

République Algérienne Démocratique Et Populaire Ministère de
L'Enseignement Supérieur Et de la Recherche Scientifique.



Université Abderrahmane MIRA-Bejaia

Faculté de Technologie

Département de Génie Electrique.



Mémoire de fin d'études

En vue de l'obtention du diplôme de **Master**.

Filière: **Télécommunications**.

Spécialité : **Réseaux et Télécommunications**.

Réalisé par :

Melle MAMERI Déhia

Melle ZAIDI Numidia

Thème

**Conception et configuration d'un réseau
campus sécurisé (SONATRACH) Bejaia.**

Soutenu le 27/06/ 2019 devant le jury composé de :

Mr MEKHMUKH.A	President
Mr BERRAH. S	Rapporteur
Mr ALLICHE.A	Examineur
Mr MADDI.K	Encadreur

Année Universitaire: 2018/2019

Remerciements

Nous adressons en premier lieu notre reconnaissance à notre Dieu tout-puissant, de nous donner la santé et la volonté d'entamer et terminer ce mémoire.

Nous souhaitons adresser nos remerciements aux personnes qui nous ont aidées dans la réalisation de notre mémoire de fin d'études. En premier lieu, nous remercions les professeurs de l'université de Bejaia pour les solides notions théoriques qu'ils nous enseignaient et sur lesquelles nous nous sommes appuyées pour élaborer ce mémoire.

Nous tenons à exprimer nos vifs remerciements pour notre professeur, **Mr BERRAH Smail**, d'avoir accepté de nous encadrer pour notre projet de fin d'études, ainsi que pour son soutien, ses remarques pertinentes et son encouragement. Nous tenons également à remercier **Mr. ALLICHE Abdenour** et **Mr. MEKHEMOUKH Abdenour** de nous avoir honoré en acceptant de juger notre modeste travail.

Nous remercions notre encadreur de stage **Mr MADDI.K** pour le temps précieux qu'il nous a accordé, et tout le personnel de l'entreprise SONATRACH de Bejaia, qui nous a aidés lors de notre stage et aussi pour le stage de qualité.

Nos remerciements vont aussi à toutes nos familles, amis et toutes les personnes qui nous ont soutenus jusqu'au bout, et qui n'ont pas cessé de nous donner des conseils très importants en signe de reconnaissance.

Dédicaces

*Avec un énorme plaisir, un cœur ouvert et une immense joie, que je
dédie ce modeste travail*

*A mes très chers parent, pour leurs patiences, leurs amour, leurs
encouragements et leurs sacrifices tout au long de mon parcours ;*

A mon frère et mes sœurs ;

A mon fiancé ainsi que à toute sa famille ;

A toute ma famille ZAIDI ;

A mon binôme Déhia ainsi que sa famille ;

A tous mes amis ;

ET à tous ceux qui m'ont aidé dans l'élaboration de ce travail.

Numidia

*Avec un énorme plaisir, un cœur ouvert et une immense joie, que je
dédie ce modeste travail*

*A mes très chers parent, pour leurs patiences, leurs amour, leurs
encouragements et leurs sacrifices tout au long de mon parcours ;*

A mes frère et sœurs ;

A toute ma famille MAMERI ;

A mon binôme Numidia ainsi que sa famille ;

A tous mes amis ;

ET à tous ceux qui m'ont aidé dans l'élaboration de ce travail.

Dehia

Table des matières

Table des matières	i
Table des figures	iv
Liste des tableaux	vi
Liste des abréviations	vii
Introduction général	1
1. Généralités & Sécurité des réseaux informatiques	3
1.1 Introduction	3
1.2 Définition d'un réseau informatique	3
1.3 Classification des réseaux	4
1.3.1 La topologie	4
1.3.2 L'étendue géographique	4
1.4 Les solutions de réseaux de données	6
1.5 Modèle de réseau	6
1.5.1 Modèle OSI	6
1.5.2 Modèle TCP/IP	7
1.5.3 La comparaison entre OSI et TCP/IP	8
1.6 Description des équipements de base d'un réseau informatique	9
1.7 Les protocoles LAN	10
1.7.1 Protocole HSRP	10
1.7.2 Protocole DHCP	10
1.7.3 Protocole STP	10
1.8 Le protocole couche 2 du modèle TCP/IP	11
1.8.1 Protocole IP	11
1.8.2 Protocole EIGRP	11
1.9 Enjeux de la sécurité des réseaux informatiques	11
1.10 Les menaces sur les systèmes informatiques	12
1.10.1 Menaces accidentelles (non-intentionnelles)	12
1.10.2 Menaces intentionnelles	12
1.11 Quelques solutions de sécurité	13
1.11.1 Solution de sécurité minimum	13
1.11.2 Pare-feu et serveur proxy	13
1.11.3 Cryptographies	14
1.11.4 VLAN (Virtual Local Area Network)	15
1.11.5 VPN (Virtual Private Network)	20
1.12 Conclusion	25

2	Etude de l'existant	26
2.1	Introduction	26
2.2	Présentation de l'organisme d'accueil.	26
2.2.1	L'activité de transport par canalisation	27
2.3	Présentation de la direction régional de transport de béjaia	28
2.3.1	Département Maintenance	29
2.3.2	Département Informatique	30
2.4	Aspect réseau.	32
2.4.1	Les commutateurs utilisés dans le réseau de la DRGB.	32
2.4.2	Les routeurs utilisés dans le réseau de la DRGB	35
2.5	La structure hiérarchique du réseau SONATRACH	35
2.6	Aspect sécurité.	37
2.7	Problématique	39
2.8	Solutions proposées	39
2.9	Conclusion	40
3	Mise en œuvre et réalisation	41
3.1	Introduction	41
3.2	Présentation du simulateur Cisco « Packet Tracer »	41
3.3	Conception	42
3.4	Segmentation VLANs	44
3.5	Configuration des équipements	45
3.5.1	Configuration du nom de périphérique	45
3.5.2	Sécurisation d'accès aux périphériques	45
3.5.3	Configuration du protocole VTP	47
3.5.4	Création des VLANs	48
3.5.5	Attribution des ports des commutateurs aux VLANs	49
3.5.6	Configuration des liens trunk.	50
3.5.7	Configuration des interfaces VLANs.	51
3.5.8	Configuration DHCP.	52
3.5.9	Configuration STP	53
3.5.10	Configuration HSRP	53
3.6	Vérification et test de validation	55
3.6.1	Vérification	55
3.6.2	Tests de validation	60
3.7	Conclusion	63
4	Configuration d'un réseau virtuel VPN	65
4.1	Introduction	65
4.2	Présentation de l'architecture réseau avant la configuration	65
4.3	Configuration de l'EIGRP	67
4.4	Configuration d'un réseau opérateur	69
4.5	Configuration d'un réseau sans fil.	71
4.6	Configuration et mise en œuvre d'un tunnel VPN	75

4.7	Configuration s'un tunnel VPN IPSec	75
4.7.1	Configuration d'un VPN IPsec site à site	76
4.7.2	Configuration l'ACL pour le trafic VPN d'intérêt	77
4.7.3	Configuration des propriétés ISAKMP de phase 2 sur Routeur Sonatrach . . .	78
4.8	Vérification et test de validation	81
4.9	Conclusion	84
	Conclusion général et perspectives	85
	Bibliographie	87

Table des Figures

1.1	Classification selon l'étendue Géographique	4
1.2	Représentation d'un réseau PAN	4
1.3	Représentation d'un réseau LAN	5
1.4	Représentation d'un réseau MAN	5
1.5	Représentation d'un réseau WAN	6
1.6	Représentation du modèle OSI	7
1.7	Modèle TCP/IP	7
1.8	Représentation d'un pare-feu	13
1.9	Représentation d'un server proxy	14
1.10	La cryptographie	14
1.11	Un immeuble de bureau avec 3 VLANs	15
1.12	VLAN par port	16
1.13	VLAN par sous-réseau (adresse IP)	17
1.14	VTP server	18
1.15	VTP client	19
1.16	VTP transparent	19
1.17	Représentation d'un VPN	20
1.18	VPN d'accès à distance	22
1.19	Intranet VPN	22
1.20	Extranet VPN	23
1.21	Réseau VPN avec protocole IPsec	25
2.1	Organisation de SONATRACH	27
2.2	Réseau de transport par canalisation	28
2.3	Organisation de la direction régionale de Bejaïa	29
2.4	Organigramme du Département Maintenance SDT / RTC	30
2.5	Organigramme du Centre Informatique RTC	31
2.6	Structure réseau de SONATRACH	32
2.7	Gamme catalyst cisco 6509	33
2.8	Gamme catalyst cisco 3750	33
2.9	Gamme catalyst 3560	34
2.10	Gamme catalyst 2950	34
2.11	Représentation d'un réseau commuté	36
2.12	Partie sécurité de SONATRACH	37
2.13	Firewall Juniper ssg 550	38
3.1	Interface principale du simulateur Cisco Packet Tracer	42
3.2	Structure des départements	43
3.3	Présentation de l'architecture	43
3.4	Nomination du multilayer switch0	45
3.5	Configuration du mot de passe	46
3.6	Configuration du VTP-server	47

3.7	Configuration client-VTP.	48
3.8	Création des VLANs sur le serveur VTP	49
3.9	Attribution des ports aux VLANs.	50
3.10	Configuration des liens trunk	51
3.11	Configuration des interfaces VLANs	51
3.12	Configuration de DHCP	52
3.13	Configuration de STP.	53
3.14	Configuration de HSRP	54
3.15	Réseau local après la configuration	55
3.16	VLANs distribués dans le Switch client Sw1.	56
3.17	SVI (Switch Virtuelle Interface).	57
3.18	Attribution des adresses IP.	58
3.19	Switch multi-sw1 en mode active	59
3.20	Switch multi-sw2 en mode active	59
3.21	Test entre le multi-sw1 et le Switch d'accès	60
3.22	Test entre machines des VLANs différents	61
3.23	Test entre des machines des VLANs et commutateurs différents	62
3.24	Attribution des adresses IP par le DHCP	62
4.1	Présentation de l'architecture	66
4.2	Routage au niveau de Switch multi-SW2	67
4.3	Routage au niveau du routeur	68
4.4	Interconnexion de différents réseaux locaux	69
4.5	Interconnexion avec un réseau opérateur	69
4.6	Attribution d'adresse au serveur	70
4.7	Configuration d'un nom de domaine au serveur	70
4.8	Configuration du cloud	71
4.9	Implémentation d'un réseau externe	71
4.10	Attribution du mot de passe au point d'accès	72
4.11	Attribué le mot de passe du Tablet PC0	73
4.12	Attribué le mot de passe au Smartphone0	73
4.13	Connecter le Laptop11 au point d'accès	74
4.14	Interconnexion des différents réseaux locaux	74
4.15	Implémentation d'un VPN dans l'architecture	75
4.16	Configuration des propriétés ISAKMP de phase 1	77
4.17	Configuration d'ACL pour le trafic VPN.	77
4.18	Configuration des propriétés ISAKMP de phase 2.	78
4.19	Configuration des paramètres IPsec.	79
4.20	Architecture du réseau WAN réalisé	80
4.21	Test entre les machines des différents réseaux	81
4.22	Test du server DNS d'un réseau opérateur (Algerie télécom)	81
4.23	Vérification du tunnel avant le trafic intéressant	82
4.24	Envoi de la requête ping du server vers le multiSwitch	83
4.25	Vérification du trafic après le trafic intéressant	83

Liste des tableaux

3.1	Plan d'adressage des VLANs	45
4.1	Tableau des adresses proposé.....	76

Liste des abréviations

AES	Advanced Encryption Standard
ACL	Access Control List
AH	Authentication Header
CLI	Command Language Interface
CISCO	Corps Information Systems Control Officer
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DES	Data Encryption Standard
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IGRP	Interior Gateway Routing Protocol
ISO	International Standards Organization
LAN	Local Area Network
L2F	Layer Two Forwarding
L2TP	Layer Two Tunneling Protocol
MAC	Media Access Control
MAN	Metropolitan Area Network
PING	Packet Internet Groper
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
PAN	Personal Area Network
PAP	Password Authentication Protocol
QoS	Quality Of Service
RN	Révision Number
RTC	Transport par Canalisations
RFC	Request for comments
RIP	Routing Information Protocol
RTP	Reliable Transfer Protocol

SMTP	Simple Mail Transfer Protocol
SNAT	Source Network Address Translation
TCP/IP	Transmission Control Protocol/ Internet Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VTP	Virtual Trunking Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

Introduction Générale

De nos jours, les réseaux et les systèmes de transmission de données ont pris une importance majeure dans le fonctionnement des entreprises. L'évolution rapide des technologies de l'information et des télécommunications a permis la construction d'une infrastructure mondiale de communication, l'Internet. Pourtant, l'utilisation de ce réseau public pour échanger des données confidentielles pose pas mal de problèmes.

Dès lors que ces réseaux sont apparus comme des cibles d'attaques potentielles, leur sécurisation est devenue un enjeu incontournable pour les différentes institutions et entreprises. Cette sécurisation dont l'objectif attendu est de diminuer fortement la prise de risque, doit garantir la confidentialité, l'intégrité, la disponibilité et la non-répudiation des données. Et pour cela, de nombreux outils et moyens sont disponibles, tels que les solutions telles que : VLANs, VPNs... etc.

L'entreprise SONATRACH est un organisme de grande envergure, il joue un rôle primordial dans l'économie du pays, il est composé d'une dizaine d'entreprises de dimension nationale et internationale.

Avec l'avènement des nouvelles technologies de l'information, l'entreprise a procédé à la rénovation de son réseau de télécommunication, ce processus de modernisation des systèmes informatiques rencontre plusieurs difficultés qui sont relative à la mauvaise répartition d'architecture et partage de ressources.

L'unité de Bejaia (DRGB) fait partie du réseau étendu de SONATRACH, qui a un rôle important dans le transport des hydrocarbures, elle contient un réseau informatique contenant une centaine d'équipements finaux, répartis sur deux bâtiments (ancien et nouveau) de trois niveaux. Cette architecture pose quelques problèmes relatifs à la collision, la congestion et la sécurité.

L'objectif de notre projet est de proposer une architecture sécurisée du réseau de l'entreprise et implémenter des mécanismes et des solutions fiables en utilisant des liaisons

virtuelles (VLAN et VPN), permettant de garantir une meilleure exploitation, partage de ressources et attribution du réseau. Assurant ainsi une communication sûre et confidentielle entre les utilisateurs au sein de l'entreprise. Afin de réaliser les objectifs visés, nous avons organisé le travail en quatre chapitres :

- ✓ Le premier chapitre est consacré à la présentation des généralités sur les réseaux informatiques, en décrivant les types de réseau ainsi que ses modèles et les différents protocoles utilisés, et sur la sécurité des réseaux informatiques : les objectifs de la sécurité informatique, les différentes attaques et leurs types et quelques solutions de sécurité d'un réseau informatique.
- ✓ Le deuxième chapitre est dédié à une étude préalable dans laquelle nous avons présenté l'organisme d'accueil SONATRACH, exposer la problématique et proposer une solution à cette dernière.
- ✓ Le troisième chapitre décrit la première partie pratique de notre projet, dont laquelle nous avons présenté l'environnement de travail ainsi que la configuration et segmentation d'un réseau virtuel VLAN.
- ✓ Le dernier chapitre comprend la deuxième partie pratique, dont laquelle nous allons configurer un réseau virtuel VPN.

Enfin, notre mémoire s'achève par une conclusion générale résumant les connaissances acquises durant la réalisation du projet et quelques perspectives.

Généralités & Sécurité des réseaux informatiques

1.1 Introduction

Un réseau de communication est l'ensemble des ressources matérielles et logicielles liées à la transmission et l'échange d'informations entre différentes entités.

La sécurité des réseaux informatiques, est devenue un enjeu majeur du fait de la rapidité des évolutions technologiques et de l'augmentation des risques qui en résultent.

L'objectif de ce chapitre est de présenter quelques concepts de base sur les réseaux informatiques, les protocoles, les menaces sur les réseaux informatiques ainsi que quelques solutions de sécurité (pare-feu, serveur-proxy, cryptographie) en se basant sur les solutions VLANs et VPNs.

1.2 Définition d'un réseau informatique

Un réseau est un moyen de communication qui permet à des individus ou à des groupes d'échanger des données et de partager des ressources, il a pour fonction d'assurer le transfert des données entre deux usagers ou plus par l'intermédiaire d'un ensemble d'équipements matériels et logiciels.

❖ Critères de choix d'un type de réseau

- Taille de l'entreprise ou de l'organisme,
- Niveau de sécurité requis,
- Type d'activité,
- Le trafic sur le réseau,
- Besoins des utilisateurs du réseau,
- Le coût.

1.3 Classification des réseaux

Les réseaux informatiques peuvent être classés selon les critères suivants :

1.3.1 La topologie

- La topologie physique : décrit la manière avec laquelle les différents nœuds sont reliés entre eux. (Bus, Étoile, Anneau...etc.).
- La topologie logique : désigne la façon avec laquelle l'information est transmise d'un nœud à l'autre, les plus courantes sont Ethernet et Token Ring.

1.3.2 L'étendue géographique

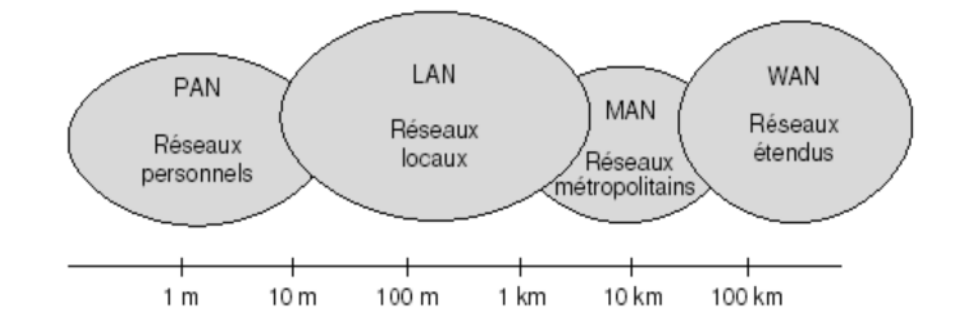


Figure 1.1- Classification selon l'étendue Géographique.

✓ Réseau personnel (PAN)

Un réseau PAN acronyme Personal Area Network, est un réseau domestique assurant l'interconnexion d'équipements ou périphériques (Laptop, Smartphone, PC, etc.), dans un espace d'une dizaine de mètres basés sur la technologie Bluetooth, Wi-fi....



Figure 1.2--Représentation d'un réseau PAN.

✓ Réseau local (LAN)

Un réseau local LAN acronyme Local Area Network, est une infrastructure constituée d'équipements interconnectés entre eux, permettant l'échange et le partage des ressources communes limitées à une zone géographique restreinte. Il représente le cœur de la majeure partie de l'activité informatique dans une entreprise [1].

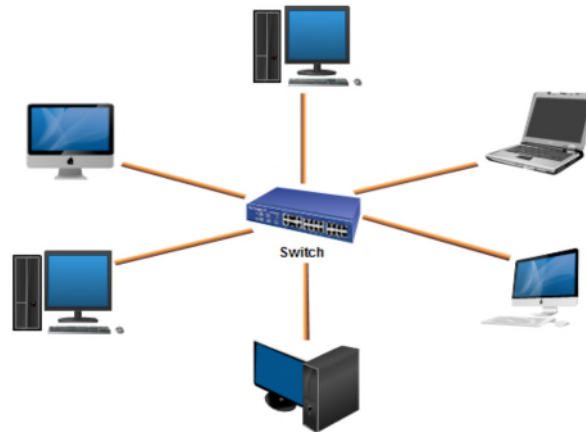


Figure 1.3- Représentation d'un réseau LAN.

✓ Réseau métropolitain (MAN)

Un réseau métropolitain appelé MAN acronyme de Metropolitan Area Network, est également nommé réseau fédérateur assurant des communications jusqu'à une distance de 100 km, interconnectant ainsi les réseaux LAN [1].

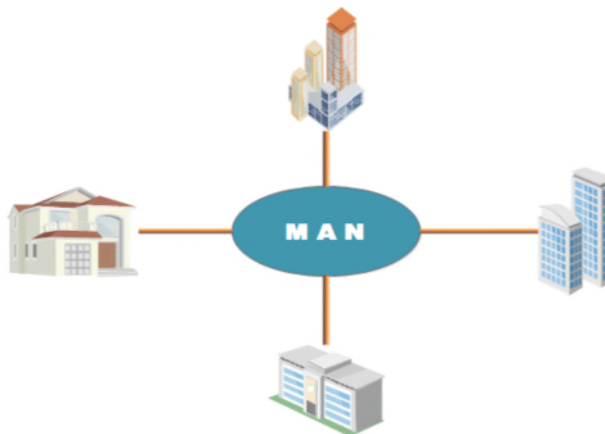


Figure 1.4- Représentation d'un réseau MAN.

✓ Réseau étendu (WAN)

Un réseau étendu appelé WAN acronyme de Wide Area Network, permet d'interconnecter des réseaux LANs sur des grandes distances géographiques (plus de 100 km), Les WANs fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau [1].

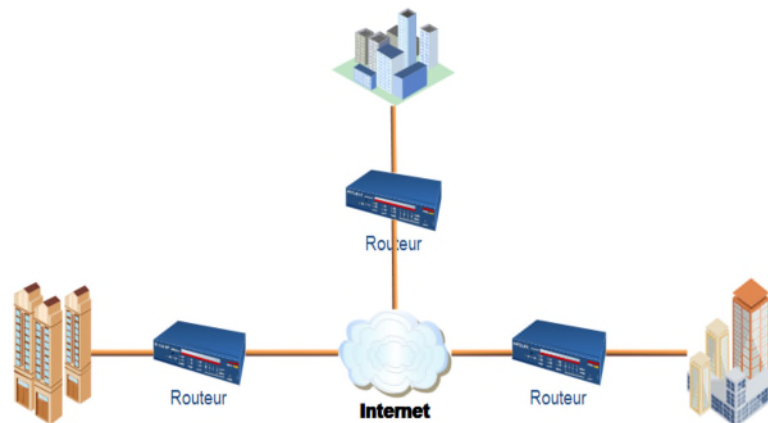


Figure 1.5.

Figure 1.5- Représentation d'un réseau WAN

1.4 Les solutions de réseaux de données

La plupart des réseaux informatiques sont classés en réseaux locaux LAN et en réseaux WAN. Les réseaux locaux sont généralement situés à l'intérieur d'un immeuble ou d'un complexe et servent aux communications internes, alors que les réseaux WAN couvrent une grande distance et relient des villes et des pays. Un réseau WAN interconnecte plusieurs réseaux LANs.

1.5 Modèle des réseaux

1.5.1 Modèle OSI

Le modèle OSI (Open Systems Interconnection) « Interconnexion de systèmes ouverts » est un modèle de communication entre ordinateurs proposé par l'ISO (International Standard Organisation), il décrit la manière dont les matériels et les logiciels coopèrent pour assurer la communication réseau. Il est organisé en sept couches successives en remplissant des tâches bien spécifiques. Ce modèle est obsolète vu l'apparition du nouveau modèle d'application (TCP/IP) qui est plus répandu [2] :

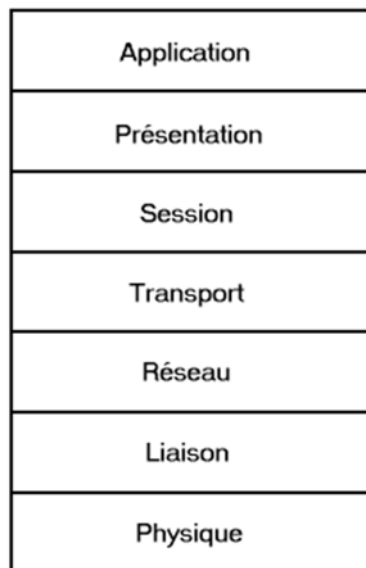


Figure 1.6- Représentation du modèle OSI.

1.5.2 Modèle TCP/IP

Le modèle TCP/IP acronyme de Transmission Control Protocol/Internet Protocol désigne communément une architecture réseau à quatre couches, dans laquelle les protocoles TCP et IP jouent un rôle prédominant, constituant ainsi la structure la plus courante. Afin de comprendre les tâches de chacune des couches, on va présenter brièvement ci-dessous ce modèle:

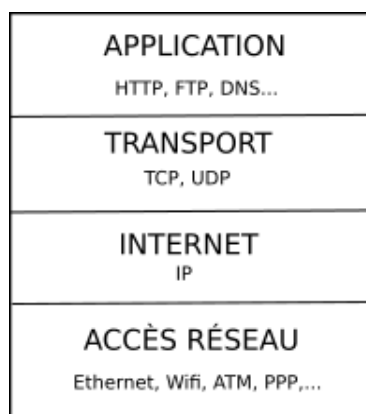


Figure 1.7- Modèle TCP/IP.

1. Couche Application

Les concepteurs du modèle TCP/IP estiment que les protocoles du niveau supérieur devaient inclure les détails des couches session et présentation. Ils ont donc simplement créé une couche application qui gère les protocoles de haut niveau, les questions de représentation, le code et le contrôle du dialogue. Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.

2. Couche Transport

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

3. Couche Internet

Le rôle de la couche Internet consiste à envoyer des paquets source à partir d'un réseau quelconque de l'inter réseau et à les faire parvenir à destination, indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol). L'identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

4. Couche accès réseau

Cette couche a un sens très large on l'appelle également la couche hôte réseau. Elle se charge de tout dont un paquet IP a besoin pour établir une liaison physique avec l'hôte de destination. Cela comprend les détails sur les technologies LAN et WAN, ainsi que tous les détails dans la couche physique et liaison de données du modèle OSI.

1.5.3 La comparaison entre OSI et TCP/IP

Le modèle TCP/IP et le modèle OSI ont beaucoup de points communs, comme ils ont des points de différence, on distingue [W2] :

1. Similitudes

- Les deux sont basés sur le concept d'empilement de protocoles,
- Les couches au-dessus de la couche transport sont des couches orientées vers des applications utilisateurs,
- Les couches au-dessous et y compris la couche de transport sont là pour fournir un service de transport et la manière de communication entre les différents utilisateurs.

2. Différences

- Le nombre des couches diffère d'un modèle à un autre pour le modèle OSI, il y a sept couches ; alors que pour le modèle TCP/IP seulement quatre couches,
- Le modèle TCP/IP est utilisé pour les réseaux internet contrairement au modèle OSI.

1.6 Description des équipements de base d'un réseau informatique

• Unité hôte

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

• Commutateur (Switch)

Un commutateur réseau est un équipement qui relie plusieurs câbles ou fibres dans un réseau informatique ou un réseau de télécommunication, fonctionne au niveau de la couche 2. Il permet d'effectuer une vérification des erreurs avant le transfert des données, ce qui le rend très efficace car il ne transfère pas les paquets comportant des erreurs et transmet les bons paquets de manière sélective au port correct uniquement.

• Routeur

Un routeur est un équipement assurant le routage des paquets, implémenté au niveau de la couche 3 du modèle OSI (couche réseau), permettant la configuration de l'adresse IP, du routage par défaut, du routage statique et dynamique, de la traduction d'adresses réseau (NAT) statique et dynamique, du nom d'hôte, de la bannière, du mot de passe secret, des comptes d'utilisateurs et d'autres options.

- **Point d'accès**

Un point d'accès sans fil est un dispositif qui permet aux périphériques sans fil de se connecter à un réseau câblé ou à un réseau internet à l'aide d'une connexion radio.

1.7 Les protocoles

On distingue plusieurs protocoles qui sont utilisés dans les réseaux LAN à savoir :

1.7.1 Protocole HSRP

Le protocole HSRP (Hot Standby Routing Protocol) est un protocole propriétaire de continuité de service implémenté dans les routeurs CISCO pour la gestion des liens de secours. HSRP sert à augmenter la tolérance aux pannes sur le réseau en créant un routeur virtuel à partir de deux (ou plus) routeurs physique : un « actif » et l'autre « en attente » ou « standby » en fonction des priorités accordées à chacun de ces routeurs.

1.7.2 Protocole DHCP

Le protocole DHCP acronyme Dynamic Host Configuration Protocol, il fournit une configuration dynamique des adresses IP et des informations associées aux ordinateurs configurés pour l'utiliser (clients DHCP). Ainsi chaque hôte du réseau obtient une configuration IP dynamiquement au moment du démarrage. Le serveur DHCP lui attribuera notamment une adresse IP et un masque et éventuellement l'adresse d'une passerelle par défaut.

1.7.3 Protocole STP

Le protocole STP acronyme Spanning Tree Protocol, il empêche la boucle de se former en configurant un chemin sans boucle sur l'ensemble du réseau, grâce à des ports bloqués stratégiquement placés. Les commutateurs qui exécutent le protocole STP sont capables d'assurer la continuité des communications en cas de panne en débloquant dynamiquement les ports préalablement bloqués et en autorisant le trafic à emprunter les chemins de substitution [W3].

1.8 Le protocole couche 2 du modèle TCP/IP

1.8.1 Protocole IP

Le protocole IP acronyme Internet Protocol est un protocole réseau du niveau trois du modèle OSI, qui permet d'émettre des paquets d'informations à travers le réseau, il offre un service d'adressage unique pour l'ensemble des usagers. Ce protocole est responsable de routage des paquets entre stations par l'intermédiaire des routeurs et de la transmission des données en mode sans connexion [6].

1.8.2 Protocole EIGRP

Le protocole EIGRP acronyme Enhanced Interior Gateway Routing Protocol, c'est un protocole de routage à vecteur de distance avancé qui joue le rôle d'un protocole à état de liens lors de la mise à jour des voisins et de la gestion des informations de routage. Par rapport aux protocoles à vecteur de distances simples (RIP, IGRP).

EIGRP offre notamment les avantages suivants [W4] :

- Une convergence rapide,
- Une utilisation efficace de la bande passante,
- Supporte plusieurs protocoles de la couche réseau: IPv4, IPv6... etc,
- Échange des messages entre routeurs assurés par RTP (Reliable Transfer Protocol).

1.9 Enjeux de la sécurité des réseaux informatiques

Pour atteindre les objectifs de sécurité dans un réseau, il faut respecter les exigences suivantes :

- **Confidentialité** : La protection des données émises sur le réseau, de façon à limiter l'accès aux données pour les destinataires désignés et autorisés.
- **Authentification** : C'est la procédure qui consiste, pour un système informatique à vérifier l'identité d'une personne ou d'un ordinateur afin d'autoriser son accès à des ressources (système, réseaux, application...).
- **Intégrité** : S'assurer et veiller à ce que les données transmises n'ont pas subit des perturbations ou des modifications dans le réseau.
- **Disponibilité** : S'assurer et veiller à ce que les utilisateurs autorisés puissent accéder en temps voulu et de façon fiable aux services de données.

- **Non-répudiation** : Assurer que l'entité émettrice des données ne pourra pas nier l'émission, c'est à dire identifier l'émetteur d'une transaction et d'assurer la preuve de l'authenticité [7].

1.10 Les menaces sur les systèmes informatiques

Dans un système informatique, les menaces peuvent toucher les composantes matérielles, logicielles ou informationnelles. Il existe principalement deux types de menaces [8] :

- Menaces accidentelles (non-intentionnelles);
- Les menaces intentionnelles (Passive – Active).

1.10.1 Menaces accidentelles (non-intentionnelles)

Les menaces accidentelles ne supportent aucune préméditation. Dans cette catégorie sont repris les bugs logiciels et les pannes matérielles et autre défaillances incontrôlables.

1.10.2 Menaces intentionnelles

C'est l'ensemble des actions malveillantes qui constituent la plus grosse partie du risque. Elles font principalement l'objet de mesures de protection. Parmi elles, on compte les menaces passives et les menaces actives.

1. Attaque passive

C'est une méthode qui consiste à écouter le réseau sans modifier ou détourner les données et son fonctionnement, elles sont généralement indétectables. Par exemple : Espionnage industriel et commercial, copies illicites de logiciel.

2. Attaque active

Cette attaque consiste à modifier les données et à s'introduire et se glisser dans les équipements réseau ou à perturber son fonctionnement, à titre d'exemple : virus, ver...etc.

1.11 Quelques solutions de sécurité

1.11.1 Solution de sécurité minimum

C'est l'ensemble des mesures offrant le minimum en matière de sécurité. [9]

- Sécurisation des utilisateurs par login et mot de passe dans les machines reliées au réseau,
- Installation d'un logiciel anti-virus mis à jour,
- Protection physique des machines contenant des informations sensibles,
- Suppression des informations confidentielles des machines reliées au réseau si elles n'ont pas besoin d'y être.

1.11.2 Pare-feu et serveur proxy

Le pare-feu (firewall) et le serveur proxy sont deux méthodes conçues afin d'éviter les attaques provenant d'internet par le router.

1. Pare-feu

Il s'agit d'une passerelle qui bloque les accès non autorisés au réseau, permettant de protéger un ou plusieurs périphériques finaux, des intrusions provenant notamment d'internet. La figure 1.8 suivante représente un pare-feu.

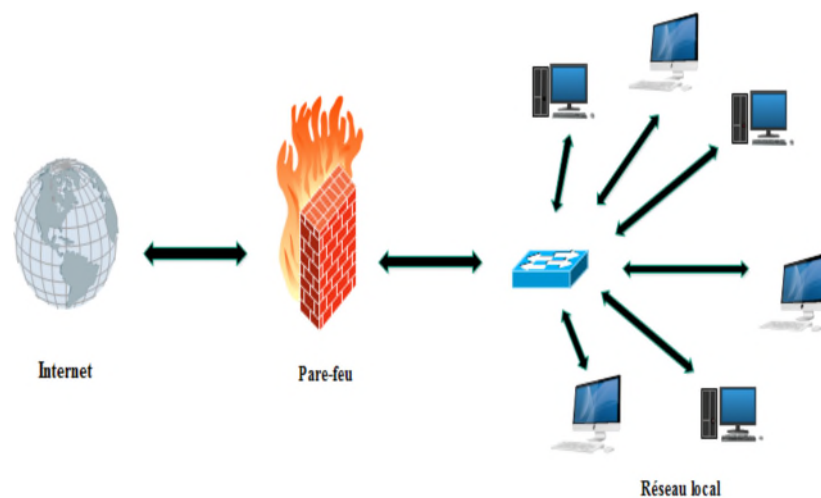


Figure1.8- Représentation d'un pare-feu.

2. Server proxy

Il s'agit d'un intermédiaire entre un périphérique final d'un réseau local et Internet.

Son objectif consiste à assurer :

- La sécurité et la protection du réseau local plus exactement de l'ordinateur connecté,
- Le filtrage et l'anonymat,
- D'accélérer la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds,
- Prendre les requêtes du client et de les transférer avec sa propre adresse IP à l'hôte cible. [10]

La figure 1.9 représente l'emplacement du serveur proxy dans un réseau.

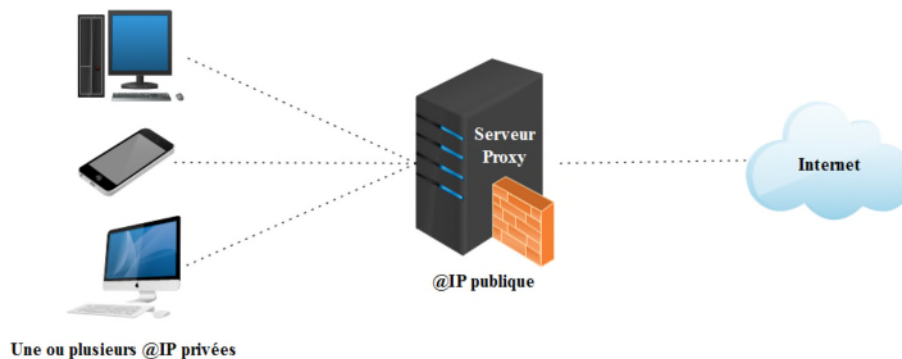


Figure 1.9- Représentation d'un server proxy.

1.11.3 Cryptographie

La cryptographie est l'art et la science qui permet l'étude des méthodes de chiffrement et de déchiffrement des données tout en permettant d'assurer l'authenticité, l'intégrité et la confidentialité de ces données. Le cryptage repose sur un codage de deux clés, (privé et publique) comme illustré sur la figure 1.10.

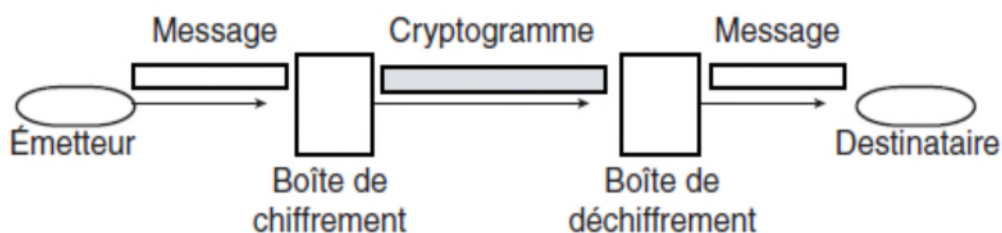


Figure 1.10- La cryptographie.

- **Cryptographie symétrique** : Elle est basée sur le principe d'utiliser une clé unique partagée pour chiffrer et déchiffrer les messages. C'est-à-dire les deux parties communicantes puissent s'échanger à l'avance la clé en secret.
- **Cryptographie asymétrique** : Contrairement à la cryptographie symétrique, la cryptographie asymétrique consiste à utiliser deux clés : une est publique pour un chiffrement connu que par l'émetteur, l'autre privée pour un déchiffrement connu par tout le monde [11].

1.11.4 VLAN (Virtual Local Area Network)

Dans un réseau commuté, les VLANs assurent la segmentation et favorisent la flexibilité de l'entreprise, offrent un moyen de regrouper des périphériques dans un LAN. Un groupe d'appareils dans un VLAN communiquent comme s'ils étaient reliés au même câble. Ils reposent sur des connexions logiques, et non des connexions physiques.

Chaque VLAN est considéré comme un réseau logique distinct. Les appareils d'un VLAN se comportent comme s'ils se trouvaient chacun sur leur propre réseau indépendant, même s'ils partagent une infrastructure commune avec d'autres VLAN. N'importe quel port du commutateur peut appartenir à un VLAN. Les paquets de monodiffusion, de diffusion et de multidiffusion ne sont transférés et diffusés que vers les terminaux appartenant au VLAN d'où ils proviennent [4].

La figure 1.11 représente les VLAN dans un immeuble d'un bureau.

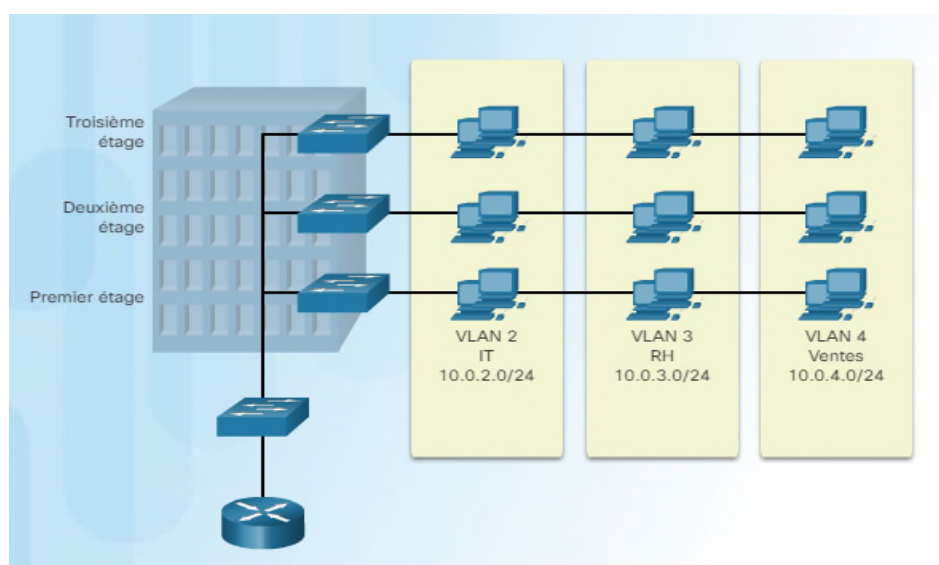


Figure 1.11- Un immeuble de bureau avec 3 VLANs

1. Avantages du VLANs

La segmentation logique des ports au sein d'un ou plusieurs réseaux physiques permet de tirer plusieurs points positifs des VLANs qui sont [12] :

- Réduction de la diffusion du trafic sur le réseau ;
- Améliorer la sécurité en n'autorisant la communication qu'entre les machines du même VLAN ;
- Simplifier les tâches d'administrateur : le déplacement d'un poste de travail d'un VLAN à un autre ne nécessite aucune manipulation physique, mais elle est gérée au niveau du commutateur ;
- Flexibilité de segmentation du réseau ;
- Augmentation considérable des performances du réseau ;
- La technologie évolutive et faible coût ;
- La régulation de la bande passante.

2. Types de VLANs

Les critères qui permettent d'identifier un VLAN sont au nombre de trois : port physique du commutateur, adresse MAC des machines et adresse sous-réseaux, définissant ainsi trois type de VLAN [13] :

- **VLANs par port (niveau 1)**

Le réseau local virtuel est défini en fonction des ports du commutateur. Un inconvénient majeur est que si une station se déplace cela implique une modification de la configuration du Port auquel elle était associée et du port auquel elle s'associe. Figure 1.12

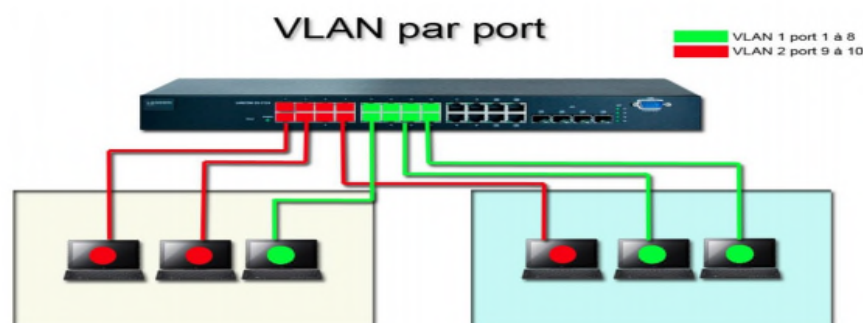


Figure 1.12- VLAN par port..

- **VLANS par adresse MAC (niveau 2)**

Dans ce cas, se sont les adresses MAC des machines qui permettent de déterminer leur appartenance au VLAN. L'identification des machines par leurs adresses MAC uniques, permet de rendre leur appartenance au VLAN indépendante de leur emplacement.

- **.VLAN par sous-réseau (de niveau 3)**

Le VLAN par sous-réseau permet de regrouper plusieurs machines suivant le sous-réseau auquel elles appartiennent. Pour créer un tel VLAN, il faut lui associer une adresse de sous-réseau. La figure 1.13 illustre la division des vlan par sous-réseau.

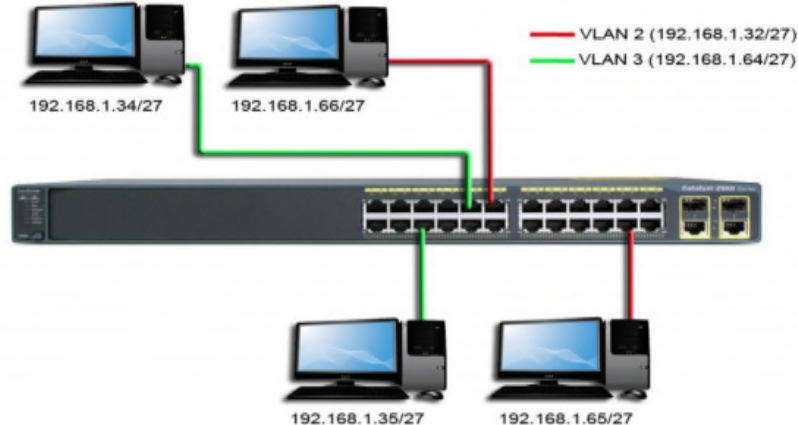


Figure 1.13– VLAN par sous-réseau (adresse IP).

3. Protocoles de transport des VLANs

- **VTP (Virtual Trunking Protocol)**

C'est un protocole de niveau 2, utilisé pour configurer et administrer les VLANs sur les périphériques CISCO. VTP permet d'ajouter, renommer ou supprimer, un ou plusieurs réseaux locaux virtuels sur un seul commutateur qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau. VTP permet ainsi d'éviter toute incohérence de configuration de VLANs sur l'ensemble d'un réseau local [14].

✓ **Fonctionnement [15]**

Les messages, VTP diffusent des annonces de création, de suppression ou de modification de VLAN. Lors de chaque création/suppression/modification, une variable appelée RN (Révision Number) s'incrémente (initialement 0 puis 1 puis 2 puis 3, etc.), le switch Server envoie un message VTP avec la nouvelle valeur du RN, les autres switchs comparent le RN reçu du switch Server avec le RN qu'ils stockent en local, si ce dernier est plus petit, alors les switchs se synchronisent avec le Server et récupèrent la nouvelle base de données des VLANs. Le switch possède 3 modes VTP : server, client et transparent :

- **VTP Server** : le switch en mode Server (mode par défaut), permet à l'administrateur de faire des modifications sur les VLANs et de les propager automatiquement vers tous les switchs du réseau. La figure 1.14 suivante représente les différentes tâches d'un VTP server.

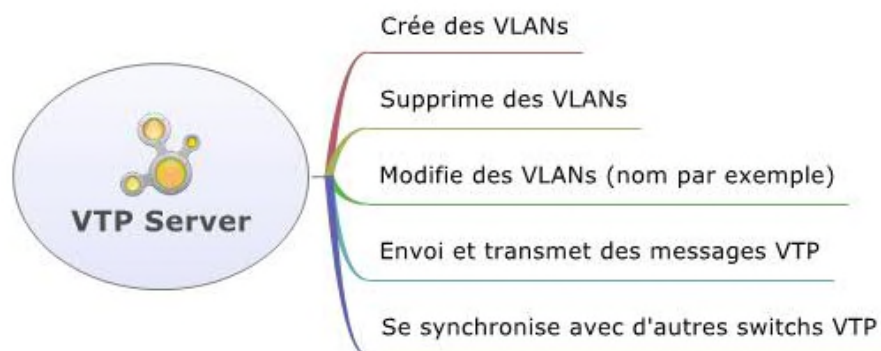


Figure 1.14- VTP server.

- **VTP Client** : Le switch en mode Client reçoit les mises à jour, les prend en charge, les transmet, mais ne permet pas à l'administrateur de faire des modifications sur les VLANs. La figure 1.15 suivante représente les différentes tâches d'un VTP client.



Figure 1.15- VTP client.

- **VTP Transparent** : Le switch en mode Transparent reçoit les mises à jour et les transmet sans les prendre en compte. Il permet à l'administrateur de faire toutes sortes de modifications sur les VLANs (en local uniquement) donc il ne propage pas ces modifications vers tous les switchs du réseau. La figure 1.16 suivante représente les différentes taches d'un VTP transparent.



Figure 1.16- VTP transparent.

- **Trunk** : Le trunk est le mécanisme qui permet d'insérer l'identifiant du VLAN sur une trame utilisateur. Toute trame se propageant sur plusieurs switchs conservera toujours l'information de son appartenance à son VLAN. Et le switch de destination saura avec quels ports la trame peut être commutée (ports appartenant au même VLAN) [16]. Le trunk peut être utilisés :

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

1.11.5 VPN (Virtual Private Network)

Un réseau privé virtuel (VPN) étend un réseau privé à travers un réseau public comme Internet. Il permet à une machine d'envoyer et de recevoir des données à travers des réseaux partagés ou publics comme s'ils étaient directement connectés au réseau privé, tout en bénéficiant des fonctionnalités, de la sécurité [17].

Ce réseau repose sur un protocole appelé protocole de tunneling, il permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Le tunneling consiste à construire un chemin virtuel après avoir identifier l'émetteur et le destinataire, la source chiffre les données et les transmet en empruntant ce chemin virtuel. La figure 1.17 suivante représente un VPN.

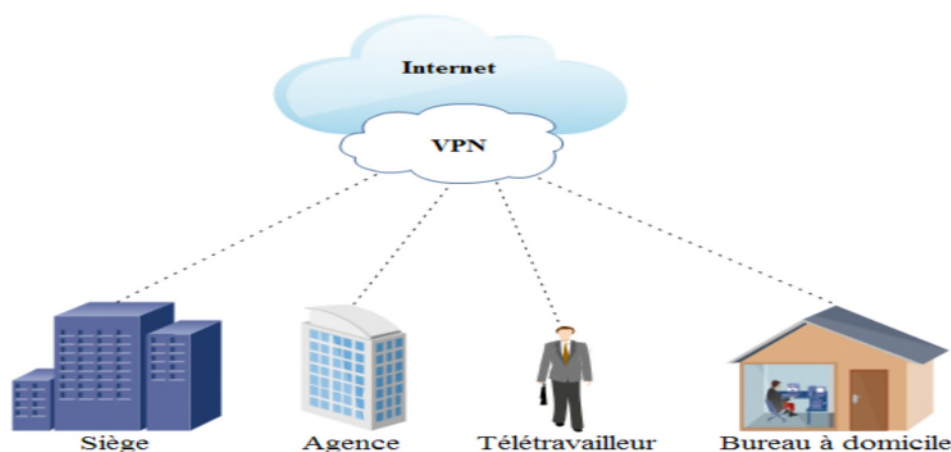


Figure 1.17- Représentation d'un VPN.

1. Objectif et fonctionnalité des VPN

Les VPNs existent pour protéger d'une manière efficace, sécurisée et privée les données qui sont transmises entre deux réseaux à partir de l'infrastructure commune, partagées et entretenues séparément entre les deux réseaux. Pour réaliser cette tâche, une implémentation VPN confidentielle doit respecter quatre objectifs : [18]

- **Confidentialité des données** : Protège le contenu des messages contre toute interprétation par des sources non authentifiées ou non autorisées.
- **Intégrité des données** : Garantit que le contenu du message n'a pas été falsifié ou modifié lors du transport de la source à la destination.
- **Non-répudiation de l'expéditeur** : Moyen d'empêcher un expéditeur de nier faussement avoir envoyé un message au destinataire.
- **Authentification des messages** : Garantit qu'un message a été envoyé à partir d'une source authentique et que les messages sont envoyés vers des destinations authentiques.

2. Différents Types de réseau VPN

Il existe deux types de VPN de base qui sont : VPN d'accès à distance et VPN de site à site. [19]

- **VPN d'accès à distance**

Les VPN d'accès à distance permettent aux utilisateurs mobiles ou à domicile d'accéder à distance aux ressources d'une entreprise via un VPN.

Dans une situation de VPN d'accès à distance, chaque utilisateur a besoin de son propre client VPN. Lorsque l'utilisateur est connecté au réseau via le client VPN, le logiciel crypte le trafic avant de le diffuser sur Internet. La passerelle VPN, qui est située à la périphérie du réseau cible, décrypte ensuite les données et envoie les informations à l'hôte approprié à l'intérieur du réseau privé. La figure 1.18 représente un VPN d'accès à distance.

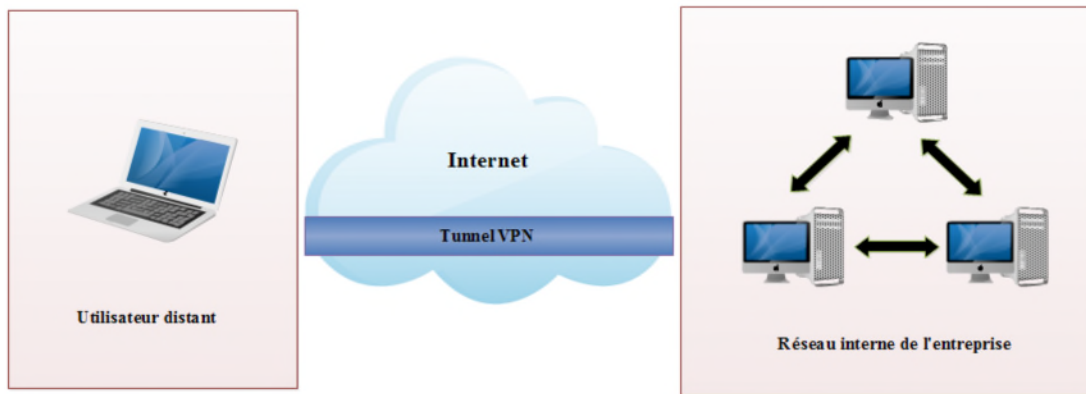


Figure 1.18-VPN d'accès à distance.

- **VPN de site à site**

Un VPN de site à site permet aux bureaux situés dans plusieurs emplacements fixes d'établir des connexions sécurisées entre eux sur un réseau public tel qu'Internet. Le VPN de site à site étend le réseau de l'entreprise, en mettant les ressources informatiques d'un emplacement à la disposition des employés d'autres sites. Il existe deux types de VPN de site à site [20]:

- ✓ **L'intranet VPN**

L'Intranet VPN favorise la communication entre les départements interne d'une entreprise et ses sites distants. Les VPNs s'appuient alors sur le réseau d'un opérateur ou d'un ISP. Il est nécessaire de développer un fort chiffrement afin de protéger les informations sensibles qui peuvent circuler tels que les bases de données clients. Comme l'illustre la figure 1.19 suivante.

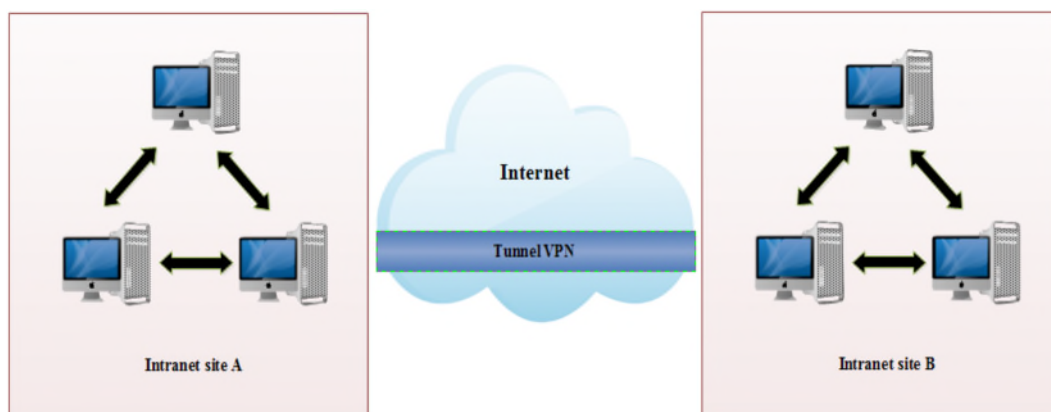


Figure 1.19-Intranet VPN.

✓ L'extranet VPN

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. La figure 1.20 représente un extranet VPN.

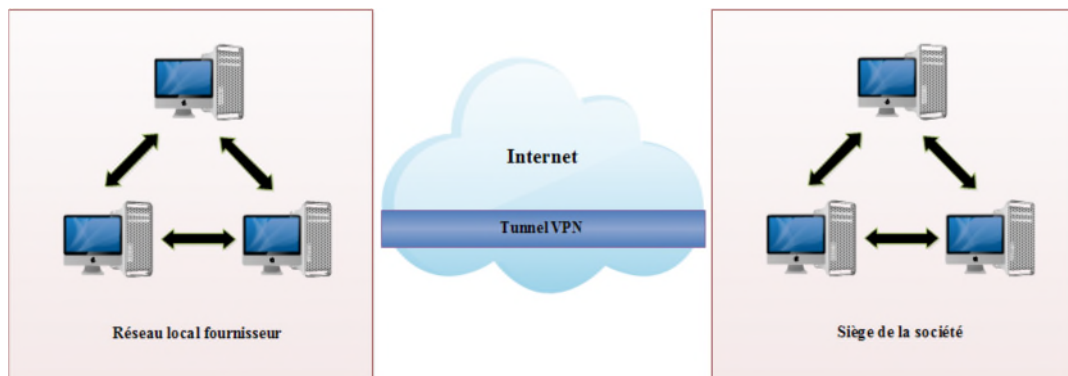


Figure 1.20- Extranet VPN.

3. Avantages d'un VPN

Les technologies VPNs permettent de connecter des endroits à travers le monde de manière sécurisée et cohérente. Parmi les principaux avantages d'un VPN on peut distinguer :

- **Sécurité** : assure des communications sécurisées et chiffrées ;
- **Simplicité** : utilise les circuits de télécommunication classique;
- **Économie** : utilise internet en tant que média principal de transport, ce qui évite les coûts liés à une ligne dédiée ;
- **Evolutivité** : les réseaux privés virtuels utilisent l'infrastructure Internet dont les FAI et les opérateurs, facilitant l'ajout de nouveaux utilisateurs pour les entreprises. Ces derniers, peuvent augmenter leurs capacités sans élargir sensiblement leur infrastructure.

4. Principaux protocoles de VPN

Les protocoles les plus communément utilisés dans le cadre de VPN qu'il soit de l'entreprise ou de l'opérateur et qui sont classés selon leurs places dans les couches du modèle OSI, sont décrits dans ce qui suit.

4.1 Protocole de niveau 2

- **Protocole PPP (Point to Point Protocole) :** A été conçu de façon à mettre en place entre un poste de travail et internet une liaison permettant à l'ordinateur de faire partie d'internet lorsqu'il en a besoin. C'est le protocole utilisé de manière classique par les fournisseurs d'accès internet. [21]
- **Protocole PPTP (Point To Point Tunneling Protocol) :** Est un protocole réseau qui permet le transfert sécurisé entre un client distant et un serveur privé. Il permet la création de VPN à travers des réseaux basés sur TCP/IP. Il peut de même être utilisé pour créer VPN entre deux ordinateurs dans le même réseau local. PPTP est utilisé pour des liaisons site à site il encapsule les paquets PPP dans des datagrammes IP pour la transmission sur internet ou un autre réseau public basé sur IP. [22]
- **L2TP (Layer Tow Tunneling Protocol) :** Il est issu de la convergence du protocole PPTP, le protocole L2TP est l'un des protocoles VPN implémenté nativement sur les machines Windows, ce qui explique son succès. Il fait intervenir deux composants lors de la construction du lien :
 - Un LAC (L2TP Access Concentrator) qui représente le point de terminaison physique de communication distante (hot distant).
 - Un LNS (L2TP Network Server) qui est un point de terminaison coté du réseau central, de toutes les sessions PPP établies [23].

4.2 Protocole de niveau 3

- **IPSec (Internet Protocol Security):** IPSec a été développé en tant que standard de sécurité Internet sur la couche 3 et a été standardisé par l'IETF depuis 1995. Il peut être aussi utilisé pour encapsuler le trafic des couches applicatives. IPSec s'agit plutôt d'un ensemble de protocoles, de normes et de mécanismes qui sont fusionnés pour une seule technologie. IPSec utilise deux modes pertinents : le

mode transport et le mode tunnel. Le premier offre essentiellement une protection aux protocoles de niveau supérieur, le second permet d'encapsuler des datagrammes IP dans d'autres datagrammes IP, dont le contenu est protégé. la figure 1.21 illustre un réseau VPN avec le protocole Ipsec [24].

IPsec fait appel à deux mécanismes de sécurité pour le trafic IP :

- AH (Authentication Header) : est employé pour assurer l'authentification des machines aux deux extrémités du tunnel. Il permet aussi de vérifier l'unicité et l'intégrité des données grâce à l'attribution d'un numéro de séquence et un code de vérification de ces données.
- ESP (Encapsulation Security Payload) : répond au besoin de cryptage des données. Il peut aussi gérer l'authentification et la vérification de l'intégrité mais d'une manière moins poussée que le AH.

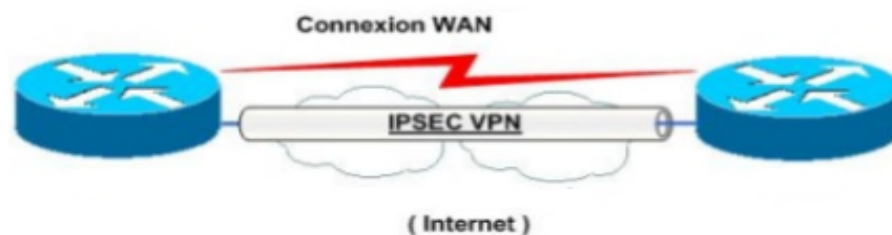


Figure 1.21- Réseau VPN avec protocole IPsec.

1.12 Conclusion

Au cours de ce chapitre, nous avons parcouru des généralités sur les réseaux informatiques en soulignant leurs importances, ainsi que leurs différents équipements de base.

Ce chapitre nous a permis de comprendre le concept de la sécurité informatique et plus particulièrement la sécurité des réseaux, où nous avons présenté ses objectifs, les attaques informatiques et les différentes solutions qui permettent de garantir la sécurité, tel que le firewall, la cryptographie, les VLANs, et enfin les VPNs.

A l'issue de ce chapitre, nous avons détaillé les différentes catégories et possibilités pour le déploiement d'un VLAN et d'un VPN, leurs rôles et leurs différents protocoles utilisés

Le prochain chapitre sera consacré à la présentation de l'organisme d'accueil et nous allons proposer des solutions pour subvenir les besoins de ce dernier.

Chapitre 2

Etude de l'existant

2.1 Introduction

Afin d'améliorer nos connaissances dans le domaine des réseaux, il est indispensable de développer nos capacités professionnelles. Pour cela, nous avons suivi un stage pratique au service télécommunication et au service informatique de l'entreprise SONATRACH de Bejaia (TRC).

Dans ce chapitre, nous allons présenter le groupe SONATRACH ainsi que sa structure hiérarchique, ensuite nous exposerons la problématique suivie de la solution proposée.

2.2 Présentation de l'organisme d'accueil

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

Pour la réalisation de ces objectifs, SONATRACH est divisé en cinq branches différentes représentées ci-après :

- Exploration-Production (E&P);
- Transport Par Canalisations (TRC);
- Liquéfaction et Séparation (LQS);
- Raffinage et Pétrochimie (RPC);
- Commercialisation (COM);

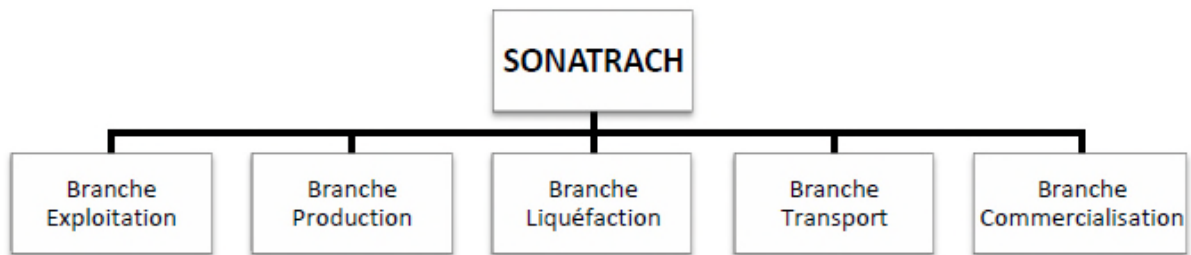


Figure 2.1 –Organigramme de SONATRACH.

2.2.1 L'activité de 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 activités affectées à la branche transport par canalisation sont :

- L'exploitation des ouvrages de transport des hydrocarbures et des installations portuaires à quai et en haute mer ;
- La maintenance des ouvrages de transport des hydrocarbures et des installations de chargements portuaires à quai et en haute mer ;
- Les études et développement, à l'exception des études relevant de la direction corporate business development et marketing (BDM) et la réalisation de projets relevant de la direction centrale engineering et project management.

Elle compte 5 régions transport, trois directions opérationnelles et deux centres dispatching :

- Région transport Est Skikda (RTE);
- Région transport Centre Bejaïa (RTC);
- Région Transport Ouest Arzew (RTO);
- Région Transport Houad El Hamra (RTH);
- Région Transport In Aminos (RTI);
- Direction Gazoduc Pedro Duran Farell (GPDF);
- Direction des Gazoducs Enrico Mattei (GEM);
- Direction des Gazoducs Hassi R'mel (GHR) ;

- Le Centre de Dispatching d'Hydrocarbures Liquides (CDHL);
- Le Centre National de Dispatching Gaz (CNDG).

Cartographie actuelle du Réseau de Transport

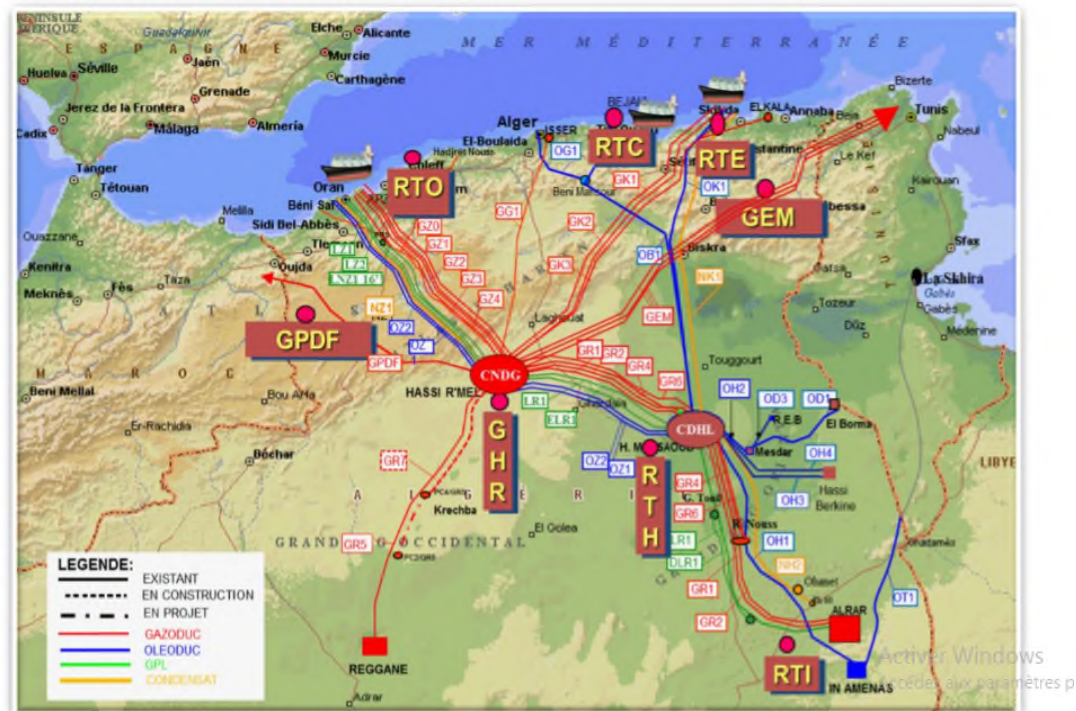


Figure 2.2- Réseau de transport par canalisation.

2.3 Présentation de la direction régionale de transport de Bejaïa

La direction régionale de transport de Bejaïa (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 [5].

La figure 2.3 représente l'organisation de la direction régionale de Bejaïa

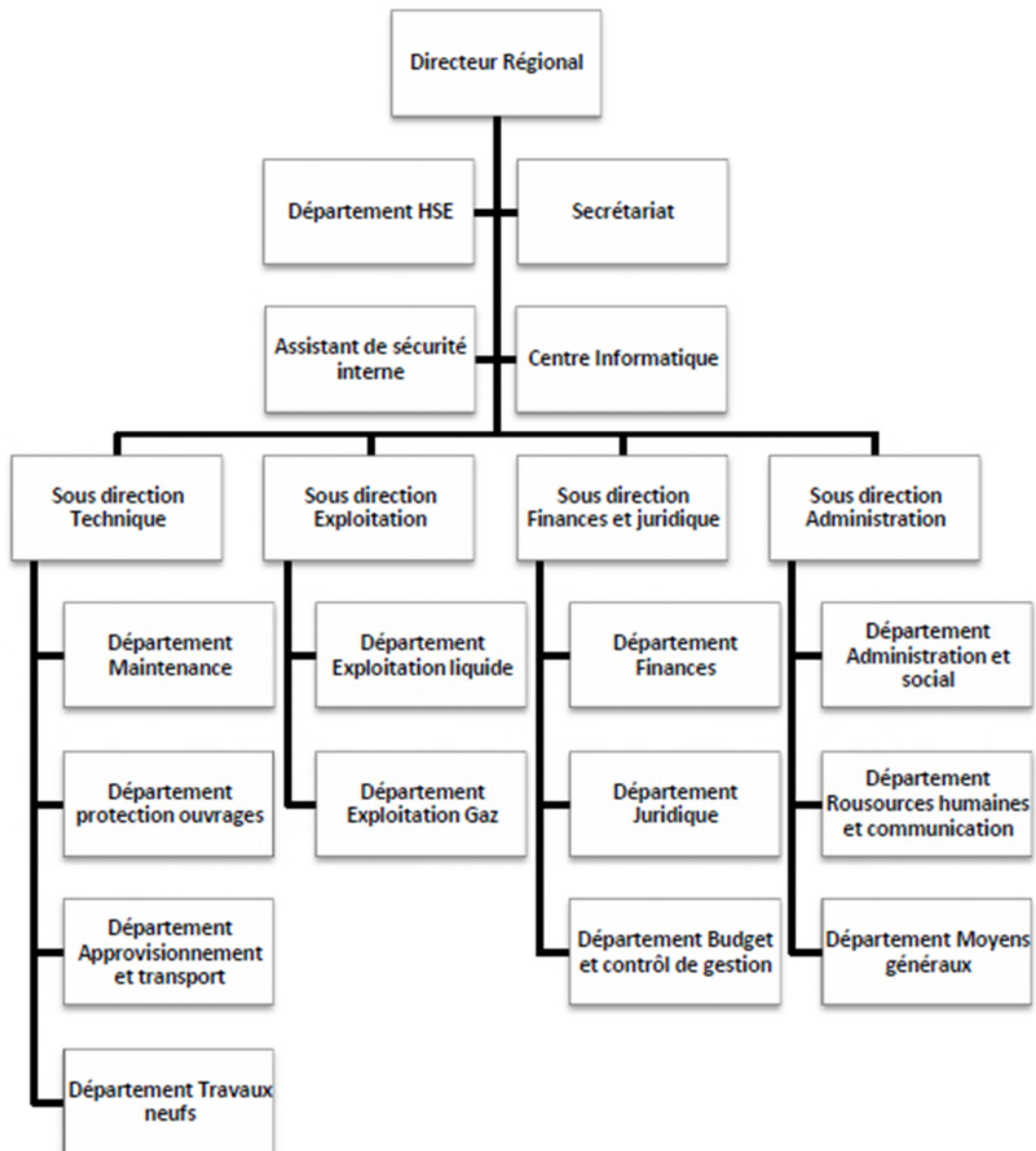


Figure 2.3- Organisation de la direction régionale de Bejaïa.

2.3.1 Département Maintenance

Le Département maintenance est rattaché à la sous-direction technique, a pour mission d'assurer la maintenance des installations et du matériel de production et garantir leur bon fonctionnement, en la réglementation en matière de sécurité dans l'entreprise. Ses missions principales sont :

- Garantir et optimiser les outils de production en orientant sur les décisions d'investissements,
- Mettre en place une politique de maintenance préventive (organisation, système d'information, etc),
- Gérer l'activité du service maintenance (suivi de tableaux de bord, reporting, etc.) et coordonner l'action des prestataires [5].

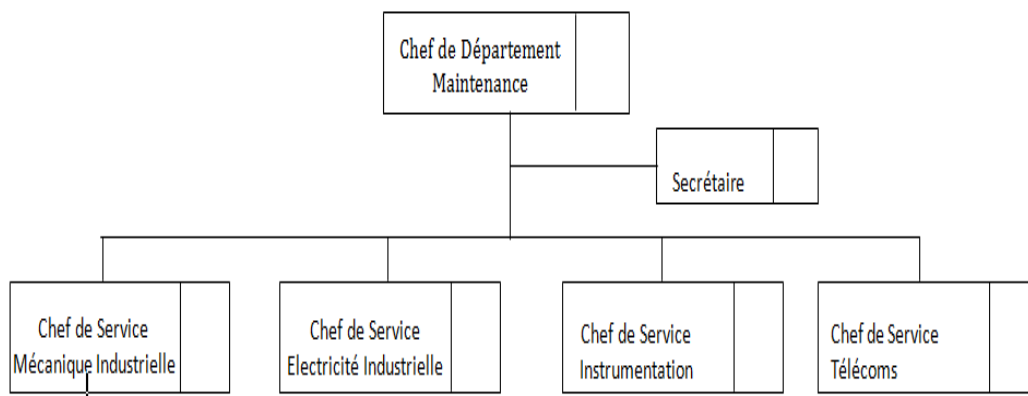


Figure 2.4 - Organigramme du Département Maintenance SDT / RTC.

Parmi les métiers représentés, on trouve les services suivants :

- Service des Télécommunications;
- Service Mécanique Industrielle;
- Service Instrumentation Industrielle;
- Service Electricité Industrielle.

2.3.2 Département 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 Bejaia (DRGB) et des autres régions [5]. Ce centre s'organise en trois services suivants :

- **Service système et réseau**

Système :

- Choix des équipements informatiques et logiciels de base;
- Mise en œuvre des solutions matérielles et logicielles retenues;

- Installation et configuration des systèmes;
- Mise en œuvre des nouvelles versions de logiciels.

Réseau :

- Assurer le bon fonctionnement et la fiabilité des communications;
 - Assurer l'administration du réseau et organiser l'évolution de sa structure;
 - Etude et choix de l'architecture du réseau à installer et la participation à sa mise en place;
 - Définition des droits d'accès à l'utilisation du réseau;
 - Assurer la surveillance permanente pour détecter les pannes;
 - Traitement des incidents survenant sur le réseau.
- **Service base de données et logiciel**
 - **Service supports**

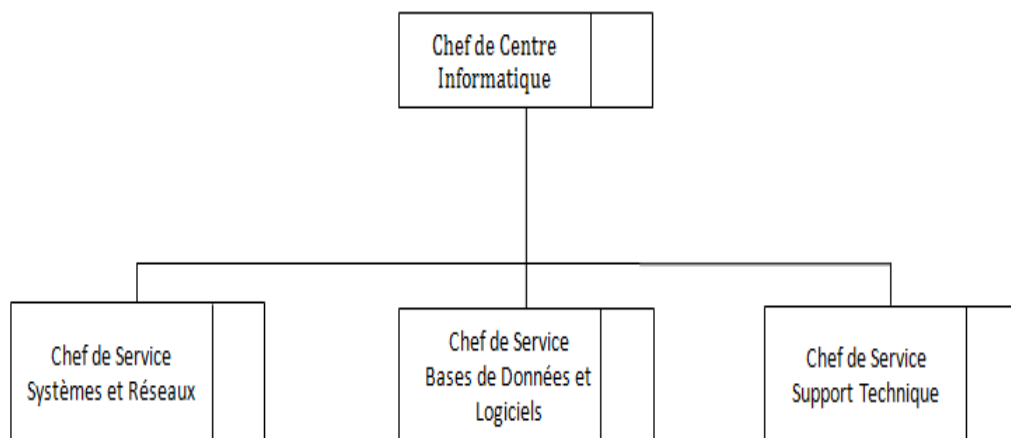


Figure 2.5- Organigramme du Centre Informatique RTC.

2.4 Aspect réseau

Le réseau de la DRGB est constitué de deux parties connectées entre elles (réseau de l'ancien bâtiment et le réseau du nouveau bâtiment). En effet ce dernier a subi une extension après la construction du nouveau bâtiment comme le montre la Figure 2.6 suivante :

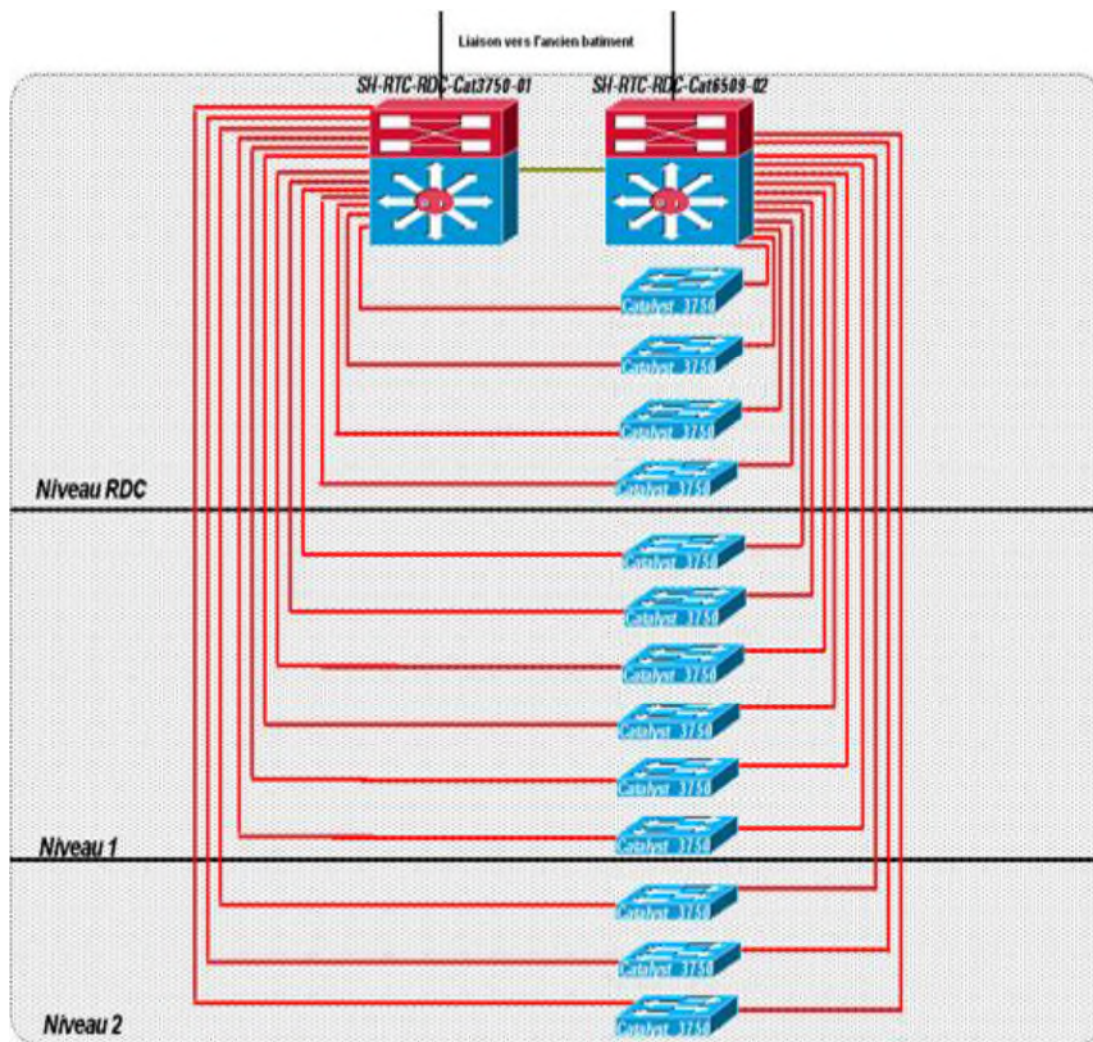


Figure 2.6- Structure réseau de SONATRACH.

2.4.1 Les commutateurs utilisés dans le réseau de la DRGB

Le réseau de la DRGB contient deux types de commutateurs [5] :

- 1. Des commutateurs intelligents :** en plus de leur fonction ils peuvent faire le routage. Dans le réseau de la DRGB, on trouve trois exemples de ce type qui sont :

- ✓ **Catalyst 6509** : C'est une gamme de commutateurs CISCO qui offre des performances et une densité de ports évolutives sur un large choix de configurations de châssis et d'interfaces LAN/WAN/MAN. Disponibles sur des châssis de 3, 6, 9 ou 13 emplacements. Les commutateurs CISCO Catalyst 6500 réunissent une gamme de modules de services intégrés comprenant la sécurité de réseau multi gigabit, la commutation de contenu, la téléphonie et des modules d'analyse de réseau.



Figure 2.7–Gamme catalyst cisco 6509.

- ✓ **Catalyst 3750** : C'est une gamme de commutateurs CISCO qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables. Cette gamme de produits dispose de la technologie Cisco StackWise™, interconnectant les commutateurs au sein d'une même pile à 32 Gbps qui permet de construire un système unique de commutation à haute disponibilité, vu comme un simple commutateur virtuel.



Figure 2.8–Gamme catalyst cisco 3750.

- ✓ **Catalyst 3560** : C'est une gamme de commutateurs CISCO empilables, il fournit une haute disponibilité et des fonctionnalités avancées de qualité de service et de la sécurité afin d'améliorer l'exploitation du réseau.



Figure 2.9 – Gamme catalyst 3560.

2. Des commutateurs non intelligents : Ce type de commutateurs ne permet pas de faire le routage. Le réseau de la DRGB (Direction Régionale de Béjaia) contient le type suivant :

- ✓ **Catalyst 2950** : C'est une gamme de commutateurs CISCO destinée à la commutation d'étages dédiée Ethernet 10/100/1000 Mbits/s fixe, offrant des performances, une souplesse et une administration exceptionnelle. Cette gamme de commutateurs 10/100/1000 à détection automatique offre de nombreuses fonctionnalités avancées de qualité de service et de traitement des flux multicast. L'interface de gestion Web fournit des fonctions d'administration faciles à utiliser via la suite CMS (Cisco Cluster Management Suite) et le logiciel Cisco IOS intégré.



Figure 2.10 – Gamme catalyst 2950.

2.4.2 Les routeurs utilisés dans le réseau de la DRGB

Le réseau de la DRGB contient les deux types de routeurs suivants :

- ✓ **CISCO 1700** : C'est une gamme de routeurs d'accès modulaires souples et sécurisés utilisée lorsqu'il s'agit de réseaux WAN.
- ✓ **CISCO 1941** : C'est une gamme de routeurs à services intégré haut débit qui permet aux petits bureaux d'exploiter des services sécurisés simultanés comme le pare-feu, les VPN et les réseaux LAN sans fil.

2.5 La structure hiérarchique du réseau SONATRACH

Afin de mieux répondre aux besoins des entreprises, la conception d'un réseau doit s'effectuer suivant un modèle hiérarchique (réseau commuté).

- **Le réseau commuté**

Le réseau commuté est un réseau convergent, appelé aussi réseau campus utilisé dans l'entreprise pour adapter au mode de gestion des activités quotidiennes par celle-ci. Cette technologie permet le partage en temps réel des ressources entre plusieurs personnes distantes, comme s'elles étaient au même endroit. Ce réseau prend en charge des fonctionnalités telles que la qualité de service, la sécurité renforcée, la prise en charge de la technologie sans fil, la téléphonie IP et les services de mobilité [W1].

Ce réseau est caractérisé par trois couches, chacune peut être considérée comme un module bien défini et structuré, avec des rôles et des fonctions spécifiques, ces couches sont les suivantes :

- **Couche accès** : Elle sert d'interface avec les périphériques finaux (ordinateurs, les imprimantes et les téléphones sur IP), afin de fournir l'accès au reste du réseau. La couche d'accès peut inclure des routeurs, des commutateurs, des ponts, des concentrateurs et des points d'accès sans fil. Son rôle principal est de fournir un moyen de connecter et de contrôler les périphériques qui sont autorisés à communiquer sur le réseau.

- **Couche distribution** : Elle regroupe les données reçues à partir des commutateurs de la couche d'accès, avant qu'elles ne soient transmises vers la couche cœur du réseau, afin de les transmettre aux destinataires. La couche de distribution gère le flux du trafic réseau. Elle délimite les domaines de diffusion via des fonctions de routage entre les réseaux locaux virtuels (VLANs) définis au niveau de la couche d'accès. Les commutateurs de la couche distribution sont généralement des périphériques très performants qui offrent une disponibilité et une redondance élevée afin de garantir la fiabilité.
- **Couche Core** : Est de réseau fédérateur, Elle connecte plusieurs couches du réseau de campus, son objectif principal d'assurer l'isolation des défaillances et la connectivité haut débit de ce réseau.

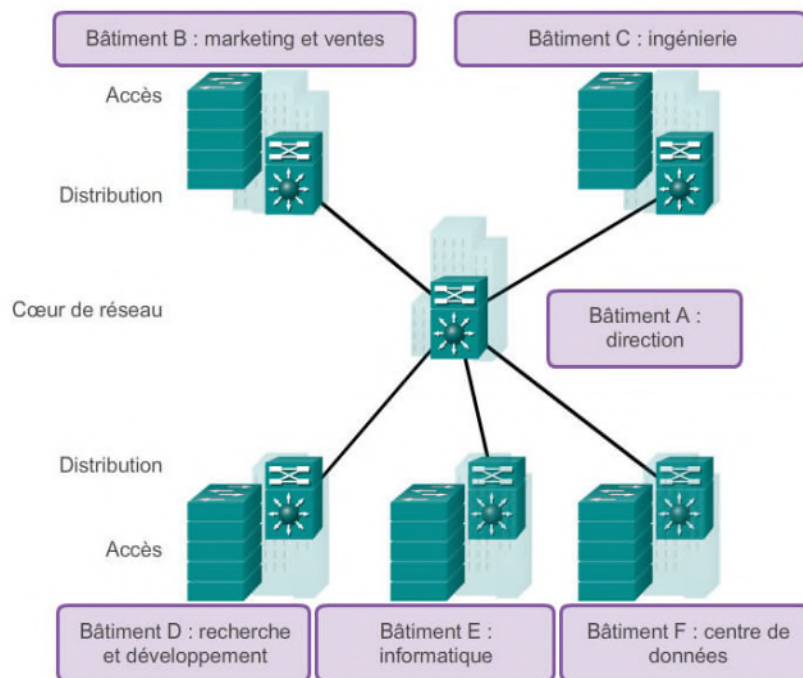


Figure 2.11- Représentation d'un réseau commuté.

2.6 Aspect sécurité

La figure 2.12, représente l'architecture sécurisée de SONATRACH avec ses différents serveurs de protection :

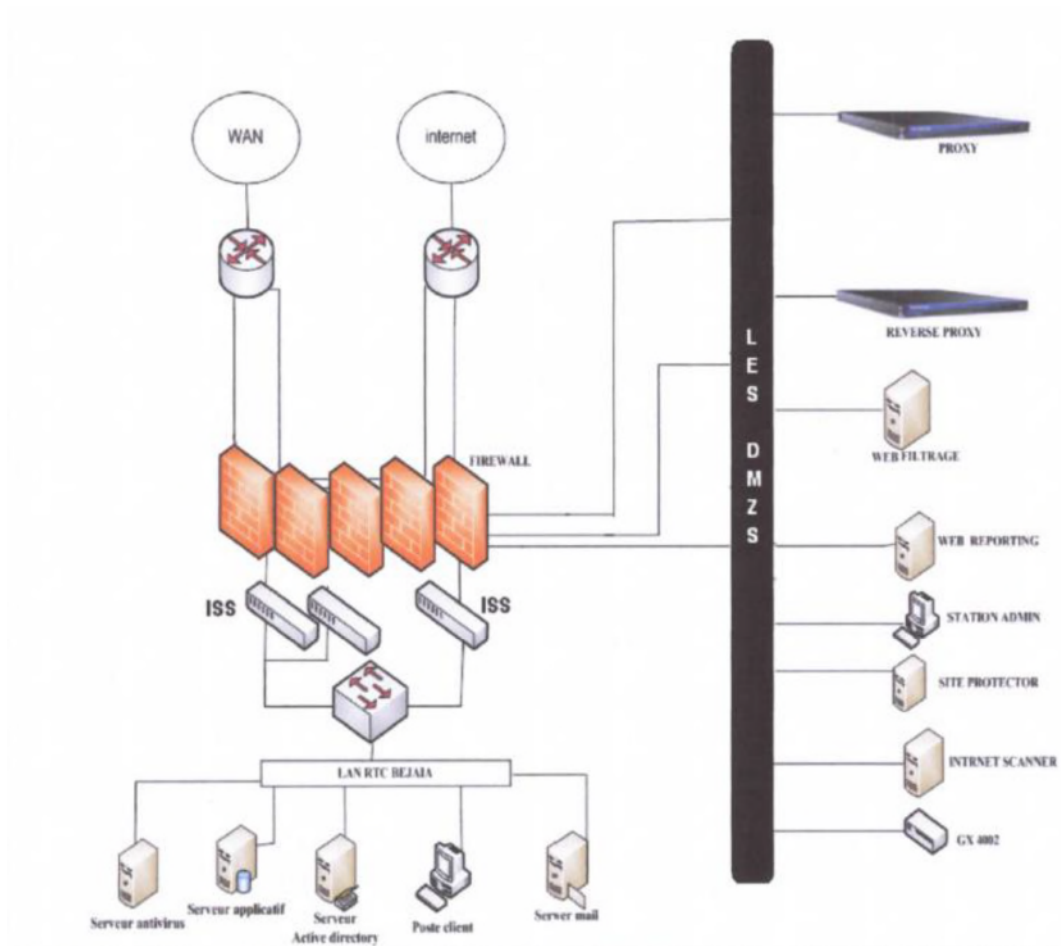


Figure 2.12- Partie sécurité de SONATRACH.

- ✓ **Serveur antivirus** : les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de programme modifiant ou supprimant des fichiers, que ce soit des documents infectés de l'utilisateur ou des fichiers nécessaires au bon fonctionnement de l'ordinateur. Un antivirus vérifie les fichiers et courriers électroniques, les secteurs de boot (pour détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD... etc.), les données qui transitent sur les éventuels réseaux (dont internet) etc [5].

- ✓ **Serveur filtrage web** : permet d'interdire l'accès à des sites au contenu répréhensible ou plus simplement de bloquer les bannières publicitaires. Les règles de filtrage sont mises à jour automatiquement dans l'établissement à partir d'une base de données. Les sites filtrés sont classés par catégories (adultes, piratages, publicités) modifiables; ainsi c'est l'établissement qui maîtrise sa politique de filtrage [5].

- ✓ **Serveur reporting** : c'est un outil complet et de rapport facile à utiliser qui permet d'évaluer l'utilisation de l'Internet par des employés de l'entreprise, identifier tous les problèmes possibles avec accès à l'Internet ou à l'exploitation de bande passante réseau en générant des rapports détaillés, des résumés ou des graphiques. Il est utilisé pour montrer comment la connexion Internet est utilisée et pour affiner les stratégies de filtrage afin de maximiser les ressources du réseau [5].

- ✓ **Firwall juniper ssg 550** : représente une nouvelle classe de dispositif de sécurité construite à cet effet qui offre un parfait mélange de haute performance, de sécurité et de connectivité LAN/WAN pour les déploiements du bureau régional et de leurs branches. Avec un réseau éprouvé et la protection au niveau application, le SSG 550 peut être mis en œuvre [5].



Figure 2.13- Firewall Juniper ssg 550.

Firewall juniper ssg 550 représenté dans la figure 2.13 contient un ensemble de règles structurées en trois zones qui se présentent comme suit :

- **La zone trust** : C'est la zone la plus confiante, car elle autorise le trafic sortant et interdit le trafic entrant et c'est pour cela que la RTC lui a confiée son réseau LAN.
- **La zone untrust** : C'est une zone qui autorise de trafic entrant et interdit le trafic sortant.

- **La DMZ (Demilitarized Zone)** : C'est une zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet derrière le par-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (DNS, HTTP, DHCP). Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise et, pour certains, depuis le réseau externe. Le but est ainsi d'éviter toute connexion directe au réseau interne [5].

2.7 Problématique

Après avoir analysé l'état actuel du réseau informatique de SONATRACH, nous avons soulevé des problèmes de fragilité vis-à-vis de la mauvaise répartition de l'architecture de celui-ci, d'où provient la congestion (plusieurs communications sont envoyées simultanément sur le réseau), conséquence d'une demande excessive en bande passante dépassant ainsi la quantité disponible, et la collision (lorsque deux périphériques ou plus dans le même réseau essaient de communiquer en même temps), qui rend le réseau vulnérable et exposé à l'intrusion des malveillants.

2.8 Solutions proposées

L'objectif de notre projet est la conception et la réalisation d'un modèle du réseau de l'entreprise, dont le but est d'améliorer la sécurité, et de faciliter la mise en œuvre d'un système d'information de l'entreprise. Ce modèle est basé sur un réseau local LAN interconnecté avec un réseau WAN, en utilisant des technologies de réseau étendu et des protocoles de routage dynamique. Nous avons suggéré un ensemble de propositions et de solutions qui peuvent remédier aux différentes lacunes soulevées durant notre stage :

- La segmentation du réseau en VLANs qui facilitent la gestion et le regroupement des postes;
- Contrôle de routage inter VLANs;
- Utilisation de la redondance matérielle au niveau de la couche Core afin de remédier aux pannes;
- Utilisation du Protocol Spanning-Tree dans notre réseau pour l'élimination des boucles Existantes;
- Utilisation de la Haute disponibilité dont le but d'optimiser la durée d'exécution en temps réel;

- Cryptage et chiffrement des équipements à l'aide des mots de passe;
- Installation d'un VPN pour crypter et chiffrer les données sortantes et entrantes de l'entreprise.

2.9 Conclusion

Dans ce chapitre, nous avons présenté l'entreprise SONATRACH en général et la Région Transport Centre Bejaïa (RTC) en particulier, et de l'étudier assez profondément afin de voir ses lacunes et ses faiblesses, cette étude nous a conduit à proposer des solutions pour palier à ces dernières.

Dans le chapitre suivant, nous allons faire la réalisation des objectifs cités précédemment, à savoir la conception du réseau et l'installation du matériel et sa configuration.

Chapitre 3

Configuration et segmentation d'un réseau virtuel VLAN

3.1 Introduction

Dans ce chapitre nous allons procéder à la conception et à la réalisation du réseau, ainsi que sa configuration. Ceci est une étape cruciale pour la mise en place de tout ce que nous avons vu dans les chapitres précédents. En se basant sur les différentes configurations nécessaires à l'implémentation sur les réseaux LAN, en utilisant l'outil CISCO appelé « Packet Tracer ».

Dans ce contexte, nous allons présenter les configurations réalisées, ainsi que les tests de validation pour confirmer le bon fonctionnement de ce réseau.

3.2 Présentation du simulateur Cisco « Packet Tracer »

Le « Cisco Packet Tracer » est l'un des programmes les plus répandus et qui est caractérisé par sa simplicité d'installation et d'exécution, sa librairie riche et sa licence gratuite, il permet de réaliser simuler, visualiser, créer et évaluer des plans d'infrastructure d'un réseau en temps réel.

Cisco Packet Tracer est un moyen d'apprentissage de la réalisation de divers réseaux et de découvrir le fonctionnement des différents éléments constituant un réseau informatique. Son objectif est de schématiser, configurer et de voir toutes les possibilités d'une future mise en œuvre réseau.

Le simulateur Cisco Packet Tracer possède une interface principale et différents équipements pour la réalisation d'une infrastructure réseau, figure 3.1.

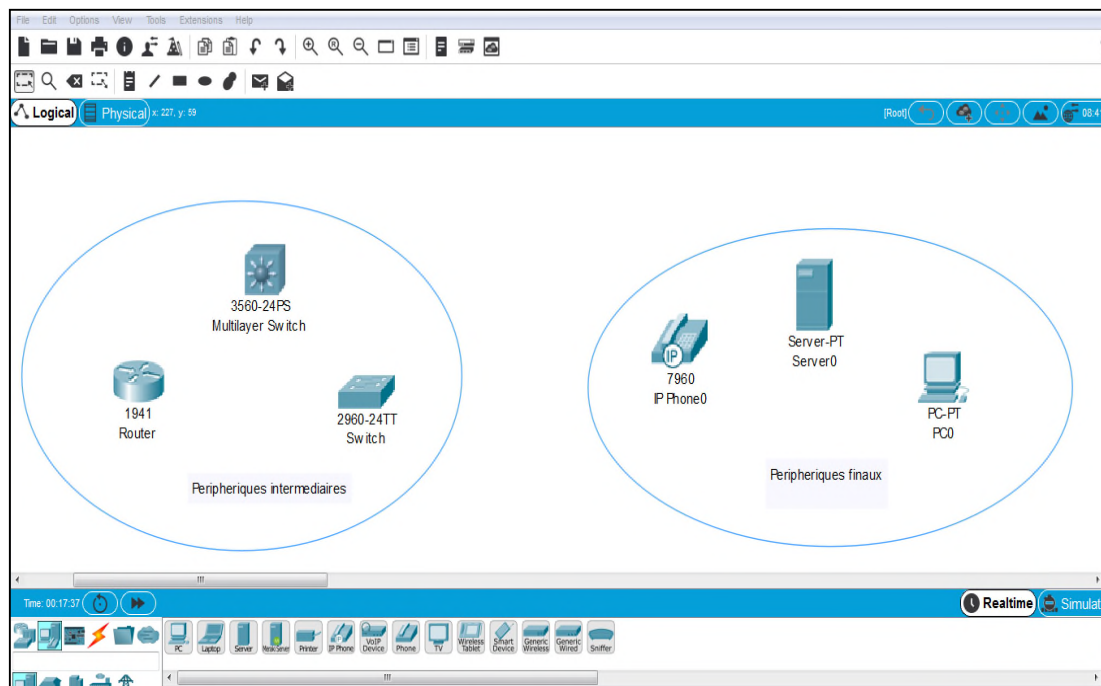


Figure 3.1- Interface principale du simulateur Cisco Packet Tracer.

- **Interface commande de Packet Tracer**

L'utilisateur accède à l'interpréteur de commandes à l'aide d'une interface en ligne de commande « CLI ».

CLI est une interface de simulateur Packet Tracer qui permet la configuration des équipements du réseau à l'aide d'un langage de commandes, c'est-à-dire que c'est à partir des commandes introduites par l'utilisateur du logiciel que la configuration sera réalisée.

3.3 Conception

Rappelant que le stage effectué au sein de l'entreprise s'est déroulé au niveau des deux services, à savoir Informatique et Télécommunication (Technique) et qui sont en relation avec les départements : Maintenance, Exploitation, HSE, Transport, Administration et serveur, tels que indiquer sur la figure 3.2.

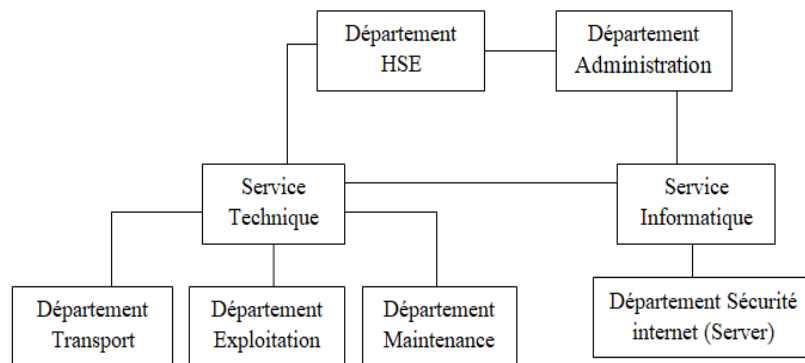


Figure 3.2 - Structure des départements.

Le réseau actuel de SONATRACH est dépourvu d'une architecture organisée qui permet une bonne gestion et exploitation des ressources. C'est dans ce cadre, qu'on a adopté une stratégie afin de répondre à ces besoins, basée sur l'attribution des VLANs à chaque département, les six VLANs sont interconnectés via quatre switches, ces derniers sont reliés à deux multiswitchs qui sont en liaison direct au routeur principal de l'entreprise.

- **Présentation de l'architecture du réseau avant la configuration**

La figure 3.3 illustre l'architecture réseau LAN que nous avons réalisé sur « PACKET TRACER », en se basant sur le réseau hiérarchique de l'entreprise décrit précédemment.

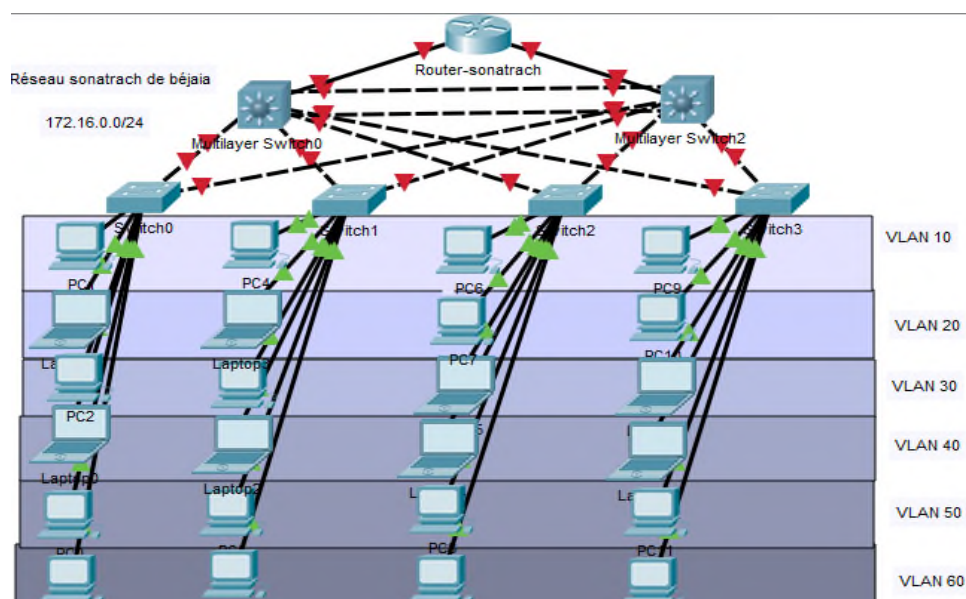


Figure 3.3 - Présentation de l'architecture.

3.4 Segmentation VLANs

La notion de VLAN est un concept qui permet de réaliser une sécurité optimale des réseaux de façon indépendante du système de câblage. Ces réseaux nous permettrons :

- D'améliorer la gestion du réseau.
- Plus de souplesse pour l'administration. Augmenter la sécurité sur le réseau.
- Réduction de la diffusion du trafic sur le réseau

- **Plan d'adressage**

Le plan d'adressage est la stratégie qui s'applique afin de permettre l'accessibilité des différentes entités d'un réseau de la manière la plus optimale.

L'objectif premier du plan d'adressage est d'éviter la duplication accidentelle des adresses, c'est-à-dire, il permet de désigner un équipement sans ambiguïté, car une adresse IP affectée ne doit pas être réutilisée.

- **Adressage des VLANs**

L'adresse du réseau est 172.16.0.0/24 avec une possibilité de création de 254 sous réseaux, avec un masque 255.255.255.0

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

Le tableau 3.1 suivant montre le plan d'adressage des VLANs :

VLAN-id	Nom VLAN	Adresse sous réseau
10	Maint	172.16.10.0/24
20	Expl	172.16.20.0/24
30	HSE	172.16.30.0/24
40	Trans	172.16.40.0/24
50	Admin	172.16.50.0/24
60	Server	172.16.60.0/24

Tableau 3.1- Plan d'adressage des VLANs.

3.5 Configuration des équipements

On va procéder à la configuration de tous les équipements du réseau.

3.5.1 Configuration du nom de périphérique

Cette configuration consiste en l'attribution d'un nom au périphérique en utilisant la commande « *hostname* » en mode configuration global.

```
Switch > enable
```

```
Switch #configuration terminal
```

```
Switch (config) #hostname MULTI-SW1
```

```
MULTI-SW1 (config) #
```

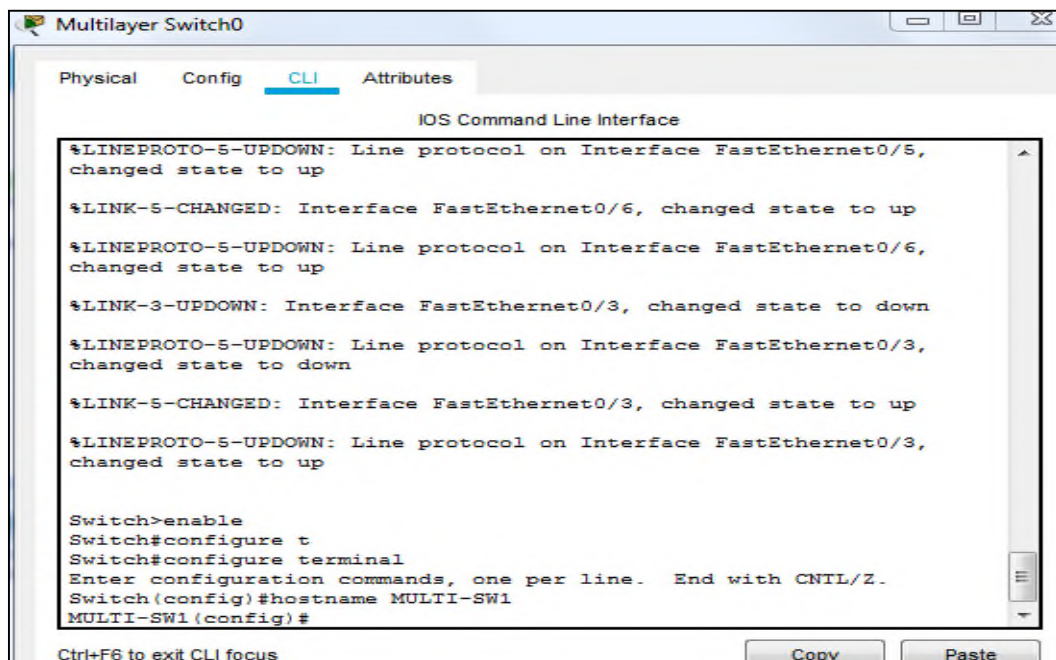


Figure 3.4- Nomination du multilayer switch0.

3.5.2 Sécurisation d'accès aux périphériques

Il faut savoir qu'IOS (International Standardization Organization) utilise des modes organisés hiérarchiquement pour faciliter la protection des périphériques. Dans le cadre de ce dispositif de sécurité, IOS peut accepter plusieurs mots de passe, ce qui permet d'établir différents privilèges d'accès au périphérique. La figure 3.5 représente une configuration d'un accès à distance (Telnet).

Pour spécifier un mot de passe sur une ligne, on utilise la commande « *password* » dans le mode de configuration de la ligne. Pour activer la vérification du mot de passe à la connexion, on utilise la commande « *login* » dans le mode de configuration de la ligne.

- **Configurer la ligne console :**

```
multi-SW1 >enable
multi-SW1#configuration terminal
multi-SW1(config)#line console 0
multi-SW1(config-line)#password AX32cv
multi-SW1(config-line)#login
```

- **Configurer le terminal virtuel (vty) :**

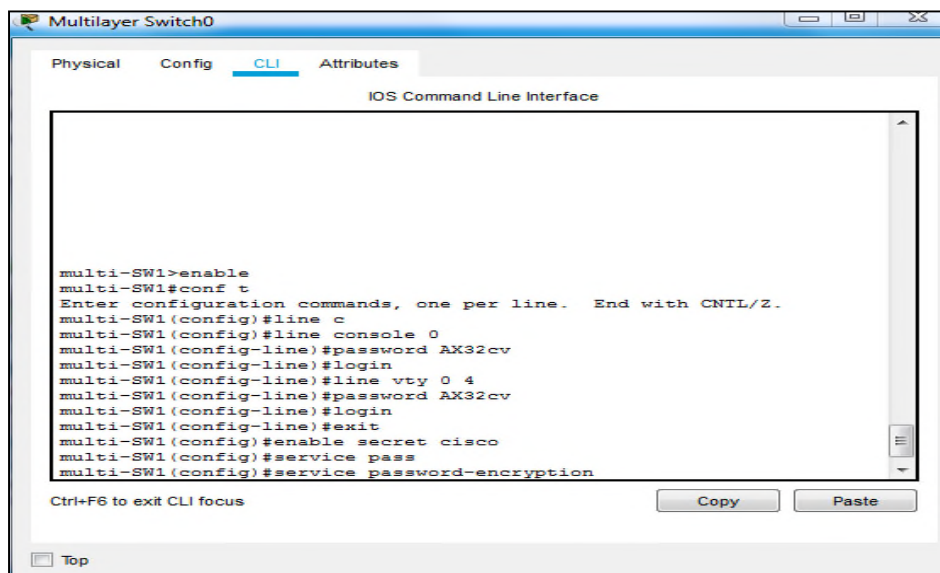
```
multi-SW1(config-line)#line vty 0 4
multi-SW1(config-line)# password AX32cv
multi-SW1(config-line)# login
multi-SW1(config-line)#exit
```

- **Définir le mot de passe du mode d'exécution privilégié :**

```
multi-SW1(config)#enable secret cisco
```

La commande « *service password-encryption* » est pour le chiffrement des mots de passes configurés .

```
multi-SW1(config)#service password-encryption
```



```
Multilayer Switch0
Physical Config CLI Attributes
IOS Command Line Interface

multi-SW1>enable
multi-SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
multi-SW1(config)#line c
multi-SW1(config-line)#line console 0
multi-SW1(config-line)#password AX32cv
multi-SW1(config-line)#login
multi-SW1(config-line)#line vty 0 4
multi-SW1(config-line)#password AX32cv
multi-SW1(config-line)#login
multi-SW1(config-line)#exit
multi-SW1(config)#enable secret cisco
multi-SW1(config)#service pass
multi-SW1(config)#service password-encryption

Ctrl+F6 to exit CLI focus
```

Figure 3.5 - Configuration du mot de passe.

Cette configuration de base s'applique aux niveaux de tous les switches et Multiswitchs, en tenant compte de la variation des noms d'un switch à un autre.

3.5.3 Configuration du protocole VTP

L'ensemble des commutateurs cœur de LAN seront configurés comme des serveurs VTP. Donc, se sont eux qui gèrent l'administration de l'ensemble des VLANs. Un nom de domaine « Sonatrach » est attribué, permet à tous les Switchs d'être dans le même "groupe d'amis".

La figure 3.6 représente la configuration du serveur VTP au niveau du Multiswitch.

```
Password : AX32cv
multi-SW1 >enable
password : cisco
multi-SW1#configuration terminal
multi-SW1(config)# vtp mode server
multi-SW1(config)# vtp domain Sonatrach
```

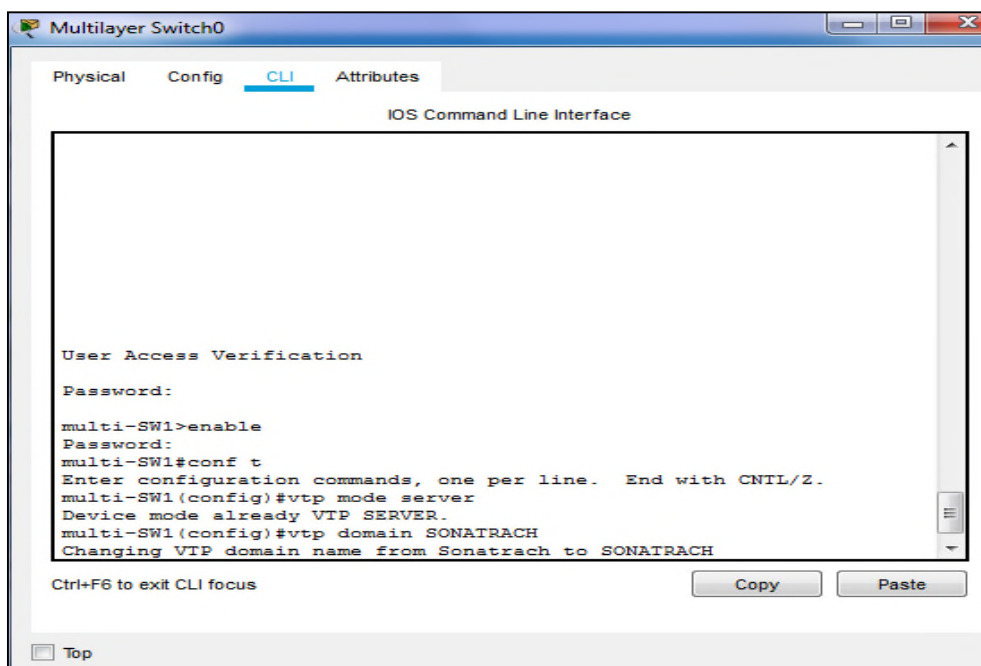


Figure 3.6 - Configuration du VTP-server.

Par ailleurs, la configuration des clients VTP sera au niveau de tous les commutateurs accès. Un Switch en mode client ne permet pas à l'administrateur de faire des modifications sur les VLANs. On reçoit un message d'erreur quand nous essayons de créer un VLAN. La figure 3.7 montre la configuration au niveau de SW2.

```
Password : AX32cv
SW2> enable
password :cisco
SW2# configure terminal
SW2 (config)# vtp mode server
SW2 (config)# vtp domain Sonatrach
```

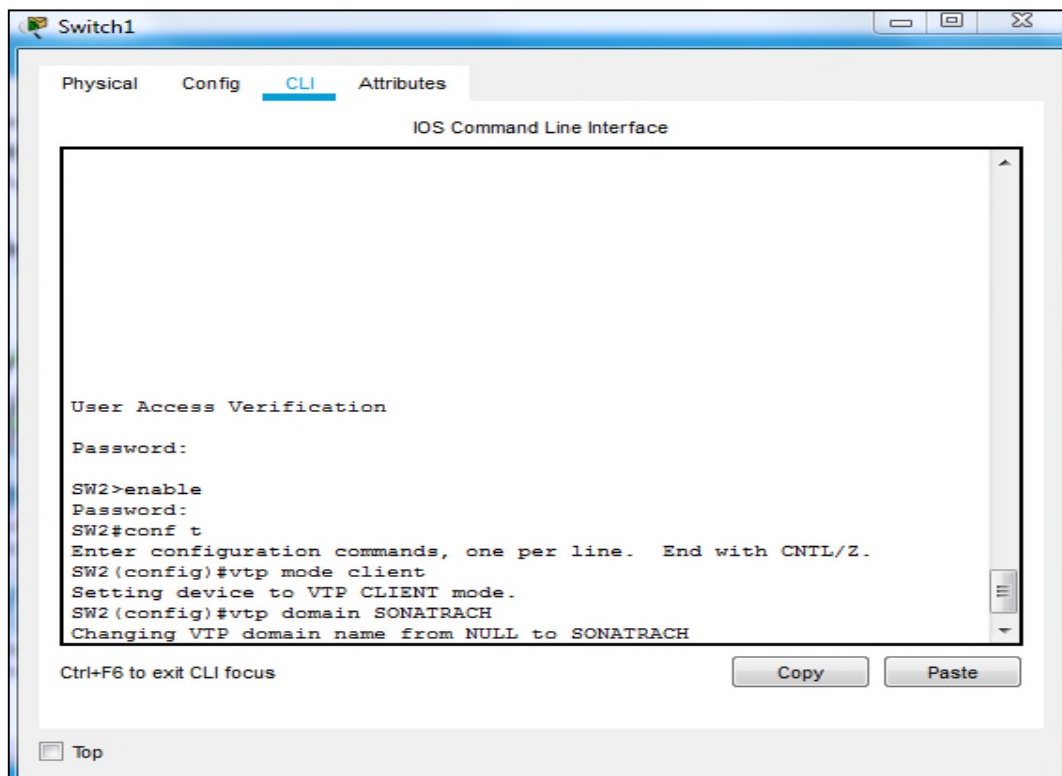


Figure 3.7 - Configuration client-VTP.

3.5.4 Création des VLANs

La création des VLANs est faite au niveau des MultiSwitch (VTP server) comme le montre la figure 3.8.

```
Multi-SW1#configure terminale
Multi-SW1(config)# vlan 10
Multi-SW1(config-vlan)# name Maint
Multi-SW1(config-vlan)# exit
```

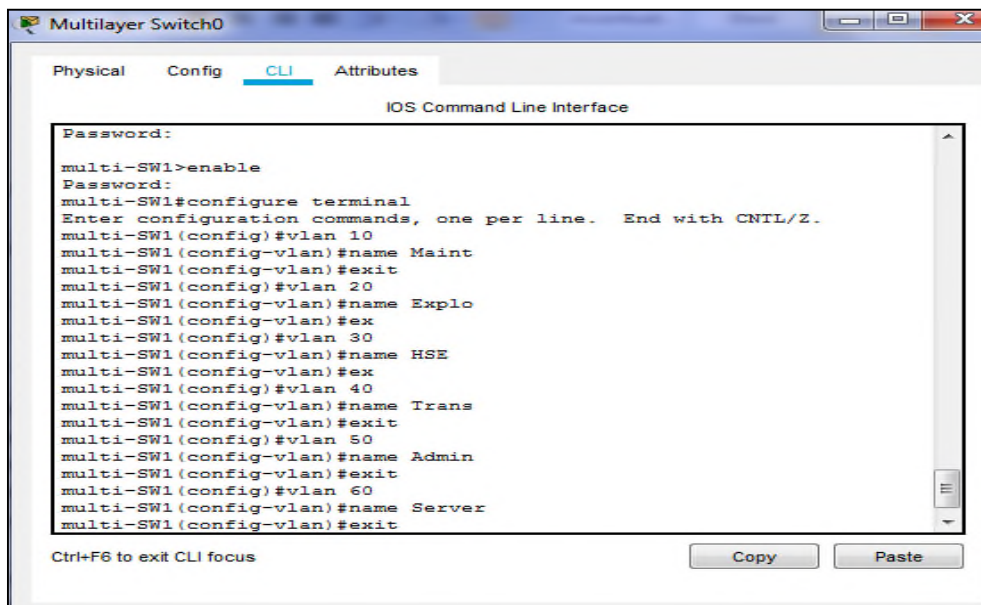


Figure 3.8 - Création des VLANs sur le serveur VTP.

La création et la configuration de tous les VLANs s'effectue au niveau du "VTP-serveur" d'une manière similaire ; néanmoins une variation des noms est nécessaire.

3.5.5 Attribution des ports des commutateurs aux VLANs

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

```
SW1(config)# interface f0/3
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 10
SW1(config-if)# interface f0/4
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 20
SW1(config-if)# interface f0/5
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 30
SW1(config-if)# interface f0/6
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 40
SW1(config-if)# interface f0/7
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 50
SW1(config-if)# interface f0/8
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 60
```

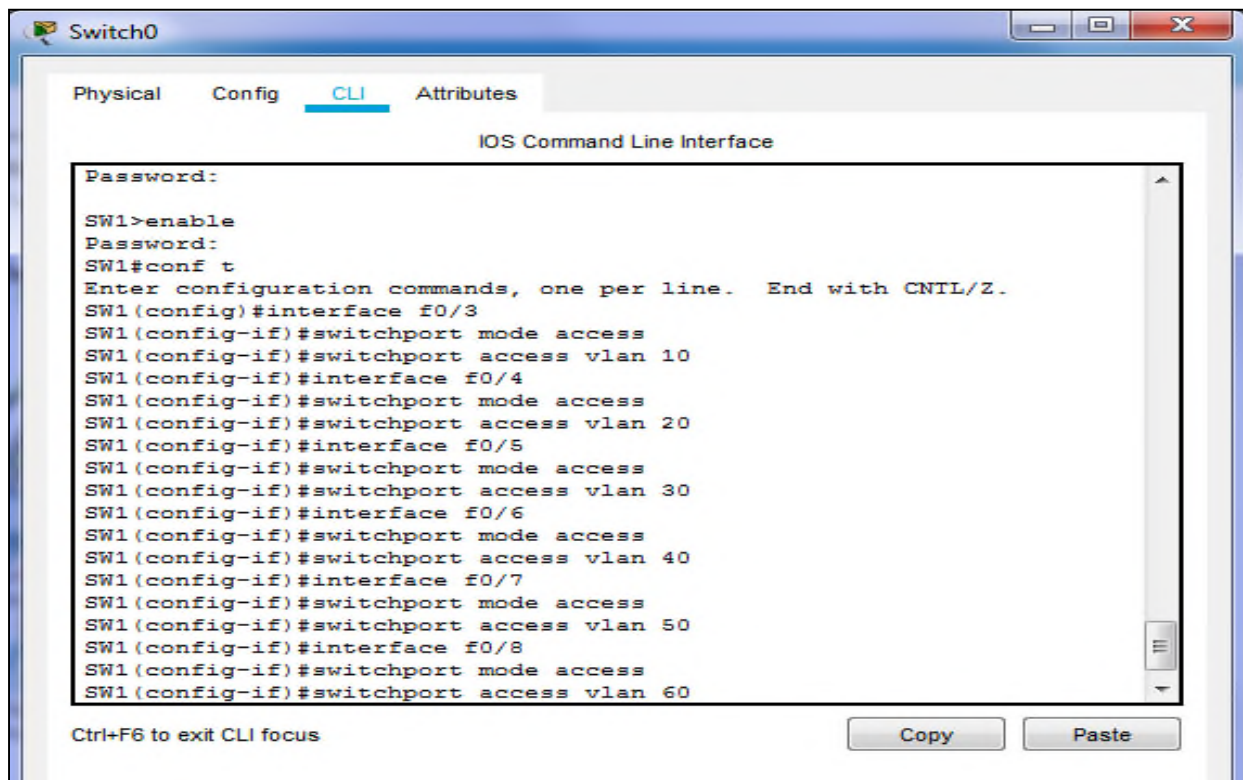


Figure 3.9 - Attribution des ports aux VLANs.

3.5.6 Configuration des liens trunk

Les interfaces des équipements d'interconnexion à configurer en mode trunk, existent toutes entre l'ensemble des commutateurs accès et le commutateur cœur. Les commandes suivantes permettent d'associer un port à un vlan en mode trunk en utilisant la commande « *range* » qui pourra réunir toutes les interfaces en une seule fois. Figure 3.10

```
Multi-SW2(config)#interface range f0/1-6
```

```
Multi-SW2(config-if)#switchport trunk encapsulation dot1q
```

```
Multi-SW2(config-if)#switchport mode trunk
```

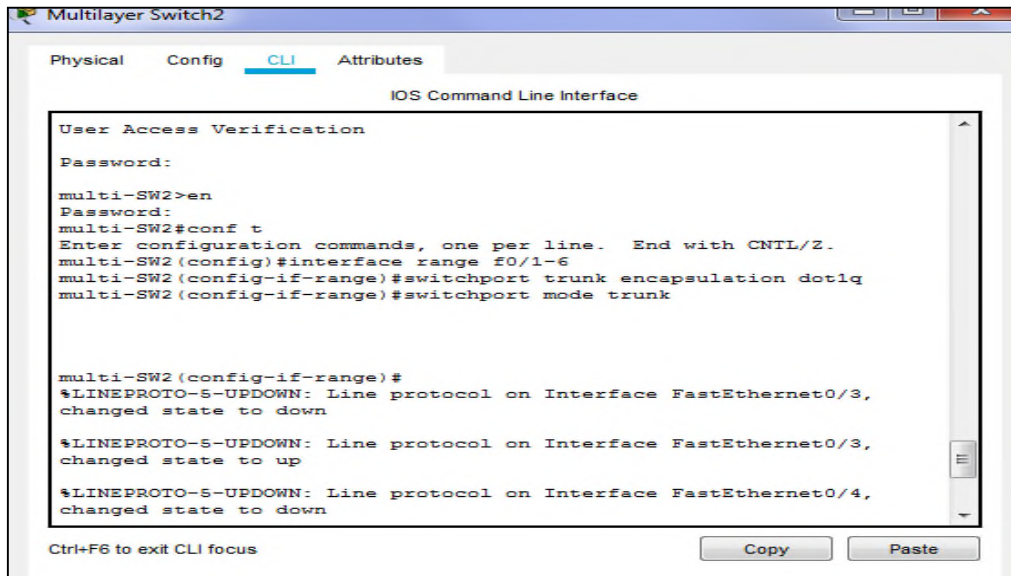


Figure 3.10 - Configuration des liens trunk.

La configuration de l'agrégation trunk se fera sur le reste de tous les switches.

3.5.7 Configuration des interfaces VLANs

La configuration des interfaces VLANs est faite au niveau du MultiSwitch en donnant des adresses IP pour les VLANs, comme le montre la figure 3.11.

```

multi-SW1(config)#interface vlan 10
multi-SW1(config-if)#ip address 172.16.20.252 255.255.255.0
multi-SW1(config-if)#exit

```

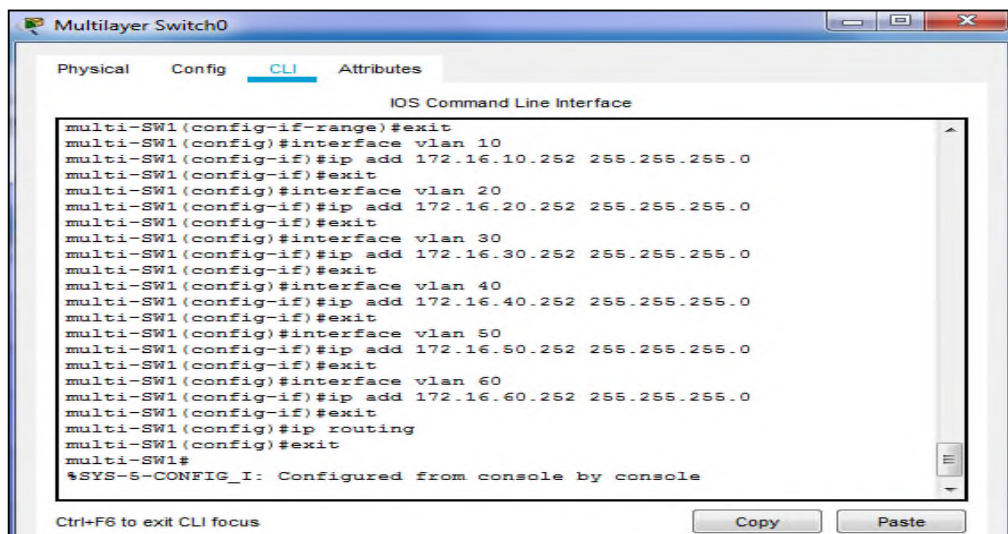


Figure 3.11 - Configuration des interfaces VLANs.

Il faut ensuite activer la fonction de routage avec la commande « *ip routing* ».

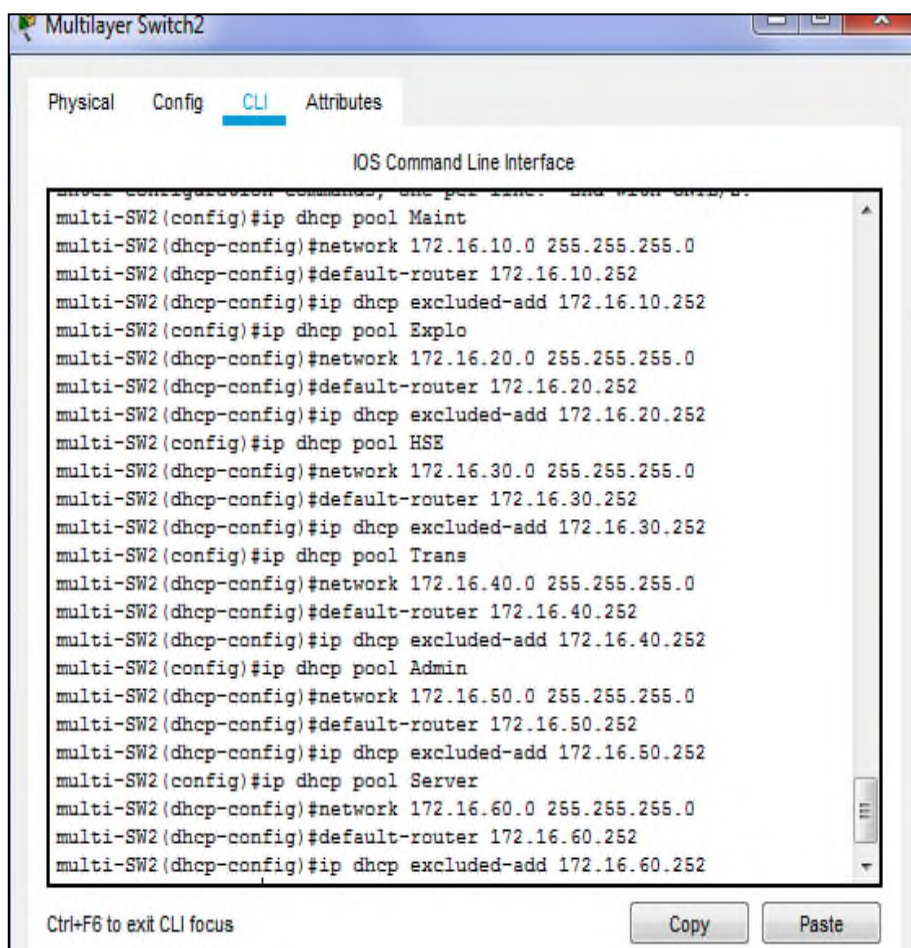
La configuration de tous les VLANs s'effectue au niveau du « multi-SW2 » d'une manière similaire; néanmoins le changement des id-VLAN et de l'adresse IP est indispensable.

3.5.8 Configuration de DHCP

Afin de simplifier à l'administrateur la gestion et l'attribution des adresses IP, on utilise le protocole DHCP qui permet de configurer les paramètres réseaux client, au lieu de les configurer sur chaque ordinateur client. La figure 3.12 illustre les commandes qui nous permettent de configurer ce protocole au niveau de MultiSwitch .

Le protocole DHCP devra donc distribuer une adresse sur la plage IP 172.16.0.0/24 avec une exclusion des adresses 172.16.0.252 ainsi que la passerelle par défaut ;

```
Multi-SW2(config)# ip dhcp pool Maint
Multi-SW2(dhcp-config)# network 172.16.10.0 255.255.255.0
Multi-SW2(dhcp-config)# default-router 172.16.10.252
Multi-SW2(dhcp-config)# ip dhcp excluded-add 172.16.10.252
```



```
Multilayer Switch2
Physical Config CLI Attributes
IOS Command Line Interface
multi-SW2 (config)# ip dhcp pool Maint
multi-SW2 (dhcp-config)# network 172.16.10.0 255.255.255.0
multi-SW2 (dhcp-config)# default-router 172.16.10.252
multi-SW2 (dhcp-config)# ip dhcp excluded-add 172.16.10.252
multi-SW2 (config)# ip dhcp pool Explo
multi-SW2 (dhcp-config)# network 172.16.20.0 255.255.255.0
multi-SW2 (dhcp-config)# default-router 172.16.20.252
multi-SW2 (dhcp-config)# ip dhcp excluded-add 172.16.20.252
multi-SW2 (config)# ip dhcp pool HSE
multi-SW2 (dhcp-config)# network 172.16.30.0 255.255.255.0
multi-SW2 (dhcp-config)# default-router 172.16.30.252
multi-SW2 (dhcp-config)# ip dhcp excluded-add 172.16.30.252
multi-SW2 (config)# ip dhcp pool Trans
multi-SW2 (dhcp-config)# network 172.16.40.0 255.255.255.0
multi-SW2 (dhcp-config)# default-router 172.16.40.252
multi-SW2 (dhcp-config)# ip dhcp excluded-add 172.16.40.252
multi-SW2 (config)# ip dhcp pool Admin
multi-SW2 (dhcp-config)# network 172.16.50.0 255.255.255.0
multi-SW2 (dhcp-config)# default-router 172.16.50.252
multi-SW2 (dhcp-config)# ip dhcp excluded-add 172.16.50.252
multi-SW2 (config)# ip dhcp pool Server
multi-SW2 (dhcp-config)# network 172.16.60.0 255.255.255.0
multi-SW2 (dhcp-config)# default-router 172.16.60.252
multi-SW2 (dhcp-config)# ip dhcp excluded-add 172.16.60.252
Ctrl+F6 to exit CLI focus
Copy Paste
```

Figure 3.12 - Configuration de DHCP.

La même configuration sera établie pour Explo, HSE, Trans, Admin et Server, une variation des adresses IP est nécessaire.

3.5.9 Configuration de STP

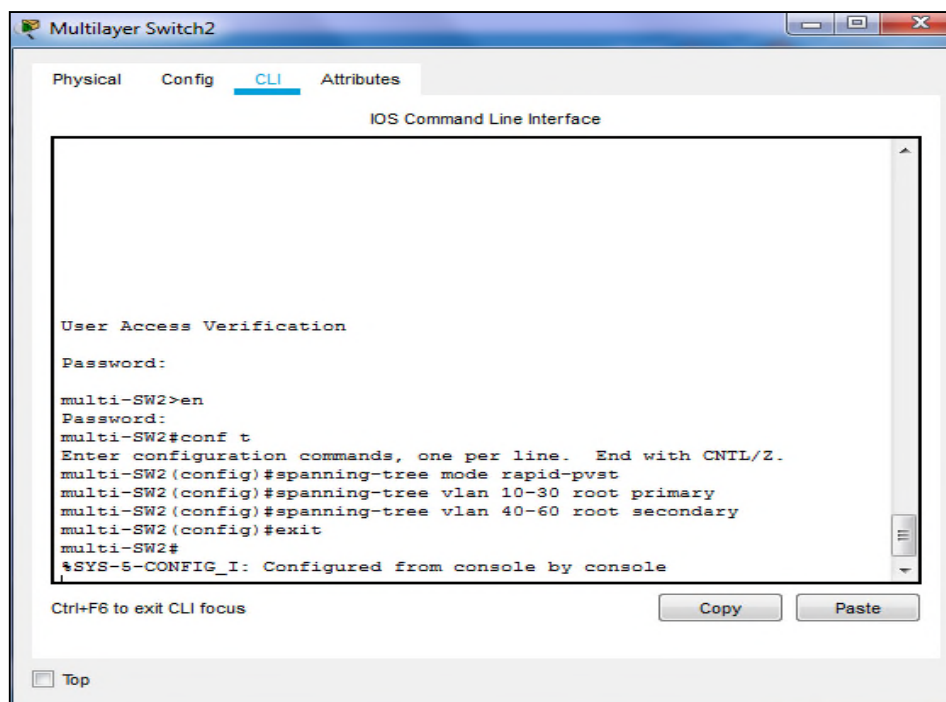
La figure 3.13 illustre les commandes qui nous permettent de configurer le protocole STP, et d'affecter un root primaire ou secondaire à un VLAN.

```
Multi-SW2(config)# spanning-tree mode rapid-pvst
```

```
Multi-SW2(config)# spanning-tree vlan 10-30 root primary
```

```
Multi-SW2(config)# spanning-tree vlan 40-60 root secondary
```

La commande « *spanning-tree mode rapid-pvst* », son rôle est de configurer le mode du protocole rapid PVST.



```
Multilayer Switch2
Physical Config CLI Attributes
IOS Command Line Interface

User Access Verification
Password:

multi-SW2>en
Password:
multi-SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
multi-SW2 (config)#spanning-tree mode rapid-pvst
multi-SW2 (config)#spanning-tree vlan 10-30 root primary
multi-SW2 (config)#spanning-tree vlan 40-60 root secondary
multi-SW2 (config)#exit
multi-SW2#
%SYS-5-CONFIG_I: Configured from console by console

Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

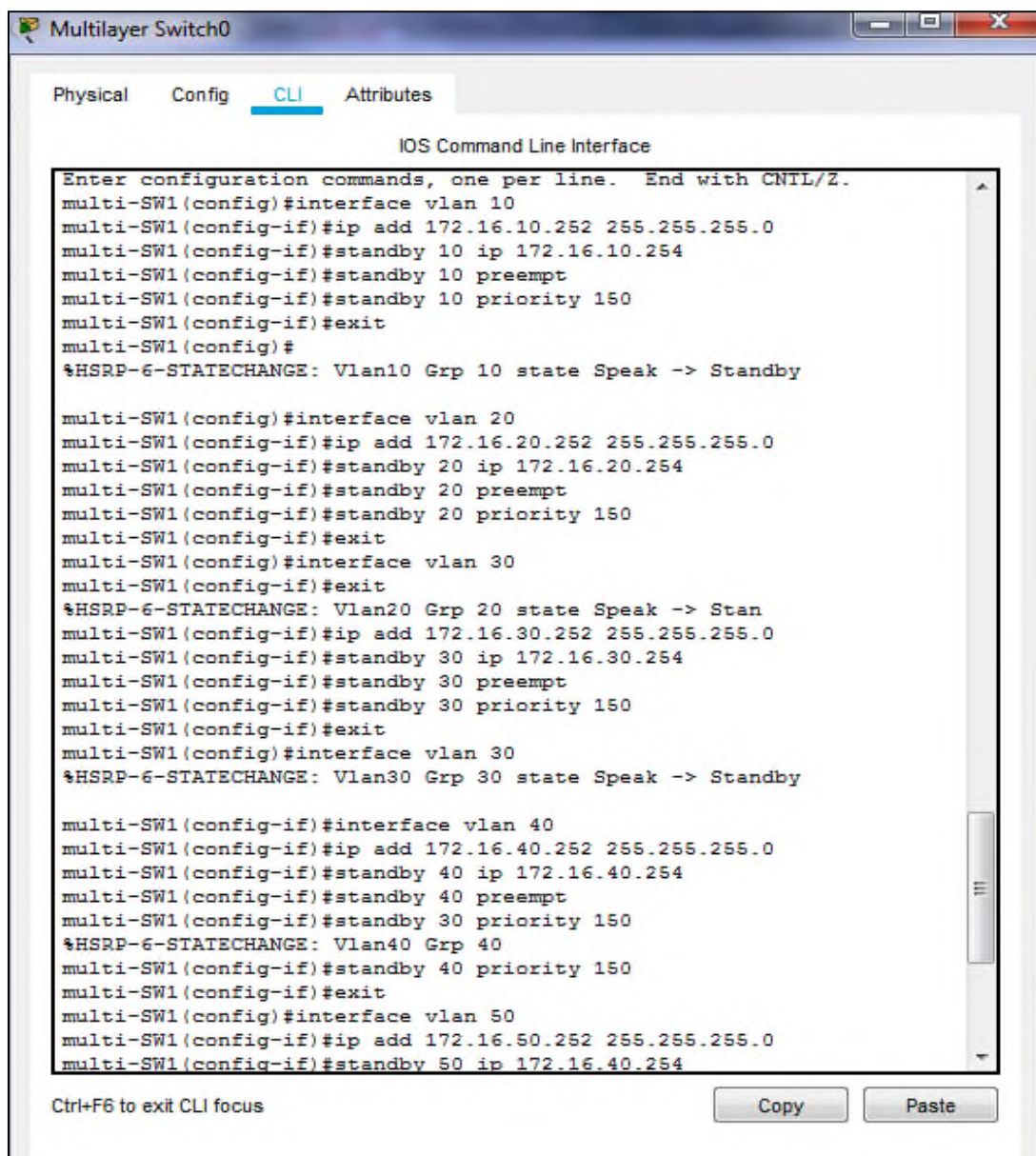
Figure 3.13 - Configuration de STP.

3.5.10 Configuration de la haute disponibilité HSRP

La configuration de la haute disponibilité s'effectue au niveau des Switchs multicouches on utilise deux sortes de configurations HSRP : la première lorsqu'un VLAN est prioritaire, la deuxième lorsqu'il est secondaire. La figure ci-dessous montre les VLANs prioritaires par rapport aux VLANs secondaires sur l'un des MultiSwitchs, et sur l'autre les priorités des VLANs seront renversées.

La commande « *standby preempt* » donne la priorité au multiswitch de protocole Cisco HSRP (Hot Standby Router Protocol) pour que ce dernier devienne actif immédiatement

La priorité de base est de 100. Avec une priorité de 150, multi-SW1 devient le routeur actif, On active l'option « *preempt* », qui permet au multiswitch actif de reprendre son rôle après une panne.



```
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
multi-SW1(config)#interface vlan 10
multi-SW1(config-if)#ip add 172.16.10.252 255.255.255.0
multi-SW1(config-if)#standby 10 ip 172.16.10.254
multi-SW1(config-if)#standby 10 preempt
multi-SW1(config-if)#standby 10 priority 150
multi-SW1(config-if)#exit
multi-SW1(config)#
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby

multi-SW1(config)#interface vlan 20
multi-SW1(config-if)#ip add 172.16.20.252 255.255.255.0
multi-SW1(config-if)#standby 20 ip 172.16.20.254
multi-SW1(config-if)#standby 20 preempt
multi-SW1(config-if)#standby 20 priority 150
multi-SW1(config-if)#exit
multi-SW1(config)#interface vlan 30
multi-SW1(config-if)#exit
%HSRP-6-STATECHANGE: Vlan20 Grp 20 state Speak -> Stan
multi-SW1(config-if)#ip add 172.16.30.252 255.255.255.0
multi-SW1(config-if)#standby 30 ip 172.16.30.254
multi-SW1(config-if)#standby 30 preempt
multi-SW1(config-if)#standby 30 priority 150
multi-SW1(config-if)#exit
multi-SW1(config)#interface vlan 30
%HSRP-6-STATECHANGE: Vlan30 Grp 30 state Speak -> Standby

multi-SW1(config-if)#interface vlan 40
multi-SW1(config-if)#ip add 172.16.40.252 255.255.255.0
multi-SW1(config-if)#standby 40 ip 172.16.40.254
multi-SW1(config-if)#standby 40 preempt
multi-SW1(config-if)#standby 40 priority 150
%HSRP-6-STATECHANGE: Vlan40 Grp 40
multi-SW1(config-if)#standby 40 priority 150
multi-SW1(config-if)#exit
multi-SW1(config)#interface vlan 50
multi-SW1(config-if)#ip add 172.16.50.252 255.255.255.0
multi-SW1(config-if)#standby 50 ip 172.16.40.254
```

Figure 3.14- Configuration de HSRP.

La figure 3.15 suivante illustre le réseau local que nous avons réalisé dans le simulateur Packet Tracer après la configuration des deux MultiSwitchs distribution :

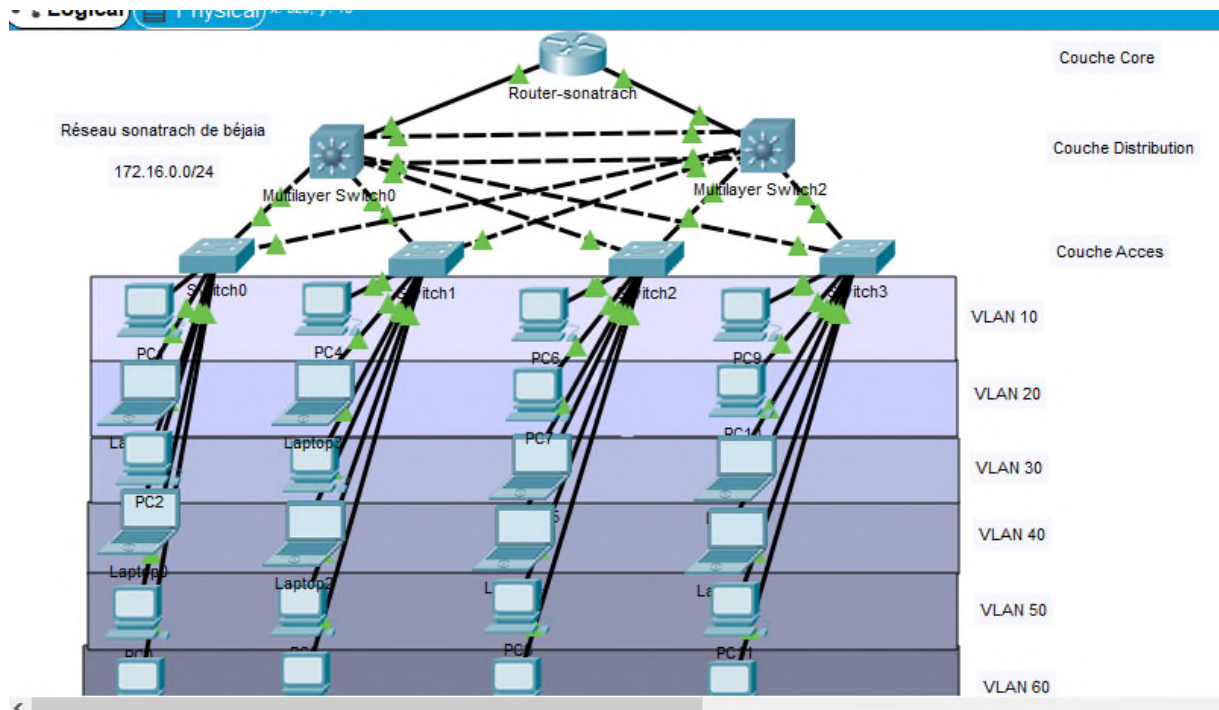


Figure 3.15- Réseau local après la configuration.

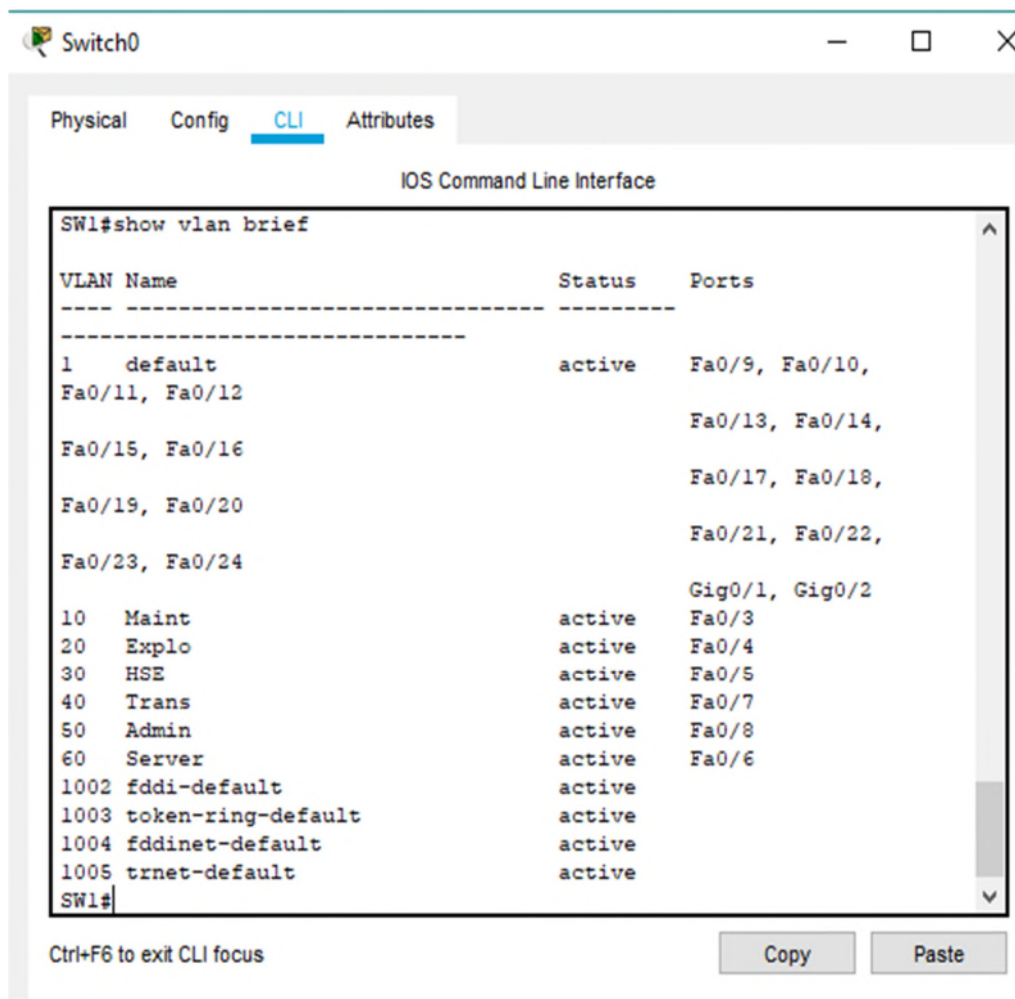
3.6 Vérification et test de validation

3.6.1 Vérification

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

1. Contrôle des réseaux locaux virtuels créés sur le Switch server

Nous nous sommes servis de la commande « *show vlan brief* » sur les Switchs client (s0, s1, s2, s3,) pour prouver que le serveur VTP a distribué sa configuration du réseau local virtuel à tous les commutateurs clients.



```
SW1#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gig0/1, Gig0/2
10 Maint	active	Fa0/3
20 Explo	active	Fa0/4
30 HSE	active	Fa0/5
40 Trans	active	Fa0/7
50 Admin	active	Fa0/8
60 Server	active	Fa0/6
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

SW1#

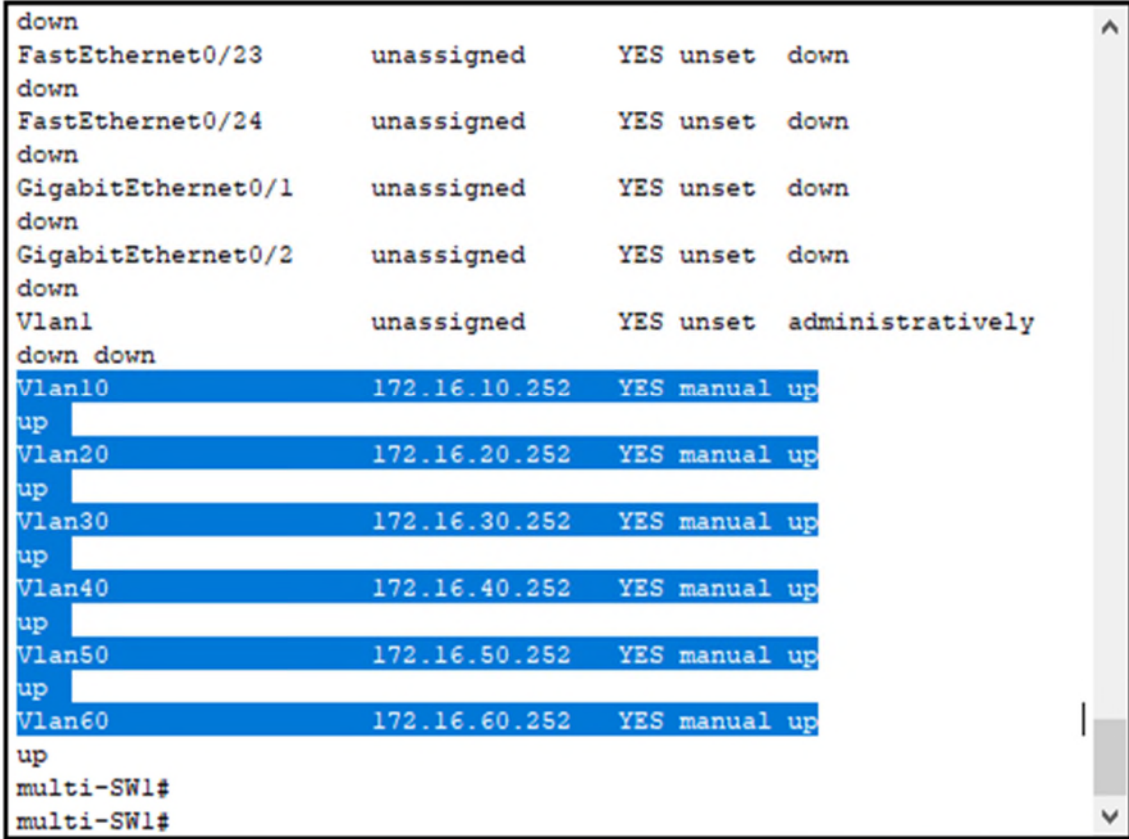
Ctrl+F6 to exit CLI focus

Copy Paste

Figure 3.16 - VLANs distribués dans le Switch client Sw1.

2. Vérification du routage inter VLAN

A l'aide de la commande « *show IP interface brief* » qui permet d'afficher un résumé des informations sur l'état des interfaces, on peut avoir l'état des Switches Virtuelle Interface (SVI) comme le montre la capture suivante. Figure 3.17.



```
Physical  Config  CLI  Attributes
IOS Command Line Interface
down
FastEthernet0/23      unassigned      YES unset  down
down
FastEthernet0/24      unassigned      YES unset  down
down
GigabitEthernet0/1    unassigned      YES unset  down
down
GigabitEthernet0/2    unassigned      YES unset  down
down
Vlan1                  unassigned      YES unset  administratively
down down
Vlan10                 172.16.10.252  YES manual  up
up
Vlan20                 172.16.20.252  YES manual  up
up
Vlan30                 172.16.30.252  YES manual  up
up
Vlan40                 172.16.40.252  YES manual  up
up
Vlan50                 172.16.50.252  YES manual  up
up
Vlan60                 172.16.60.252  YES manual  up
up
multi-SW1#
multi-SW1#
```

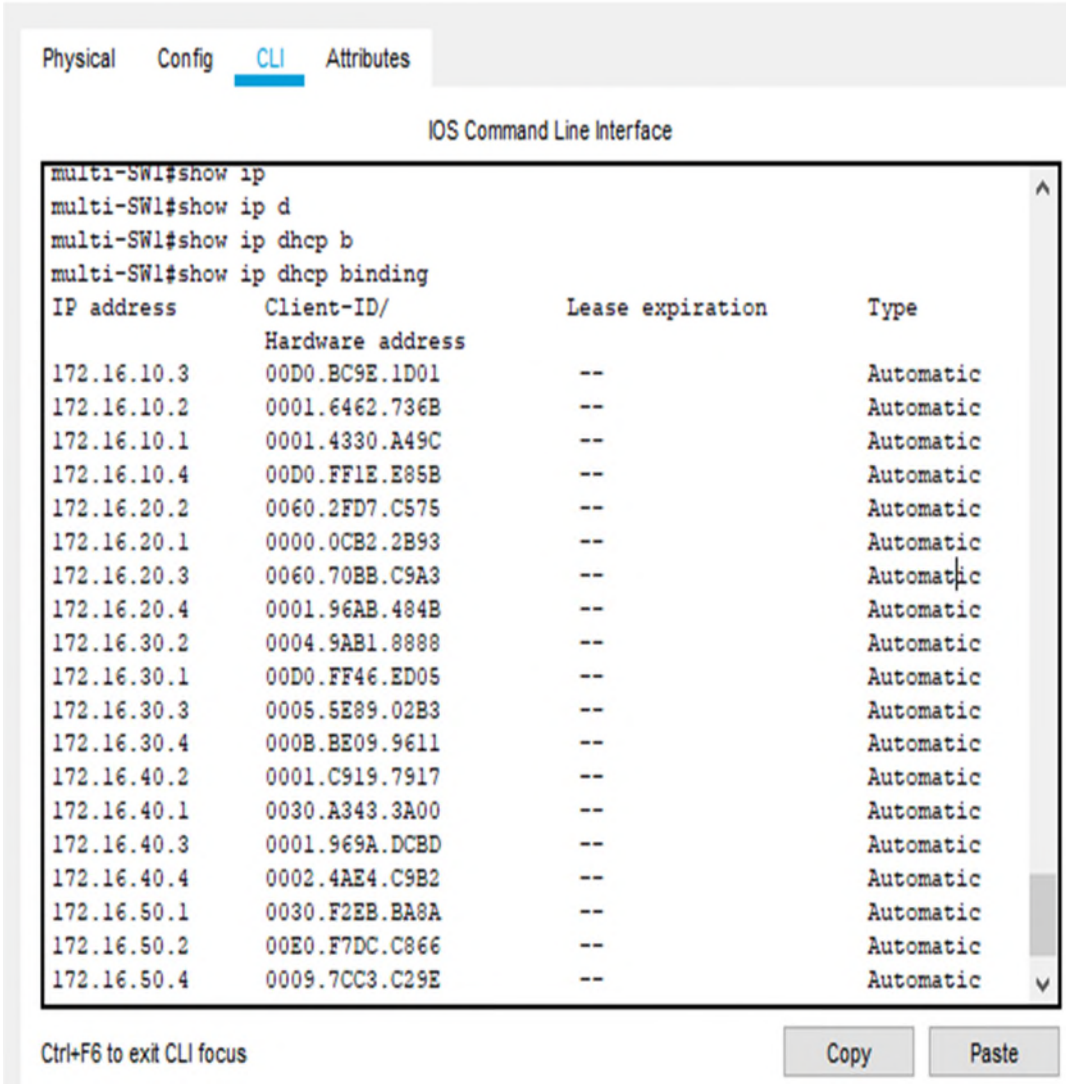
Ctrl+F6 to exit CLI focus

Copy Paste

Figure 3.17 - SVI (Switch Virtuelle Interface).

3. Vérification de la distribution des adresses IP avec le DHCP

Il est possible de vérifier que chaque poste a bien récupéré une adresse DHCP à l'aide de la commande « *show ip dhcp binding* » :



```
multi-SWI#show ip
multi-SWI#show ip d
multi-SWI#show ip dhcp b
multi-SWI#show ip dhcp binding
IP address      Client-ID/      Lease expiration  Type
                Hardware address
172.16.10.3     00D0.BC9E.1D01  --                Automatic
172.16.10.2     0001.6462.736B  --                Automatic
172.16.10.1     0001.4330.A49C  --                Automatic
172.16.10.4     00D0.FF1E.E85B  --                Automatic
172.16.20.2     0060.2FD7.C575  --                Automatic
172.16.20.1     0000.0CB2.2B93  --                Automatic
172.16.20.3     0060.70BB.C9A3  --                Automatic
172.16.20.4     0001.96AB.484B  --                Automatic
172.16.30.2     0004.9AB1.8888  --                Automatic
172.16.30.1     00D0.FF46.ED05  --                Automatic
172.16.30.3     0005.5E89.02B3  --                Automatic
172.16.30.4     000B.BE09.9611  --                Automatic
172.16.40.2     0001.C919.7917  --                Automatic
172.16.40.1     0030.A343.3A00  --                Automatic
172.16.40.3     0001.969A.DCBD  --                Automatic
172.16.40.4     0002.4AE4.C9B2  --                Automatic
172.16.50.1     0030.F2EB.BA8A  --                Automatic
172.16.50.2     00E0.F7DC.C866  --                Automatic
172.16.50.4     0009.7CC3.C29E  --                Automatic
```

Ctrl+F6 to exit CLI focus

Copy Paste

Figure 3.18-Attribution des adresses IP.

4. Vérification de HSRP

Nous utilisons la commande « *show standby brief* » en mode privilégié pour vérifier l'état de HSRP. Cette commande nous indique quel Switch est actif et qui est en attente.

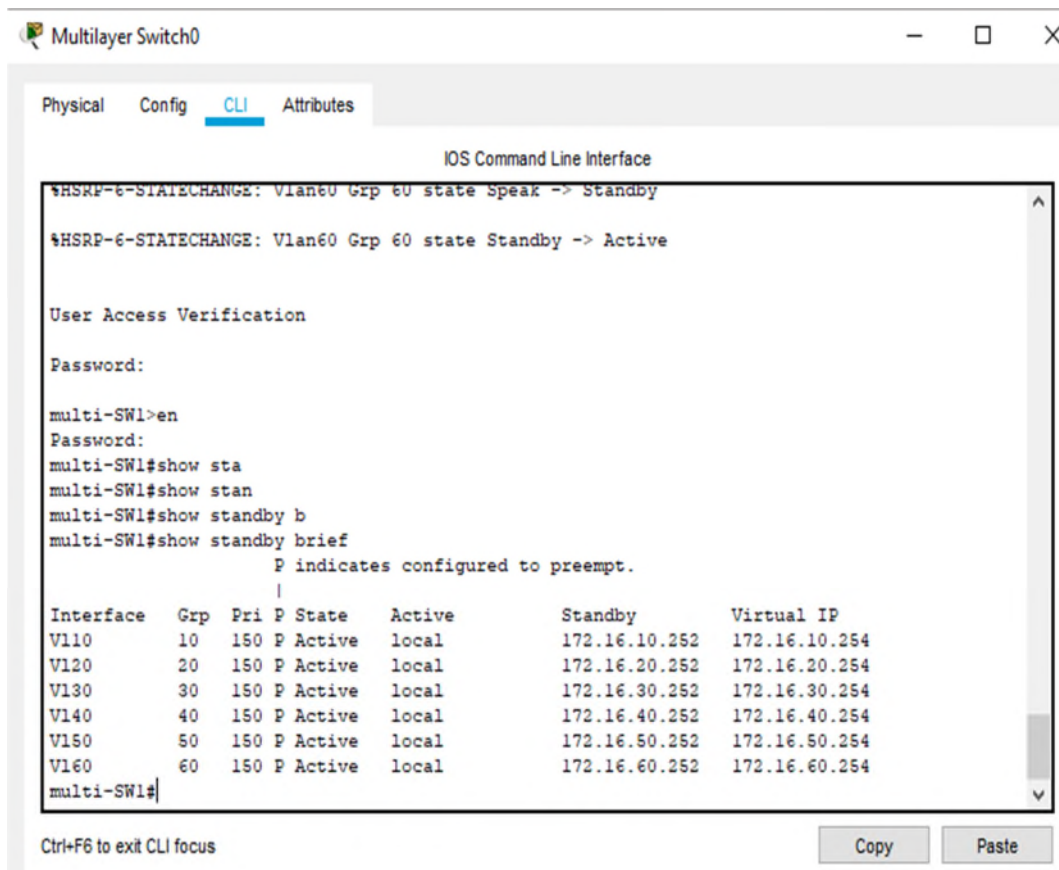


Figure 3.19-Switch multi-sw1 en mode active.

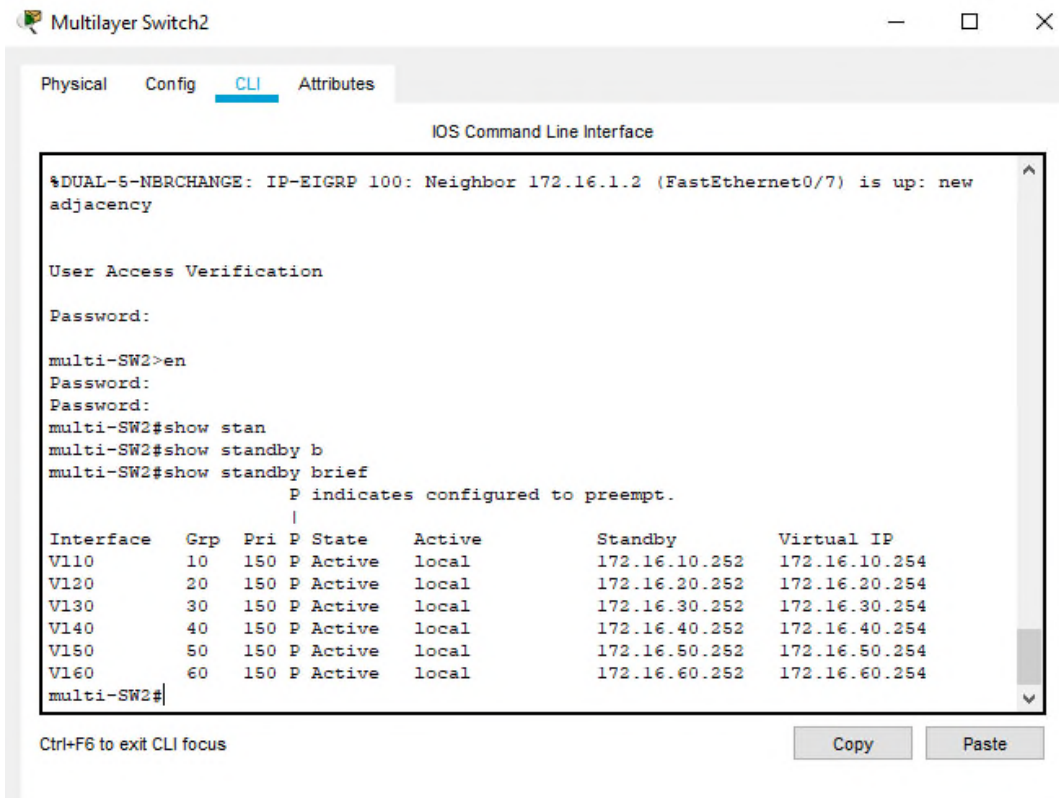


Figure 3.20- Switch multi-sw2 en mode active.

3.6.2 Tests de validation

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

1. Vérification de la communication entre les équipements d'interconnexion

On teste les communications inter-Switch et entre Switch et Switch multifonction.

- Exemple : Test réussi entre le multi-SW1 et le Switch d'accès, 5 paquets envoyés et 5 paquets reçus, figure 3.21.

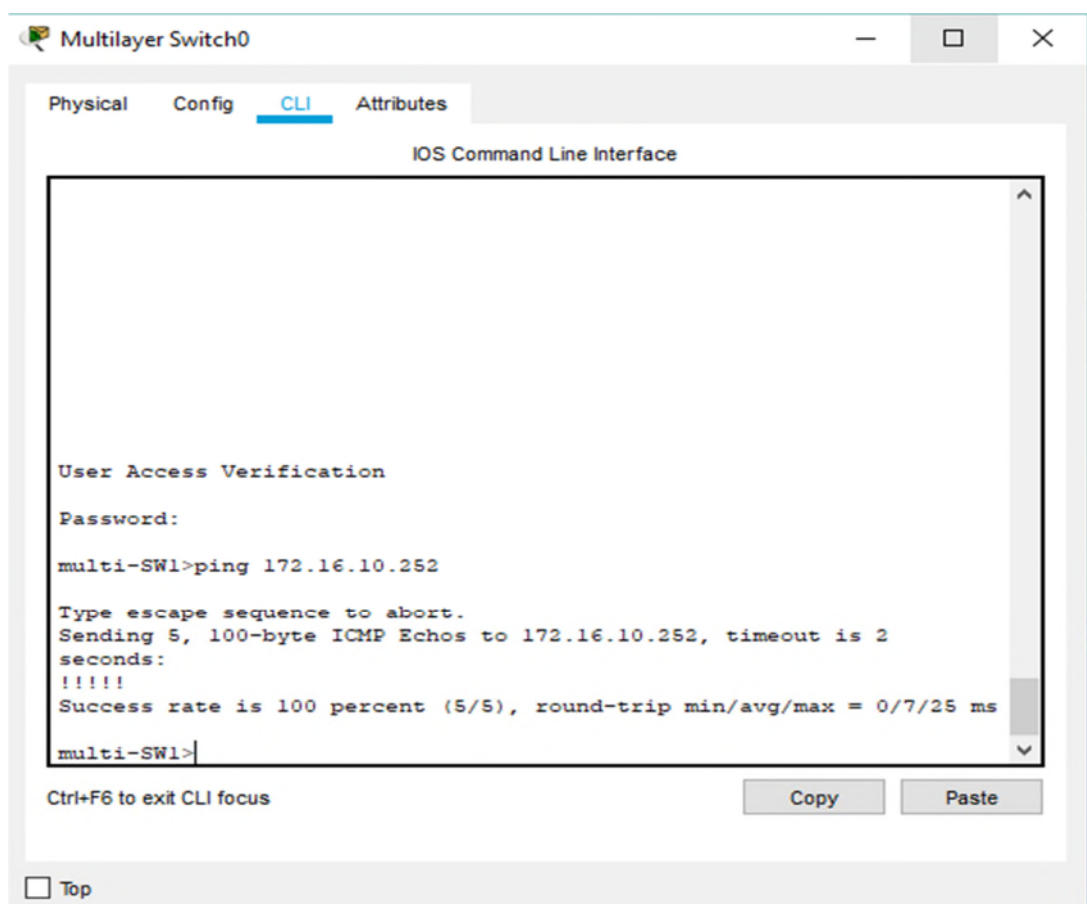


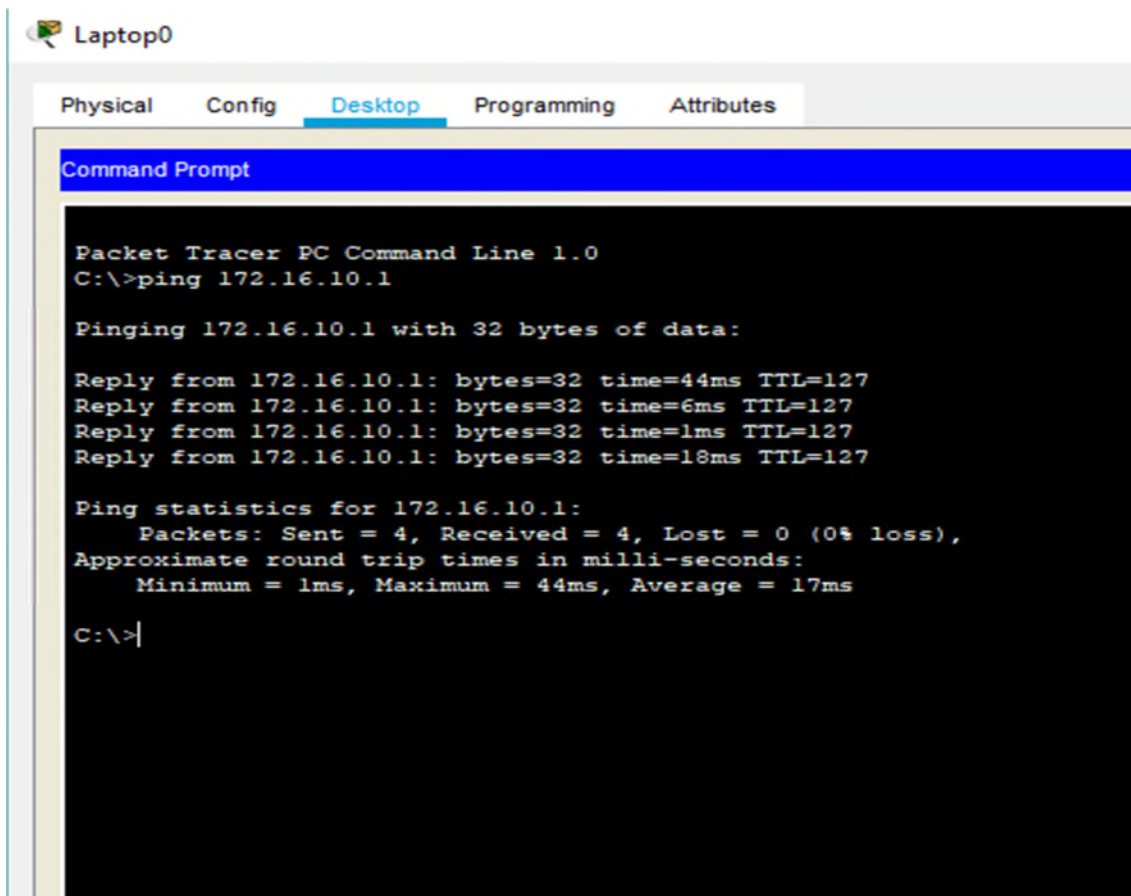
Figure 3.21 - Test entre le multi-sw1 et le Switch d'accès.

2. Vérification de la communication entre les PCs

- **Test entre PCs différents VLANs sur un même commutateur**

A ce stade, on peut vérifier l'accessibilité des différents équipements dans un même réseau mais dans deux VLANs distincts à partir du Laptop0. (172.16.40.1) en essayant d'accéder au PC 0 (172.16.10.1).

La figure 3.22 illustre le succès du test effectué entre les différents VLANs sur un même commutateur, 4 paquets envoyés et 4 paquets reçus.



```
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.1

Pinging 172.16.10.1 with 32 bytes of data:

Reply from 172.16.10.1: bytes=32 time=44ms TTL=127
Reply from 172.16.10.1: bytes=32 time=6ms TTL=127
Reply from 172.16.10.1: bytes=32 time=1ms TTL=127
Reply from 172.16.10.1: bytes=32 time=18ms TTL=127

Ping statistics for 172.16.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 44ms, Average = 17ms

C:\>|
```

Figure 3.22- Test entre machines des VLANs différents.

- **Test entre PC des VLAN et commutateur distincts**

On peut aussi vérifier l'accessibilité des équipements des VLANs situés dans un réseau local commun. Depuis le Laptop 1 (172.16.20.2), essayons d'accéder au Laptop 6 (172.16.30.1), les deux se trouvant dans des VLANs et des commutateurs accès différents. La figure suivante

illustre le succès du test effectué entre différents PC et commutateurs 4 paquets envoyés et 4 paquets reçus.

```
C:\>ping 172.16.30.1

Pinging 172.16.30.1 with 32 bytes of data:

Reply from 172.16.30.1: bytes=32 time=16ms TTL=127
Reply from 172.16.30.1: bytes=32 time<1ms TTL=127
Reply from 172.16.30.1: bytes=32 time=36ms TTL=127
Reply from 172.16.30.1: bytes=32 time=10ms TTL=127

Ping statistics for 172.16.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 36ms, Average = 15ms
```

Figure 3.23- Test entre des machines des VLANs et commutateurs différents.

- **Vérification des adresses IP des PCs attribuées par le DHCP**

La figure 3.24 montre l'attribution des adresses IP par le DHCP pour le PC1 qui se trouve sur le VLAN 10, pareil pour tous les PCs et Laptop qui se trouvent sur les autres VLANs.



Figure 3.24- Attribution des adresses IP par le DHCP.

3.7 Conclusion

Au cours de ce chapitre, nous avons pu décrire l'ensemble des configurations réalisées au niveau des LANs concernant les VLANs, VTP, STP, DHCP, HSRP et les résultats obtenus par cette simulation montrent que la segmentation du réseau en VLANs apporte une sécurisation des données échangées entre les différents départements de l'entreprise SONATRACH, une amélioration de la gestion d'une manière dynamique en évitons des collision, ainsi qu'une meilleure organisation du réseau (réduction de la congestion) sans avoir eu recours au réaménagement des équipements et sans même toucher à l'infrastructure du réseau.

Les tests de validation et de vérification effectués confirment et prouvent l'efficacité et la fiabilité de ce réseau LAN.

Configuration d'un réseau virtuel VPN

4.1 Introduction

Afin de résoudre les problèmes relatifs à la sécurité du réseau de l'entreprise SONATRACH, dans le cas d'un échange de données avec un réseau entreprise externe connectées au réseau public, tel qu'Algérie télécom, il est indispensable d'implémenter un VPN qui assure la sécurité du trafic échangé.

Ce présent chapitre consiste à l'installation et à la configuration d'un VPN entre ces deux entreprises. Cette réalisation a été effectuée sur la plate-forme du simulateur Cisco « PACKET TRACER ». Les configurations réalisées, sont présentées ainsi que toutes les étapes sont illustrées avec une description du fonctionnement de chacun des composants. Enfin, des tests de validations pour confirmer le bon fonctionnement du réseau seront réalisés.

4.2 Présentation de l'architecture réseau avant la configuration

La figure 4.1 illustre l'architecture réseau Wan que nous allons réaliser. Dans ce contexte, nous allons interconnecter le réseau réaliser à base des VLANs avec deux réseaux des entreprises externes, en implémentant un tunnel (VPN) entre deux entreprises dans notre cas, réseau SONATRACH et réseau entreprise externe.

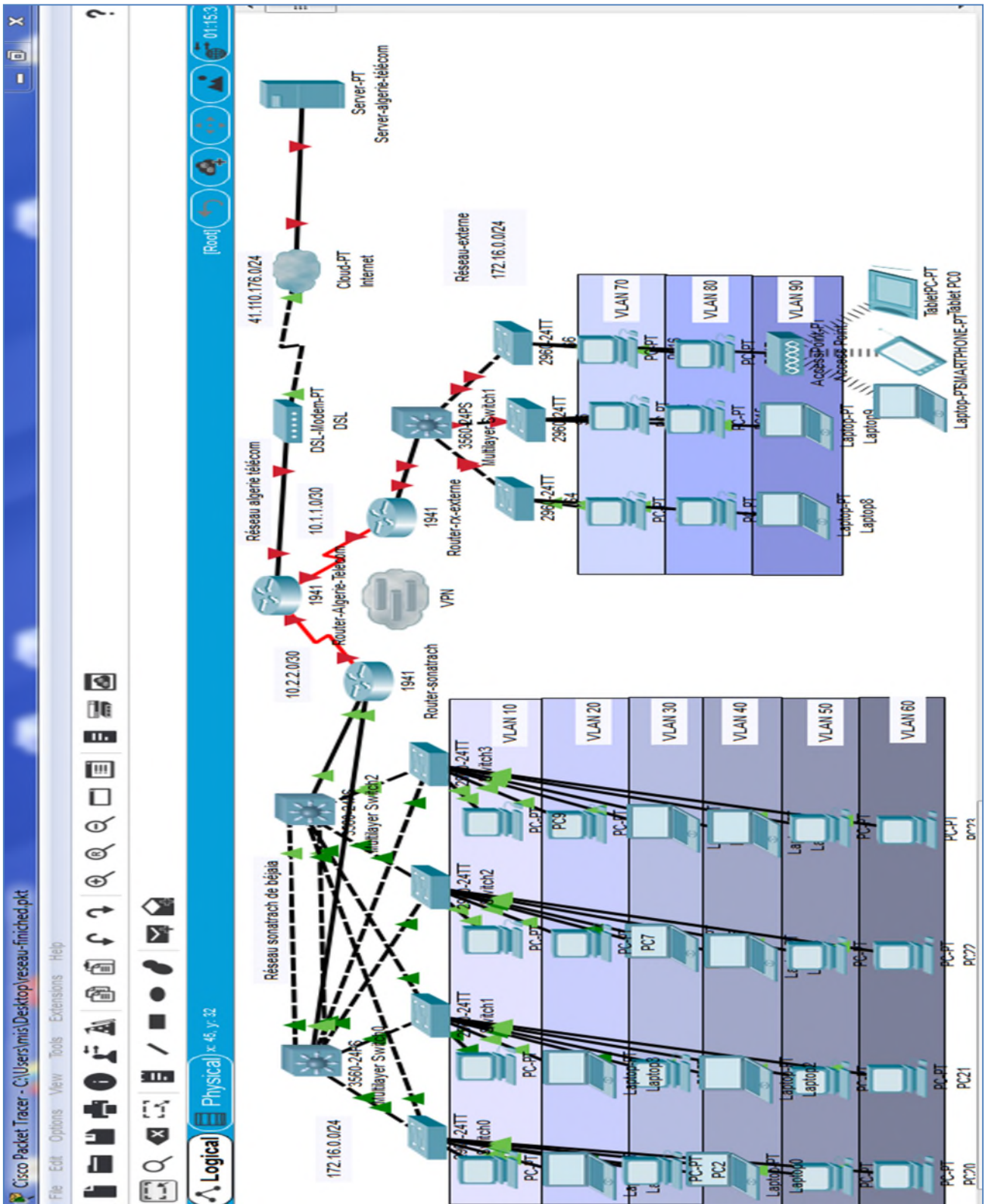


Figure 4.1 - Présentation de l'architecture.

4.3 Configuration de l'EIGRP

L'implémentation du protocole EIGRP se fera au niveau de tous les routeurs et de tous les Multiswitch.

- **Au niveau du multi-SW2**

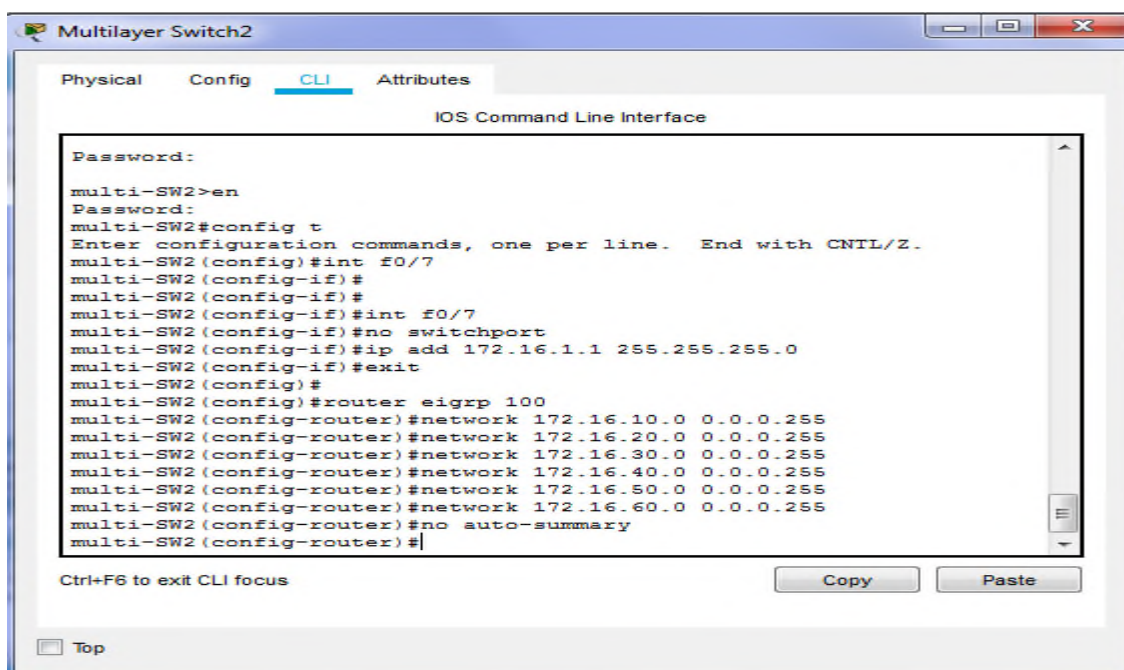
On commence par l'attribution d'une adresse IP à l'interface 0/7 de multi-SW2.

```
Multi-SW2(config) # interface f0/7
Multi-SW2(config-if) # no switchport
Multi-SW2(config-if) # ip address 172.16.1.1 255.255.255.0
Multi-SW2(config-if) # exit
```

Ensuite on active le process EIGRP à l'aide de la commande « *router eigrp 100* », la commande « *network* » permet d'activer et d'associer les interfaces à un process EIGRP.

```
Multi-SW2(config) # router eigrp 100
Multi-SW2(config-router) # network 172.16.10.0 0.0.0.255
Multi-SW2(config-router) # network 172.16.20.0 0.0.0.255
Multi-SW2(config-router) # network 172.16.30.0 0.0.0.255
Multi-SW2(config-router) # network 172.16.40.0 0.0.0.255
Multi-SW2(config-router) # network 172.16.50.0 0.0.0.255
Multi-SW2(config-router) # network 172.16.60.0 0.0.0.255
Multi-SW2(config-router) # no auto-summary
```

Pour désactiver le résumé automatique des routes dans les tables de routage, on utilise la commande « *no auto-summary* ».



```
Multilayer Switch2
Physical  Config  CLI  Attributes
IOS Command Line Interface

Password:
multi-SW2>en
Password:
multi-SW2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
multi-SW2 (config)#int f0/7
multi-SW2 (config-if)#
multi-SW2 (config-if)#int f0/7
multi-SW2 (config-if)#no switchport
multi-SW2 (config-if)#ip add 172.16.1.1 255.255.255.0
multi-SW2 (config-if)#exit
multi-SW2 (config)#
multi-SW2 (config)#router eigrp 100
multi-SW2 (config-router)#network 172.16.10.0 0.0.0.255
multi-SW2 (config-router)#network 172.16.20.0 0.0.0.255
multi-SW2 (config-router)#network 172.16.30.0 0.0.0.255
multi-SW2 (config-router)#network 172.16.40.0 0.0.0.255
multi-SW2 (config-router)#network 172.16.50.0 0.0.0.255
multi-SW2 (config-router)#network 172.16.60.0 0.0.0.255
multi-SW2 (config-router)#no auto-summary
multi-SW2 (config-router)#|

Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

Figure 4.2 - Routage au niveau de Switch multi-SW2.

- Au niveau du routeur

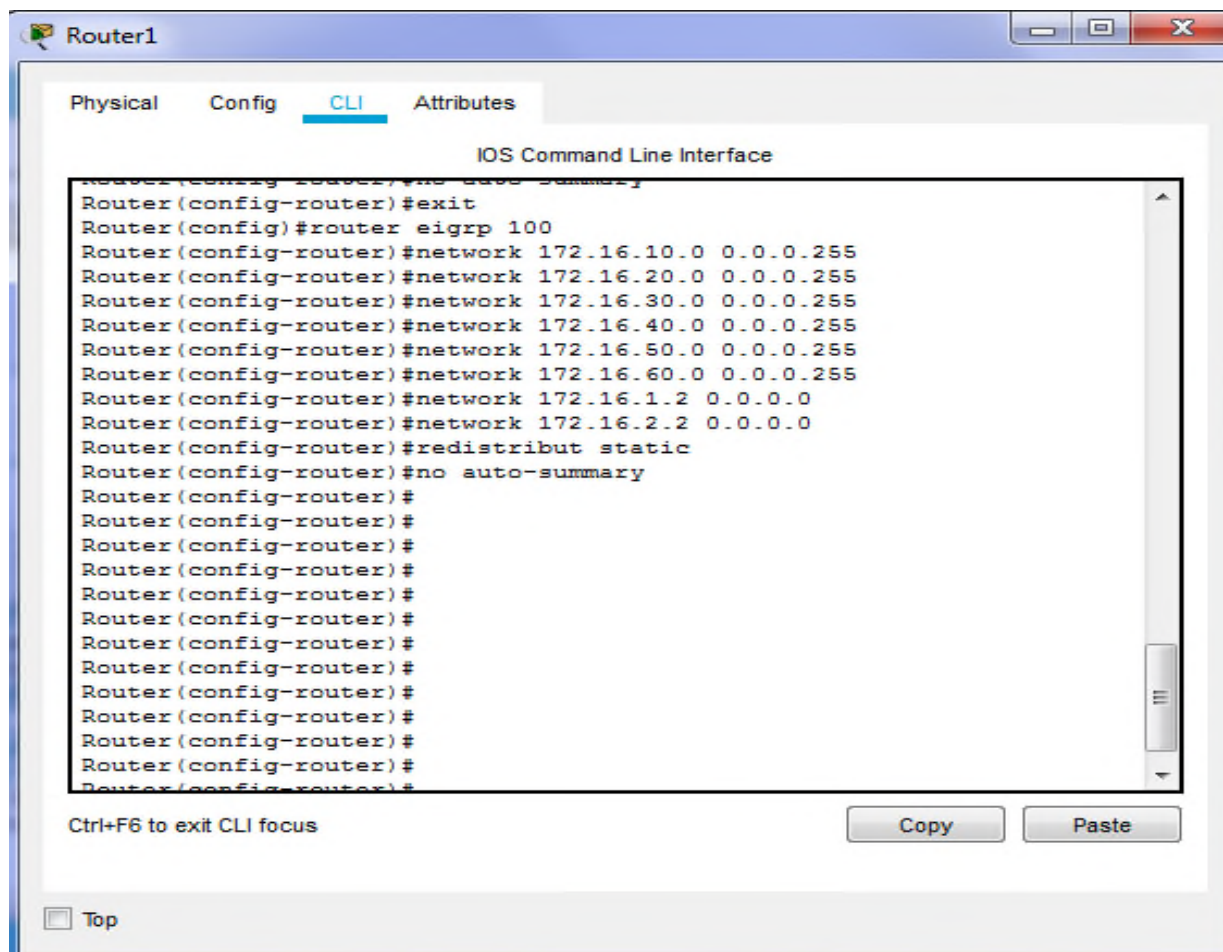


Figure 4.3 - Routage au niveau du routeur.

Une méthode de propagation d'une route par défaut statique dans le domaine du routage EIGRP consiste à utiliser la commande « *redistribute static* ». Demande au protocole EIGRP d'inclure les routes statiques dans ses mises à jour EIGRP envoyées aux autres routeurs.

La figure 4.4 montre la connexion du réseau qu'on a déjà réalisé avec le réseau d'Algérie télécom à l'aide du protocole EIGRP.

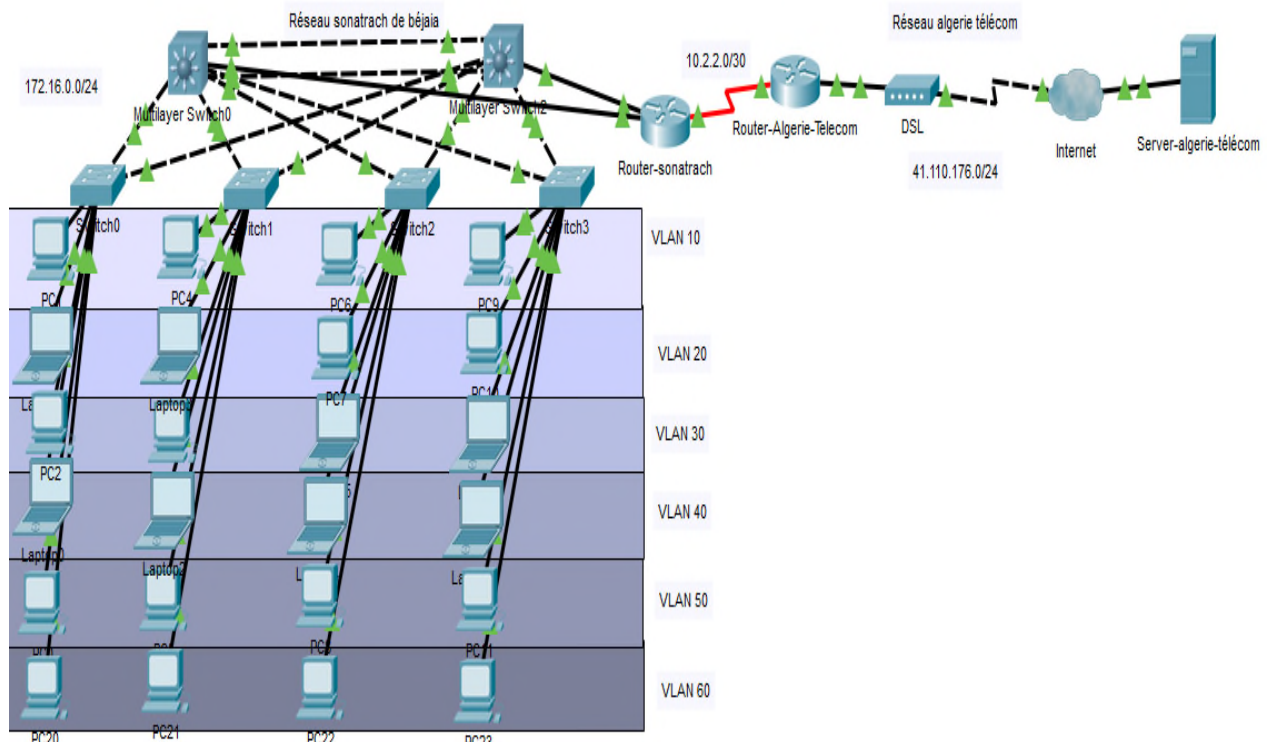


Figure 4.4 - Interconnexion de différents réseaux locaux.

4.4 Configuration d'un réseau opérateur

Cette étape consiste à configurer un réseau d'Algérie-télécom interconnecté au réseau de SONATRACH.

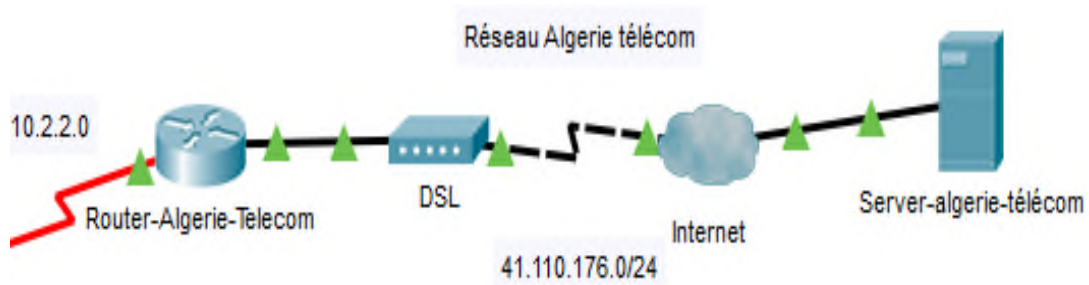


Figure 4.5 - Interconnexion avec un réseau opérateur.

- **Configuration du serveur**

Dans cette étape on attribué une adresse IP au serveur d'Algerie-télécom, figure 4.6

Adresse IP **41.110.176.10**

Masque de sous-réseau **255.255.255.0**

Passerelle par défaut **41.110.176.1**

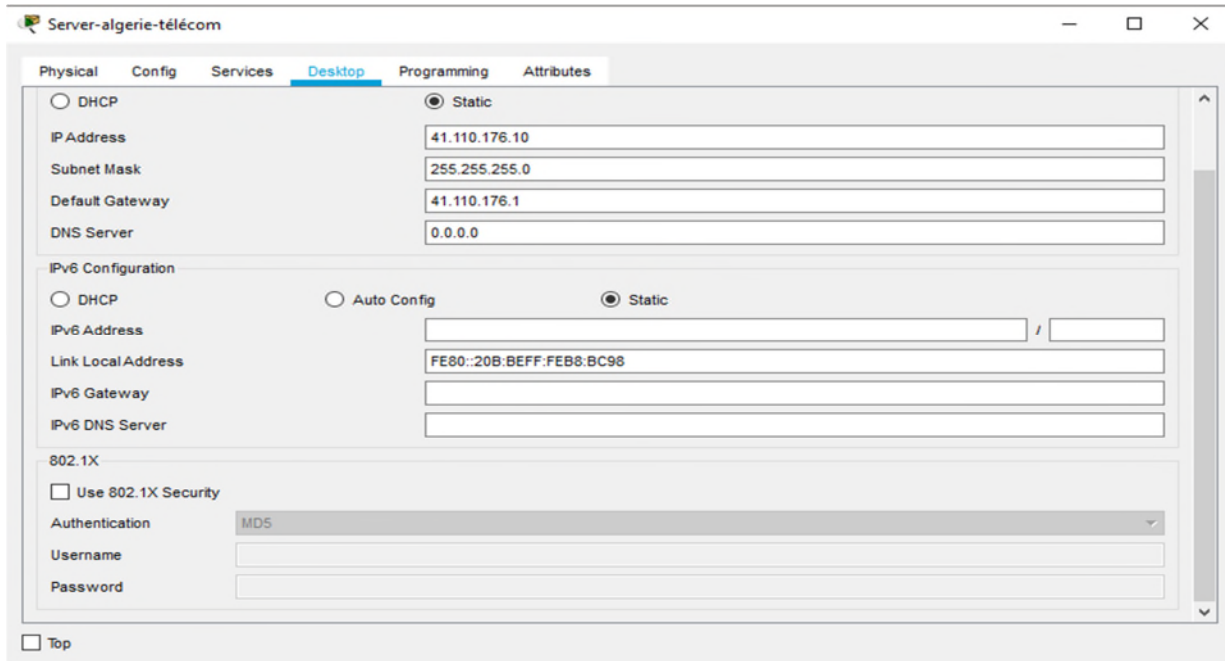


Figure 4.6-Attribution d'adresse au serveur.

- **Configuration du DSN**

La configuration DNS se fait au niveau du serveur Algerie-télécom, on attribue un nom de domaine « *www.google.com* » avec une adresse IP **41.110.176.10**

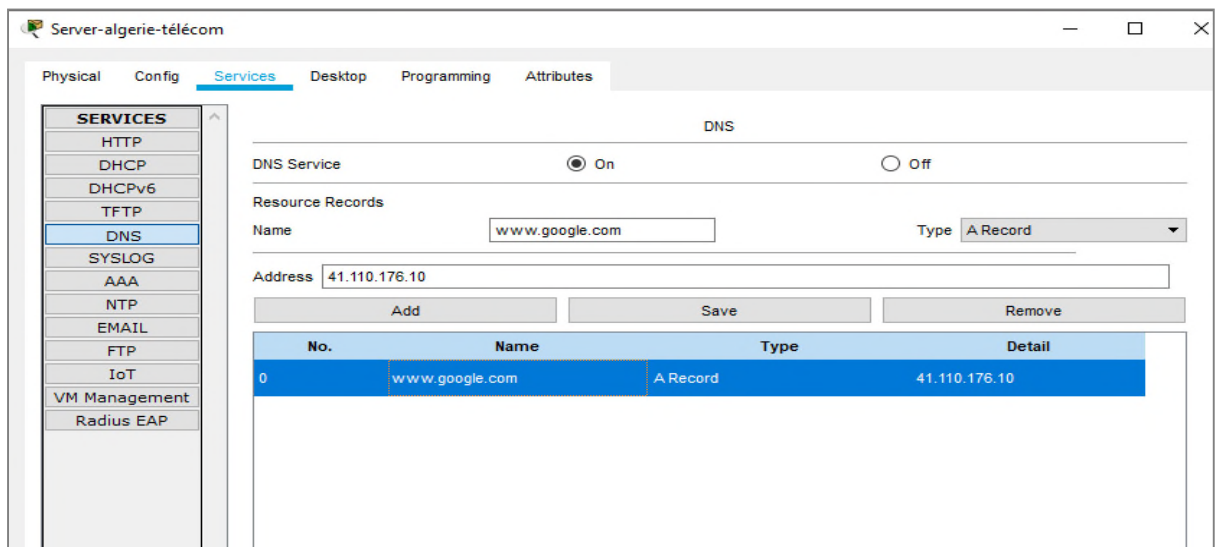


Figure 4.7- Configuration d'un nom de domaine au serveur.

- **Au niveau du cloud**

Un cloud désigne le stockage des serveurs informatiques et l'accès aux données distantes par l'intermédiaire d'internet.

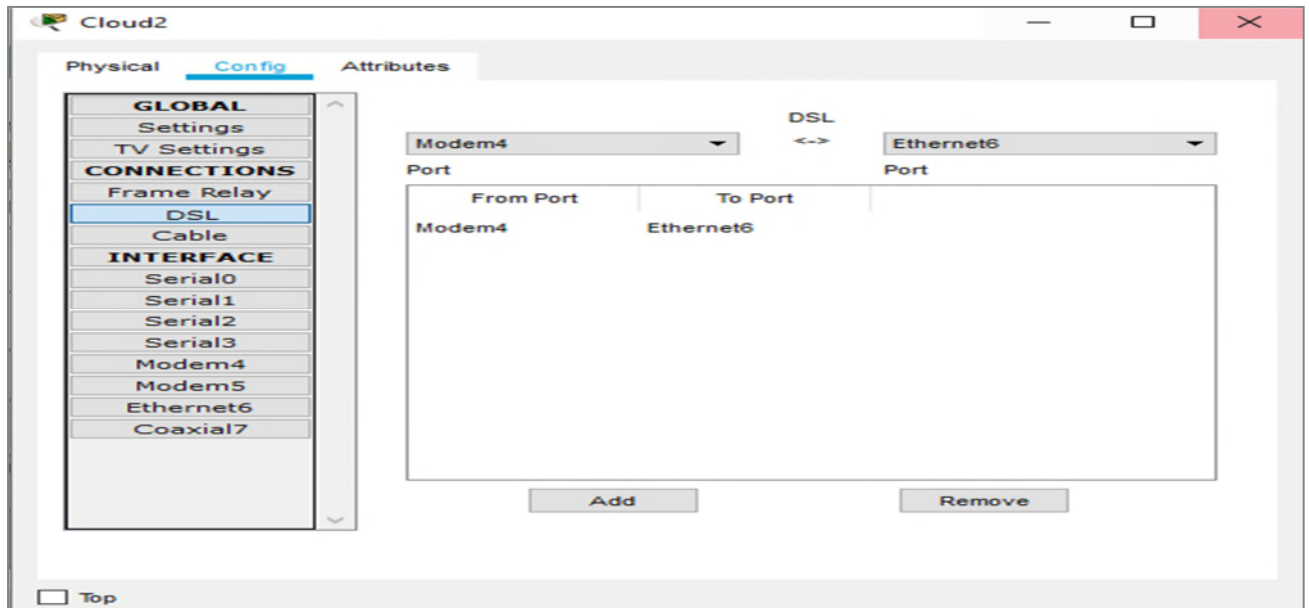


Figure 4.8-Configuration du cloud.

4.5 Configuration d'un réseau sans fil

Cette étape consiste à configurer le point d'accès sans fil sur un périphérique, et autoriser l'accès à des clients sans fil et cela dans une architecture réseau d'une entreprise externe, les mêmes étapes de configuration des équipements qu'on a réalisées dans le chapitre précédent sont appliquées pour ce réseau externe, la seule différence c'est que dans ce réseau le nombre de VLANs est trois.

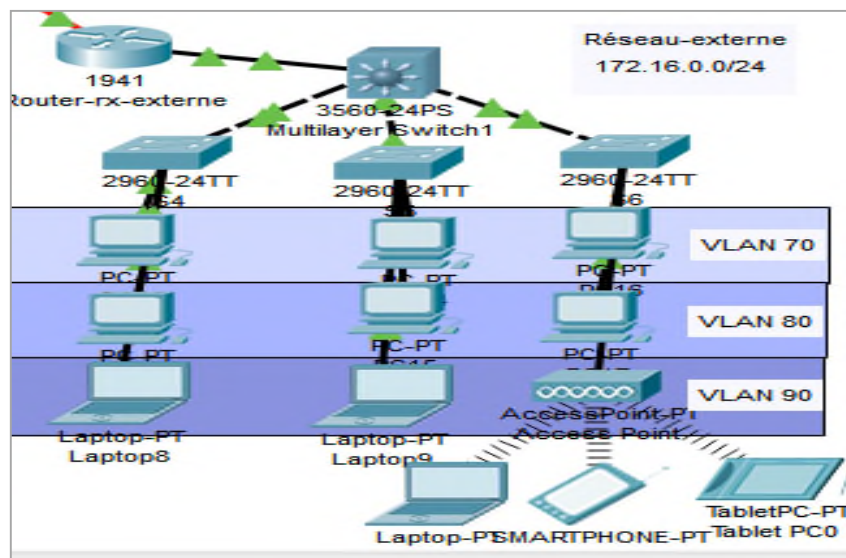


Figure 4.9 - Implémentation d'un réseau externe.

- **Au niveau du point d'accès**

Pour pouvoir sécuriser l'accès aux utilisateurs, on attribue un mot de passe sur le point d'accès. Dans le champ « PSK Pass Phrase » qui apparaît sur la fenêtre du port 1, on insère le mot de passe « *sonatrach* ».

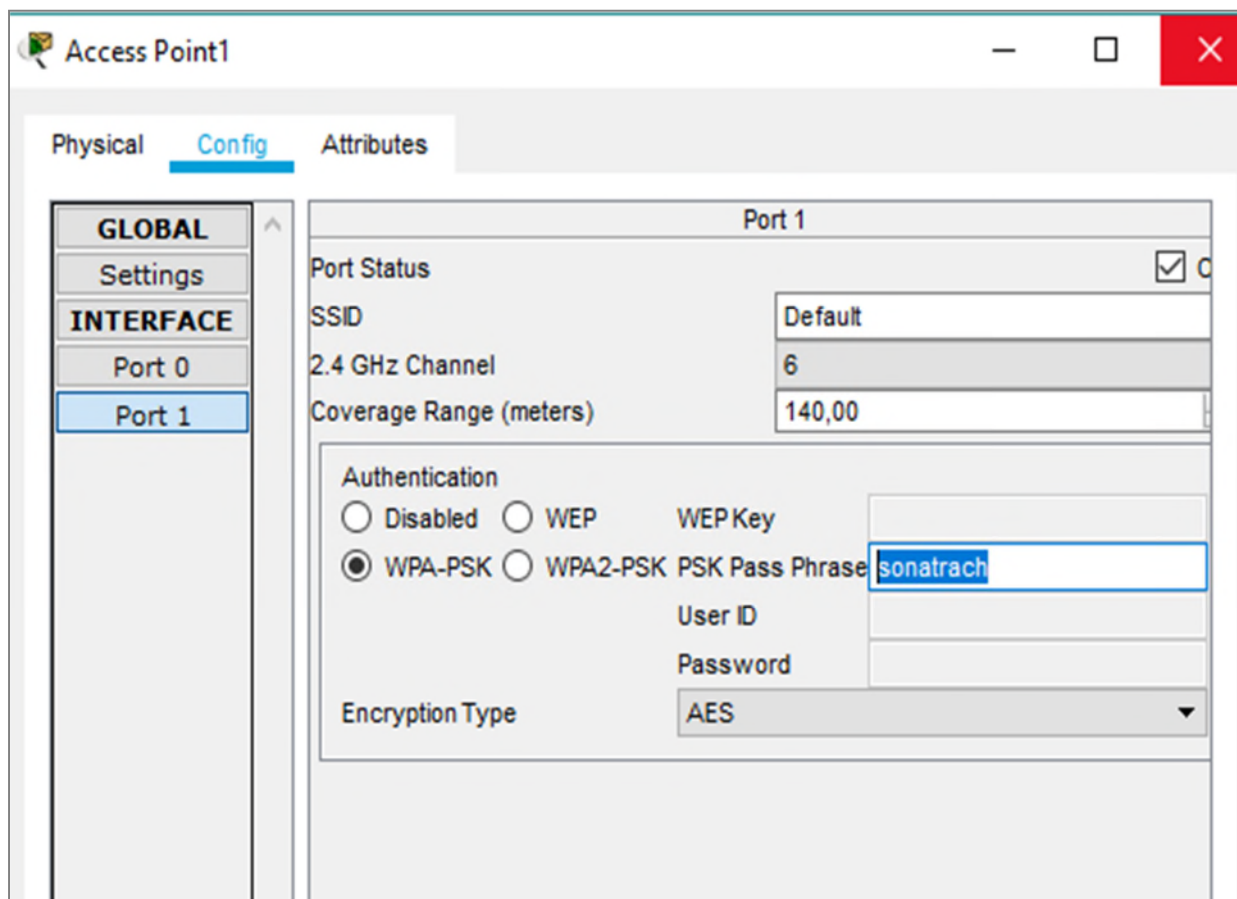


Figure 4.10 - Attribution du mot de passe au point d'accès.

Afin de communiquer entre les différents équipements finaux des différents réseaux, il va falloir connecter les équipements (Laptop 11, Smartphone0, Tablet PC0), aux points d'accès, comme est indiqué ci-dessous :

- **Pour la Tablet PC0 et Smartphone0**

On attribue directement le mot de passe « sonatrach » dans wireless0 dans le champ « PSK Pass Phrase ».

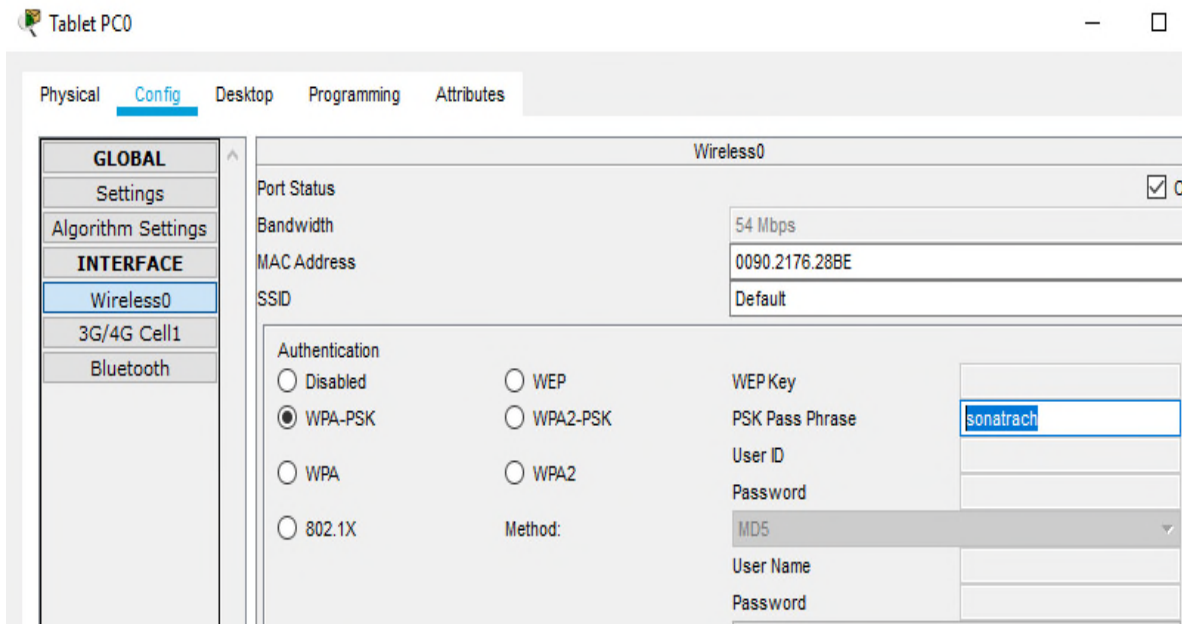


Figure 4.11 - Attribué le mot de passe du Tablet PC0.

Le même principe est utilisé pour la configuration du Smartphone.

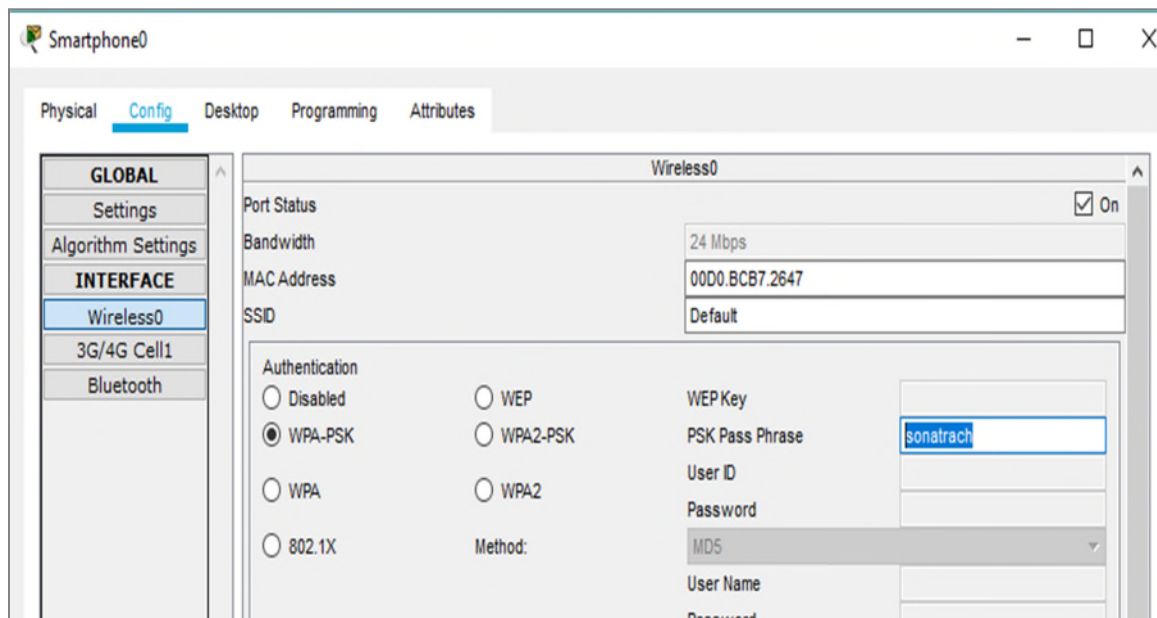


Figure 4.12 - Attribué le mot de passe au Smartphone0.

- **Pour le Laptop 11**

Dans la fenêtre Desktop, dans le champ PC wireless on insère le mot de passe « sonatrach » qu'on a configuré au niveau du point d'accès pour se connecter à ce dernier.

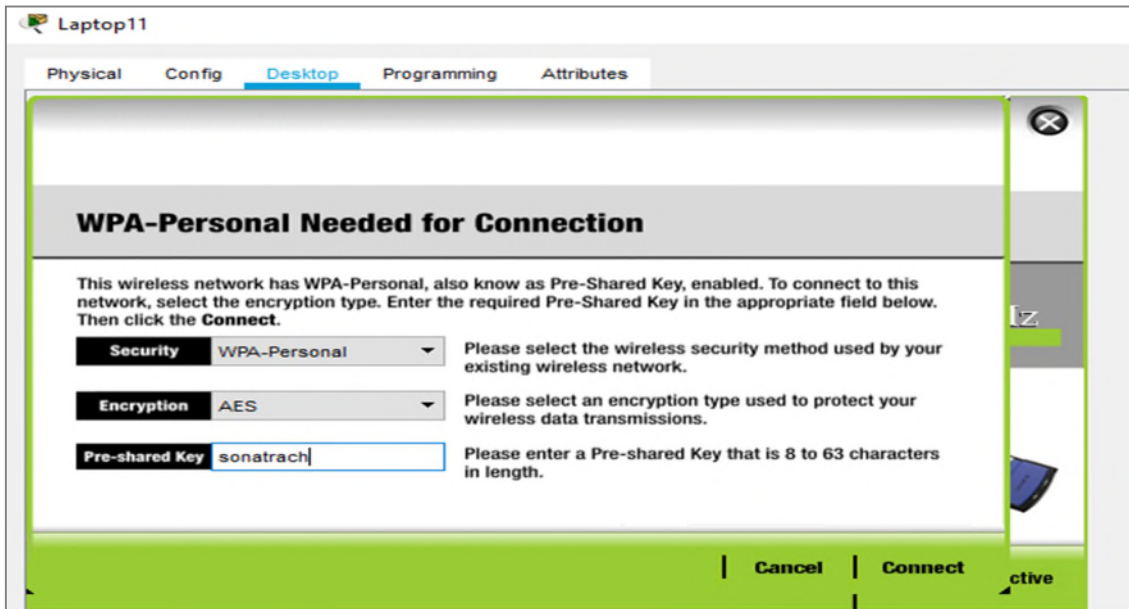


Figure 4.13 - Connecter le Laptop11 au point d'accès.

La figure 4.14 montre l'architecture finale du réseau WAN (interconnexion des réseaux locaux LAN) que nous avons réalisée

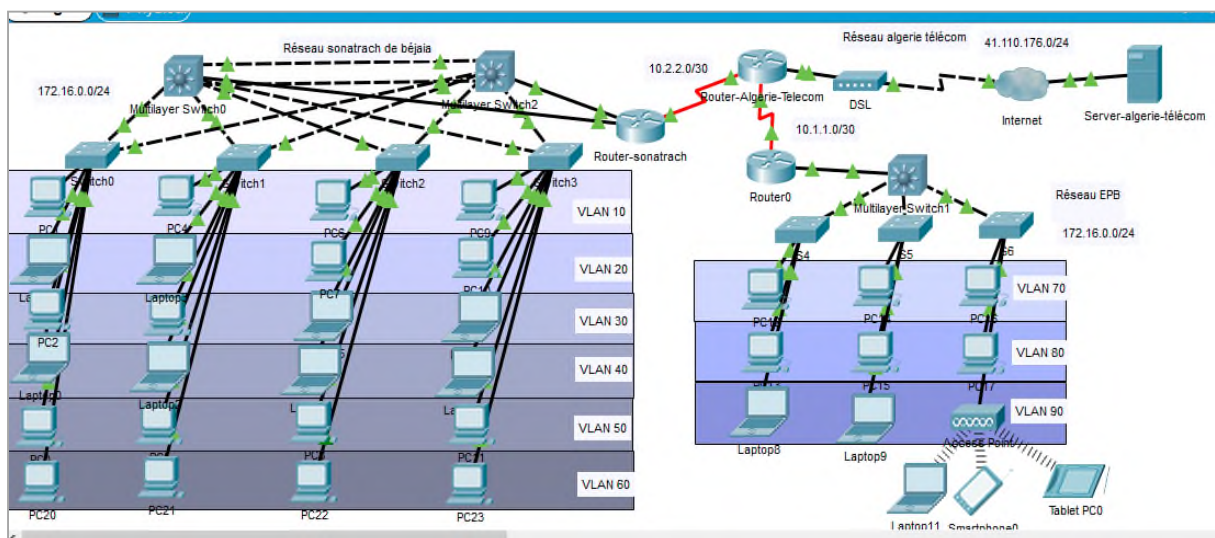


Figure 4.14 - Interconnexion des différents réseaux locaux.

4.6 Configuration et mise en œuvre d'un tunnel VPN

Dans cette section nous allons montrer la création d'un tunnel entre le site siège SONATRACH et le site du réseau-externe.

La figure 4.15 montre l'emplacement du tunnel VPN dans l'architecture.

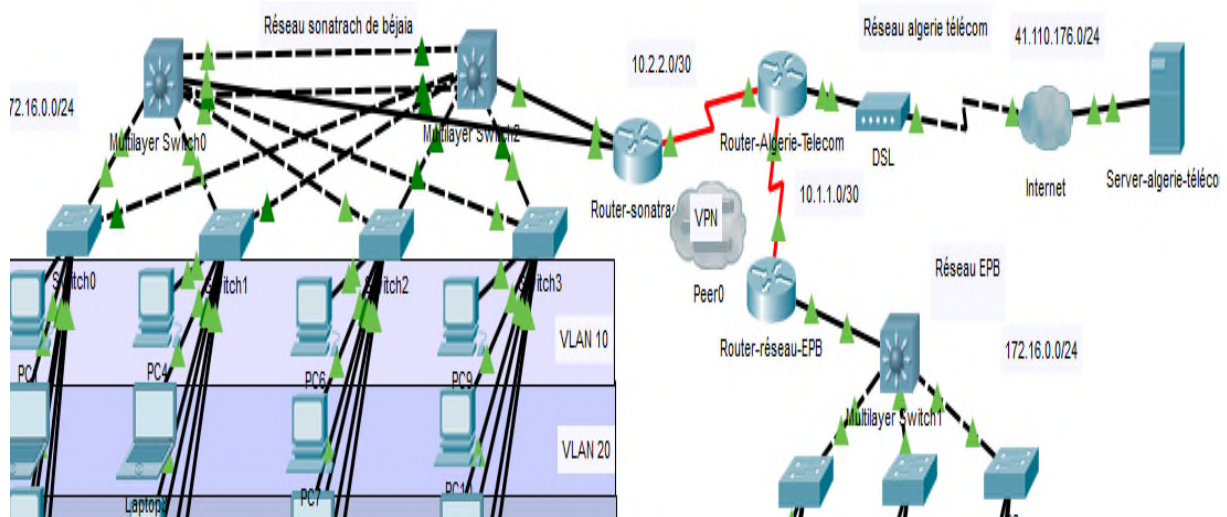


Figure 4.15- Implémentation d'un VPN dans l'architecture.

Pour sa configuration, nous allons suivre les étapes suivantes :

1. La configuration de la stratégie IKE et l'activation de IKE sur l'interface extérieure.
2. la configuration des ACLs pour le trafic VPN d'intérêt.
3. la configuration de la méthode de cryptage des données Transform-set.
4. la configuration de la crypto map.

4.7 Configuration d'un tunnel VPN IPSec

On distingue deux parties qui sont nécessaires pour réaliser le tunnel VPN IPSec :

- Configuration d'ISAKMP.
- Configuration d'IPSec (ISAKMP, crypto MAP).

Il est noté que la politique ISAKMP de phase 1 est définie de manière globale. Cela signifie que si nous avons par exemple cinq différents sites distants (ce qui est souvent le cas vu que les entreprises ont plusieurs filiales généralement), il faut configurer cinq différentes politiques ISAKMP de phase 1 (un pour chaque routeur distant).

Notre exemple de configuration se situe entre 3 branches de l'entreprise Sonatrach : Routeur de Sonatrach, Routeur-rx-externe et Routeur- Algérie-Telecom. Les 3 routeurs sont connectés à internet.

- **Table d'adressage**

Périphérique	Interface	Adresse IP	Masque
Router-rx-externe	G0/0	172.16.4.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
Router-Algerie-Telecom	G0/0	41.110.176.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
	S0/0/1	10.2.2.2	255.255.255.252
Router-reseau-Sonatrach	G0/0	172.16.1.2	255.255.255.0
	S0/0/1	10.2.2.1	255.255.255.252
Serveur-Algerie-Telecom		41.110.176.10	255.255.255.0

Table 4.1 -Tableau des adresses proposées.

Dans notre proposition nous allons configurer le tunnel VPN IPsec entre deux sites : Routeur- réseau-Sonatrach et le Routeur-rx-externe.

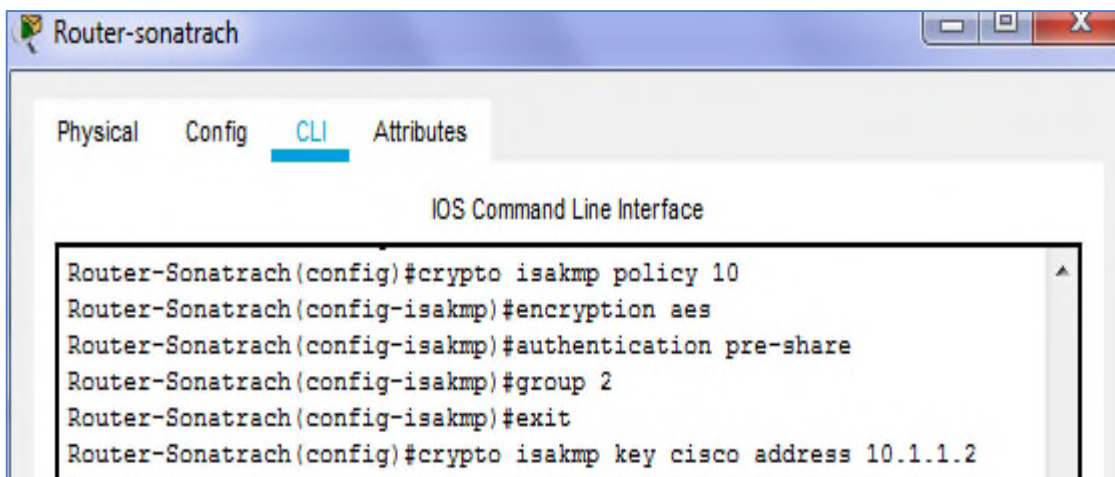
4.7.1 Configuration d'un VPN IPsec site à site

- **Configuration d'ISAKMP de phase 1 sur Router-Sonatrach**

Nous allons configurer la stratégie qui détermine quelle encryption qu'on utilise et quelle type d'authentification avec la clé de chiffrement partagée « cisco ».

- **Router-Sonatrach :**

```
Router-Sonatrach #config ter
Router-Sonatrach (config) #crypto isakmp enable
Router-Sonatrach (config) #crypto isakmp policy 1
Router-Sonatrach (config-isakmp) #authentication pre-share
Router-Sonatrach (config-isakmp) #encryption AES
Router-Sonatrach (config-isakmp) # hash sha
Router-Sonatrach (config-isakmp) #group 2
```



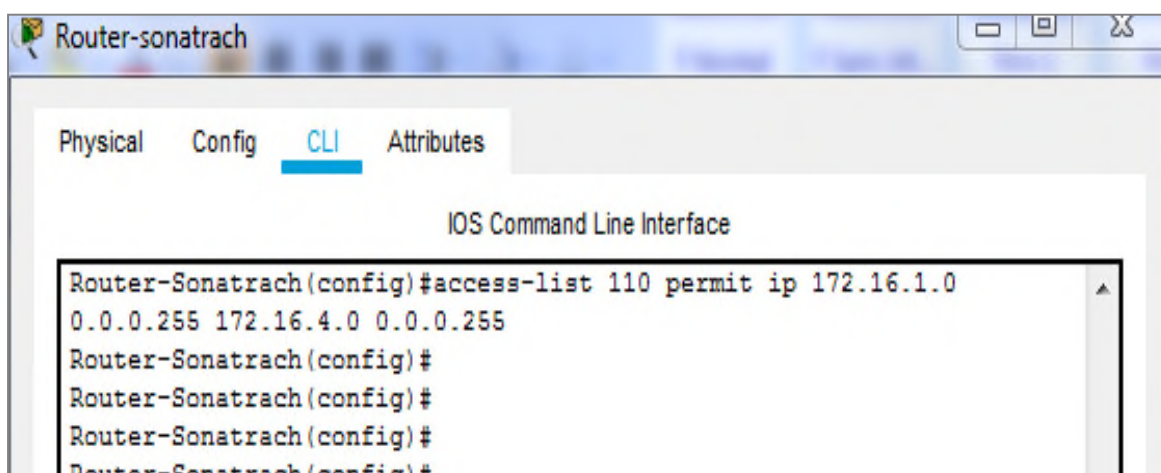
```
Router-sonatrach
Physical Config CLI Attributes
IOS Command Line Interface
Router-Sonatrach(config)#crypto isakmp policy 10
Router-Sonatrach(config-isakmp)#encryption aes
Router-Sonatrach(config-isakmp)#authentication pre-share
Router-Sonatrach(config-isakmp)#group 2
Router-Sonatrach(config-isakmp)#exit
Router-Sonatrach(config)#crypto isakmp key cisco address 10.1.1.2
```

Figure 4.16 - Configuration des propriétés ISAKMP de phase 1.

- « Policy » : qui définit la politique de connexion pour les SA (Security Association) .
- « Pre-share » : utilisation d'une clé pré-partagée comme méthode d'authentification.
- « Groupe 2 » : L'algorithme d'échange de clef Die-Hellman qui est utilisé par défaut c'est le groupe 1 qui utilise (768 bits), dans notre cas nous avons utilisé le groupe 2 (1024bits).

4.7.2 Configuration l'ACL pour le trafic VPN d'intérêt

Nous devons Configurer la liste de contrôle d'accès 110 afin d'identifier le trafic issu du LAN sur Router-Sonarach vers le LAN sur Router-rx-externe comme étant le trafic intéressant. Ce dernier déclenchera le réseau privé virtuel IPsec à implémenter, pour autant qu'il y ait du trafic entre les LAN de Router-Sonatrach et de Routeur-rx-externe. Tout autre trafic provenant des LAN ne sera pas chiffré.



```
Router-sonatrach
Physical Config CLI Attributes
IOS Command Line Interface
Router-Sonatrach(config)#access-list 110 permit ip 172.16.1.0
0.0.0.255 172.16.4.0 0.0.0.255
Router-Sonatrach(config)#
Router-Sonatrach(config)#
Router-Sonatrach(config)#
Router-Sonatrach(config)#
```

Figure 4.17- Configuration d'ACL pour le trafic VPN.

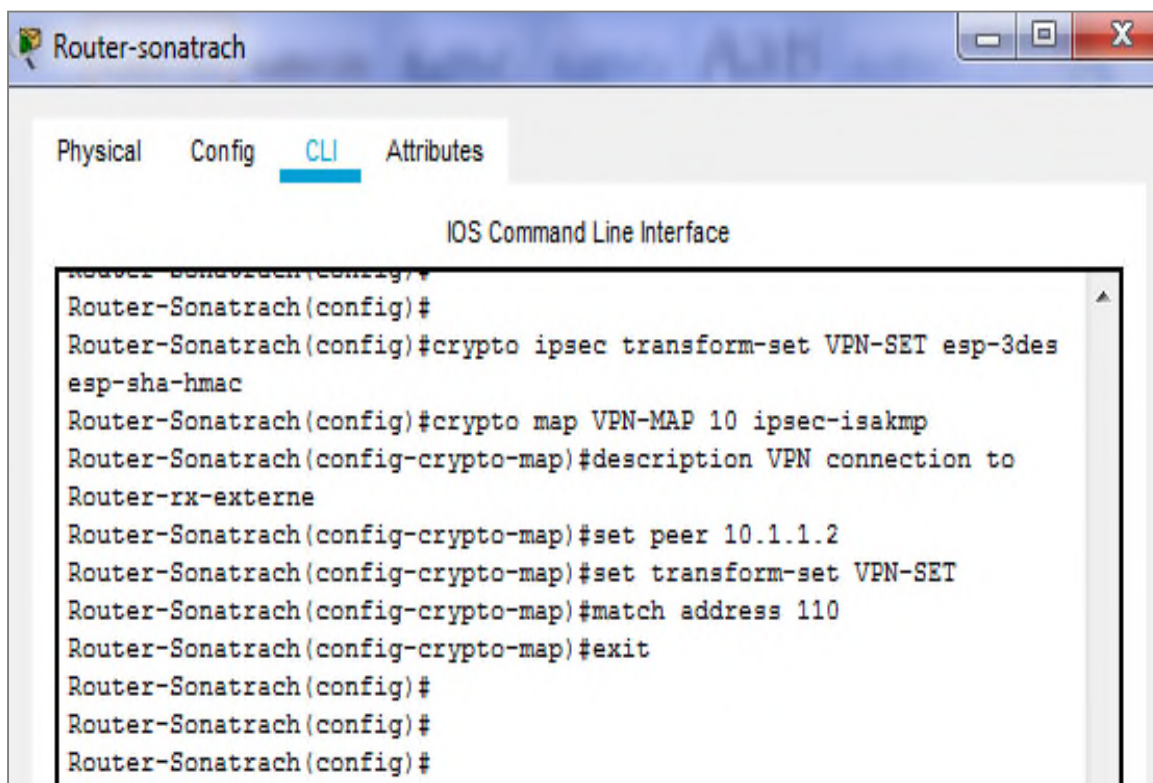
4.7.3 Configuration des propriétés ISAKMP de phase 2 sur Routeur-Sonatrach

- **Créer crypto carte**

Nous allons Créer le transform-set VPN-SET de manière à utiliser esp-3des et esp-sha-hmac. Ensuite nous allons créer la carte de chiffrement VPN-MAP qui lie ensemble tous les paramètres de phase 2. Nous allons utiliser le numéro d'ordre 10 et l'identifié comme étant une carte ipsec-isakmp.

Encryption : aes

Hash : sha



```
Router-Sonatrach
Physical Config CLI Attributes
IOS Command Line Interface
Router-Sonatrach(config)#
Router-Sonatrach(config)#crypto ipsec transform-set VPN-SET esp-3des
esp-sha-hmac
Router-Sonatrach(config)#crypto map VPN-MAP 10 ipsec-isakmp
Router-Sonatrach(config-crypto-map)#description VPN connection to
Router-rx-externe
Router-Sonatrach(config-crypto-map)#set peer 10.1.1.2
Router-Sonatrach(config-crypto-map)#set transform-set VPN-SET
Router-Sonatrach(config-crypto-map)#match address 110
Router-Sonatrach(config-crypto-map)#exit
Router-Sonatrach(config)#
Router-Sonatrach(config)#
Router-Sonatrach(config)#
```

Figure 4.18 - Configuration des propriétés ISAKMP de phase 2.

- **Appliquer crypto carte à l'interface S0/0/1**

L'étape finale consiste à appliquer le crypto MAP sur l'interface Serial 0/0/1 de sortie de notre routeur :

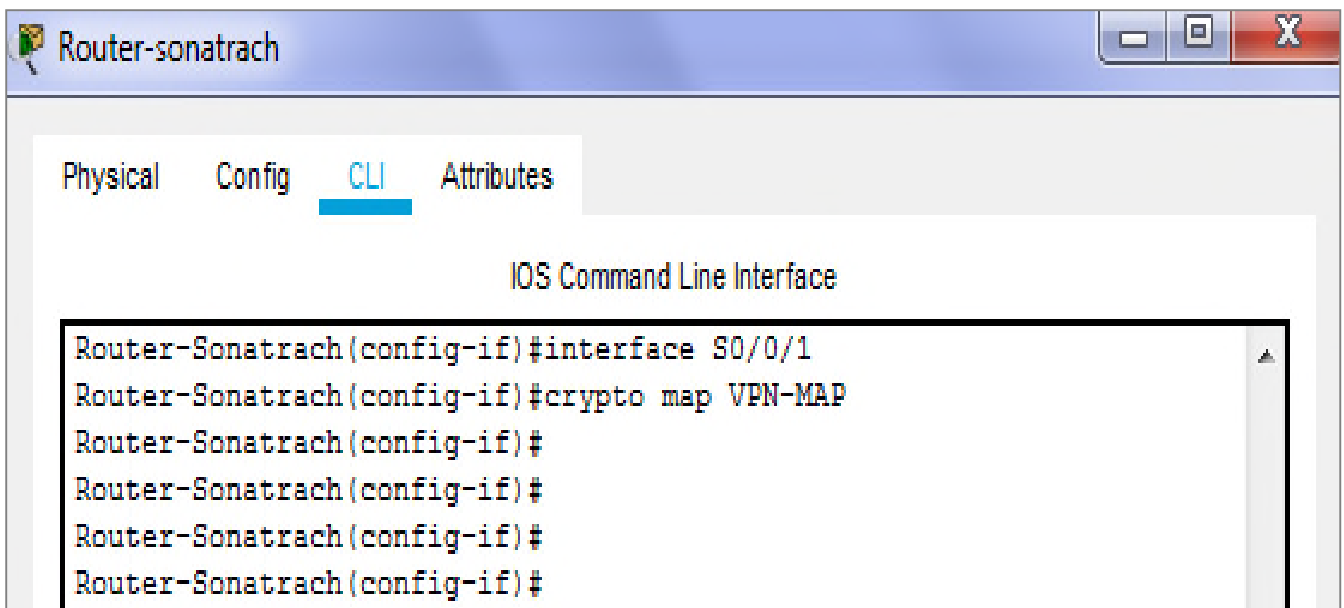


Figure 4.19-Configuration des paramètres IPsec.

À ce stade, nous avons terminé la configuration du tunnel VPN IPsec sur le routeur du site 1 <Router-rx-externe>, les mêmes étapes seront appliquées au routeur du site 2 < Router-Sonatrach >. Les paramètres pour le Router-rx-externe sont identiques, la seule différence étant les adresses IP par les pairs (sites) et les listes d'accès.

La figure 4.20 montre l'architecture finale du réseau réalisé.

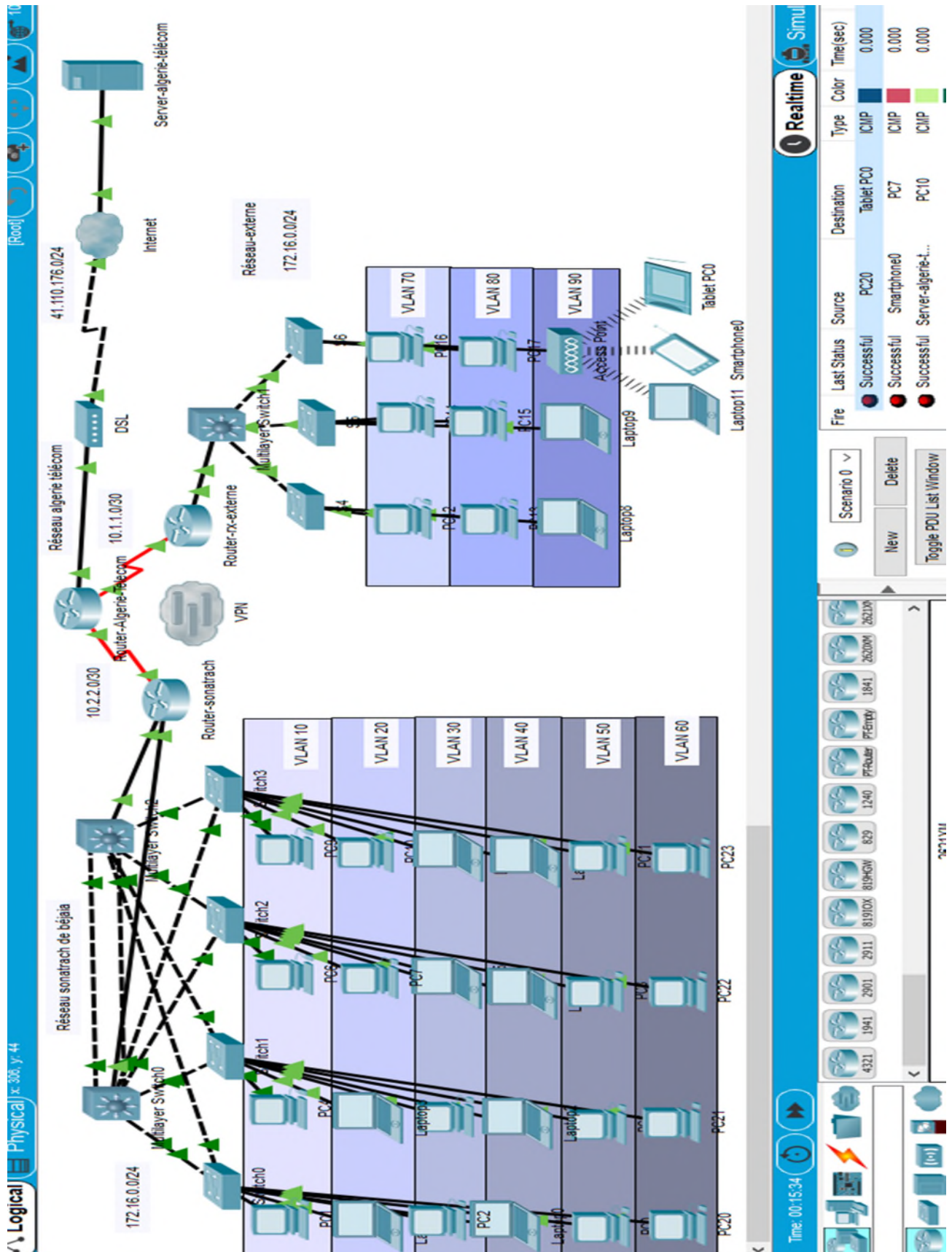


Figure 4.20 - Architecture du réseau WAN réalisé.

4.8 Vérification et test de validation

- **Vérification de la haute disponibilité**

La figure 4.21 illustre le succès du test effectué entre le PC1 du réseau de SONATRACH et le PC 17 du réseau externe d'une autre entreprise, On a 4 paquets envoyés et 3 paquets reçus.

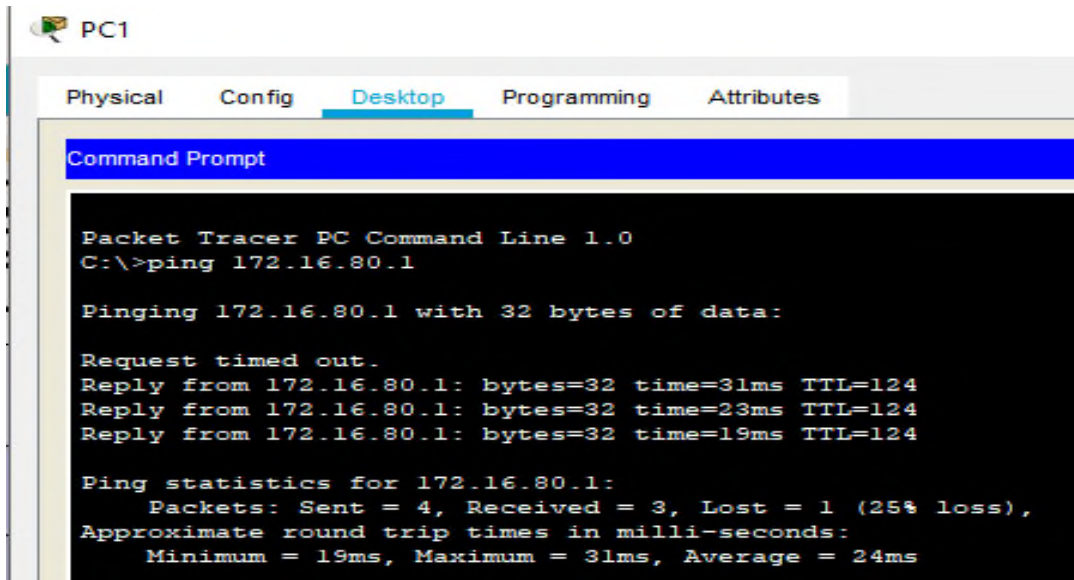


Figure 4.21- Test entre les machines des différents réseaux.

- **Vérification du réseau opérateur**

Pour vérifier le bon fonctionnement du serveur, on essaye d'accéder à ce dernier à partir du PC 19 dans la fenêtre Desktop, dans le champ « web browser » on saisit le nom du domaine « www.google.com », une interface du serveur s'affiche.

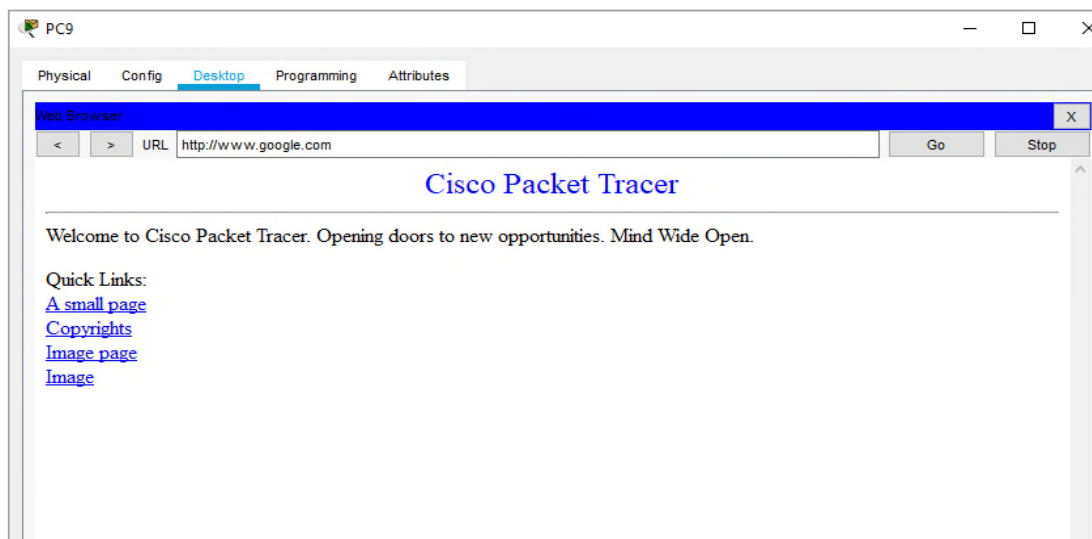


Figure 4.22- Test du server DNS d'un réseau opérateur (Algerie télécom).

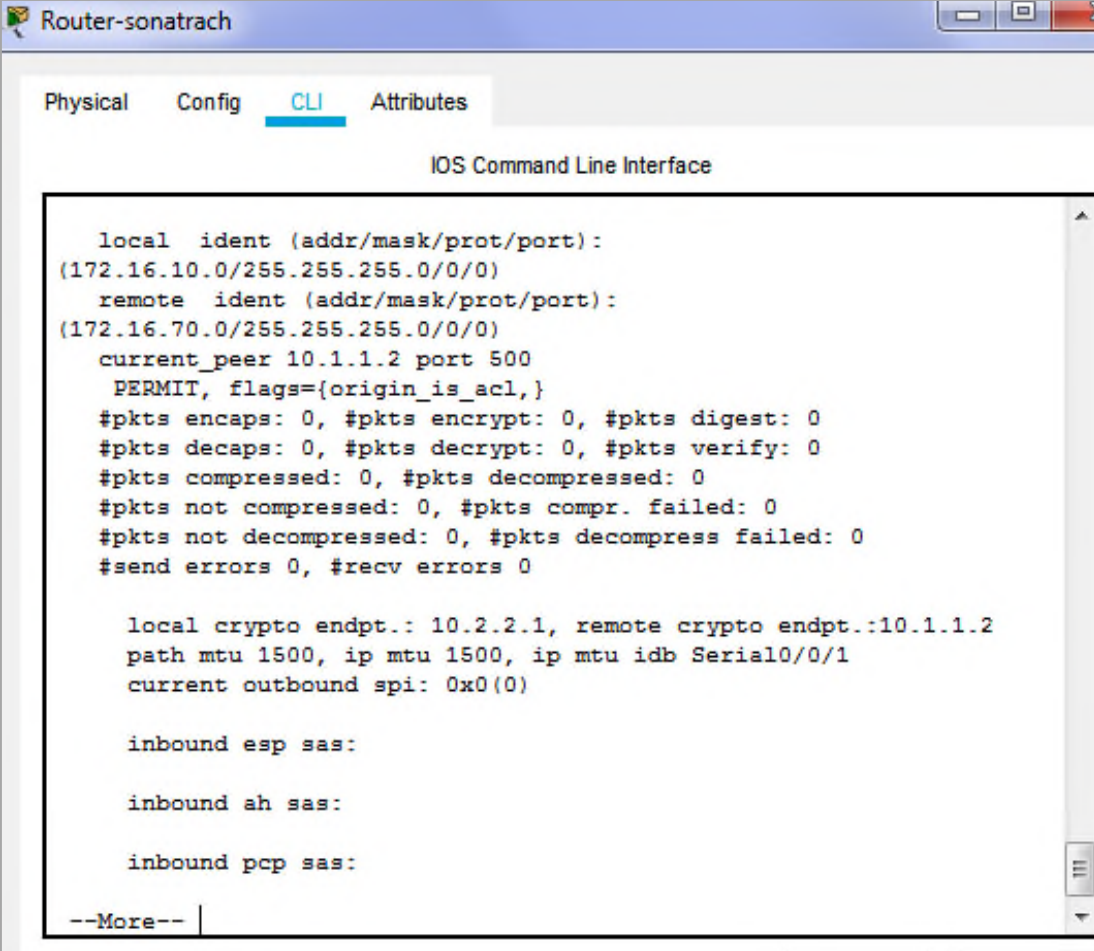
1. Test de Tunnel VPN IPsec

- **Vérifiez le tunnel avant le trafic intéressant.**

Un trafic intéressant c'est le trafic qui passe dans le tunnel VPN

On exécute la commande « `show crypto ipsec sa` » sur Router-sonatrach.

Router-sonatrach (config)# show crypto ipsec sa



```
Router-sonatrach
Physical  Config  CLI  Attributes
IOS Command Line Interface

local ident (addr/mask/prot/port):
(172.16.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(172.16.70.0/255.255.255.0/0/0)
current_peer 10.1.1.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.2.2.1, remote crypto endpt.:10.1.1.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/1
current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcp sas:

--More--
```

Figure 4.23 - Vérification du tunnel avant le trafic intéressant.

Le nombre de paquets encapsulés, chiffrés, décapsulés et déchiffrés est défini à 0 (absence du trafic intéressant)

- **Création du trafic intéressant.**

On envoie une requête « *ping* » du PC-rx-externe vers le PC-rx-Sonatrach, cette requête a réussi, 4 paquets envoyés, 3 reçus.

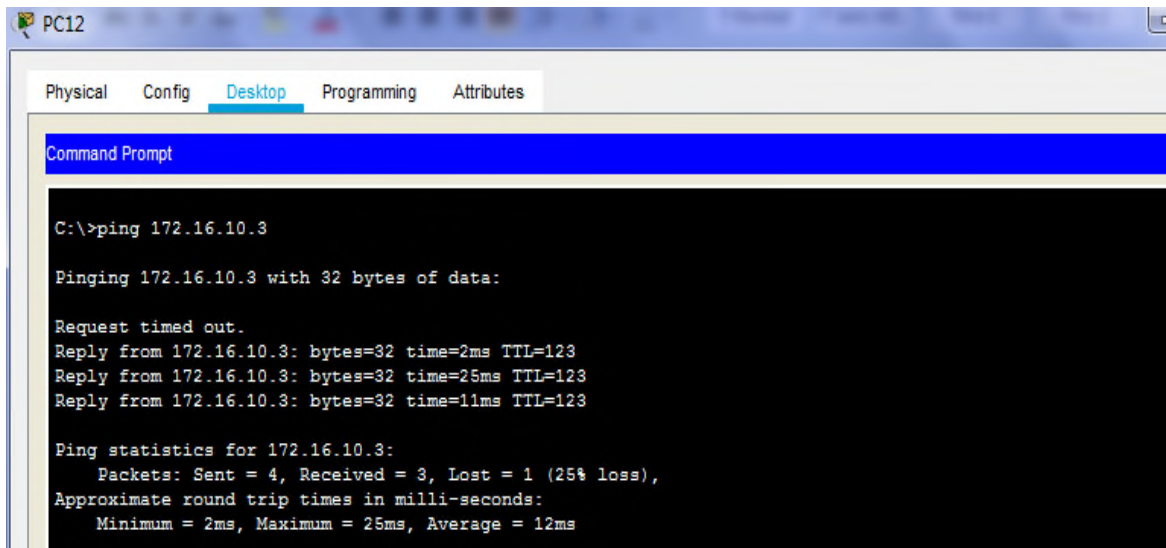


Figure 4.24 – Envoie de la requête ping du PC-rx-externe vers le PC-rx-Sonatrach.

- **Vérification du tunnel après le trafic intéressant**

Sur Router-sonatrach, on réexécute la commande « *show crypto ipsec sa* ».

Router-sonatrach # show crypto ipsec sa

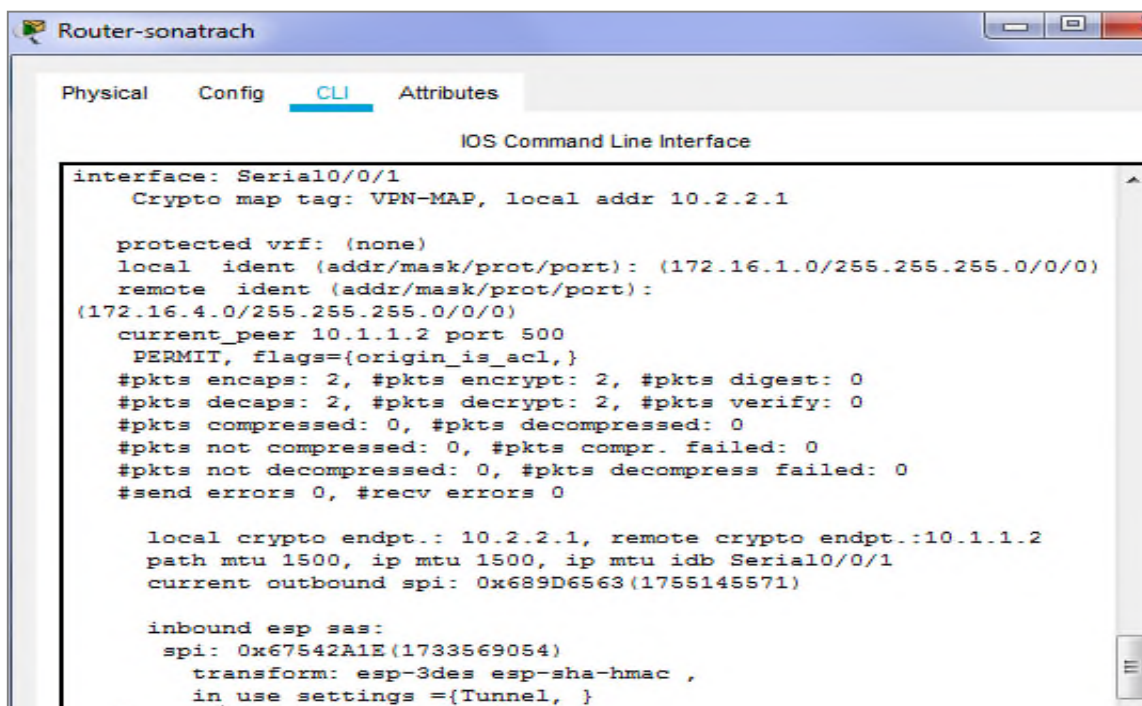


Figure 4.25 – Vérification du trafic après le trafic intéressant.

On peut noter que le nombre de paquets est supérieur à 0, ce qui indique que le tunnel VPN IPsec fonctionne (présence du trafic intéressant).

4.9 Conclusion

Au cours de ce chapitre, nous avons pu au premier lieu concevoir une architecture généralisée du réseau de l'entreprise SOANTRACH à une autre entreprise et un opérateur qui est supposé Algérie télécom, et de configurer un tunnel VPN sécurisé entre le réseau SONATRACH et le réseau d'une entreprise externe et d'offrir un accès distant.

Les tests de validation et de vérification effectués confirment et prouvent l'efficacité et la fiabilité de ce réseau WAN.

Conclusion générale et perspectives

L'utilisation de la technologie de l'information à l'échelle mondiale s'est opérée plus vite que quiconque aurait pu imaginer, son évolution rapide a induit un bouleversement des interactions sociales, commerciales, politiques et même personnelles. Au terme de ce projet, nous avons pu exploiter nos connaissances théorique et pratique pour configurer une architecture sécurisée basée sur les VPNs et d'une segmentation en VLANs pour l'entreprise SONATRACH Bejaia. L'objectif de cette configuration consiste à améliorer les performances du réseau et d'offrir une flexibilité ainsi qu'une facilité d'administration.

En effet, notre travail est divisé en deux grandes parties, à savoir l'approche théorique qui était subdivisée en deux chapitres : le premier fournit des généralités à propos des réseaux et la sécurité informatiques où nous avons basé de façon claire sur les notions des VLANs et VPNs et leurs fonctionnements, ainsi que les différents protocoles utilisés pour la mise en œuvre de ce réseau et le deuxième qui est dédié à la présentation de l'organisme d'accueil, et exposait la problématique,. La deuxième partie a porté sur la réalisation et la configuration des différents protocoles sur notre réseau. Dont nous avons pu résoudre en mettant en place une solution basée sur les VLANs et VPN site-à-site qui consiste à mettre au point une liaison permanente, distante est sécurisée entre les différents sites de l'entreprise SONATRACH.

Sur le plan conception notre travail nous a permet de comprendre le fonctionnement des équipements CISCO et leurs fonctionnalités, maîtriser les notions de VLANs et VPN connues pour leurs complications et enfin savoir exploiter le logiciel de simulation Packet Tracer.

Les résultats obtenus lors des simulations effectuées sur Packet tracer ont montré le bon fonctionnement du VLAN et VPN au sein de l'entreprise permettant ainsi l'amélioration des problèmes relatifs à la congestion, collision et sécurisation des données échangées entre les sites distants.

Ce projet a été bénéfique sur tous les plans, en particulier, il nous a permis d'acquérir une expérience personnelle et professionnelle. Ce fut une occasion afin de ce se familiariser avec l'environnement du travail et de la vie professionnelle ainsi que d'élargir et d'approfondir nos connaissances sur l'administration des réseaux informatiques.

En guise de perspectives nous envisageons d'intégrer un serveur firewall robuste ainsi que de configurer un serveur d'authentification tel que RADIUS pour s'assurer que la bonne personne est bien affectée au bon VLAN. Comme nous envisageons d'utiliser aussi d'autres environnements de travail tels que « BESON » ou « OPEN NETWORK » qui vont nous permettre de simuler et d'exécuter plusieurs équipements réseaux d'une manière fluide et stable.

Bibliographie

- [1] Guy Pujolle. Cours réseaux et télécoms. Edition Eyrolles, 2004.
- [2] Philippe Atelin. Réseaux informatiques Notions fondamentales (Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, WiFi,...). Editions ENI, 2009.
- [3] KOUASSI T. ingénieur en conception informatique, Centre d'expertise et de perfectionnement en informatique « Etude et optimisation du réseau local », these doctorat, 2007.
- [4] Meilleur pratique en matière de vlan, livre blanc, IN www.fluKenetworks.com, fluKe corporation, 2004.
- [5] Document RTC SONATRACH.
- [6] Philippe Mathon. Wndows Server 2003 : Les services réseau TCP/IP. Edition ENI, 2003.
- [7] BOUKRAM A. Introduction à la Sécurité Informatique, Mémoire master Département Informatique, Université de Bejaia. 2015.
- [8] Joële MUSSET. Sécurité informatique : Ethical hacking : Apprendre l'attaque pour mieux se défendre, 2009.
- [9] Didier Godart. Sécurité informatique : risques, stratégies et solutions. Edipro, 2002.
- [10] Steven Andrés, Brian Kenyon, and Erik Pack Birkholz. Security Sage's guide to hardening the network infrastructure. Syngress, 2004.
- [11] Antoine Joux. La réduction des réseaux en cryptographie. Ecole Normale Supérieure (Paris). Laboratoire d'Informatique, 2004.
- [12] TOUAZI DJ. . Conception et réalisation d'une segmentation logique dynamique et portable du réseau intranet de l'université de béjaia. 2012.
- [13] Dale Liu. Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Preparation Kit. Syngress, 2009.
- [14] Richard Froom, Balaji Sivasubramanian, and Erum Frahim. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide : Foundation Learning for SWITCH 642-813. Cisco Press, 2010.

- [15] Steve A Rouiller. Virtual lansecurity : weaknesses and counter measures.available at uploads. askapache. com/2006/12/vlan-security-3. pdf , 2006.
- [16] Todd Lammle and William Tedder. CCNA Routing and Switching Deluxe Study Guide : Exams 100-101, 200-101, and 200-120. John Wiley& Sons, 2014.
- [17] L Xavier and K Thomas. Réseauxprivésvirtuels-vpn.Frameiptcpip,2004.
- [18] Guillaume Desgeorge. La sécurité des réseaux, Disponible sur <http://www.guill.net/>. 2000
- [19] Khaled TRABELSI and Haythem AMARA. Mise en place des réseauxLAN interconnectés en redondance par 2 réseaux WAN. thèse, Université Virtuelle de Tunis, 2011.
- [20] A. braham et L. Medjkoune, Proposition d'une solution VPN cas université de Bejaia.Mémoire de master (en informatique), université de Bejaia, 2016.
- [21] Adrien Miller and Philippe Jean Dit Pannel. Sécurité avec ip : Les solutions. 2003.
- [22] Philippe Mathon. Windows Server 2003 : les services réseaux TCP/IP.Editions ENI, 2003.
- [23] Etienne GALLET DE SANTERRE. Protocole l2tp. Techniques de l'ingénieur. Télécoms, (TE7579), 2006.
- [24] Ali Larab, Pierre Gaucher, and Patrick Martineau. Intégration du protocoleipsec dans un réseau domestique pour sécuriser le bloc des sousréseaux fan. 2010.

Webographie

- [W1] <https://ipcisco.com/course/ccna/>, 26 mai 2019
- [W2] <https://cisco.goffinet.org/ccna/fondamentaux/modeles-tcp-ip-osi/#1-mod%A81E-tcpip>, 28 mars 2019
- [W3] Portail.jacquenod.net/Web/Commutateur/DPDF/CI-commutateurpdf.pdf, 18 avril 2019
- [W4] git.meleeweb.net/school/ETNA.git/plain/2eme.../cours/Cours%205a.pdf, 24 avril 2019

Résumé

L'utilisation du système informatique dans les entreprises engendre plusieurs problèmes de sécurité, de ce fait il est devenu indispensable d'implémenter une politique qui protège les données contre toutes attaques ou menaces qui proviennent soit de l'intérieur ou de l'extérieur. L'objectif de ce projet consiste à concevoir et configurer un réseau sécurisé de l'entreprise SONATRACH, afin de lui fournir un partage efficace de données en utilisant les réseaux privés virtuels VPNs, associés au protocole de tunneling IPsec ainsi que les VTPs qui permet de gérer de façon centralisé les VLANs. Pour mettre notre solution en pratique nous avons utilisé le simulateur « PACKET TRACER », qui offre la possibilité d'implémenter un réseau physique virtuel et de simuler le comportement des protocoles sur ce réseau.

Mots clés : VPN, protocole de tunneling IPsec, VTP, VLAN, PACKET TRACER.

Abstract

The use of the computer system in enterprises leads to several security problems; As a result, it has become essential to implement a policy that protects data against attacks or threats from inside or outside. The objective of this project is to concept and configure a secure network of the SONATRACH company, in order to provide it with an efficient data sharing using the VPNs virtual private networks, associated with the IPsec tunneling protocol as well as the VTPs which allows for the centralized management of VLANs. To put our solution into practice we have used the «PACKET TRACER» simulator, which offers the possibility to implement a virtual physical network and to simulate the behavior of the protocols on this network.

Keywords: VPN, tunneling protocol IPsec, VLAN, PACKET TRACER.