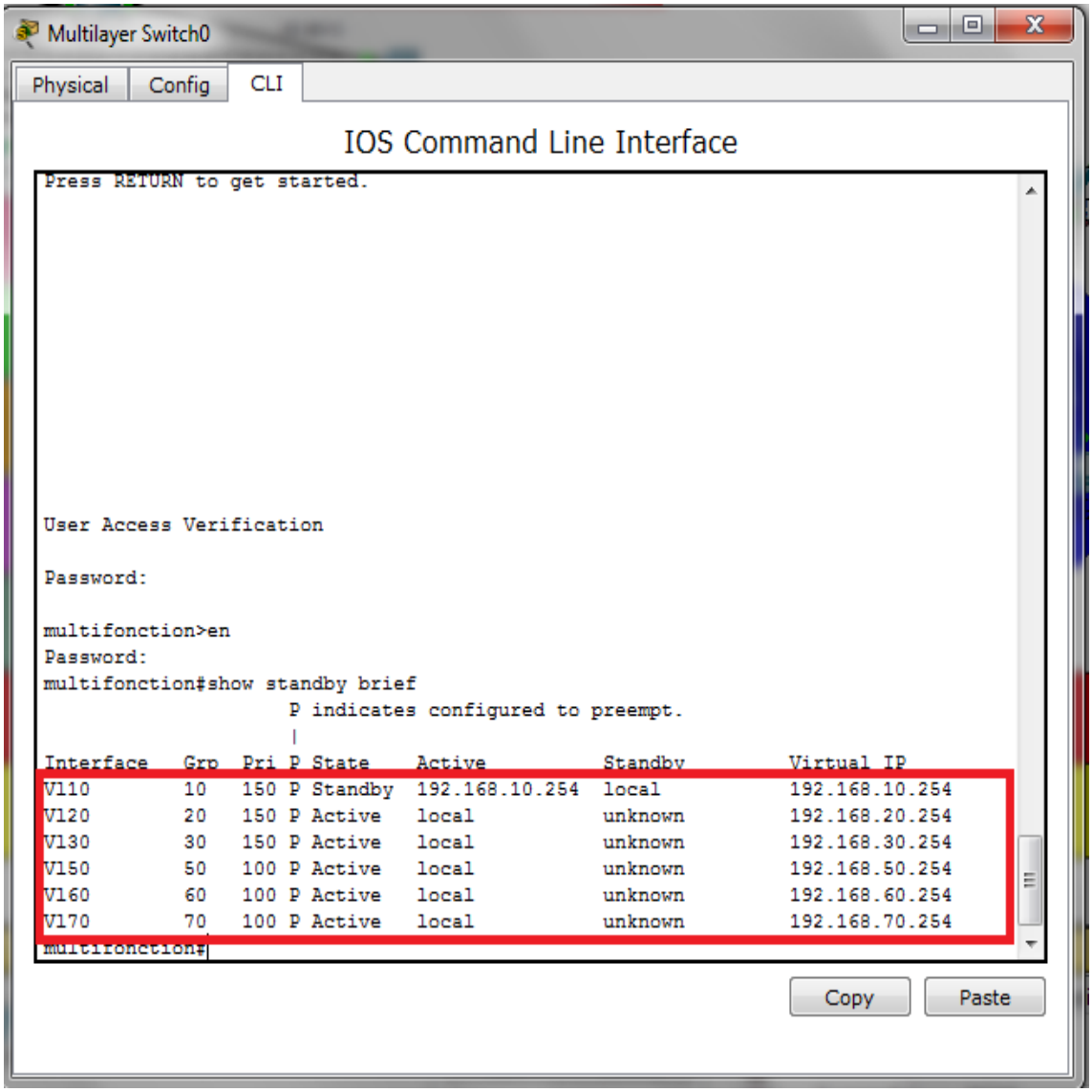

FIG. 4.24 – Switch multifonction en mode active

4.8 Tests 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 un paquet au destinataire. Si l'équipement récepteur reçoit ce paquet donc la communication est réussie.

4.8.1 Test inter-VLANs

La figure 4.23 montre que le test réussi entre PC17 qui appartient au VLAN10 et le PC4 qui appartient au VLAN 30 :

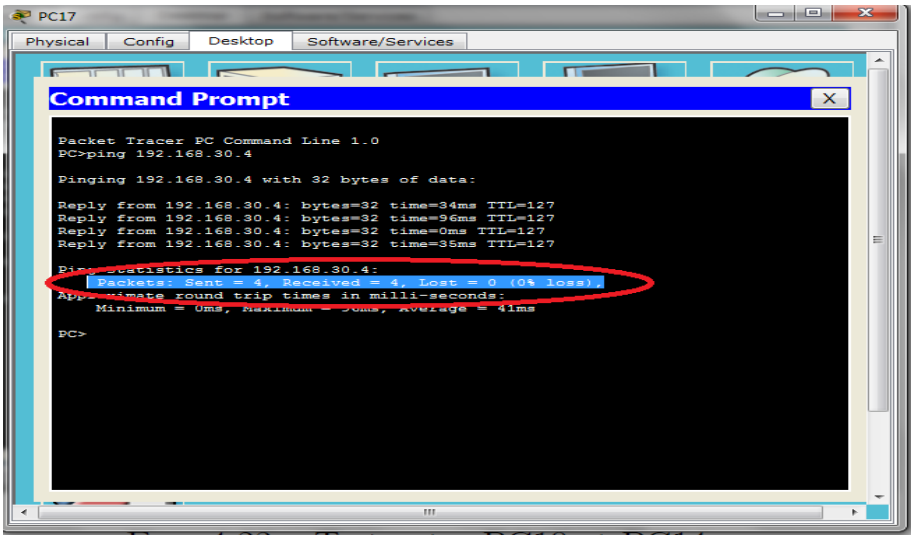

Fig. 4.25 – Test entre PC4 et PC17

4.8.2 Test intra-VLANs

La figure 4.24 montre que le Test réussi entre PC5 et PC19 qui appartient au même VLAN 40 :

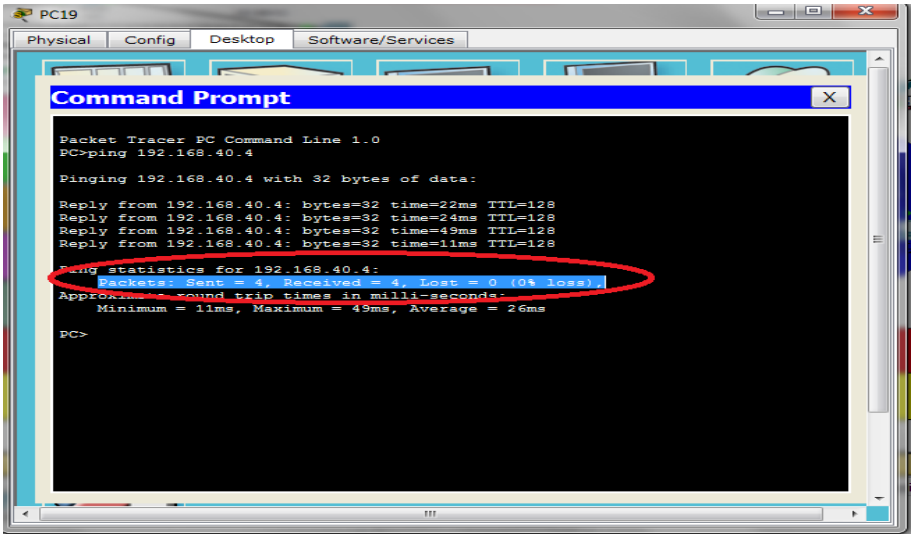

FIG. 4.26 – Test enter PC5 et PC19

4.8.3 Test la Haute disponibilité

Dans ce cas de figure on teste la connectivité entre les PC et les commutateurs distincts lorsque le switch multifonction est défectueux. A partir du PC3 appartenant au VLAN10 essayons d'accéder au PC8 qui appartient au VLAN20.

La figure 4.25 montre le succès du test effectué entre deux PC des VLANs distincts lorsqu'un Switch multifonction est en panne.

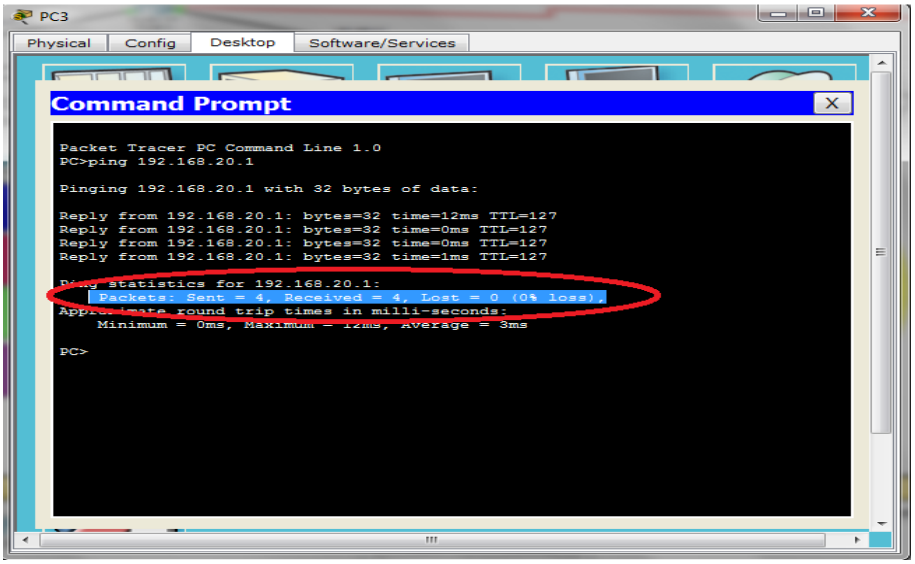

FIG. 4.27 – Test entre les machines des différents VLANs lorsqu'un des Switchs multifonction est défectueux

4.9 Conclusion

Dans ce chapitre nous avons présenté la structure du réseau utilisé au niveau de l'entreprise SONATRACH. Nous avons mis l'accent sur la présentation de quelques interfaces, qui porte sur l'ensemble des configurations, puis nous avons effectué un ensemble de tests de validation afin de prouver l'efficacité du réseau.

Conclusion générale

Pour mettre en œuvre ce projet, nous avons acquis les connaissances nécessaires à la création d'un réseau d'entreprise efficace et extensible. Nous avons étudié des notions relatives au réseau, tels que les VLANs, les trunks, le routage inter-VLAN, l'agrégation des ports, le spanning tree ainsi que la haute disponibilité, et aussi nous avons étudié les protocoles de routage à base de distance (RIP) et les protocoles à état de lien (OSPF) nous avons montré les avantages et les inconvénients de chacun d'entre eux. Les problèmes liés à ces protocoles de routage ont été également présentés.

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 matériaux dont on aura besoin, ce qui a facilité considérablement leur configuration sur Packet Tracer.

Le travail que nous avons accompli a pour principal objectif la mise en œuvre d'un réseau commuté au sein de la SONATRACH ce projet nous a permis de mettre en pratique les connaissances acquises durant le cycle de notre formation , de se familiariser avec un environnement dynamique et d'avoir une idée plus profonde et plus pratique sur l'importance du réseau dans une entreprise.

Bibliographie

[1] Pillou. J, " tout sur les réseaux internet ", DUNOD, 2007.

[2] Pujolle.G, "les réseaux ", 5éme édition, EYROLLES, Aout 2006.

[3] Dordoigne.J, "réseau informatique, notion fondamentales ", 4éme édition ENI, février 2011.

[4] Peter. O'Dell, "Le réseau local", Dunod, 1991.

[5] Pierre Erny, " les réseaux informatique d'entreprise ", 1998.

[6] Sylvain " le modèle TCP/IP ", source http ://www.frameip.com/tcpip/, 2003, 22/05/2016.

[7] Danièle Dromard, Dominique Seret, " Architecture des réseaux ", PEARSON France, 2013, ISBN : 978-2-7440-7664.

[8] Bapatiste Wicht, " Introduction au réseau ", 03 Mars 2007, source http ://babitiste-wicht.devloppez.com/tutoriel/reseau/introduction,25/05/2016.

[9] www.frameip.com/routage, 29/04/2016.

[10] www.it-connect.fr/routage-statique-et-routage-dynamique, 29/04/2016.

[11] Cisco Networking Academy, 2007-2008, http ://lcna.gphmii.sk, 30/05/2016.

[12] www.it-connect.fr/routage-statique-et-routage-dynamique, 30/04/2016.

[13] Bernard Adrien, " Routage ", 06 juin 2004, source http ://www.techno-science.net, 20/05/2016

[14] Fréderic Jacquenod, " Cours Réseaux : les matériels d'interconnexion ", source Http ://www.netalya.com/fr/reseaux5.asp, 02/04/2016.

[16] Khelalfa, Halim M, " introduction à la sécurité Informatique ", SECINFO04, 2000.

[17] Support de cour réseau EISTI " http : //www.elstl.fr ",05/05/2016.

[18] LESCOP Yves V1.6, " sécurité informatique ",2002

[19] A.Mokhetari, " La Sécurité dans les Echanges et la Sauvegarde des Données", Université de Versailles.2000-2001.

[20] M.Badra, "le transport et la sécurisation des échanges sur les réseaux sans fil", thèse de doctorat, l'Ecole Nationale Supérieure des Télécommunications, 2004.

[21] BELHADI HAKIMA, " la sécurité des données informatique cryptographier ", mémoire de fin d'études master 2, université de Bejaïa.

[22] M.Badra, "le transport et la sécurisation des échanges sur les réseaux sans fil", thèse de doctorat, l'Ecole Nationale Supérieure des Télécommunications, 2004.

[23] Messaoudi S.et Ichalalene S, " la sécurité des réseaux informatiques ", mémoire de DEUA, université de Bejaïa, 2004.

[24] Touazi .D, "protocole RIP", cours mastre 2, université de béjaia, 2012.

[25] Cisco, "Networking Academy", 2007-2008.

[26] Babakhoya A. " Sécurité de routage ", Mémoire de Magistère en informatique, Université Abderrahmane Mira Béjaia, 2004-2005.

[27] Baures M, Wullens. " Evaluation de l'implémentation du protocole OSPF ", ENAC, 2009-2010.

[28] LA Chi Anh. " Etude et validation de l'application du paradigme des pots de miel aux attaques visant les protocoles de routage ", Institut Eurécom Sophia Antipolis, Septembre 2006.

[29] "Meilleur pratique en matière de vlan ", IN www.fluKenetworks.com, fluKe corporation, 2004.

[30] "le protocole VTP (Vlan Trunking Protocole) ", avril 2012.

[31] GILBERT Held, " les réseaux locaux virtuels, Conception, mise en œuvre et administration ", Aout 1998.

[32] Analysing the InterSwitch Link protocol, CISCO network ACADEMY, http ://www.firewalle.cx/vlan.php, 01/06/2016.

[33] Florent Nolot, " Des protocoles de Spaning Tree ", Mastre2 informatique, Université de Reims, 2008.

[34] wapiti.telecomlille1.eu/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2006-ttnfa2007/DiStefano-Wong/Protocole HSRP.html, 02/05/2016.

[35] www.authsecu.com/hsrp-cisco-securité/hsrp-cisco-sécurité.php, 07/06/2016.

[36] Collectif, Dictionnaire Hachette encyclopédie illustré, paris, Ed. Hachette livre, 1998, pages 928.

[37] cours CCNA 2, "Notion de base sur les routeurs et le routage", 2015.

[38] CISCO. Simple Configuration for Authentification in OSPF.2005.

[39] cours CCNA 2, "Notion de base sur les routeurs et le routage", 2015.

[40] La sécurité du protocole HSRP Par Sébastien Fontaine(SebF), source http ://www.it-connect.fr/mise-en-place-du-protocole-hsrp, 08/04/2016.

[41] www.ietf.org/meeting/86-IEEE-8021-Thaler.pdf, 29/05/2016.

RÉSUMÉ

Les protocoles de routage assurent la connectivité du réseau et maintiennent des routes afin que les données envoyées par une source puissent atteindre leur destination. Les protocoles de routage utilisés actuellement dans l'internet, comme RIP et OSPF sont conçus pour opérer dans un environnement sain sans routeur malicieux. L'objectif de ce projet est l'étude et configuration d'un réseau de moyenne dimension, cas d'étude de l'entreprise SONATRACH. Pour atteindre l'objectif fixé, on explique les notions fondamentales des réseaux informatiques, ensuite les notions de base sur la sécurité des réseaux. On finit par présenter quelques protocoles, et leurs configurations à l'aide du simulateur Packet tracer. .

Mots clés : Routage, VLAN, Packet Tracer, HSRP, SONATRACH, RIP, OSPF.

ABSTRACT

Routing protocols provide network connectivity and maintain roads so that the data sent by a source to reach their destination. Routing protocols currently used in the Internet, such as RIP and OSPF are designed to operate in a healthy environment without malicious router. The objective of this project is the design and configuration of a medium sized network, In our case, the study of the Sonatrach company. To achieve this objective, the basic concepts of computer networks are explained , then the basics of network security . We finally, present some protocols and their configurations using the simulator Packet tracer.

Key words : Routing, VLAN, Packet Tracer, HSRP, SONATRACH, RIP, OSPF.