

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE

UNIVERSITE ABDERRAHMANE MIRA DE BEJAIA



FACULTE DES SCIENCES EXACTES
DEPARTEMENT D'INFORMATIQUE

En vue de l'obtention du diplôme de master professionnel en informatique
Option : Administration et Sécurité des Réseaux

THEME

**Etude et configuration d'un réseau de
campus (SONATRACH Béjaïa)**

Réalisé par :

Melle : BOURNANE Fazia

Melle : KHELFAOUI Yasmina

Encadré par :

M. AISSANI Sofiane

Membres du jury :

Présidente : Mme KOUICEM Amal

Examinatrice : Mme ZIDANI Ferroudja

-Promotion 2015-

Remerciements

Tout d'abord, nous tenons à adresser nos vifs remerciements à tous ceux qui nous ont aidées de près ou de loin à élaborer ce travail :

Nous exprimons nos sincères remerciements et nos profondes reconnaissances à DIEU le tout puissant et miséricordieux qui nous a donné la force et la patience d'accomplir ce travail.

Nous présentons nos sincères gratitudes à notre famille pour nous avoir toujours soutenues

Nous remercions nos encadrateurs :

À la RTC, M. SOUADIH K. et M. TIAB A.

À l'université, M. AISSANI S.

Nous présentons tous nos respects et nos sincères remerciements aux membres du jury qui ont accepté d'évaluer notre travail.

À la fin, nous tenons à remercier tous nos amis et camarades de promotion pour les meilleurs et pires moments passés ensemble.

Dédicace

Je dédie ce mémoire

À mes chers parents ma mère et mon père

*Pour leur patience, leur amour, leur soutien, et leurs
encouragements.*

À mon frère Loucif

À mes sœurs Noura, Karima, Zakia et Nassiba

À mes nièces Rania et Céline

À mon neveu Yacine et mon cousin Amine

*À mes amis et mes camarades en particulier Ridha, Hana, Katia,
Laythmasse et Hadeka*

À mon binôme Yasmina

*Sans oublier tous les professeurs que ce soit du primaire, du moyen, du
secondaire ou de l'enseignement supérieur.*

B.FAZIA

Dédicace

Je dédie ce mémoire

À mes chers parents mon père et ma mère

*Pour leur patience, leur amour, leur soutien, et leurs
encouragements.*

À mes frères Mounir, Riad et mon beau frère Samir

À mes sœurs Sihem, Hanane et ma belle sœur Sabiha

À ma nièce Nihad

À tous mes cousins et cousines

*À mes amis et mes camarades en particulier Riad, Hana, Laythmase
et Katia*

A mon binôme Fazia

*Sans oublier tous les professeurs que ce soit du primaire (Habiba), du
moyen, du secondaire ou de l'enseignement supérieur.*

K. Yasmîna

Table des matières

Table des matières	i
Liste des figures	v
Liste des tableaux	vii

Introduction générale.....	1
----------------------------	---

Chapitre I : Présentation de l'organisme d'accueil

Introduction	2
I. Présentation de Sonatrach	2
I.1. Organigramme.....	3
I.2. Présentation de la branche transport par canalisations (TRC)	3
I.3. Présentation de la direction régionale de transport de Béjaïa (DRGB).....	4
I.3.1. Structure de la DRGB	5
II. Présentation du centre informatique	5
II.1. Organigramme du centre informatique	6
II.2. Rôle de chaque service.....	Erreur ! Signet non défini.
II.2.1. Service système et réseau	6
II.2.2. Service base de données et logiciels	7
II.2.3. Service supports	8
Conclusion.....	8

Chapitre II: Conception d'un réseau de campus

Aucune entrée de table des matières n'a été trouvée.Liste des acronymes	57
---	----

Références bibliographiques	59
-----------------------------------	----

ANNEXES

Annexe A1 61
Annexe A2 64

Liste des figures

Chapitre I : Présentation de l'organisme d'accueil

Figure 1 : Branches de Sonatrach.....	3
Figure 2 : Organisation de la direction régionale de Béjaïa.....	5
Figure 3 : Organigramme du centre informatique.....	6

Chapitre II: Conception d'un réseau de campus

Figure 1 : Modèle OSI.....	9
Figure 2 : Modèle TCP/IP	11
Figure 3 : Modele hiérarchique à trois couches	13
Figure 4 : Commutateurs modulaires	15
Figure 5 : Commutateur à configuration fixe.....	15
Figure 6 : Commutateur à configuration empilable	16

Chapitre III : Concepts des VLANs et étude de quelques protocoles

Figure 1 : Différents chemins.....	23
Figure 2 : Tempête de broadcas	24
Figure 3 : Réception multiple d'une trame	25
Figure 4 : Réseau avec STP	26
Figure 5 : Gestion des ports par le protocole STP	27

Chapitre IV: Réalisation

Figure 1 : Création d'un équipement sur le simulateur Cisco.....	31
Figure 2 : Présentation de l'architecture	32
Figure 3 : Interface CLI.....	34
Figure 4 : Configuration du mot de passe	35
Figure 5 : Nomination du multilayer switch1	36
Figure 6 : Configuration des VTP-server.....	36
Figure 7 : Configuration client-VTP	37

Figure 8 : Création des VLANs sur le serveur VTP	38
Figure 9 : Attribution des ports aux VLANs.....	39
Figure 10 : Configuration des liens trunk	40
Figure 11 : Configuration des interfaces VLAN.....	41
Figure 12 : Routage inter-vlan	41
Figure 13 : Configuration de DHCP	42
Figure 14 : Configuration de STP	43
Figure 15 : Configuration de HSRP	44
Figure 16 : Réseau local après la configuration	45
Figure 17 : Routage au niveau du Switch multi_sw0.....	46
Figure 18 : Routage au niveau du routeur	47
Figure 19 : Interconnexion de différents réseaux locaux	47
Figure 20 : VLANs distribués dans le Switch client s0	48
Figure 21 : SVI (Switch Virtuelle Interface).....	49
Figure 22 : Attribution des adresses IP	50
Figure 23 : Switch multi-sw1 en mode active.....	51
Figure 24 : Switch multi-sw1 en mode standby.....	51
Figure 25 : Test entre le Switch multifonction (multi-sw1) et le Switch d'accès.....	52
Figure 26 : Test entre machines des VLANs différents	53
Figure 27 : Test entre des machines des VLANs et commutateurs différents	54
Figure 28 : Attribution des adresses IP par le DHCP.....	54
Figure 29 : Test entre les machines des différents VLANs lorsque le switch cœur (multi-sw1) est défectueux	Erreur ! Signet non défini.

Liste des tableaux

Chapitre II: Conception d'un réseau de campus

Tableau 1 : Rôle des couches OSI	10
Tableau 2 : Rôle des couches TCP/IP	11
Tableau 3 : Fonctionnalités des commutateurs au niveau des 3 couches	17

Chapitre IV: Réalisation

Tableau 1 : Plan d'adressage des VLANs.....	33
--	----

Introduction générale

Parmi les éléments essentiels à l'existence humaine, le besoin de communication arrive juste après le besoin de survie. Par conséquent, le partage de l'information est devenu l'un des domaines d'étude les plus importants. Depuis l'antiquité, l'homme n'a jamais cessé de fournir des efforts intellectuels aussi bien que physiques afin de trouver des moyens ou des outils pour maintenir la communication dans sa vie quotidienne, et parmi ces outils, il existe l'ordinateur qui est une machine qui permet la manipulation des données. D'un point de vue initial, l'idée de relier plusieurs ordinateurs entre eux a pris sa part d'étude et de recherche d'où est apparue la notion des réseaux informatiques.

Le réseau informatique est composé d'un ensemble d'équipements (ordinateurs, routeurs, Switchs....), qui échangent des informations de multiples formes (texte, image, vidéo.....) entre eux via un dispositif de communications.

Pour relier un réseau à un autre, il faudra utiliser un périphérique d'interconnexion de niveau trois du modèle OSI (routeur, passerelle...). Ces derniers consistent à choisir la manière de transmettre un paquet IP à travers les divers réseaux.

L'objectif principal de notre projet consiste justement à configurer et à mettre en place un réseau de campus d'une entreprise, ainsi qu'à assurer l'échange des informations entre l'ensemble des équipements de ce dernier.

Notre rapport se subdivise en quatre principaux chapitres :

Dans le premier chapitre intitulé « présentation de l'organisme d'accueil », nous allons établir une description générale de l'entreprise SONATRACH et du centre informatique où nous avons effectué notre stage.

Le deuxième chapitre concerne la conception du réseau de campus où nous allons présenter un réseau local et les éléments indispensables qui contribuent à la réalisation de ce dernier.

Nous allons rajouter le troisième chapitre pour expliquer les concepts des VLANs et l'étude des protocoles VTP, STP, HSRP et DHCP

Enfin, nous allons entreprendre la phase de réalisation qui concerne la configuration des différents protocoles, ainsi que les tests de validation pour vérifier si vraiment les objectifs ont été atteints.

Chapitre I

Présentation de l'organisme d'accueil

Chapitre II

Conception d'un réseau de campus

Chapitre III

Concepts des VLANs et étude de quelques protocoles

Chapitre IV

Réalisation

Annexes

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 centre informatique de l'entreprise Sonatrach de Bejaia (RTC) que nous allons vous présenter ci-dessous.

La « SONATRACH » est une entreprise nationale par son histoire et son orientation, d'un grand poids économique, et internationale par son domaine d'activité, industrie pétrolière et gazière. Elle se situe au premier plan par l'importance de ses activités : prospection, forage, production...etc.

Le réseau informatique prend une place de plus en plus importante dans l'activité de l'entreprise. Pour cela, ses informations doivent être gérées, centralisées et accessibles en temps réel.

I. Présentation de Sonatrach

Sonatrach, avant d'avoir ce nom, était la société pétrolière de gérance (SOPEG) fondée le 12 mars 1956 par la compagnie française des pétroles Algérie (C F P A) et la société nationale de recherche et exploitation des pétroles en Algérie (S N R E P AL). Après l'indépendance, et grâce au décret n° 36/491 de la nationalisation des hydrocarbures, la SOPEG est devenue sonatrach.

SONATRACH est un acronyme de « Société Nationale de Transport et de Commercialisation des Hydrocarbures », c'est une société Algérienne créée le 31/12/1963. Ses activités principales étaient le transport et la commercialisation des hydrocarbures, et à partir de 1966, son champ d'action s'élargit et englobe la recherche et la transformation des hydrocarbures.

I.1. Organigramme

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

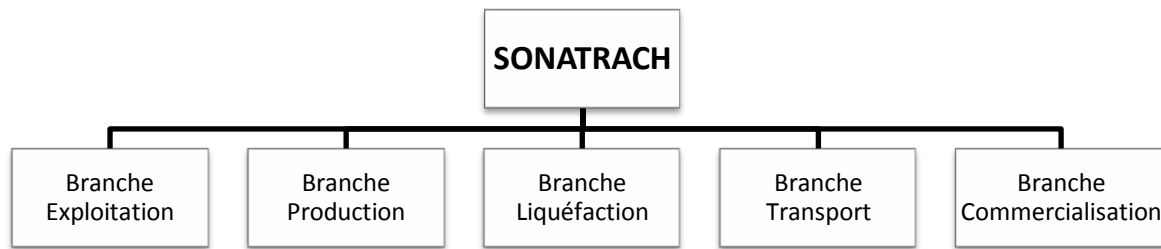


Figure 1 : Branches de Sonatrach

I.2. Présentation de la branche transport par canalisations (TRC)

L'activité de transport par canalisations (TRC) est en charge de l'acheminement des hydrocarbures pétroles brut, gaz et condensat vers les ports pétroliers, les zones de stockage et les pays d'exploitation.

Les missions affectées à la branche transport par canalisations sont :

- La gestion et l'exploitation des ouvrages et canalisations de transport d'hydrocarbures.
- La coordination et le contrôle de l'exécution des programmes de transport arrêtés en fonction des impératifs de production et de commercialisation.
- La maintenance, l'entretien et la protection des ouvrages et canalisations.
- L'exécution des révisions générales des machines tournantes et équipements.
- La conduite des études, la réalisation et la gestion des projets de développement des ouvrages et canalisations.
- Les installations de pompage et de stockage pour répondre aux besoins de SONATRACH dans les meilleures conditions d'économie, de qualité, de sécurité et de respect de l'environnement.
- Gère l'interface transport des projets internationaux du groupe ou en partenariat.

La Sonatrach possède cinq directions régionales de transport des hydrocarbures :

- La direction régionale Est (Skikda).
- La direction régionale Centre (Bejaïa).
- La direction régionale Ouest (Arzew).
- La direction régionale de Haoud-EL-Hamra.
- La direction régionale de Ain Amenas.

I.3. Présentation de la direction régionale de transport de Béjaïa (DRGB)

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.

I.3.1. Structure de la DRGB

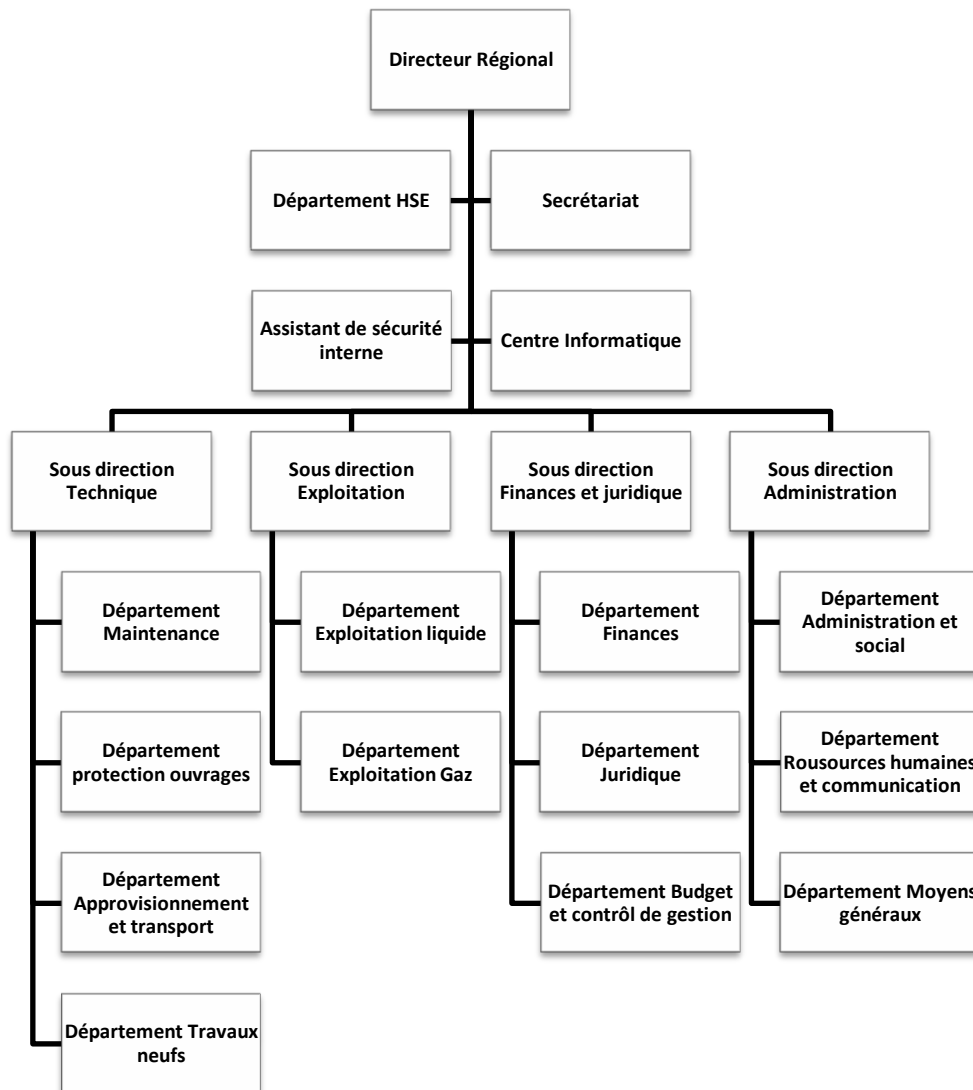


Figure 2 : Organisation de la direction régionale de Béjaïa

II. Présentation du centre informatique

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

II.1. Organigramme du centre informatique

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

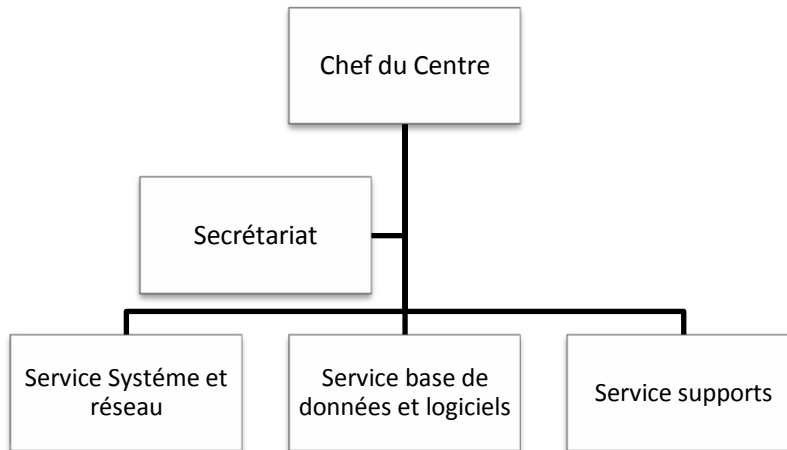


Figure 3 : Organigramme du centre informatique

II.2. Rôle de chaque service

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

II.2.1. Service système et réseau

Ce service est divisé en deux sections :

❖ Système

Son rôle est :

- Choix des équipements informatique et logiciel de base.
- Mise en œuvre les solutions matériels et logiciels retenues.
- Installation et configuration des systèmes.
- Orientation des travaux de l'équipe de développement par une bonne utilisation des ressources de l'ordinateur.
- Mise en œuvre des nouvelles versions de logiciels.
-

❖ Réseau

A pour rôle :

- Assurer le bon fonctionnement, la fiabilité des communications, l'administration du réseau et organiser l'évolution de sa structure.
- Conduite de l'étude pour le choix de l'architecture du réseau à installer.
- Participer à la mise en place des réseaux.
- Définir les droits d'accès à l'utilisation du réseau.
- Assurer la surveillance permanente pour détecter et prévenir les pannes.
- Traitement des dysfonctionnements et incidents survenant sur le réseau.

II.2.2. Service base de données et logiciels**❖ Base de données**

Son rôle est :

- Conçoit les bases de données et assure l'optimisation et le suivi de la gestion des données informatiques.
- Installe, configure et exploite le SGBD et ses bases.
- Met en oeuvre et gère les procédures de sécurité (accès, intégrité).
- Gère la sauvegarde, la restauration et la migration des données.
- Assure la cohérence et la qualité des données introduites par les utilisateurs.

❖ Logiciels

A pour rôle :

- Etude et conception des systèmes d'information.
- Développement et maintenance de l'application informatique pour TRC.
- Déploiement des applications et formation des utilisateurs.

II.2.3. Service supports

Son rôle est :

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

Conclusion

Dans ce chapitre, nous avons présenté l'entreprise Sonatrach de Béjaïa (RTC) où nous avons suivi notre stage pratique.

Dans le chapitre suivant, nous allons définir un réseau local et les éléments indispensables qui contribuent à la réalisation de ce dernier.

Introduction

Le réseau de campus évolue pour supporter les nouvelles applications métiers mais aussi les nouvelles applications multimédia et collaboratives nécessaires à l'entreprise. Toutes ces applications reposent sur des fondations bien définies.

Dans ce chapitre, nous allons présenter un réseau local et les éléments indispensables qui contribuent à sa réalisation.

I. Concepts des réseaux

I.1. Modèle OSI [1]

OSI (Open Systems Interconnection) est un modèle pour l'interconnexion des systèmes ouvert, dans le but de rationaliser les différentes fonctions que doit remplir un réseau. Le modèle est dit ouvert, si les communications entre les divers équipements provenant de constructeurs différents s'effectuent conformément au modèle OSI.

Selon une publication éditée par l'ISO, un réseau est organisé en sept couches, chacune d'elles est responsable d'une certaine action ou service permettant de préparer les informations en vue de leur transmission sur les réseaux. Le modèle OSI proposé par l'ISO, est illustré à la figure 1 :

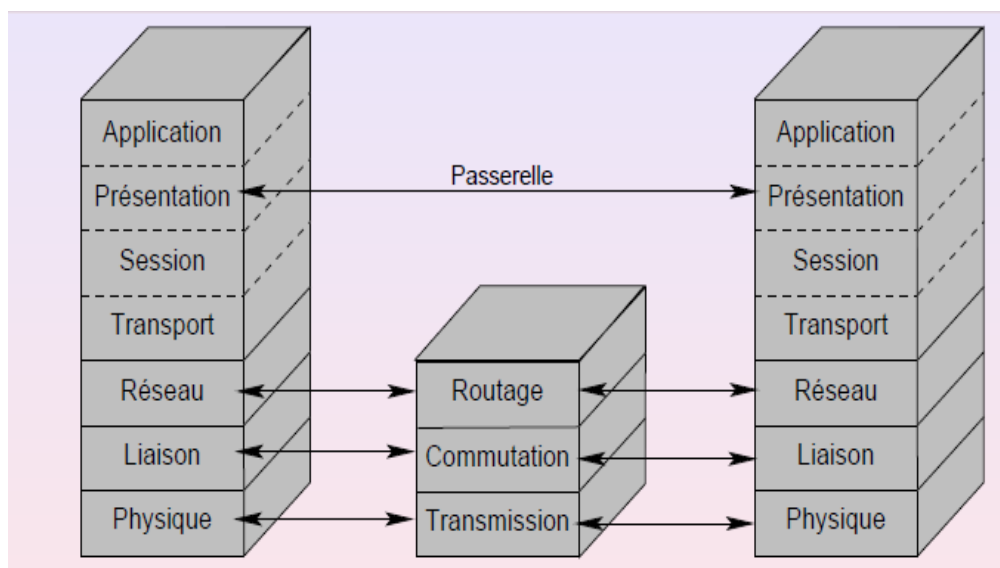


Figure 1 : Modèle OSI

I.1.1. Rôle des sept couches

Chaque couche réseau définie par le modèle a un rôle bien précis, qui va du transport du signal codant les données à la présentation des informations pour l'application destinataire, le tableau suivant résume le rôle de chaque couche

Numéro	Nom	Rôle
Couche 7	Application	<ul style="list-style-type: none"> • Cette couche assure l'interface de communication avec l'utilisateur, à travers des logiciels adéquats. • Elle gère également la communication entre applications, comme pour le courrier électronique.
Couche 6	Présentation	<ul style="list-style-type: none"> • Elle assure la mise en forme des données : paramètre internationaux, pages de codes, formats divers...
Couche 5	Session	<ul style="list-style-type: none"> • Elle gère l'établissement, la gestion et coordination des communications.
Couche 4	Transport	<ul style="list-style-type: none"> • est chargée du transport des données, de leur découpage en paquets et de la gestion des éventuelles erreurs de transmission
Couche 3	Réseau	<ul style="list-style-type: none"> • Cette couche fournit les moyens de communication et détermine la fonction de routage qui achemine le transfert des paquets d'une extrémité à une autre. • Elle gère l'adressage de transmission des données entre l'émetteur et le récepteur.
Couche 2	Liaison de données	<ul style="list-style-type: none"> • Assure la transmission des trames entre les systèmes d'une manière correcte, donc, c'est elle qui se charge de la détection et la correction des erreurs de transmission en appliquant des protocoles de contrôle.
Couche 1	Physique	<ul style="list-style-type: none"> • Elle a pour rôle la transmission bit à bit sur le support, entre l'émetteur et le récepteur, des signaux électriques, électromagnétiques ou lumineux, qui codent des données numériques (0 ou 1).

Tableau 1: Rôle des couches OSI

I.2. Modèle TCP/IP [2]

L'architecture des réseaux informatique TCP/IP qui porte le nom principaux protocoles qui constituent ce modèle, à savoir TCP et IP est un ensemble de protocoles définis en quatre couches permettant l'échange des informations entre les différents systèmes. Ce modèle est une abstraction du modèle OSI qui est un modèle théorique, contrairement au modèle TCP/IP qui est un modèle totalement pratique. La figure 2 ci-dessous présente le modèle TCP/IP :

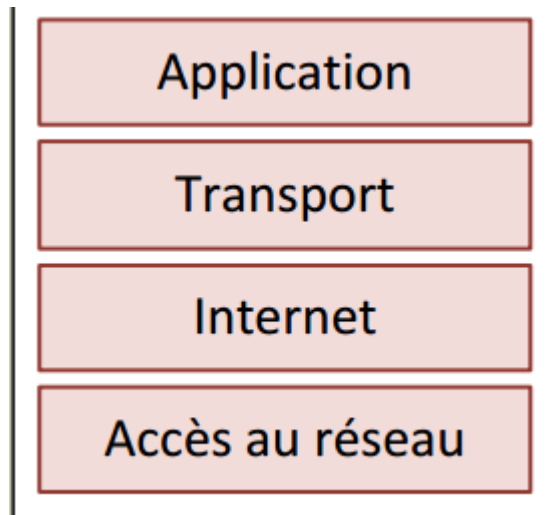


Figure 2 : Modèle TCP/IP

I.2.1. Rôle des quatre couches

Chaque couche définie par le modèle TCP/IP a un rôle bien précis, le tableau suivant résume le rôle de chaque couche :

Nom	Rôle
Couche Application	<ul style="list-style-type: none"> • Elle englobe l'application standard du réseau (Telnet, SMTP, FTP, ...).
Couche transport	<ul style="list-style-type: none"> • Elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission.
Couche interréseau	<ul style="list-style-type: none"> • Elle est chargée de fournir le paquet de données (datagramme).
Couche accès réseau	<ul style="list-style-type: none"> • Elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé.

Tableau 2 : Rôle des couches TCP/IP

I.3. Définition d'un réseau local [W1]

Les réseaux locaux, encore appelés LAN (local area network) sont constitués des moyens de communication internes à un établissement, donc entièrement maîtrisés par l'entreprise. C'est un système de communication de données limité à une zone géographique restreinte (jusqu'à 10 Km environ) et utilisant des débits moyens élevés (de 100 kbps à 50 Mbps). La zone servie peut être un simple bâtiment, un complexe de bâtiments ou un « campus ». Le réseau utilise une forme de commutation et n'emploie pas les circuits des

opérateurs publics, mais peut contenir des passerelles ou des ponts vers d'autres réseaux public ou privés.

I.4. Définition d'un réseau de campus [W2]

Un réseau de campus est un réseau propriété de LAN ou un ensemble de réseaux locaux interconnectés servant une entreprise, un organisme gouvernemental, une université ou une organisation similaire. Dans ce contexte, un campus englobe un ensemble de bâtiments à proximité. Les utilisateurs finaux dans un réseau de campus peuvent être dispersés plus largement (dans un sens géographique) que dans un seul réseau local, mais ils ne sont généralement pas aussi dispersés comme ils le seraient dans un réseau étendu WAN. Les réseaux de campus utilisent généralement les technologies LAN, comme Ethernet, Token Ring, Fast Ethernet et Gigabit Ethernet.

II. Modèle de réseau hiérarchique [3]

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

II.1. Modèle de conception hiérarchique à trois couches

Cisco a développé un modèle à trois couches pour concevoir un réseau de campus :

❖ La couche d'accès (Access Layer)

Cette couche est constituée des périphériques finaux tels que les ordinateurs, les imprimantes et les téléphones IP. Elle peut aussi contenir des routeurs, des commutateurs, des concentrateurs et des points d'accès sans fil.

Le rôle de cette couche est de connecter les périphériques finaux au reste du réseau et de vérifier s'ils sont autorisés.

❖ La couche de distribution (Distribution Layer)

Cette couche contient essentiellement des commutateurs de niveau 2 et 3 (fonction de routage) et sert d'interconnexion entre la couche d'accès et la couche de cœur de réseau.

Son rôle est de gérer le flux du trafic à l'aide de stratégies et de délimiter les domaines de diffusion via des fonctions de routage inter VLAN.

❖ La couche cœur de réseau (Core Layer)

La couche cœur est considérée comme étant le réseau fédérateur à haut débit de l'interréseau et assure la connexion aux ressources internet. Le trafic au niveau de cette couche est important et rapide.

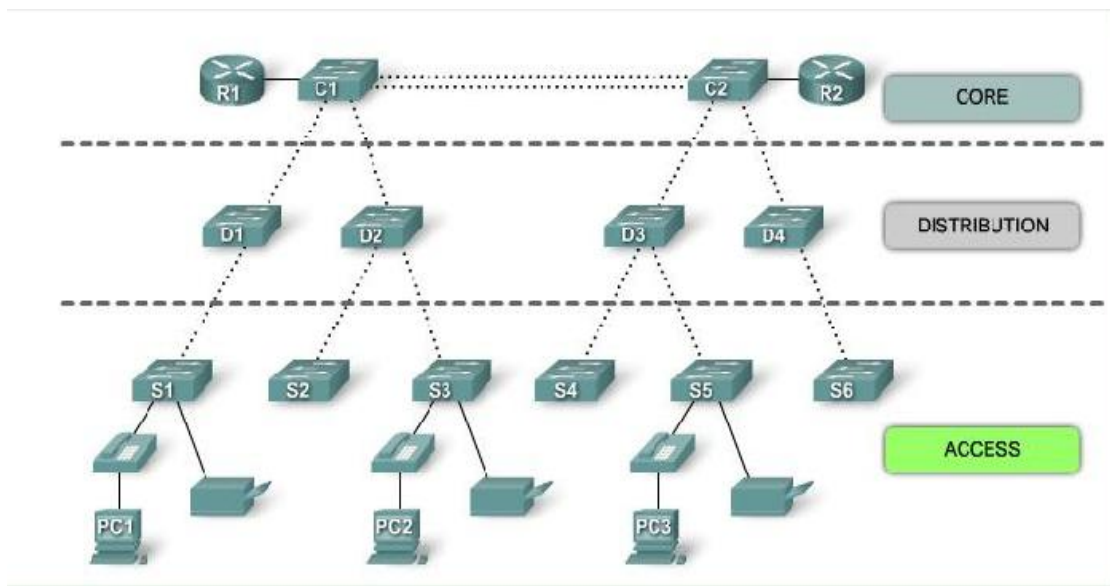


Figure 3: Modèle hiérarchique à trois couches

II.2. Avantage d'un réseau hiérarchique

- ❖ **Evolutif** : ces réseaux peuvent s'étendre plus facilement.
- ❖ **Redondant** : la redondance au niveau de la couche cœur de réseau et de la couche de distribution permet d'assurer une continuité de service pour la couche d'accès.
- ❖ **Performant** : la mise en place d'agrégat de liens entre les commutateurs de la couche de distribution et ceux de la couche cœur du réseau permet d'augmenter la vitesse.
- ❖ **Sécurité** : la sécurité du réseau peut être renforcée avec la mise en place de la sécurité des ports au niveau de la couche d'accès et la mise en place des stratégies de sécurité et/ou des listes de contrôle d'accès au niveau de la couche de distribution.

- ❖ **Cout de gestion diminué** : la cohérence de paramétrage entre les différents commutateurs de même couche permet une simplification de la gestion.
- ❖ **Maintenance** : la conception modulaire d'un réseau hiérarchique permet une mise à jour plus aisée.

II.3. Principes du modèle d'un réseau hiérarchique

Pour mettre en place correctement un réseau hiérarchique, il faut commencer par étudier la couche d'accès et définir les périphériques finaux. Pour les autres couches, il faut étudier ces éléments :

- ❖ **Les liens agrégés** : il faut identifier les ports permettant la liaison entre les commutateurs de chaque couche et surtout estimer les débits nécessaires et disponibles pour mettre en place les liens agrégés permettant d'augmenter la bande passante disponible.
- ❖ **Les liens redondants** : en plus des liens agrégés, il faut prévoir des liens redondants permettant d'assurer la continuité de service sur la couche de distribution et la couche cœur de réseau en cas de défaillance d'un commutateur sur ces couches.

III. Commutation

III.1. Définition d'un commutateur [W3]

Un commutateur réseau (switch), est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique. Il s'agit le plus souvent d'un boîtier disposant de plusieurs (entre 4 et 100) ports Ethernet. Il a donc la même apparence qu'un concentrateur (hub).

Contrairement à un concentrateur, un commutateur ne se contente pas de reproduire sur tous les ports chaque terme informatique qu'il reçoit. Il sait déterminer sur quel port il doit envoyer une trame, en fonction de l'adresse à laquelle cette trame est destinée. Les commutateurs sont souvent utilisés pour remplacer des concentrateurs. Un commutateur de niveau 2 ne s'occupe pas du protocole IP. Il utilise les adresses MAC et non les adresses IP pour diriger les données. Les commutateurs de niveau 2 forment des réseaux de niveau 2 (Ethernet). Ces réseaux sont reliés entre eux par des routeurs (ou des commutateurs de niveau 3) pour former des réseaux de niveau 3 (IP).

III.2. Différents types de commutateurs [W4]

Il existe trois types de commutateurs :

❖ Commutateurs modulaires

Offrent une plateforme haute performances destinée aux réseaux fédérateurs, environnements de campus. Les commutateurs modulaires représentés dans la figure 4 optimisent le réseau grâce à des options permettant une croissance évolutive. Par exemple, 16 cartes de ligne peuvent être ajoutées pour un total de 128 ports.



Figure 4: Commutateurs modulaires

❖ Commutateur à configuration fixe

Le commutateur à configuration fixe représenté sur la figure 5 apporte aux postes de travail une connectivité faste Ethernet et gigabit Ethernet optimise les services LAN sur les réseaux d'entreprises. Ce commutateur offre une sécurité intégrée sur le réseau et une qualité de service (QoS) évoluée pour distribuer des services intelligents à la périphérie du réseau.



Figure 5 : Commutateur à configuration fixe

❖ Commutateurs empilables

C'est une nouvelle gamme de commutateurs administrables empilables Ethernet, qui offre toutes les capacités avancées pour assumer un environnement réseau plus exigeant à un tarif abordable, ces commutateurs fournissent une connectivité faste Ethernet 24 à 48 ports et gigabit Ethernet de 24 à 52 ports. En outre, ces commutateurs

sont faciles à déployer et à gérer. Le commutateur empilable représenté dans la figure 6 :



Figure 6 : Commutateur à configuration empilable

III.3. Fonctionnalités d'un commutateur [4]

Un commutateur accomplit les fonctions suivantes :

- ❖ **Découverte:** le commutateur prend connaissance des adresses MAC du réseau en examinant l'adresse MAC de chaque trame qu'il reçoit.
- ❖ **Transmission ou filtrage:** le commutateur décide de transmettre ou de filtrer une trame en fonction de son adresse MAC de destination.
- ❖ **Evitement de boucle:** il crée un environnement exempt de boucle en collaboration avec les autres commutateurs à l'aide du protocole Spanning-Tree (STP).

III.4. Fonctionnalités des commutateurs au niveau des 3 couches [4]

Chaque commutateur a sa fonction au niveau de chaque couche du model hiérarchique du réseau :

	Accès	Distribution	Cœur
Agrégation de la bande passante	✓	✓	✓
Fast Ethernet /Gigabit Ethernet	✓		
Ethernet Gigabit/Ethernet 10 Gigabits		✓	✓
Débit de transfert élevé		✓	
Prise en charge de la couche 3		✓	✓
Sécurité des ports	✓		
Qualité de service (QoS)	✓	✓	✓
Composants redondants		✓	✓
Stratégies de sécurité/listes de contrôle d'accès		✓	

Tableau 3 : Fonctionnalités des commutateurs au niveau des 3 couches

III.5. Fonctionnalités de commutation [4]

❖ Commutation niveau 2 (Layer 2 Switching)

Il prend en charge les fonctionnalités suivantes:

- Utiliser pour connecter les utilisateurs finaux au réseau.
- Permet de réduire le domaine de collision.
- Si le réseau grandit, risque de générer les boucles de communication.
- Prend connaissance des adresses MAC du réseau en analysant les adresses MAC sources.
- Construit et maintient une table d'adresse MAC et leur association aux switch ports.
- Envoie les trames dont les destinations inconnues à tous les ports exceptés le port auquel il a reçu les trames.

❖ Commutation niveau 3 (Layer 3 Switching)

- Un Layer 3 switching ne fonctionne pas sur la base des adresses MAC.
- Il oriente le trafic sur la base des adresses IP.
- Il peut exécuter des fonctions de routage de la couche 3.

❖ Commutation multi niveau

- Un Switch multi niveau combine les fonctionnalités des couches 2,3 et 4.
- Faible délai d'acheminement.
- Réseaux facilement et rapidement agrandissable.

V.1. Différents types de communications

- ❖ **Communication Ethernet Monodiffusion** : communication depuis un expéditeur vers un destinataire spécifique du réseau.
- ❖ **Communication Ethernet Diffusion** : communication depuis un expéditeur vers tous les destinataires réseau.
- ❖ **Communication Ethernet Multidiffusion** : communication depuis un expéditeur vers un nombre défini de destinataire appartenant à un groupe de multidiffusion.

Conclusion

Ce chapitre nous a permis d'avoir une bonne compréhension des concepts de base et d'éclaircir les différentes idées du réseau LAN, nous avons vu le modèle de référence OSI et le modèle TCP/IP, la définition d'un réseau local, ses différentes couches et les éléments physiques qui le constituent. Dans le chapitre suivant, nous allons entamer les concepts des VLANs et quelques protocoles sur lesquels se fondent les réseaux informatiques.

Introduction

Dans les entreprises et l'industrie de manière générale, les premiers objectifs de l'adoption des réseaux informatiques étaient d'ordre technique comme le partage des ressources. Ces réseaux d'entreprise ont, ensuite, évolué pour permettre d'offrir de nombreux types de services, parmi lesquels, les courriels, la téléphonie et l'accès à l'information.

A travers ce chapitre, nous allons aborder quelques notions fondamentales sur lesquelles se fondent les réseaux informatiques, en particulier les réseaux virtuels. Nous allons terminer par l'étude des protocoles VTP, STP, HSRP et le service DHCP.

I. Virtuels LAN [5]

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

I.1. Typologie de VLAN

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

❖ VLAN de niveau 1 ou VLAN par port

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

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

❖ VLAN de niveau 2 ou VLAN MAC

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

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

❖ VLAN de niveau 3 ou VLAN d'adresses réseaux

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

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

I.2. Avantage de VLAN [W5]

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :

- La réduction des messages de diffusion (notamment les requêtes ARP) limités à l'intérieur d'un VLAN.
- les diffusions d'un serveur peuvent être limitées aux clients de ce serveur.
- La création de groupes de travail indépendants de l'infrastructure physique.
- possibilité de déplacer la station sans changer de réseau virtuel.

- L'augmentation de la sécurité par le contrôle des échanges inter-VLAN utilisant des routeurs (filtrage possible du trafic échangé entre les VLANs).

II. Protocole VTP [6]

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

II.1. Concept de VTP

VTP est un protocole propriétaire de CISCO, il est chargé de gérer les VLANs d'une manière centralisée et évite ainsi aux administrateurs du réseau de se connecter autant de fois qu'il y a de commutateurs dans un réseau pour ajouter, modifier ou supprimer la configuration d'un appelé serveur VTP, afin de distribuer ces informations de configuration VLAN d'un bout à l'autre du réseau commuté. Un tel protocole réduit les délais d'administration et de maintenance des réseaux VLAN. A noter que ce protocole s'applique au niveau de la couche liaison de données du modèle OSI.

II.2. Principe de fonctionnement

Le protocole VTP définit la notion de domaine VTP. Un domaine VTP est composé d'un ou plusieurs équipements interconnectés qui partagent le même nom. Il regroupe des commutateurs pour qu'ils échangent leurs informations de configurations envoyés par le serveur VTP de chaque domaine concerné et plusieurs domaines VTP peuvent cohabiter dans le même réseau local.

Dans un environnement VTP, un commutateur peut assurer un des trois rôles qui définissent les trois modes de fonctionnement suivants :

❖ Mode serveur VTP

Un commutateur en mode serveur est chargé de diffuser la configuration aux commutateurs du domaine VTP en envoyant des messages connus sous le nom « trames VTP », c'est le seul commutateur du domaine capable d'ajouter, supprimer ou renommer des VLAN dans le domaine VTP concerné. Le serveur VTP indique régulièrement le nom de domaine VTP et toutes les informations de configuration VLAN enregistrées dans la mémoire NVRAM du commutateur, y compris le dernier numéro de révision de la configuration VLAN.

❖ Mode client VTP

Un commutateur en mode client est chargé d'appliquer la configuration émise par un commutateur en mode serveur, ce mode ne donne pas la possibilité de créer, modifier ou supprimer des informations VLAN. Donc, il faut d'abord appliquer la modification au sein du serveur VTP pour qu'elle se propage aux différents commutateurs en mode client du même domaine VTP. Contrairement aux serveurs VTP, les informations de configuration VLAN sont totalement perdues lors de la réinitialisation de la mémoire NVRAM du commutateur client.

❖ Mode transparent VTP

Un commutateur en mode transparent ne fait que diffuser les annonces VTP et les configurations du domaine VTP auquel il appartient à travers ses ports de liaison sans prendre en compte leurs contenus. Donc, le commutateur transparent joue le rôle d'un intermédiaire de communication pour permettre aux clients VTP d'échanger les informations de configuration VLAN avec le serveur VTP.

III. Trafic Entre-VLAN [7]

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

Le concept d'agrégation ou bien le trunk qui utilise la norme IEEE. 1Q pour l'identification des trames, est indispensable, il consiste à regrouper plusieurs liaisons virtuelles sur une liaison physique unique, la fonction d'un trunk est de transporter les informations des VLANs entre plusieurs commutateurs interconnectés et donc d'étendre la portée des VLANs à un ensemble de commutateurs.

Les interfaces entre le commutateur distribution (SW-Dist) et tous les commutateurs Accès (SW-Accès), ainsi que l'interface entre le SW-Dist et le router, doivent être toutes configurées en mode trunk, afin qu'elles puissent transporter les informations des différents VLANs.

IV. Protocole STP (Spanning Tree Protocol) [w6]

L'un des problèmes d'une topologie réseau est la redondance. C'est-à-dire, la possibilité pour une trame d'atteindre le destinataire en empruntant plusieurs chemins. Cette possibilité augmente la fiabilité du réseau en évitant la paralysie des transmissions en cas de panne d'une des matériels d'interconnexion. La figure suivante montre le problème d'avoir plusieurs chemins en cas d'une défaillance d'un lien :

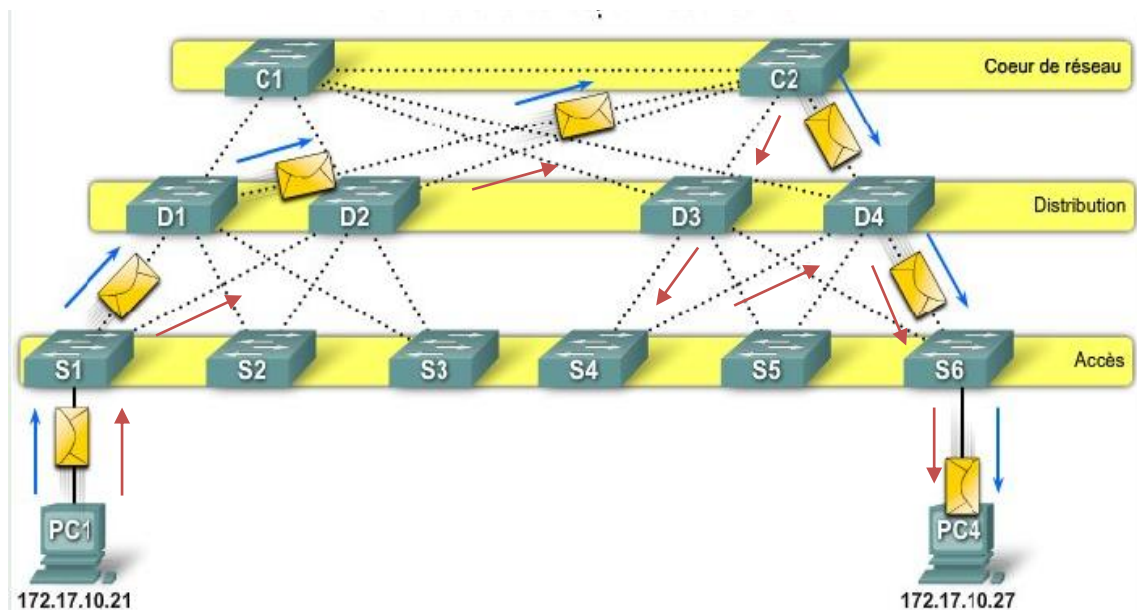


Figure 1 : Différents chemins

IV.1. Problèmes

❖ Tempête de broadcast

Une trame de broadcast est envoyée vers le commutateur A par le poste A. Ce commutateur A renvoie alors la trame vers tous les ports (sauf le port entrant) y compris en direction du commutateur B. Le commutateur B va dupliquer et renvoyer la trame vers tous les ports (sauf entrant) et donc vers le commutateur A et ainsi de suite. La trame va être dupliquée et ce schéma de communication va recommencer en boucle.

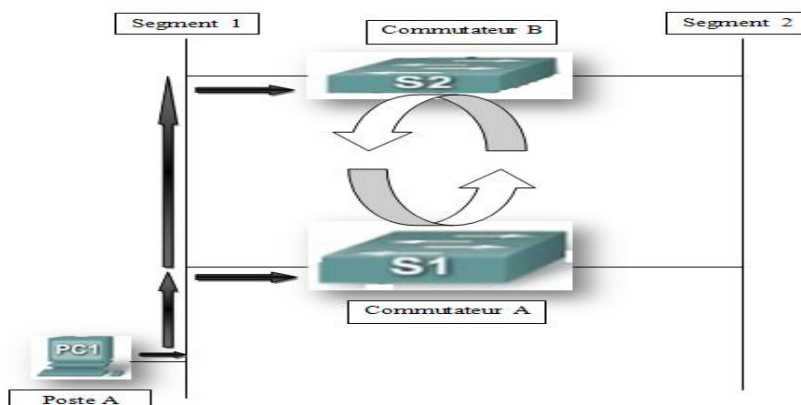


Figure 2 : Tempête de broadcast

❖ Réception multiple d'une trame

Dans le schéma qui suit, il est tout à fait possible que le matériel B (Poste B) reçoive via le commutateur A ET le commutateur B la même trame en provenance du poste A. Les matériels ne sont pas capables de gérer ce type de communication d'où une perturbation importante des communications.

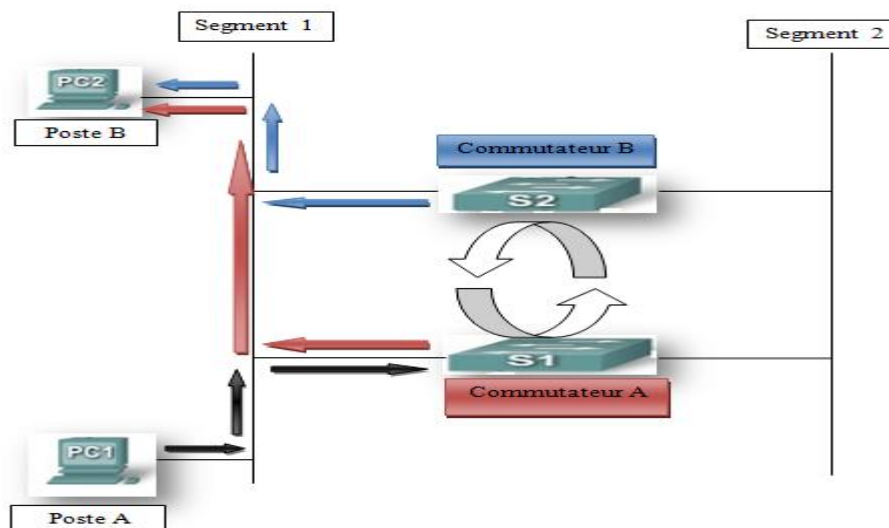


Figure 3: Réception multiple d'une trame

❖ Instabilité de la table des adresses Mac

Dans le cas où la trame est dupliquée et transite du poste A vers le commutateur A en passant par son port 0 et si dans le même temps, cette trame est envoyée du commutateur B vers le commutateur A sur son port 1. Alors, la table des adresses Mac du commutateur A va constamment se remettre à jour en indiquant une fois sur 2 (lors de l'envoi par le commutateur B) un port erroné ou du moins non optimum.

IV.2. Solution spanning tree

Pour éviter ces phénomènes, il est nécessaire de mettre en place un processus de suppression des boucles de façon logique : le spanning tree (STP : Spanning Tree Protocol).

Ce protocole travaille au niveau 2 de la couche OSI et est implémenté généralement sur les commutateurs, ponts et routeur (matériels pontés). Historiquement créé par DEC (Digital Equipment Corporation), l'algorithme est ensuite normalisé par l'IEEE sous la dénomination

802.1d. Ce protocole permet d'éviter les boucles en bloquant certains ports sur les matériels précités et en les débloquant en cas de panne. La figure suivante montre la topologie de STP :

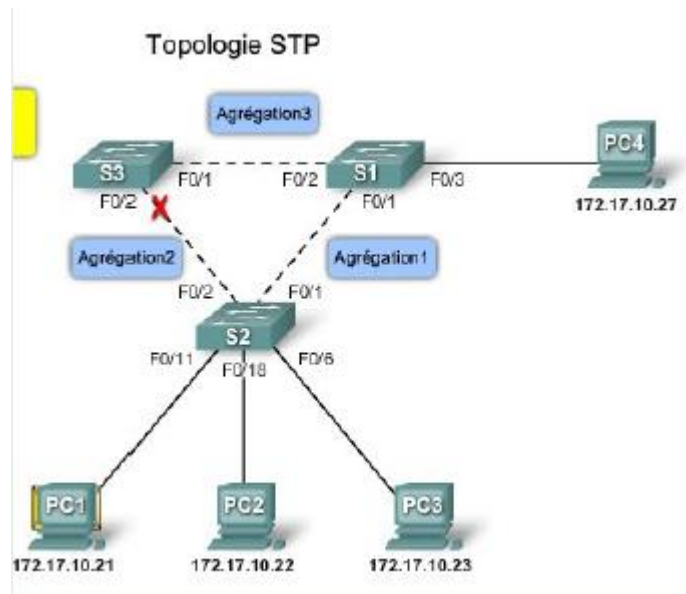


Figure 4 : Réseau avec STP

IV.3. Bridge Protocol Data Unit (BPDU)

- Le BPDU est la trame de message échangé par les commutateurs pour le protocole STP.
- Chaque BPDU contient un BID qui identifie le commutateur ayant envoyé le BPDU.
- Le BPDU contient une valeur de priorité, l'adresse mac du commutateur émetteur et un ID du système étendu facultatif. La valeur BID la plus faible est déterminée par la combinaison de ces trois champs.

IV.4. Rôle des ports

Dans le fonctionnement du STP, les ports commutateur (pont) peuvent jouer quatre rôles :

- ❖ **Ports racine:** Les ports de commutateur les plus proches de pont racine.
- ❖ **Ports désignés:** Tous les ports non racine qui sont autorisés à acheminer le trafic sur le réseau. Il transmet les trames.
- ❖ **Ports non désignés:** Tous les ports configurés dans un état de blocage pour empêcher la formation de boucles. Ce port ne transmet pas les trames.

- ❖ **Port désactivé** : est un port qui a été administrativement arrêté. C'est un port qui ne rentre pas dans le processus du protocole STP. Ce port ne transmet pas les trames.

La figure suivante montre les types des ports existant dans le protocole STP

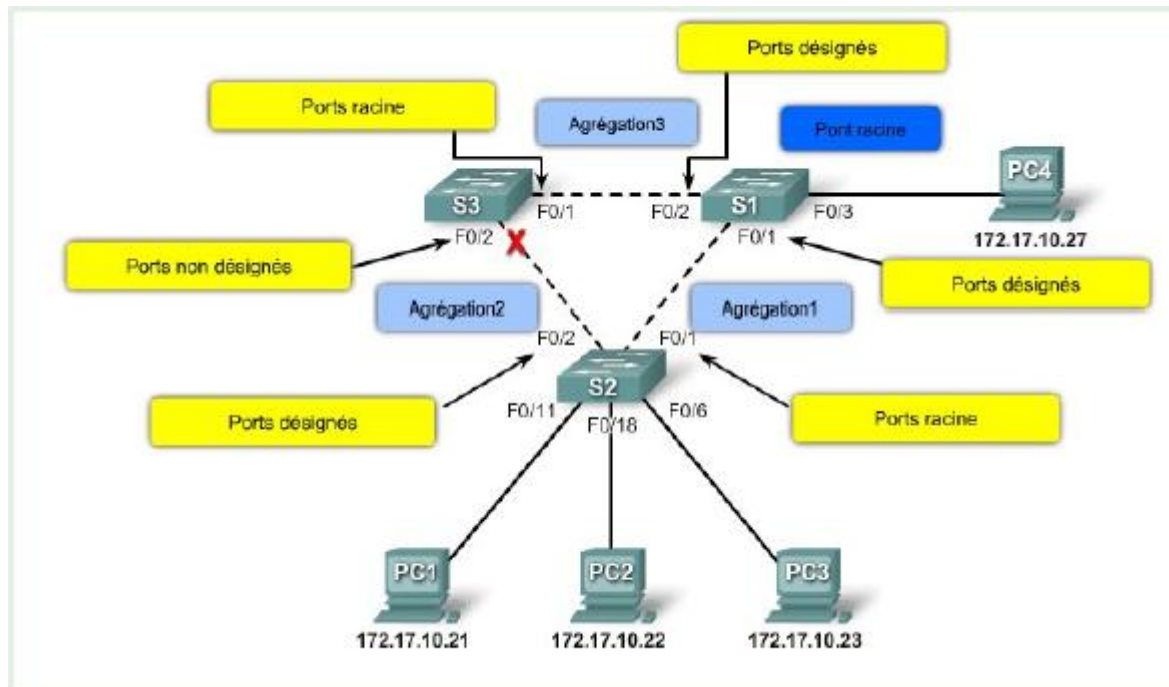


Figure 5 : Gestion des ports par le protocole STP

V. Présentation de HSRP [w7]

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 de panne sur le réseau en créant un routeur virtuel à partir de 2 (ou plus) routeurs physiques : un « actif » et l'autre (ou les autres) « en attente » ou « standby » en fonction des priorités accordées à chacun de ces routeurs.

HSRP est un protocole propriétaire aux équipements Cisco et il n'est pas activé par défaut.

V.1. Fonctionnement de HSRP

HSRP (Hot Standby Routing Protocol) est un protocole propriétaire créé par Cisco et très utilisé aujourd'hui dans nos LAN. En pratique, HSRP permet :

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

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

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

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

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

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

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

Si ces messages ne sont plus reçus par le routeur secondaire (Standby), c'est que le routeur primaire a un problème et le secondaire devient donc Actif.

L'élection se fait un peu à la manière de spanning-tree, en prenant en compte une priorité. Cette priorité est composée d'un paramètre « priority » compris entre 1 et 255 (255 étant le plus prioritaire) et de l'adresse IP de l'interface.

A priorités statiques égales, la plus haute adresse IP sera élue.

Plusieurs groupes HSRP peuvent exister au sein d'un même routeur sans que cela ne pose problème. Seuls les routeurs du même numéro de groupe s'échangeront les messages HSRP.

VI. Protocole DHCP [8]

Le protocole DHCP (Dynamic Host Configuration Protocol) 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, auprès du serveur DHCP. Le serveur DHCP lui attribuera notamment une adresse IP, un masque et éventuellement l'adresse d'une passerelle par défaut.

VI.1. Rôle d'un service DHCP

- Un serveur DHCP (Dynamic Host Configuration Protocol) a pour rôle de distribuer des adresses IP à des clients pour une durée déterminée.
- Au lieu d'affecter manuellement à chaque hôte une adresse statique, ainsi que tous les paramètres tels que (serveur de noms, passerelle par défaut, nom du réseau), un serveur DHCP alloue à un client, un bail d'accès au réseau, pour une durée déterminée (durée du bail). Le serveur passe en paramètres au client toutes les informations dont il a besoin.

VI.2. Avantages de DHCP

- Le protocole DHCP offre une configuration de réseau TCP/IP fiable et simple, empêche les conflits d'adresses et permet de contrôler l'utilisation des adresses IP de façon centralisée. Ainsi, si un paramètre change au niveau du réseau, comme, par exemple l'adresse de la passerelle par défaut, il suffit de changer la valeur du paramètre au niveau du serveur DHCP, pour que toutes les stations aient une prise en compte du nouveau paramètre dès que le bail sera renouvelé. Dans le cas de l'adressage statique, il faudrait manuellement reconfigurer toutes les machines.
- Les postes itinérants sont plus faciles à gérer.
- Le changement de plan d'adressage se trouve facilité par le dynamisme d'attribution.

Conclusion

Dans cette partie, nous avons étudié des concepts sur les VLANs et les différents protocoles ; cette étude nous facilitera la tâche de configuration pour entamer directement la simulation d'un réseau de campus avec le simulateur Packet tracer, qui sera l'objet du chapitre suivant.

Introduction

Ce présent chapitre consiste en la présentation de la réalisation de notre projet, en exposant les différentes configurations nécessaires à implémenter sur le LAN, en se basant sur le simulateur Cisco Packet Tracer.

Pour présenter les configurations que nous avons réalisées, nous nous sommes servis des captures d'écran qui illustrent les étapes de la configuration .Enfin, des tests de validation pour confirmer le bon fonctionnement du réseau, seront réalisés.

I. Présentation du simulateur Cisco « Packet Tracer »

Packet Tracer est un simulateur de réseau puissant développé par Cisco Systems pour faire des plans d'infrastructure de réseau en temps réel. Il offre la possibilité de créer, visualiser et de simuler les réseaux informatiques. L'objectif principal de ce simulateur est de schématiser, configurer et de voir toutes les possibilités d'une future mise en œuvre réseau.

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.

La figure1 est une image montrant l'interface principale et la création d'un équipement du simulateur Cisco Packet Tracer :

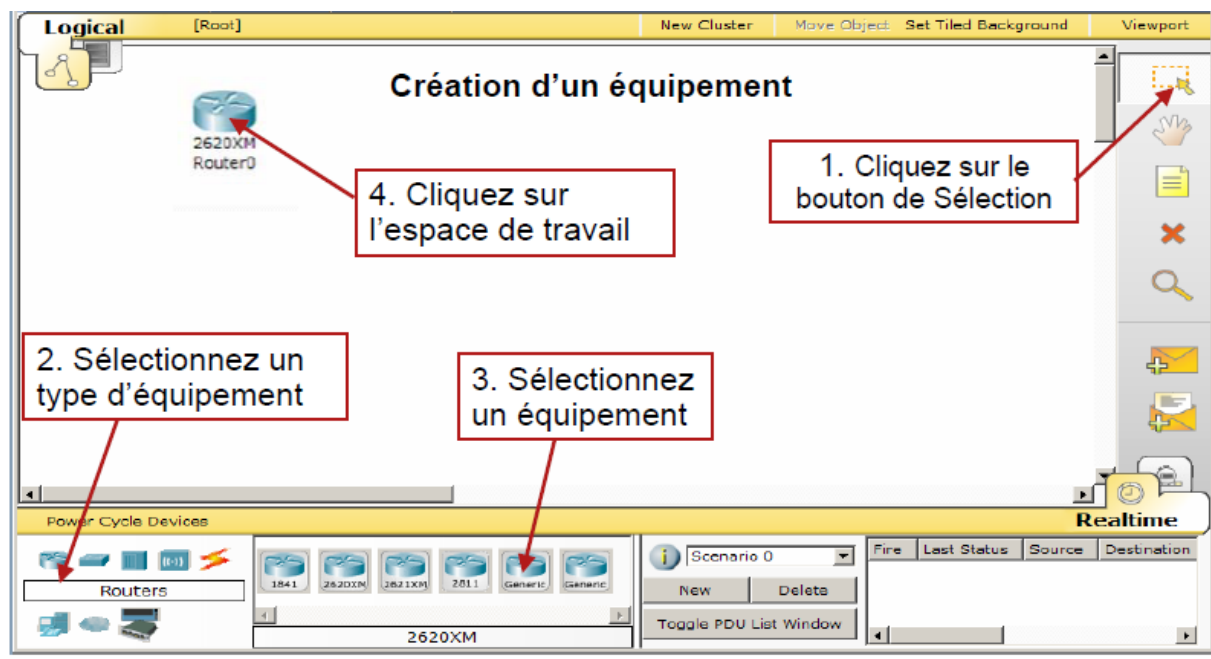


Figure 1 : Création d'un équipement sur le simulateur Cisco

I.1. Présentation de l'architecture réseau avant la configuration

La figure 2 illustre notre architecture réseau que nous allons réaliser.

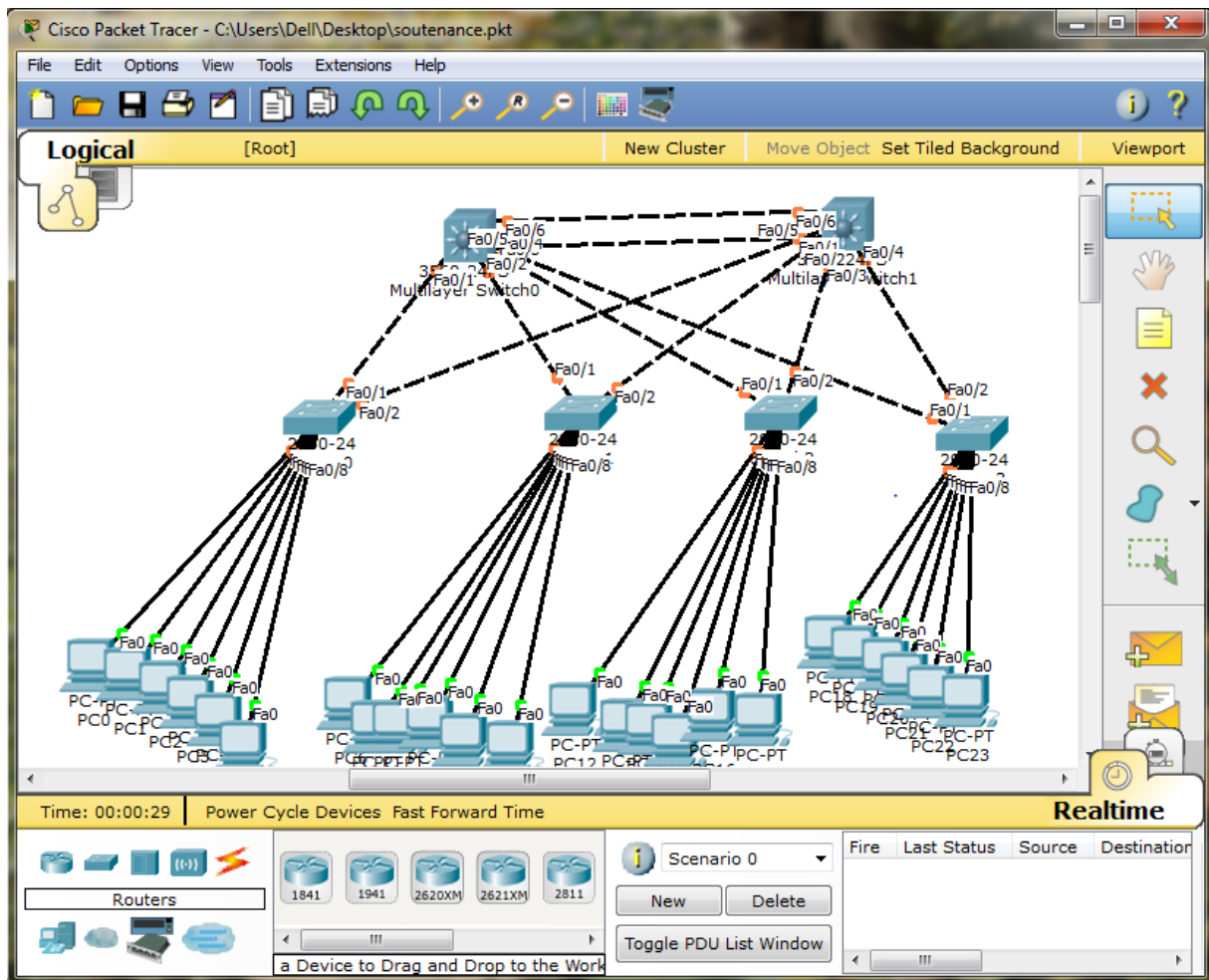


Figure2 : Présentation de l'architecture

II. Segmentation VLANs

L'organisation réseau se fera en le segmentant à l'aide des VLANs. Chaque section du réseau représente un VLAN. Par conséquent, il y'aura naissance de 6 VLANs à savoir :

Maintenance, Exploitation, HSE, Transport, Administrative et serveur

II.1. Plan d'adressage

Un réseau ne peut fonctionner sans une attribution et une configuration correcte de différentes adresses. 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.

L'élaboration d'un plan d'adressage nécessite la prise en considération de certaines règles, telles que la classe d'adressage, la définition de sous-réseau, l'attribution statique et/ou dynamique des adresses.

II.2. Adressage des VLANs

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

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

VLAN-id	Nom VLAN	Adresse sous-réseau	PCs
10	Maint	192.168.10.0/24	PC0, PC6, PC12, PC18
20	Expl	192.168.20.0/24	PC1, PC7, PC13, PC19
30	HSE	192.168.30.0/24	PC2, PC8, PC15, PC20
40	Trans	192.168.40.0/24	PC3, PC9, PC14, PC21
50	Admin	192.168.50.0/24	PC4, PC10, PC16, PC22
60	server	192.168.60.0/24	PC5, PC11, PC17, PC23

Tableau 1 : Plan d'adressage des VLANs

III. Interface commande de Packet Tracer

Toutes les configurations des équipements du réseau seront réalisées au niveau de CLI (Commande Langage Interface). 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 est réalisée.

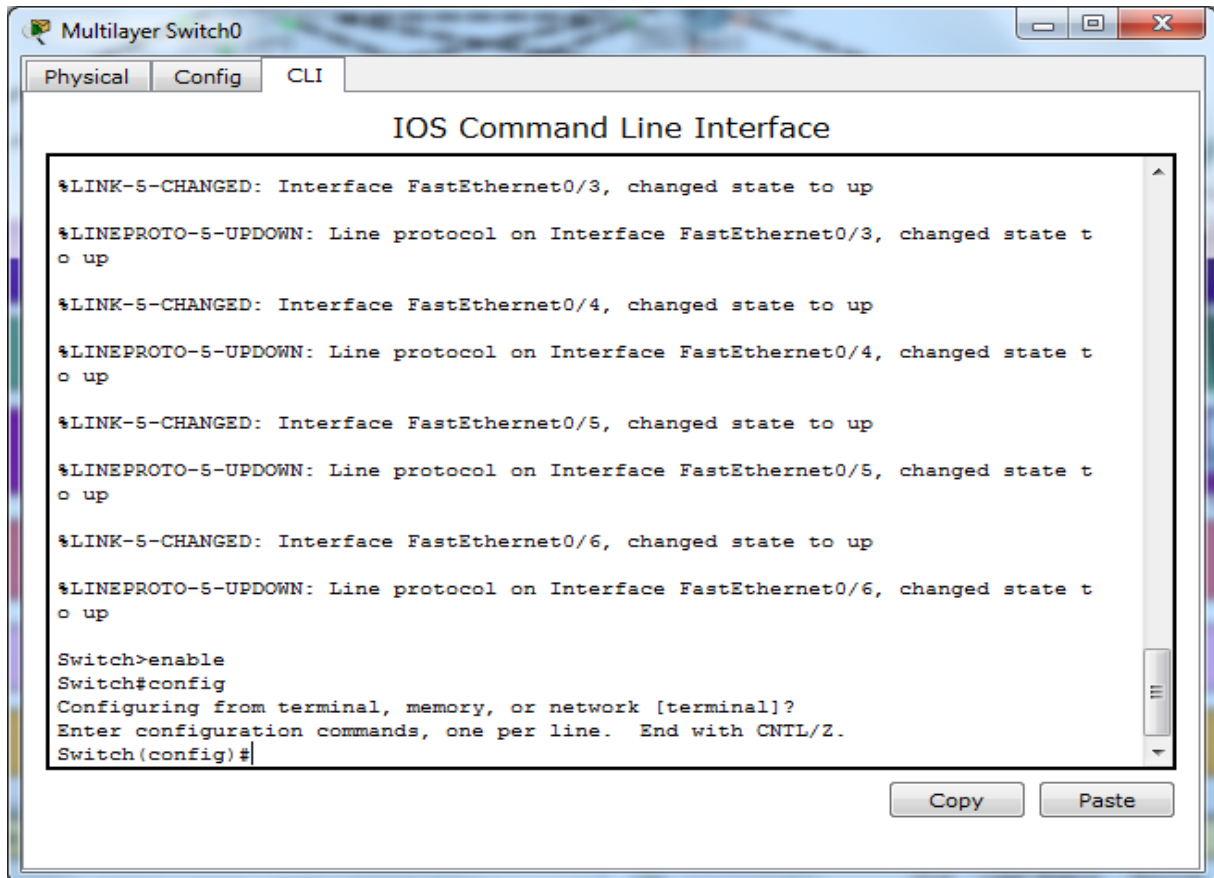


Figure 3 : Interface CLI

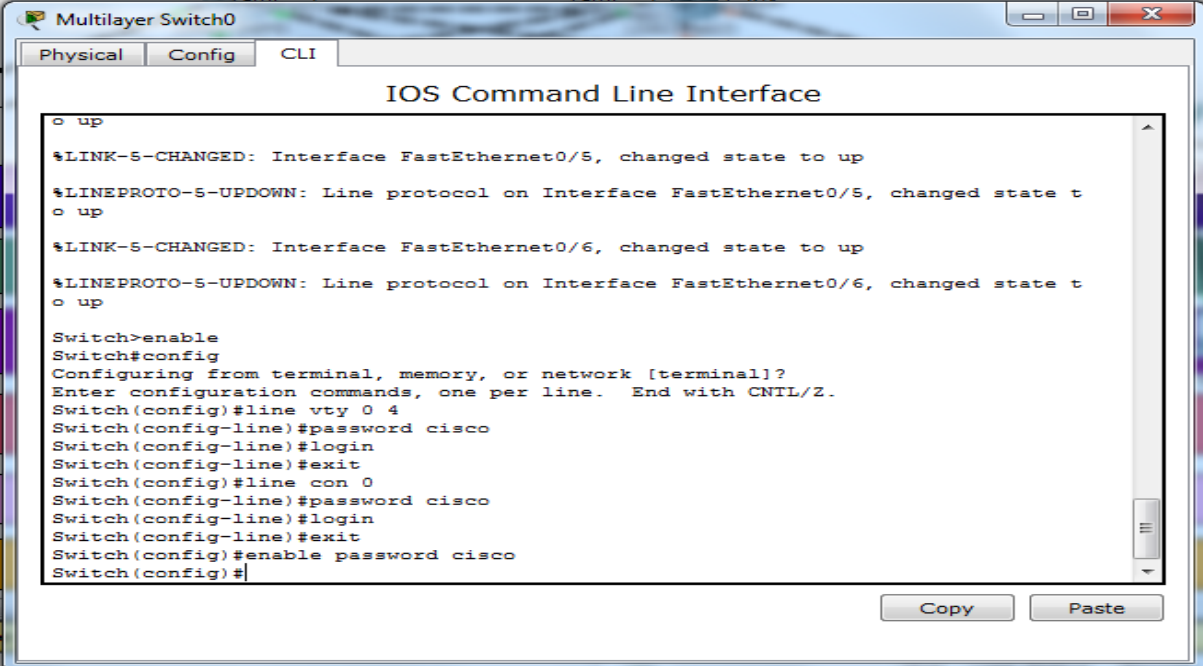
IV. Configuration des équipements

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

IV.1. Sécurisation de l'accès aux périphériques

Il faut savoir qu'IOS (International Standardization Organization) utilise des modes organisés hiérarchiquement pour faciliter la protection des périphériques. Dans le cadre de ce

dispositif de sécurité, IOS peut accepter plusieurs mots de passe, ce qui nous permet d'établir différents privilèges d'accès au périphérique.



```
o up
%LINK-S-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state t
o up
%LINK-S-CHANGED: Interface FastEthernet0/6, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state t
o up

Switch>enable
Switch#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#line vty 0 4
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line con 0
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#enable password cisco
Switch(config)#
```

Figure 4 : Configuration du mot de passe

IV.2. Configuration du Hostname

Cette étape permet de donner un nom significatif à l'ensemble des équipements constituant les LANs des stations comme par exemple la nomination du commutateur cœur multilayer switch indiquée dans la figure suivante :

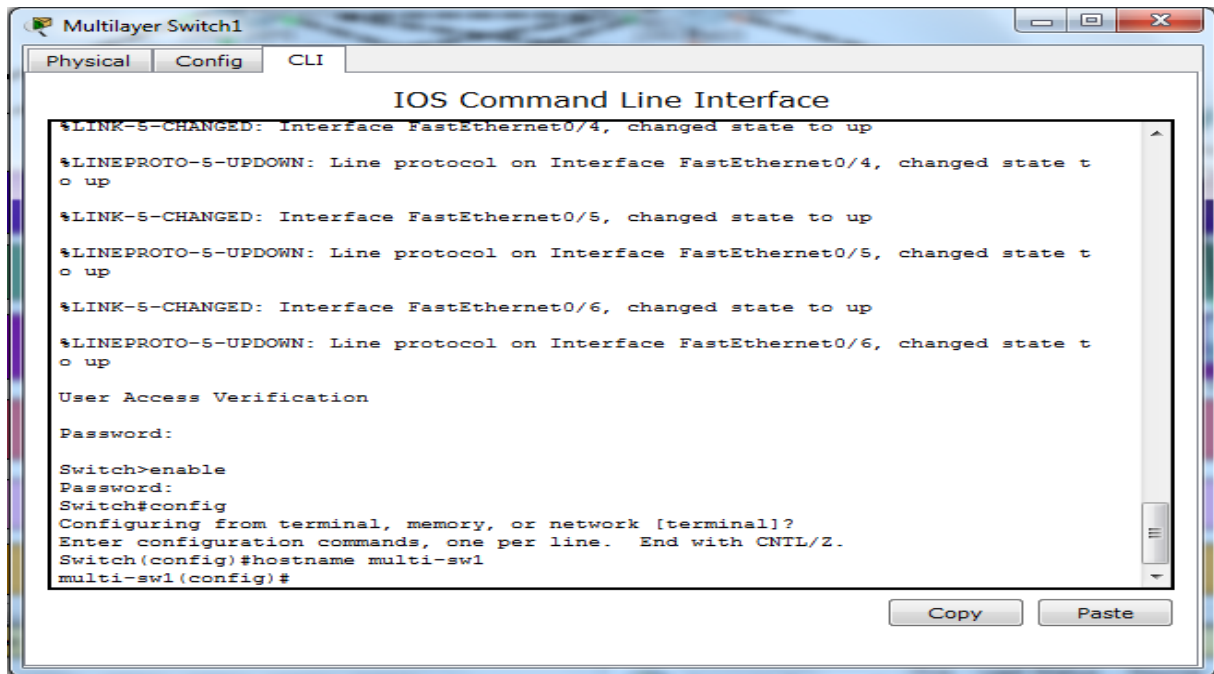


Figure 5 : Nomination du multilayer switch1

IV.3. Configuration du protocole VTP

L'ensemble des commutateurs cœur de LAN seront configurés comme des serveurs – VTP. Donc, ce sont eux qui gèrent l'administration de l'ensemble des VLANs. Un nom de domaine est attribué. La figure 6 représente la configuration du serveur VTP au niveau de Switch multifonction.

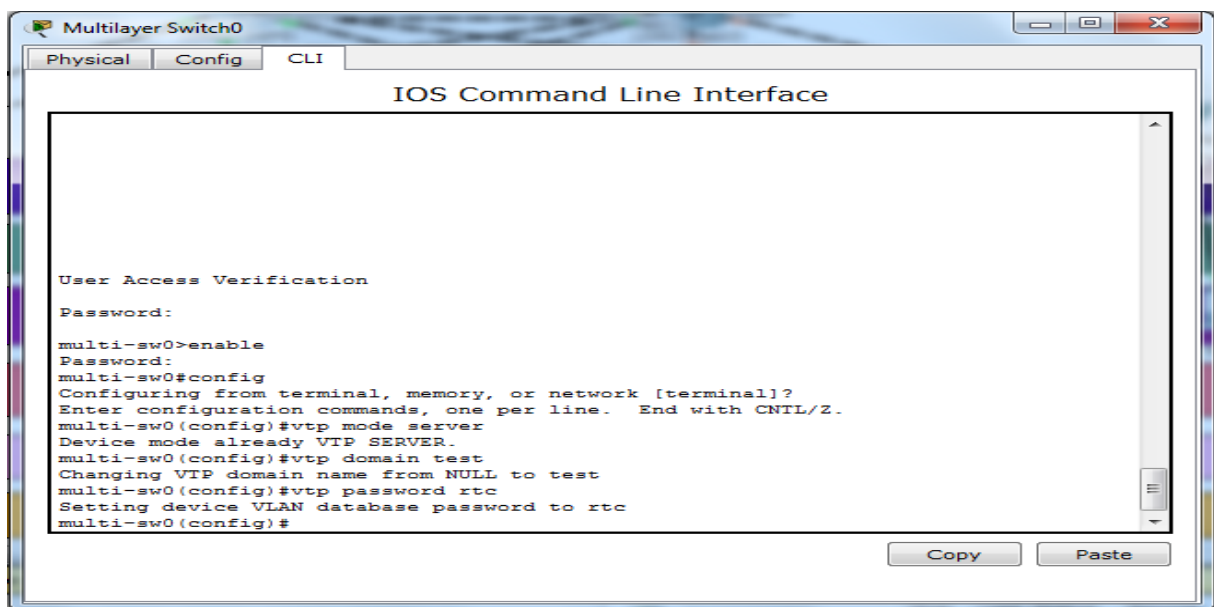
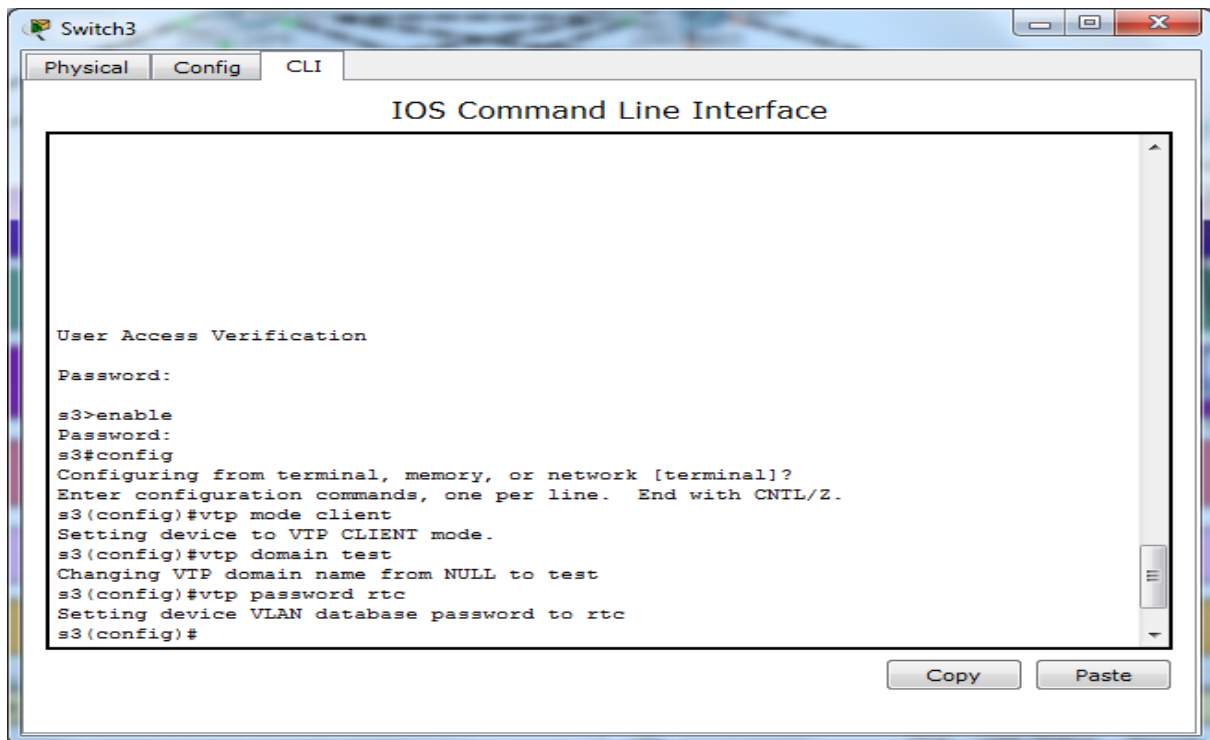


Figure 6 : Configuration des VTP-server

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



```
Switch3
Physical Config CLI
IOS Command Line Interface

User Access Verification
Password:
s3>enable
Password:
s3#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
s3(config)#vtp mode client
Setting device to VTP CLIENT mode.
s3(config)#vtp domain test
Changing VTP domain name from NULL to test
s3(config)#vtp password rtc
Setting device VLAN database password to rtc
s3(config)#
```

Figure 7 : Configuration client-VTP

IV.4. Création des VLANs

La création des VLANs est faite au niveau des commutateurs multifonction (server VTP) comme le montre la figure 8 :

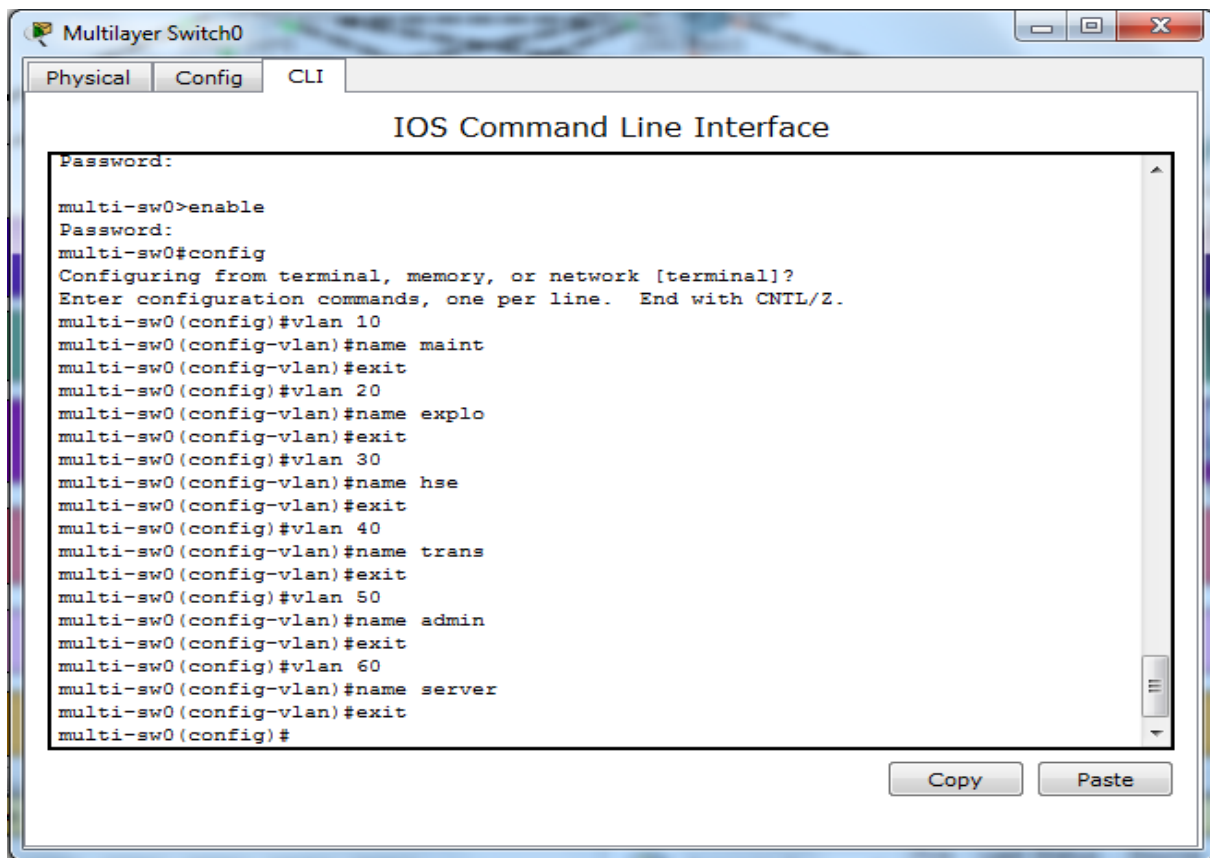
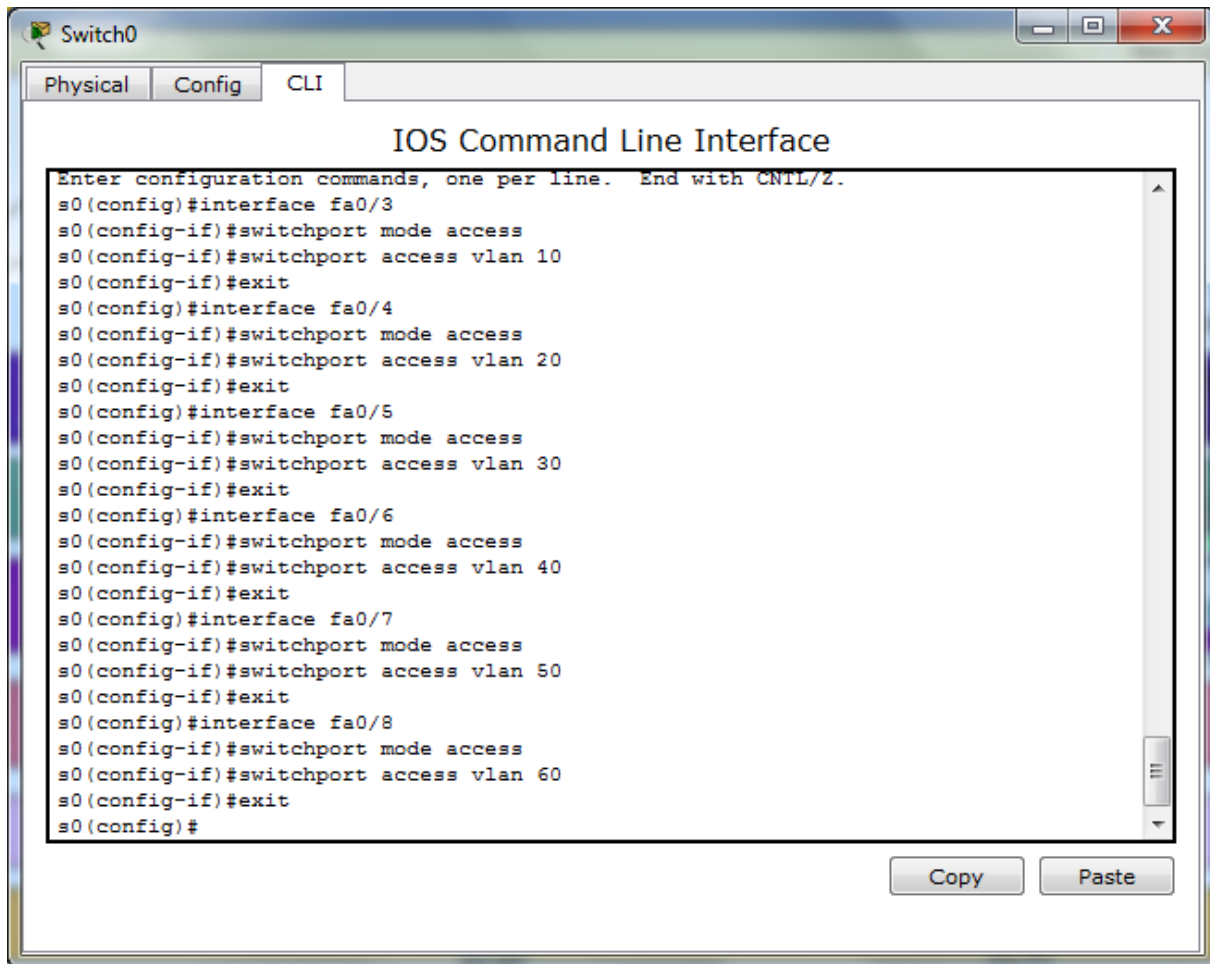


Figure 8 : Création des VLANs sur le serveur VTP

IV.5. Attribution des ports des commutateurs au 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 nous permettent d'associer un port à un VLAN en mode Accès.



```
Switch0
Physical Config CLI
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
s0(config)#interface fa0/3
s0(config-if)#switchport mode access
s0(config-if)#switchport access vlan 10
s0(config-if)#exit
s0(config)#interface fa0/4
s0(config-if)#switchport mode access
s0(config-if)#switchport access vlan 20
s0(config-if)#exit
s0(config)#interface fa0/5
s0(config-if)#switchport mode access
s0(config-if)#switchport access vlan 30
s0(config-if)#exit
s0(config)#interface fa0/6
s0(config-if)#switchport mode access
s0(config-if)#switchport access vlan 40
s0(config-if)#exit
s0(config)#interface fa0/7
s0(config-if)#switchport mode access
s0(config-if)#switchport access vlan 50
s0(config-if)#exit
s0(config)#interface fa0/8
s0(config-if)#switchport mode access
s0(config-if)#switchport access vlan 60
s0(config-if)#exit
s0(config)#
```

Figure 9 : Attribution des ports aux VLANs

IV.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 nous permettent d'associer un port à un vlan en mode trunk en s'aidant de la commande range qui pourra réunir toutes les interfaces en une seule fois.

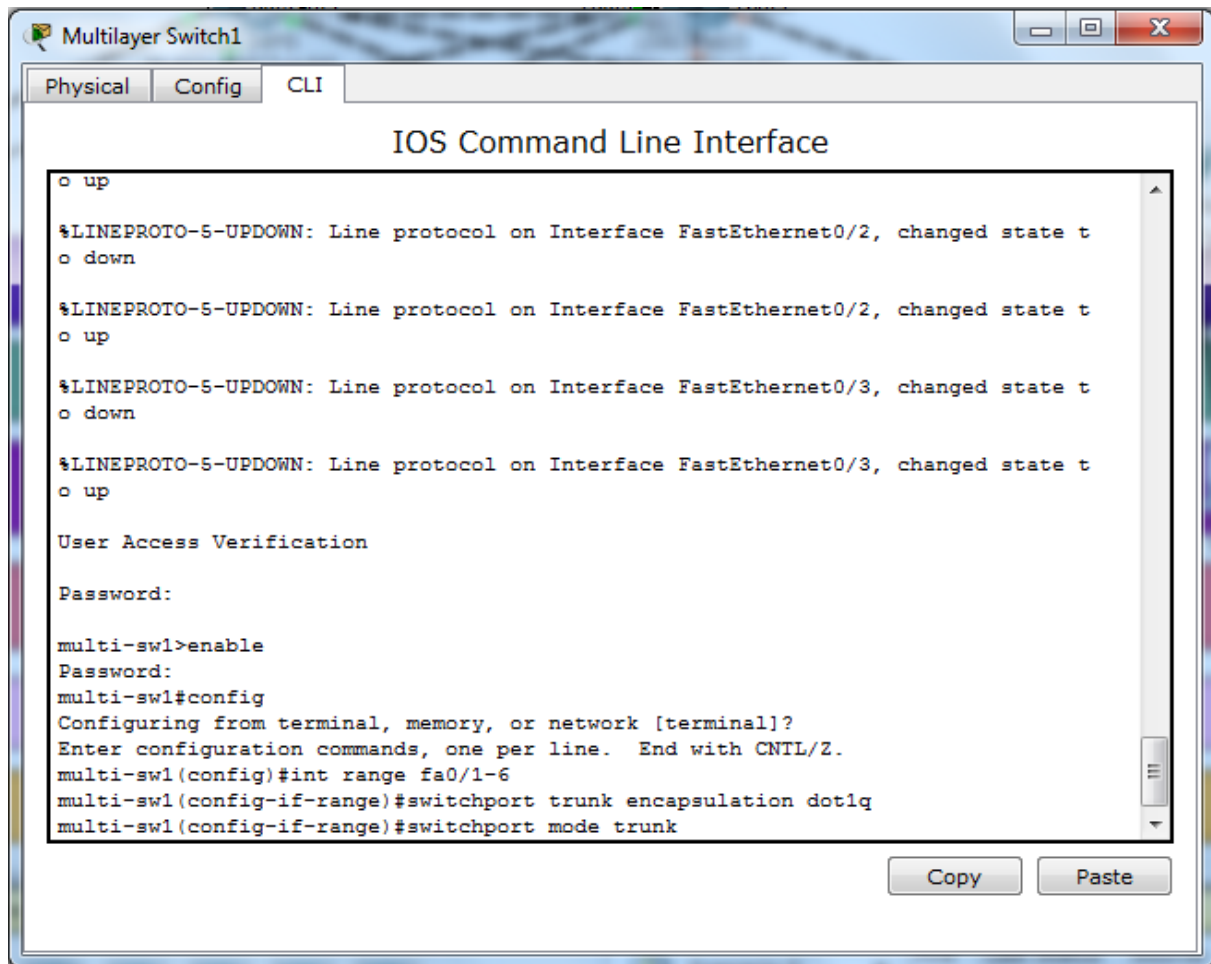


Figure 10 : Configuration des liens trunk

IV.7. Configuration des interfaces VLANs

La configuration des interfaces VLANs est faite au niveau du commutateur multifonction en donnant des adresses IP pour le VLAN.

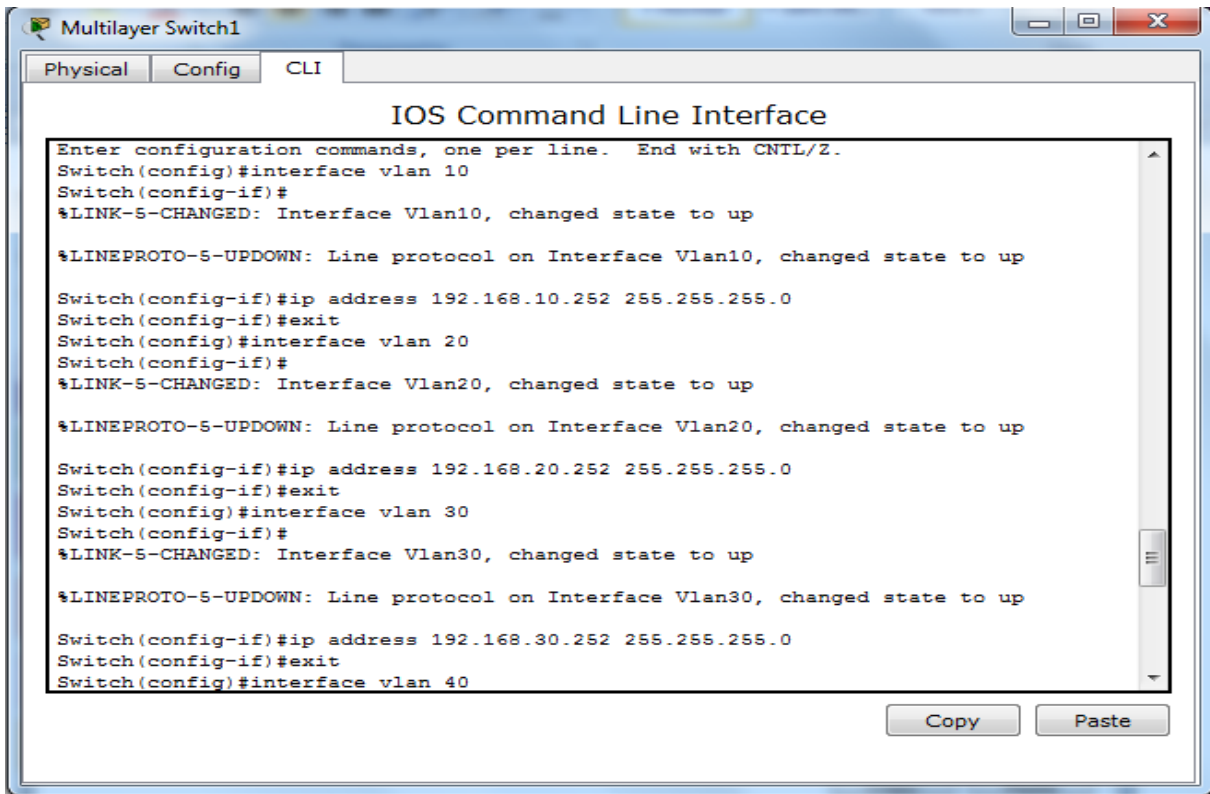


Figure 11 : Configuration des interfaces VLAN

Il faut ensuite activer la fonction de routage :

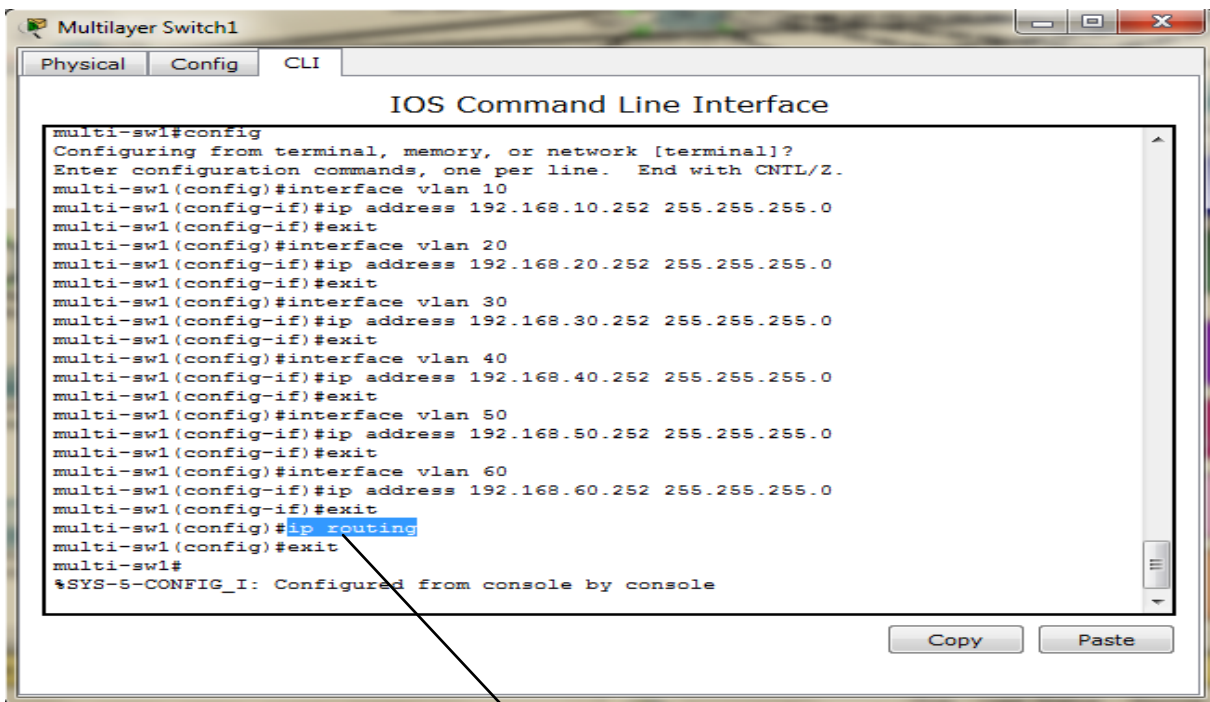
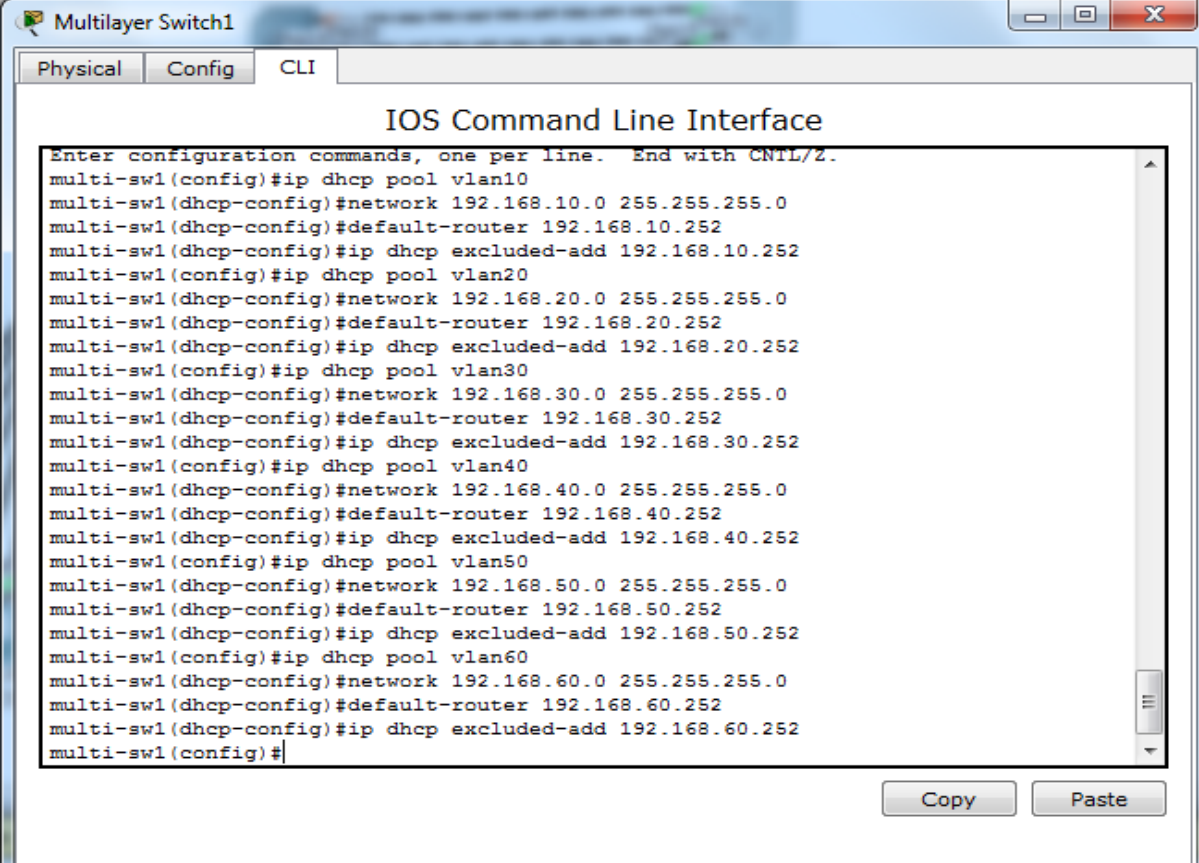


Figure 12 : Routage inter-vlan

IV.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 13 illustre les commandes qui nous permettent de configurer ce protocole :

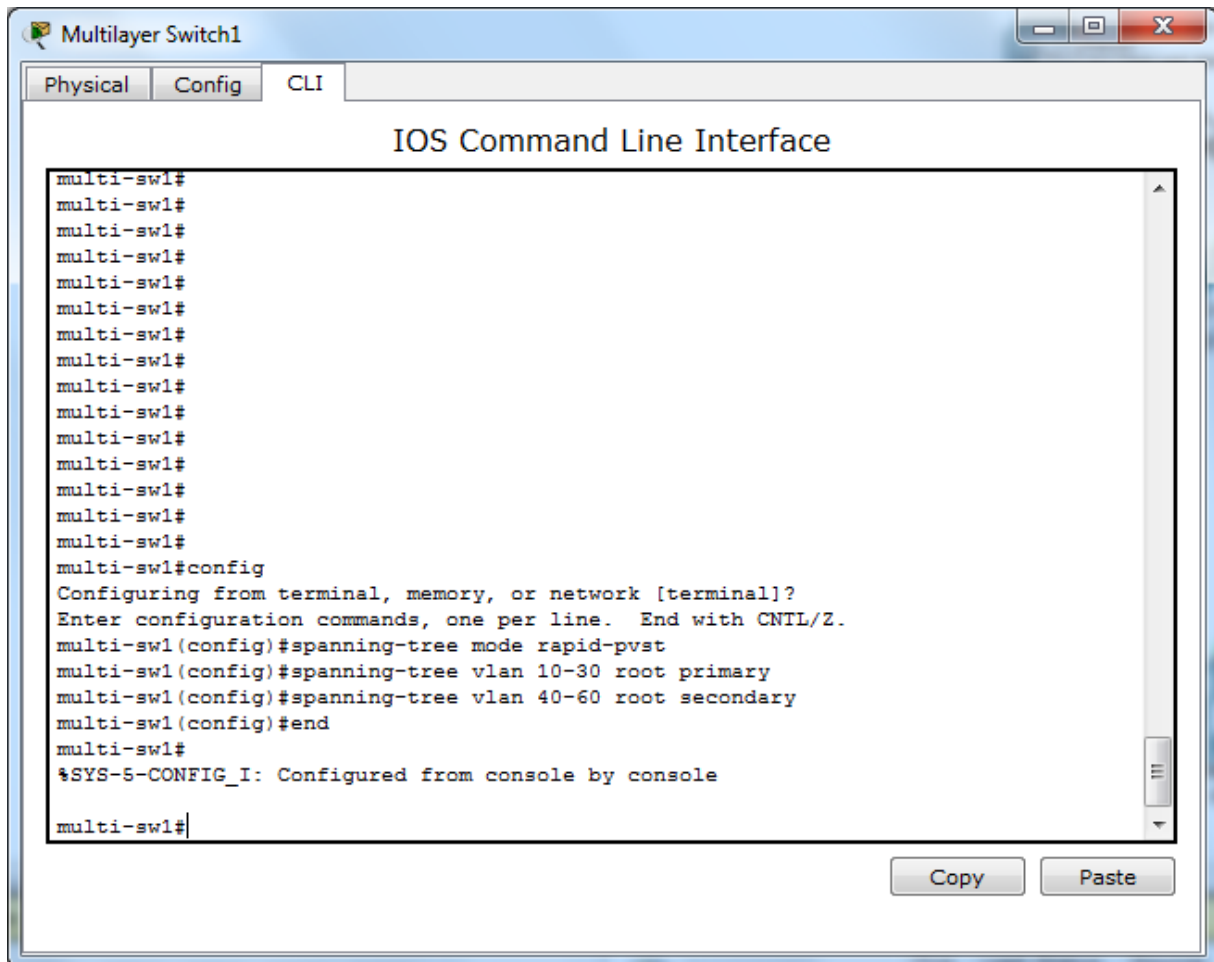


```
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
multi-sw1(config)#ip dhcp pool vlan10
multi-sw1(dhcp-config)#network 192.168.10.0 255.255.255.0
multi-sw1(dhcp-config)#default-router 192.168.10.252
multi-sw1(dhcp-config)#ip dhcp excluded-add 192.168.10.252
multi-sw1(config)#ip dhcp pool vlan20
multi-sw1(dhcp-config)#network 192.168.20.0 255.255.255.0
multi-sw1(dhcp-config)#default-router 192.168.20.252
multi-sw1(dhcp-config)#ip dhcp excluded-add 192.168.20.252
multi-sw1(config)#ip dhcp pool vlan30
multi-sw1(dhcp-config)#network 192.168.30.0 255.255.255.0
multi-sw1(dhcp-config)#default-router 192.168.30.252
multi-sw1(dhcp-config)#ip dhcp excluded-add 192.168.30.252
multi-sw1(config)#ip dhcp pool vlan40
multi-sw1(dhcp-config)#network 192.168.40.0 255.255.255.0
multi-sw1(dhcp-config)#default-router 192.168.40.252
multi-sw1(dhcp-config)#ip dhcp excluded-add 192.168.40.252
multi-sw1(config)#ip dhcp pool vlan50
multi-sw1(dhcp-config)#network 192.168.50.0 255.255.255.0
multi-sw1(dhcp-config)#default-router 192.168.50.252
multi-sw1(dhcp-config)#ip dhcp excluded-add 192.168.50.252
multi-sw1(config)#ip dhcp pool vlan60
multi-sw1(dhcp-config)#network 192.168.60.0 255.255.255.0
multi-sw1(dhcp-config)#default-router 192.168.60.252
multi-sw1(dhcp-config)#ip dhcp excluded-add 192.168.60.252
multi-sw1(config)#
```

Figure 13 : Configuration de DHCP

IV.9. Configuration de STP

La figure 14 illustre les commandes qui nous permettent de configurer le protocole STP, et d'affecter un root primaire ou secondaire à un VLAN.



The screenshot shows a window titled "Multilayer Switch1" with tabs for "Physical", "Config", and "CLI". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and responses:

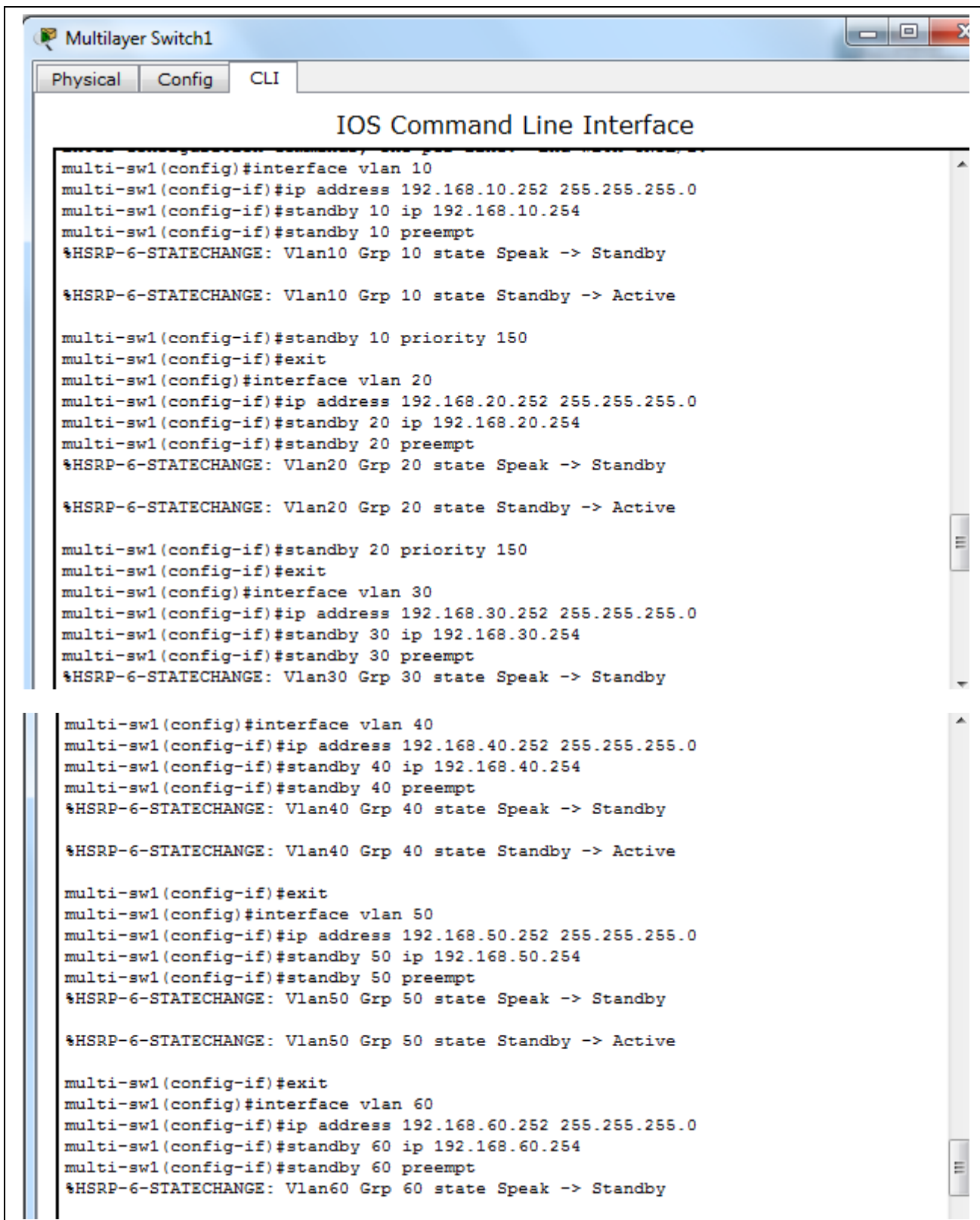
```
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#
multi-sw1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
multi-sw1(config)#spanning-tree mode rapid-pvst
multi-sw1(config)#spanning-tree vlan 10-30 root primary
multi-sw1(config)#spanning-tree vlan 40-60 root secondary
multi-sw1(config)#end
multi-sw1#
%SYS-5-CONFIG_I: Configured from console by console
multi-sw1#
```

At the bottom of the window, there are "Copy" and "Paste" buttons.

Figure 14 : Configuration de STP

IV.10. Configuration de la haute disponibilité HSRP

La configuration de la haute disponibilité s'effectue au niveau des Switchs multifonction. 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 Switchs multifonction, et sur l'autre les priorités des VLANs seront renversées.



```
Multilayer Switch1
Physical Config CLI
IOS Command Line Interface

multi-sw1(config)#interface vlan 10
multi-sw1(config-if)#ip address 192.168.10.252 255.255.255.0
multi-sw1(config-if)#standby 10 ip 192.168.10.254
multi-sw1(config-if)#standby 10 preempt
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active

multi-sw1(config-if)#standby 10 priority 150
multi-sw1(config-if)#exit
multi-sw1(config)#interface vlan 20
multi-sw1(config-if)#ip address 192.168.20.252 255.255.255.0
multi-sw1(config-if)#standby 20 ip 192.168.20.254
multi-sw1(config-if)#standby 20 preempt
%HSRP-6-STATECHANGE: Vlan20 Grp 20 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan20 Grp 20 state Standby -> Active

multi-sw1(config-if)#standby 20 priority 150
multi-sw1(config-if)#exit
multi-sw1(config)#interface vlan 30
multi-sw1(config-if)#ip address 192.168.30.252 255.255.255.0
multi-sw1(config-if)#standby 30 ip 192.168.30.254
multi-sw1(config-if)#standby 30 preempt
%HSRP-6-STATECHANGE: Vlan30 Grp 30 state Speak -> Standby

multi-sw1(config)#interface vlan 40
multi-sw1(config-if)#ip address 192.168.40.252 255.255.255.0
multi-sw1(config-if)#standby 40 ip 192.168.40.254
multi-sw1(config-if)#standby 40 preempt
%HSRP-6-STATECHANGE: Vlan40 Grp 40 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan40 Grp 40 state Standby -> Active

multi-sw1(config-if)#exit
multi-sw1(config)#interface vlan 50
multi-sw1(config-if)#ip address 192.168.50.252 255.255.255.0
multi-sw1(config-if)#standby 50 ip 192.168.50.254
multi-sw1(config-if)#standby 50 preempt
%HSRP-6-STATECHANGE: Vlan50 Grp 50 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan50 Grp 50 state Standby -> Active

multi-sw1(config-if)#exit
multi-sw1(config)#interface vlan 60
multi-sw1(config-if)#ip address 192.168.60.252 255.255.255.0
multi-sw1(config-if)#standby 60 ip 192.168.60.254
multi-sw1(config-if)#standby 60 preempt
%HSRP-6-STATECHANGE: Vlan60 Grp 60 state Speak -> Standby
```

Figure 15 : Configuration de HSRP

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

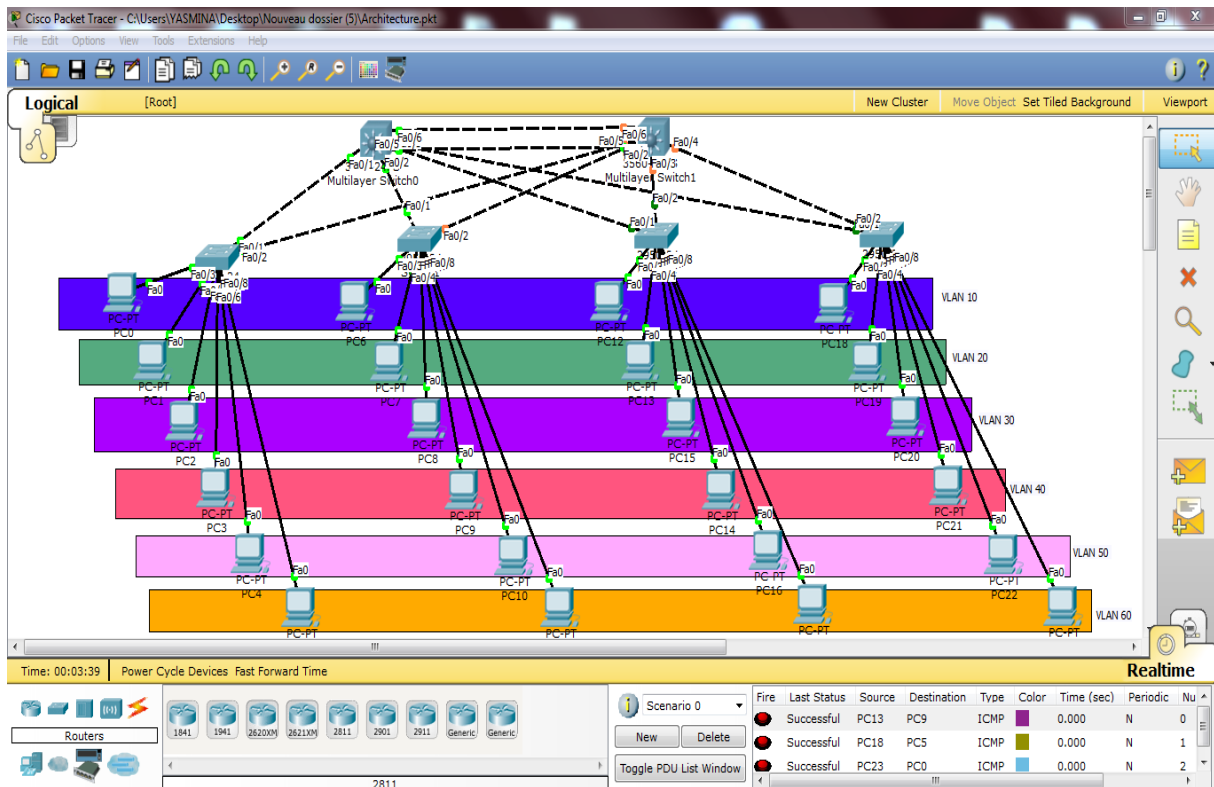


Figure 16 : Réseau local après la configuration

V. EIGRP (Enhanced Interior Gateway Routing Protocol) [w8]

EIGRP est un protocole de routage propriété de cisco qui l’a développé afin de pallier les manques d’IGRP.

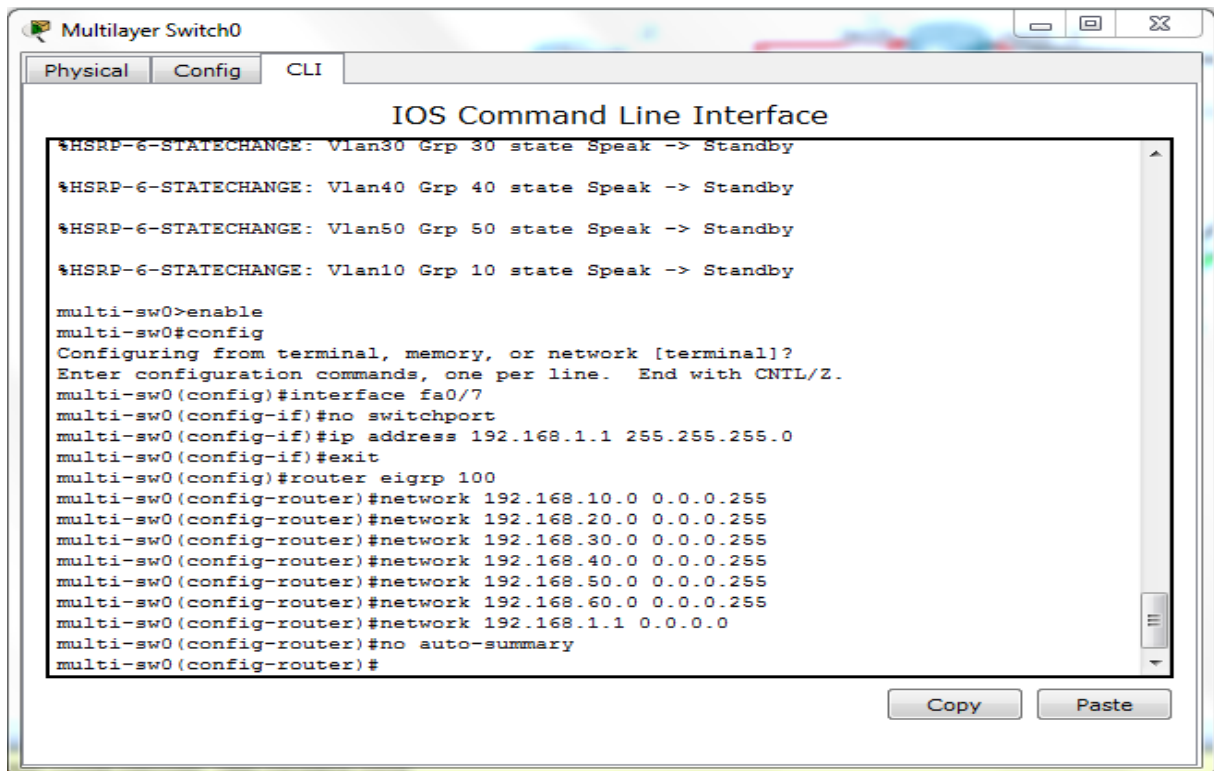
EIGRP est un protocole de routage à vecteur de distance avancé qui joue le rôle d’un protocole à état de liens lors de la mise à jour des voisins et de la gestion des informations de routage. Par rapport aux protocoles à vecteur de distance simples, EIGRP offre notamment les avantages suivants :

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

V.1. Configuration du protocole EIGRP

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

- Au niveau du Switch multifonction multi-sw0



```
Multilayer Switch0
Physical Config CLI
IOS Command Line Interface
%HSRP-6-STATECHANGE: Vlan30 Grp 30 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan40 Grp 40 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan50 Grp 50 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
multi-sw0>enable
multi-sw0#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
multi-sw0(config)#interface fa0/7
multi-sw0(config-if)#no switchport
multi-sw0(config-if)#ip address 192.168.1.1 255.255.255.0
multi-sw0(config-if)#exit
multi-sw0(config)#router eigrp 100
multi-sw0(config-router)#network 192.168.10.0 0.0.0.255
multi-sw0(config-router)#network 192.168.20.0 0.0.0.255
multi-sw0(config-router)#network 192.168.30.0 0.0.0.255
multi-sw0(config-router)#network 192.168.40.0 0.0.0.255
multi-sw0(config-router)#network 192.168.50.0 0.0.0.255
multi-sw0(config-router)#network 192.168.60.0 0.0.0.255
multi-sw0(config-router)#network 192.168.1.1 0.0.0.0
multi-sw0(config-router)#no auto-summary
multi-sw0(config-router)#
```

Figure 17 : Routage au niveau de Switch multi_sw0

- Au niveau du routeur

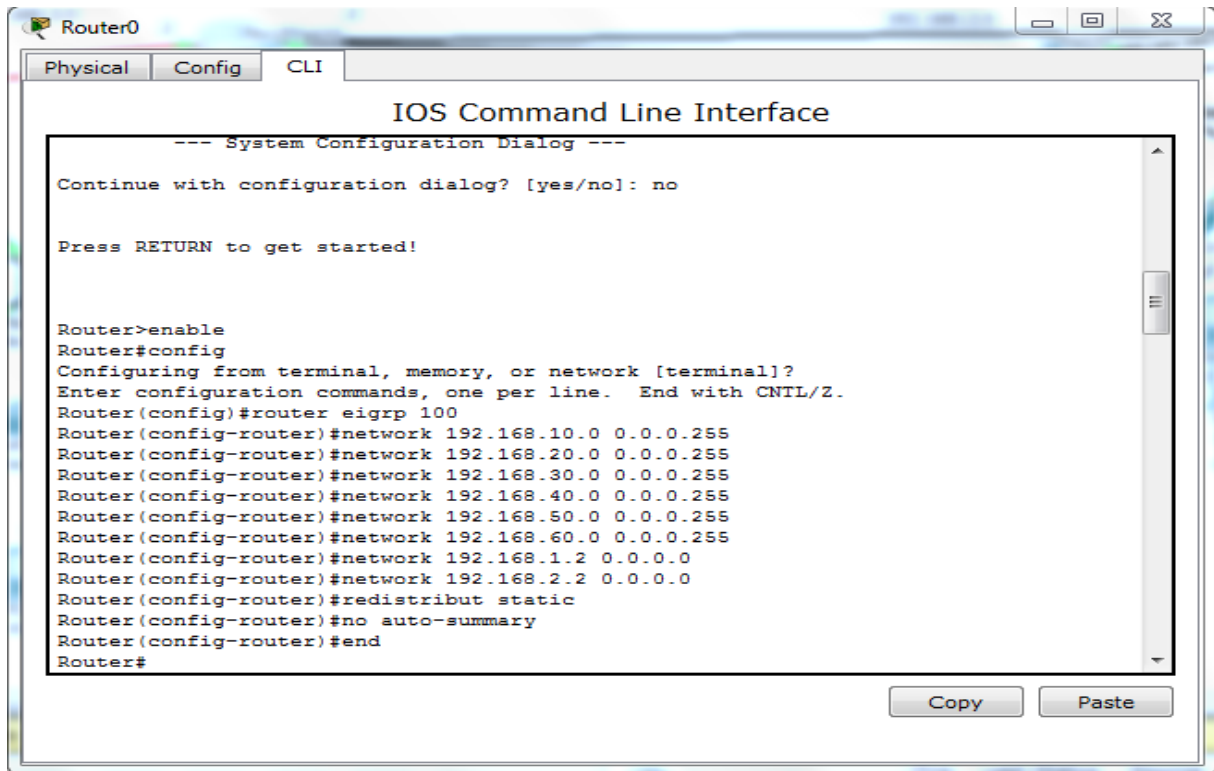


Figure 18 : Routage au niveau du routeur

La figure 19 montre la connexion du réseau que nous avons réalisé avec le réseau d'une autre station à l'aide du protocole de routage EIGRP.

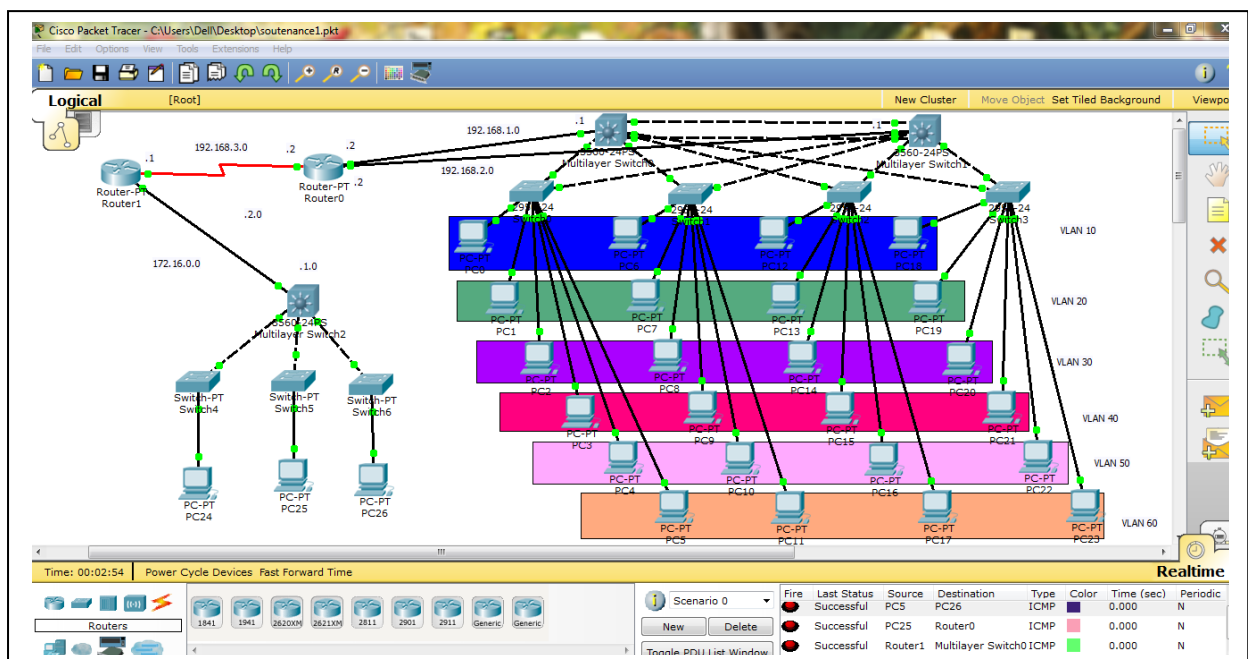


Figure 19 : Interconnexion de différents réseaux locaux

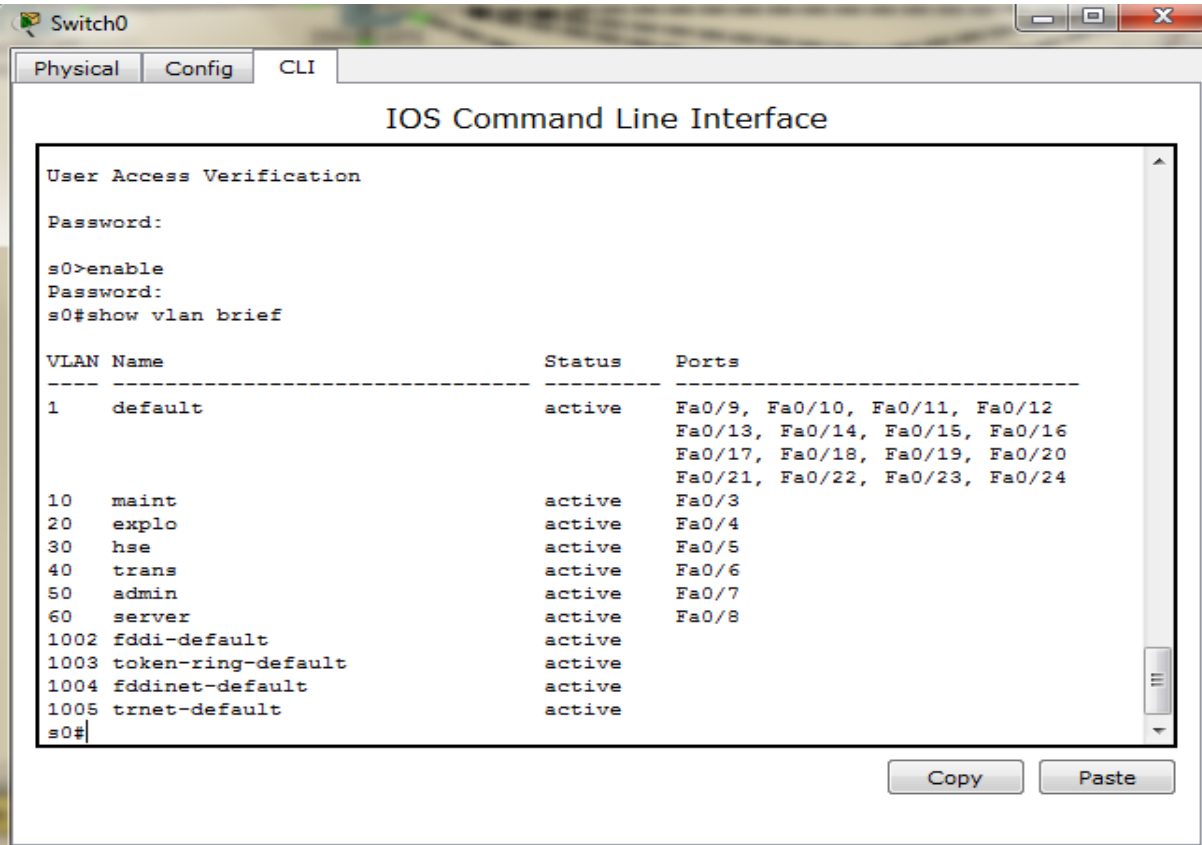
VI. Vérifications et tests de validation

VI.1. Vérifications

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

VI.1.1. Contrôle des réseaux locaux virtuels créés sur le Switch server s'ils sont distribués sur les Switchs client

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.



```
Switch0
Physical Config CLI
IOS Command Line Interface
User Access Verification
Password:
s0>enable
Password:
s0#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
10   maint                   active    Fa0/3
20   explo                   active    Fa0/4
30   hse                     active    Fa0/5
40   trans                   active    Fa0/6
50   admin                   active    Fa0/7
60   server                   active    Fa0/8
1002 fddi-default            active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active
s0#
```

Figure 20: VLANs distribués dans le Switch client s0

VI.1.2. Vérification du routage inter VLAN

A l'aide de la commande **show IP interface brief**, on peut avoir les Switchs Virtuelle Interface (SVI) comme ceci :

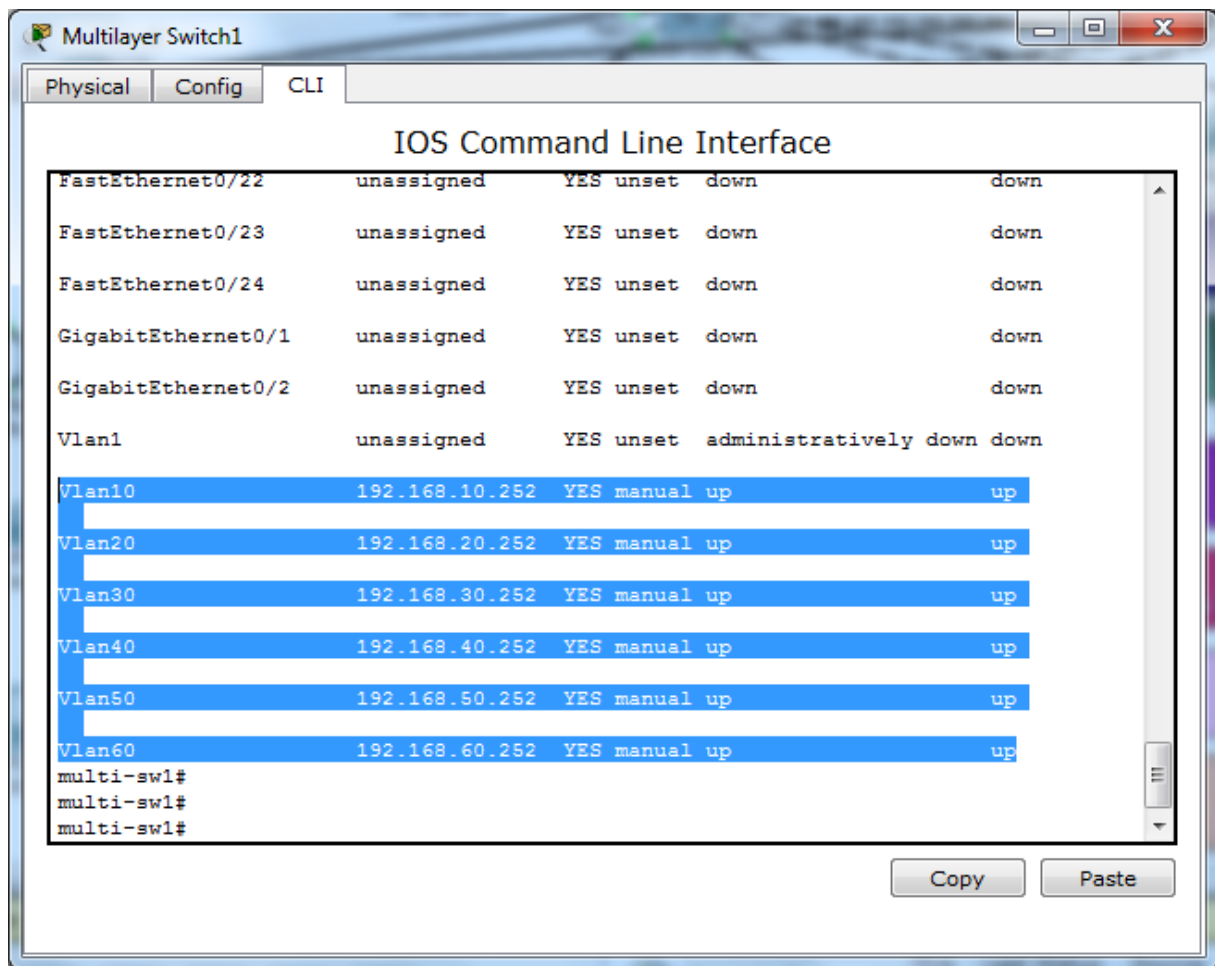
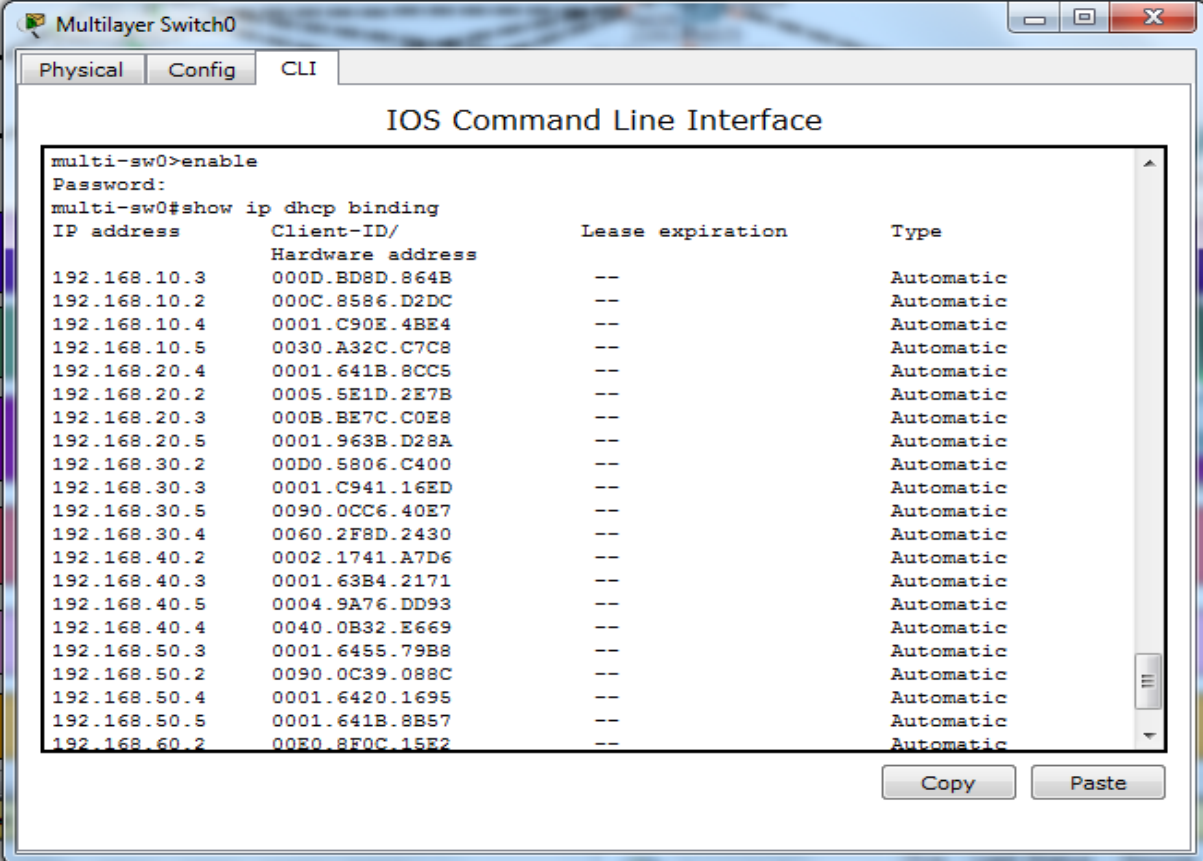


Figure 21 : SVI (Switch Virtuelle Interface)

VI.1.3. 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` :



The screenshot shows a terminal window titled "Multilayer Switch0" with tabs for "Physical", "Config", and "CLI". The main content is the "IOS Command Line Interface" where the following commands and output are displayed:

```
multi-sw0>enable
Password:
multi-sw0#show ip dhcp binding
```

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.10.3	000D.BD8D.864B	--	Automatic
192.168.10.2	000C.8586.D2DC	--	Automatic
192.168.10.4	0001.C90E.4BE4	--	Automatic
192.168.10.5	0030.A32C.C7C8	--	Automatic
192.168.20.4	0001.641B.8CC5	--	Automatic
192.168.20.2	0005.5E1D.2E7B	--	Automatic
192.168.20.3	000B.BE7C.C0E8	--	Automatic
192.168.20.5	0001.963B.D28A	--	Automatic
192.168.30.2	00D0.5806.C400	--	Automatic
192.168.30.3	0001.C941.16ED	--	Automatic
192.168.30.5	0090.0CC6.40E7	--	Automatic
192.168.30.4	0060.2F8D.2430	--	Automatic
192.168.40.2	0002.1741.A7D6	--	Automatic
192.168.40.3	0001.63B4.2171	--	Automatic
192.168.40.5	0004.9A76.DD93	--	Automatic
192.168.40.4	0040.0B32.E669	--	Automatic
192.168.50.3	0001.6455.79B8	--	Automatic
192.168.50.2	0090.0C39.088C	--	Automatic
192.168.50.4	0001.6420.1695	--	Automatic
192.168.50.5	0001.641B.8B57	--	Automatic
192.168.60.2	00E0.8F0C.15E2	--	Automatic

At the bottom of the terminal window, there are "Copy" and "Paste" buttons.

Figure 22 : Attribution des adresses IP

VI.1.4.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.

multi-sw0# show standby brief

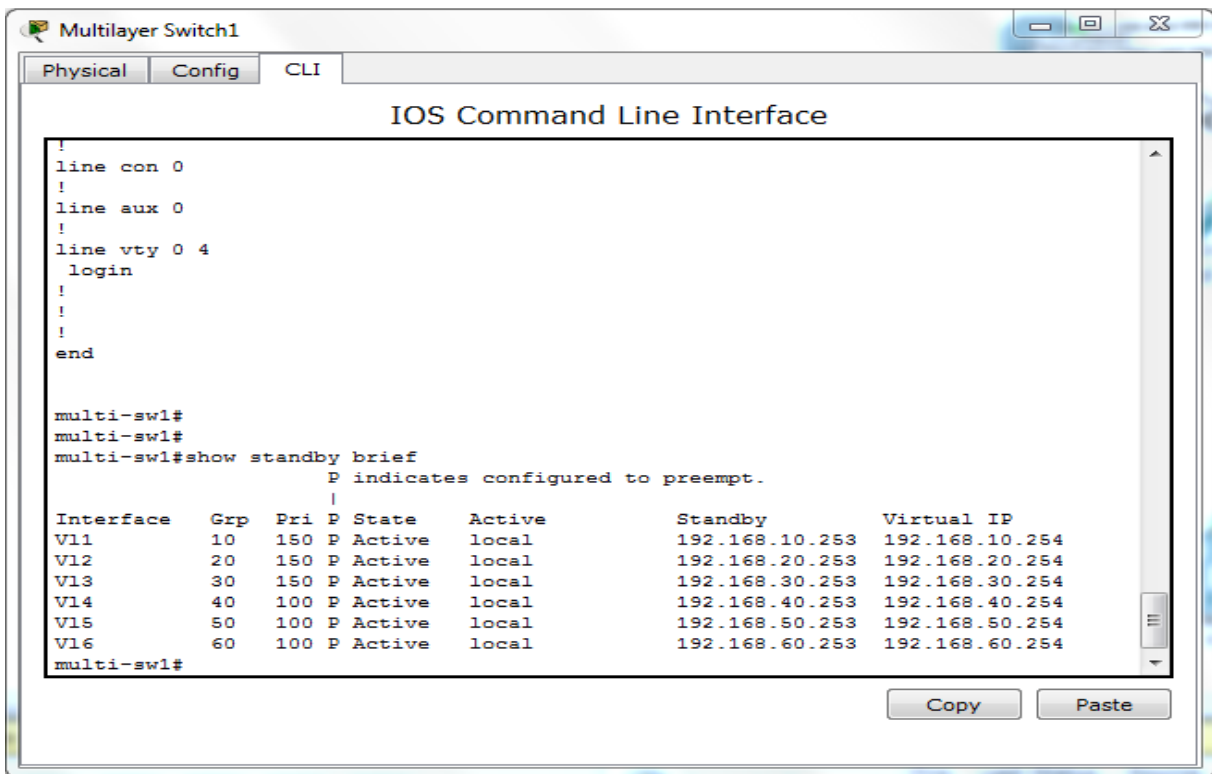


Figure 23: Switch multi-sw0 en mode active

multi-sw1# show standby brief

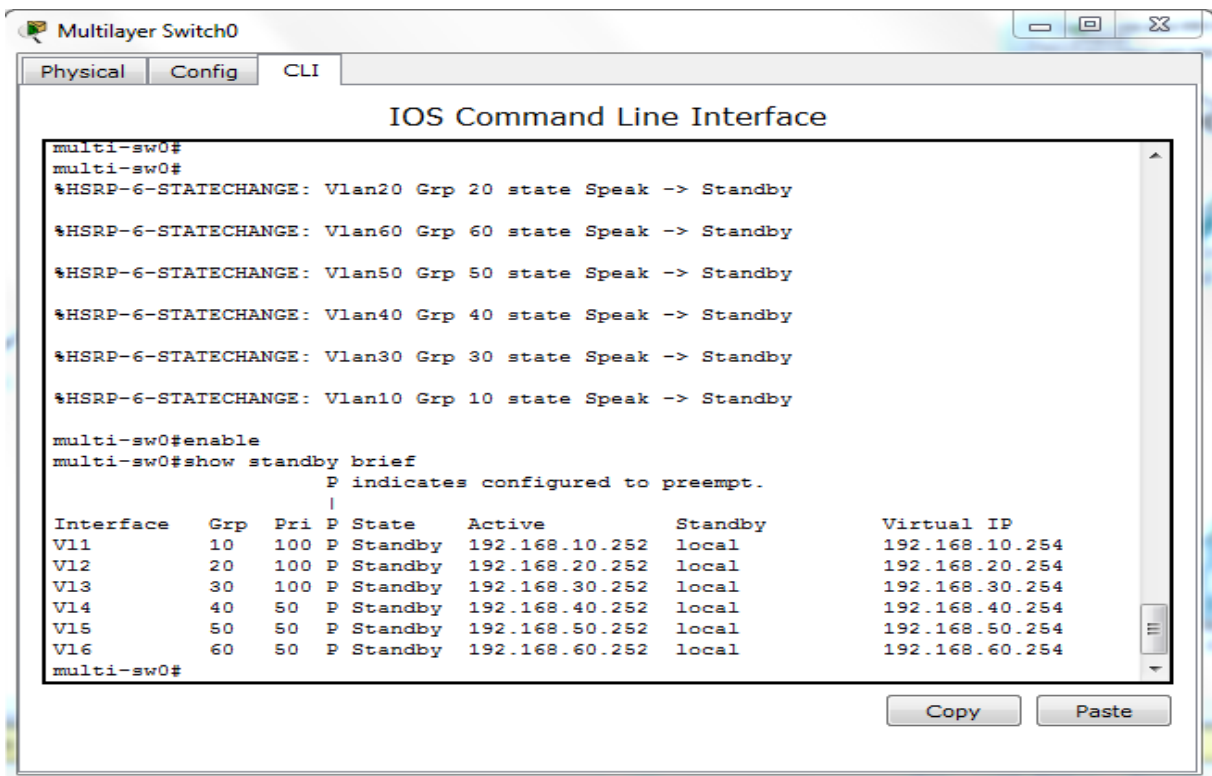


Figure 24 : Switch multi-sw1 en mode standby

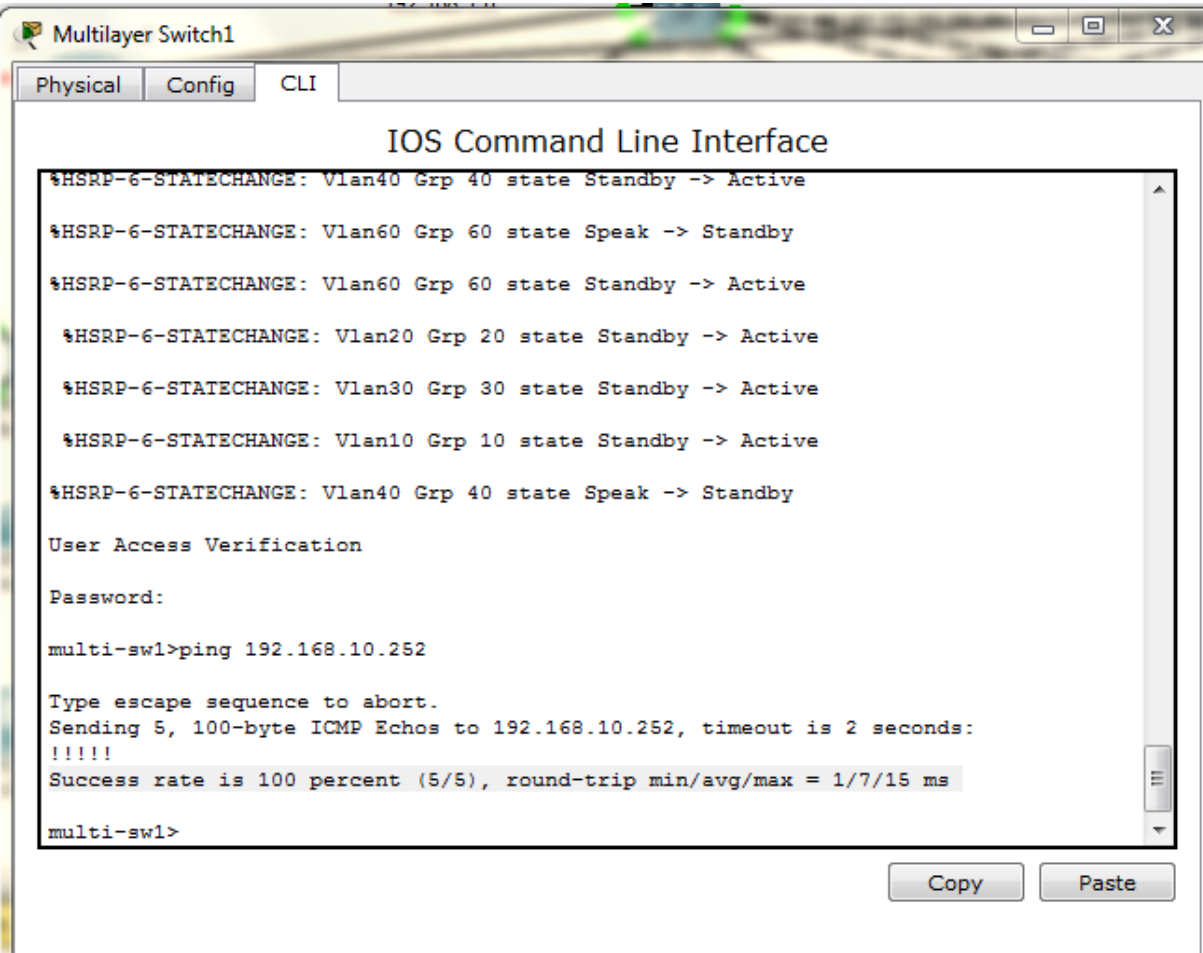
VI .2. Tests de validation

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

VI .2.1. 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 Switch multifonction (multi-sw1) et le Switch d'accès



```
Multilayer Switch1
Physical Config CLI
IOS Command Line Interface
%HSRP-6-STATECHANGE: Vlan40 Grp 40 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan60 Grp 60 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan60 Grp 60 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan20 Grp 20 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan30 Grp 30 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan40 Grp 40 state Speak -> Standby
User Access Verification
Password:
multi-sw1>ping 192.168.10.252
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.252, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/15 ms
multi-sw1>
```

Figure 25 : Test entre le Switch multifonction (multi-sw1) et le Switch d'accès

VI .2.2.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 pc 6. (192.168.10.3) en essayant d'accéder au pc 10 (192.168.50.5).

La figure 26 illustre le succès du test effectué entre les différents VLANs sur un même commutateur.

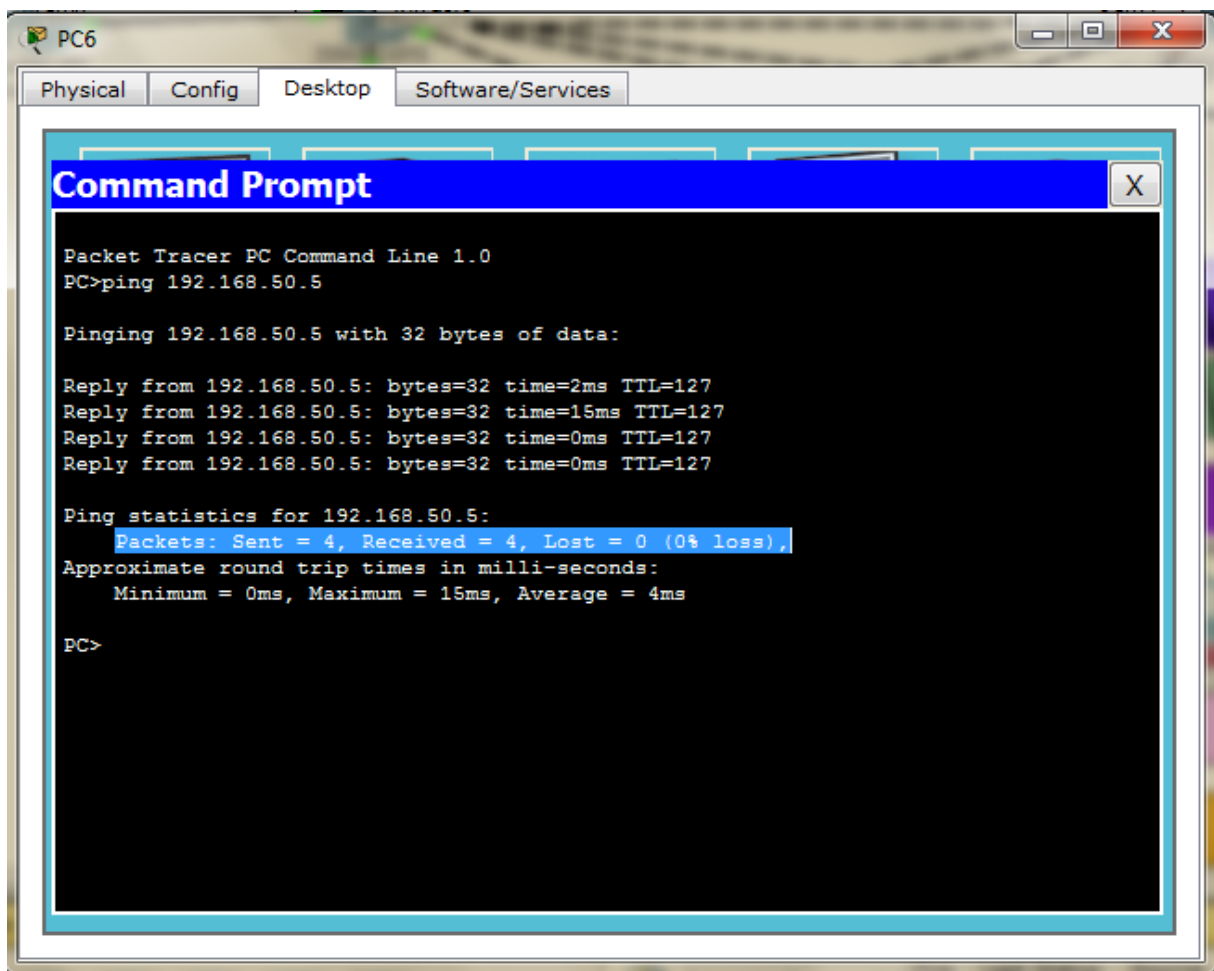


Figure 26 : Test entre machines des VLANs différents

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

On peut aussi vérifier l'accessibilité des équipements du même VLAN situé dans un réseau local commun. Depuis le PC 1(192.168.20.3), essayons d'accéder au PC 21 (192.168.40.4), les deux se trouvant dans des VLANs et des commutateurs accés différents.

La figure suivante illustre le succès du test effectué entre différents PC et commutateurs

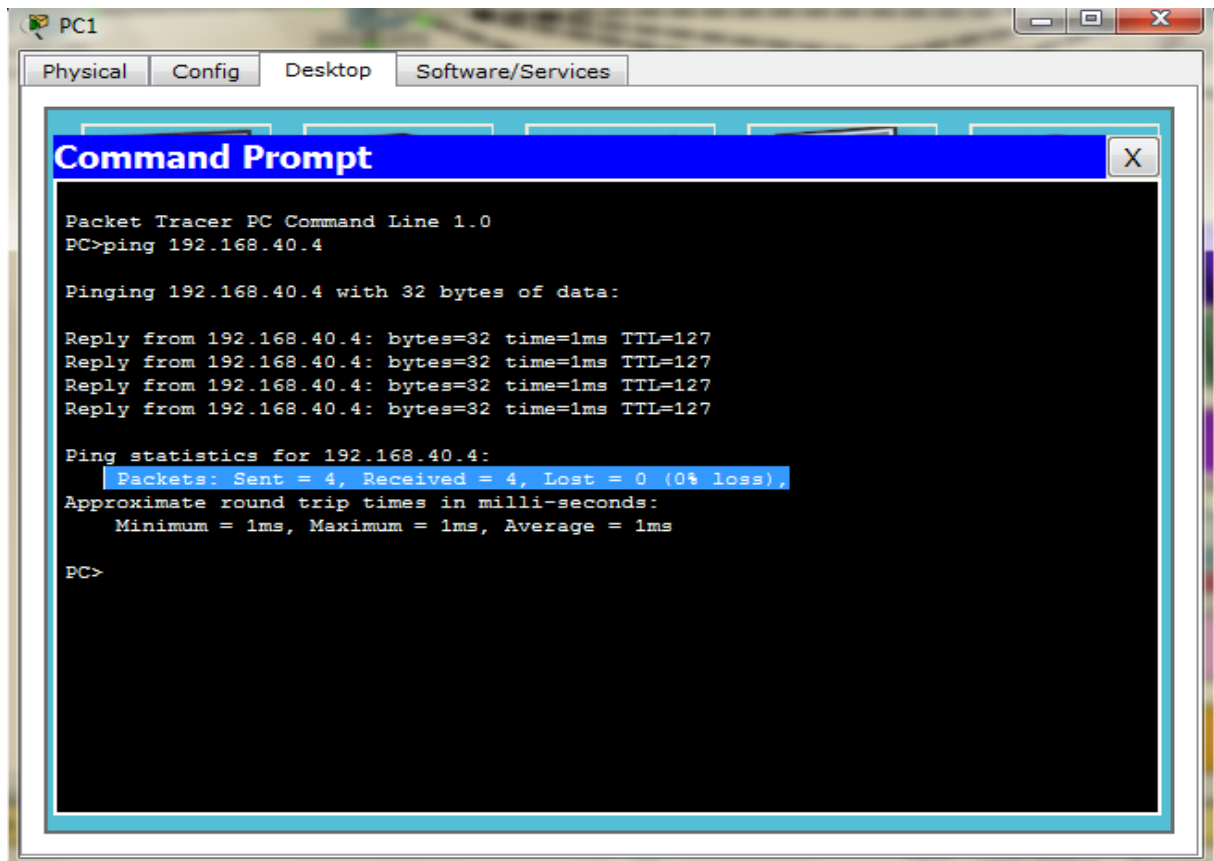


Figure 27 : Test entre des machines des VLANs et commutateurs différents

VI .2.3. Vérification des adresses IP des PCs attribuées par le DHCP

La figure 28 montre l'attribution des adresses IP par le DHCP

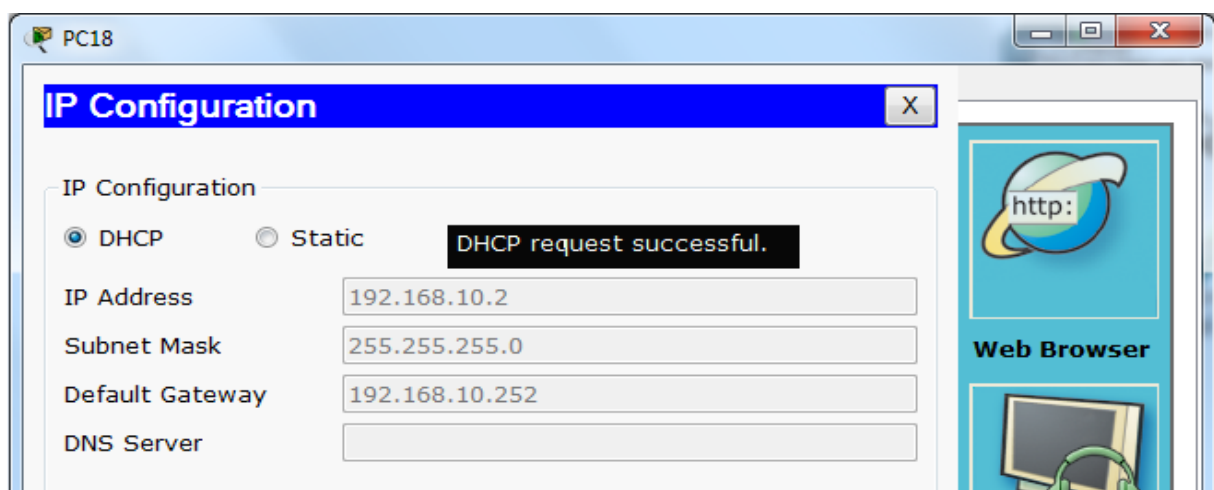
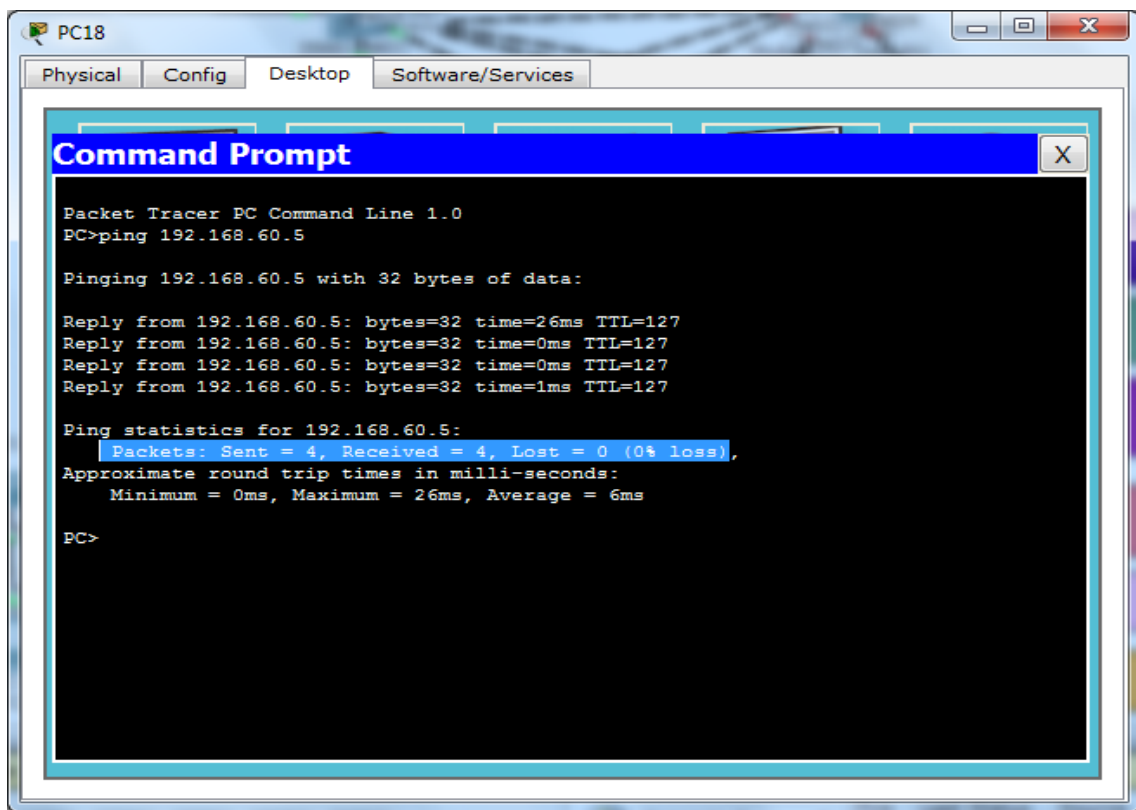


Figure 28 : Attribution des adresses IP par le DHCP

VI .2.4. Vérification de la haute disponibilité

Dans ce cas de figure, on teste la connectivité entre les PC et les commutateurs distincts lorsque l'un des Switchs cœur est défectueux (par exemple le Switch multi-sw1 est défectueux). A partir du PC 18 (192.168.10.3) appartenant au VLAN 10, essayons d'accéder au PC 11 (192.168.60.5) qui appartient au VLAN 60.

La figure 29 montre le succès du test effectué entre deux PC des VLANs distincts lorsque le Switch cœur (multi-sw1) est en panne.



```
PC18
Physical Config Desktop Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.60.5

Pinging 192.168.60.5 with 32 bytes of data:

Reply from 192.168.60.5: bytes=32 time=26ms TTL=127
Reply from 192.168.60.5: bytes=32 time=0ms TTL=127
Reply from 192.168.60.5: bytes=32 time=0ms TTL=127
Reply from 192.168.60.5: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.60.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 26ms, Average = 6ms

PC>
```

Figure 29 : Test entre les machines des différents VLANs lorsque le switch cœur (multi-sw1) est défectueux

Conclusion

Après avoir présenté une brève description de l'environnement de développement de réseau local, nous avons mis l'accent sur la présentation de quelques interfaces qui portent sur l'ensemble des configurations, la mise en place du réseau LAN que nous avons réalisé et sur l'interconnexion des deux réseaux locaux avec le routage EIGRP. Nous avons ensuite effectué un ensemble de tests de validation afin de prouver l'efficacité du réseau.

Conclusion générale

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

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

Le travail que nous avons accompli a pour principal objectif la mise en œuvre d'un réseau local. Ce projet nous a permis de mettre en pratique les connaissances acquises durant la période de notre stage pratique au sein de la SONATRACH de Béjaïa (RTC), de nous familiariser avec un environnement dynamique et d'avoir une idée plus profonde et plus pratique sur l'importance du réseau dans une entreprise.

La réalisation de ce projet a été bénéfique pour nous dans le sens où il nous a permis d'approfondir et d'acquérir de nouvelles connaissances qui seront utiles pour nous à l'avenir.

Liste des acronymes

- A** **ARP:** Address Resolution Protocol
- B** **BID:** Bridge- Identifying
BPDU: Bridge Protocol Data Unit
- C** **CISCO:** Computer Information System Company
C F P A: Compagnie Française des Pétroles Algérie
CLI: Commande Langage Interface
- D** **DEC:** Digital Equipment Corporation
DHCP : Dynamic Host Configuration Protocol
DRGB : Direction Régionale de Transport de Bejaïa
- E** **EIGRP:** Enhanced Interior Gateway Routing Protocol
- F** **FDDI:** Fibre Distributed Data Interconnect
- H** **HSRP:** Hot Standby Routing Protocol
HSE: Hygiène Sécurité et Environnement
- I** **IEEE:** Institute of Electrical and Electronics Engineer
IOS: International Standardization Organization
IP: Internet Protocol
- L** **LAN:** Local Area Network
- M** **MAC:** Medium Access Control
- N** **NVRAM:** Non-Volatile Random-Access Memory
- O** **OSI:** Open Systems Interconnection
- P** **PING:** Packet Internet Grouper
- Q** **QoS:** Quality of Service
- R** **RTC:** Région Transport Centre

- S** **SGBD** : Système de Gestion de Base de Données
- S N R E P A L** : Société Nationale de Recherche et Exploitation des Pétroles en Algérie
- SONATRACH** : Société Nationale de Transport et Commercialisation des Hydrocarbures
- SOPEG** : Société Pétrolière de Gérance
- STA**: Spanning-Tree Algorithme
- STP**: Spanning Tree Protocol
- SVI**: Switch Virtuelle Interface
- T** **TCP**: Transmission Control Protocol
- TRC**: Transport par Canalisation
- U** **UDP**: User Datagram Protocol
- V** **VLAN**: Virtual Local Area Network
- VTP**: VLAN Trunking Protocol

Références bibliographiques

[1] : Lahdir M. et Mezari R. « mise en oeuvre des réseaux locaux sous linux et windows » livre page bleues, algérie ,2006.

[2] : Atelin Ph. « Réseaux informatique-notion fondamentales », livre, Eni édition, 2009.

[3] : GRELIER F. « les principales commandes de commutation » Edition eni, Dépliant Cisco Certification CCNA, 2013 IN [www. Edition-eni.fr](http://www.edition-eni.fr)

[4] : HAGGAR S. « Conception de réseaux de campus », cours M2 Pro STIC-Info université Reims Champagne-Ardenne, 2009.

[5] : KOUASSI T. ingénieur en conception informatique, Centre d'expertise et de perfectionnement en informatique « Etude et optimisation du réseau local »,2007

[6] : « Meilleure pratique en matière de vlan », livre blanc, IN www.flukenetworks.com, fluKe corporation, 2004.

[7] : Djama K. « réalisation d'un réseau campus commuté », mémoire de fin de cycle master 2, université Abderrahmane mira 'Targa ouzamour, promotion 2013-2014.

[8] : « Rôle d'un service DHCP », Eléments de cours sur le service DHCP, Chapitre 27, IN <http://www.linux-france.org/prj/edu/archinet/systeme/ch27s02.html>

Webographie

[W1] : http://jetel.free.fr/inf_rsx.htm, 10 mai 2015

[W2] : <http://searchsdn.techtarget.com/définition/campus-network>, 14 juin 2015.

[W3]: http://www.testeur-wifi.com/le_commuteur_reseau.html, avril 2015.

[W4] : <http://www.reseaucerta.org> Roger SANCHEZ © CERTA - janvier 2006 – v1.0, avril 2015.

[W5] : [http://Qu'estce%20que%20le%20VLAN%20Trunking%20Protocol%20 \(VTP\).htm](http://Qu'estce%20que%20le%20VLAN%20Trunking%20Protocol%20(VTP).htm), mai 2015.

[W6] :portail.jacquenod.net/Web/Commutateur/DPDF/CI-commutateurpdf.pdf, 28 avril 2015.

[W7]:<http://wapiti.telecomlille1.eu/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2006-ttnfa2007/DiStefano-Wong/Protocole%20HSRP.html>, 16 mai 2015.

[W8] : git.meleeweb.net/school/ETNA.git/plain/2eme.../cours/Cours%205a.pdf, 8 juin 2015.

A1.1. Configuration des ordinateurs

Chaque équipement a besoin d'une adresse pour qu'il soit accessible et qu'il puisse communiquer avec les autres équipements du réseau. Pour cela, nous avons opté pour l'attribution dynamique des adresses IP en adoptant le protocole DHCP que nous avons configuré au niveau des Switchs multifonction ; le tableau suivant montre l'attribution des adresses IP aux ordinateurs :

PCs	Adresse IP	Masque	Passerelle	VLAN	Connecté au
PC0	DHCP	255.255.255.0	192.168.10.252	VLAN 10	Switch0 on fa0/3
PC1	DHCP	255.255.255.0	192.168.20.252	VLAN 20	Switch0 on fa0/4
PC2	DHCP	255.255.255.0	192.168.30.252	VLAN 30	Switch0 on fa0/5
PC3	DHCP	255.255.255.0	192.168.40.252	VLAN 40	Switch0 on fa0/6
PC4	DHCP	255.255.255.0	192.168.50.252	VLAN 50	Switch0 on fa0/7
PC5	DHCP	255.255.255.0	192.168.60.252	VLAN 60	Switch0 on fa0/8
PC6	DHCP	255.255.255.0	192.168.10.252	VLAN 10	Switch0 on fa0/3
PC7	DHCP	255.255.255.0	192.168.20.252	VLAN 20	Switch0 on fa0/4
PC8	DHCP	255.255.255.0	192.168.30.252	VLAN 30	Switch0 on fa0/5
PC9	DHCP	255.255.255.0	192.168.40.252	VLAN 40	Switch0 on fa0/6
PC10	DHCP	255.255.255.0	192.168.50.252	VLAN 50	Switch0 on fa0/7
PC11	DHCP	255.255.255.0	192.168.60.252	VLAN 60	Switch0 on fa0/8
PC12	DHCP	255.255.255.0	192.168.10.252	VLAN 10	Switch0 on fa0/3
PC13	DHCP	255.255.255.0	192.168.20.252	VLAN 20	Switch0 on fa0/4
PC14	DHCP	255.255.255.0	192.168.30.252	VLAN 30	Switch0 on fa0/5
PC15	DHCP	255.255.255.0	192.168.40.252	VLAN 40	Switch0 on fa0/6
PC16	DHCP	255.255.255.0	192.168.50.252	VLAN 50	Switch0 on fa0/7
PC17	DHCP	255.255.255.0	192.168.60.252	VLAN 60	Switch0 on fa0/8
PC18	DHCP	255.255.255.0	192.168.10.252	VLAN 10	Switch0 on fa0/3
PC19	DHCP	255.255.255.0	192.168.20.252	VLAN 20	Switch0 on fa0/4
PC20	DHCP	255.255.255.0	192.168.30.252	VLAN 30	Switch0 on fa0/5
PC21	DHCP	255.255.255.0	192.168.40.252	VLAN 40	Switch0 on fa0/6
PC22	DHCP	255.255.255.0	192.168.50.252	VLAN 50	Switch0 on fa0/7
PC23	DHCP	255.255.255.0	192.168.60.252	VLAN 60	Switch0 on fa0/8

Tableau A1.1 : Plan d'adressage des ordinateurs

A1.2. Configuration des équipements

Chaque équipement s'interconnecte à un autre équipement via une interface précise. Les tableaux A1.2, A1.3 et A1.4 désignent la liste des interfaces qui participeront à l'interconnexion des équipements Switch0, le Switch multilayer 0 et le switch multilayer 2 :

Port	Connecté au	VLAN	Lien
Fa0/1	muliti-sw0	VLAN 10...60	Trunk
Fa0/2	muliti-sw1	VLAN 10...60	Trunk
Fa0/3	PC0	VLAN 10	Access
Fa0/4	PC1	VLAN 20	Access
Fa0/5	PC2	VLAN 30	Access
Fa0/6	PC3	VLAN 40	Access
Fa0/7	PC4	VLAN 50	Access
Fa0/8	PC5	VLAN 60	Access

Tableau A1.2 : Configuration du switch0

Port	Connecté au	VLAN	Lien
Fa0/1	S0	Vlan 10...60	Trunk
Fa0/2	S1	Vlan 10...60	Trunk
Fa0/3	S2	Vlan 10...60	Trunk
Fa0/4	S3	Vlan 10...60	Trunk
Fa0/5	muliti-sw1	Vlan 10...60	Trunk
Fa0/6	muliti-sw1	Vlan 10...60	Trunk

Tableau A1.3 : Configuration du Switch multilayer 0

Port	Connecté au	VLAN	Lien
Fa0/1	Switch 4	Vlan 10...30	Trunk
Fa0/2	Switch 5	Vlan 10...30	Trunk
Fa0/3	Switch 6	Vlan 10...30	Trunk

Tableau A1.4 : Configuration du Switch multilayer 2

A1.3. Réseaux interconnectés directement aux routeurs et Switchs multilayer

Les routeurs et Switchs multifonction échangent les informations concernant leurs voisins du réseau par l'intermédiaire du protocole du routage EIGRP, Le tableau suivant donne une image de chaque routeur et Switch multifonction avec les réseaux qui lui sont directement connectés :

Routeurs	Interface	Adresse IP	Réseau directement connectés
Routeur 0	Fa0/0	192.168.1.2	192.168.1.0/24
	Fa0/1	192.168.2.2	192.168.2.0/24
	Se2/0	192.168.2.3	192.168.3.0/24
Routeur 1	Fa0/0	172.16.2.0	172.16.0.0/16
	Se2/0	192.168.3.1	192.168.3.0/24
Switch multi sw0	Fa0/7	192.168.1.1	192.168.1.0/24
Switch multi sw1	Fa0/7	192.168.2.1	192.168.2.0/24
Switch mltilayer2	Fa0/4	172.16.1.0	172.168.1.0/16

Tableau A1.5. Réseau interconnectés directement aux routeurs et Switch multifonction

A2.1. La norme 802.1Q

La norme 802.1q est née en 1998 pour répondre à un besoin de normalisation sur le transport des VLANs. La principale fonction de la norme est de transporter les VLANs sur le réseau, pour permettre à deux machines d'un même VLAN de communiquer au travers un nombre non défini d'équipement réseau.

Selon la norme 802.1Q, l'étiquetage de trames (méthode de distribution des ID de LAN aux autres commutateurs) est la meilleure façon de mettre en œuvre des LAN virtuels.

La méthode d'étiquetage de trames VLAN a été développée spécialement pour les communications commutées. Cette méthode place un identificateur unique dans l'en-tête de chaque trame au moment où celle-ci est acheminée dans le cœur du réseau.

L'identificateur est interprété et examiné par chaque commutateur avant la transmission à d'autres commutateurs ou équipement de station d'extrémité.

Lorsque la trame quitte le cœur du réseau, le commutateur retire l'identificateur avant de transmettre la trame à la station cible.

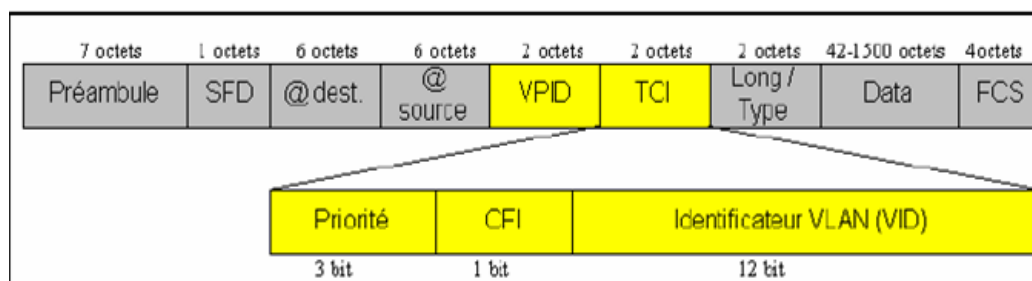


Figure A2.1. Norme 801.1Q

A2.2. Description de la norme

Elle définit, en premier lieu l'ajout de 2 octets dans la trame Ethernet. Ces deux octets ajoutent plusieurs champs pour répondre à plusieurs besoins. La norme définit alors sur la trame Ethernet le champ VPID à 0x8100 pour désigner la trame 802.1q.

- **Canonical format identifiant (CFI) :** un champ protocole définit sur 1 bit est prévu pour pouvoir utiliser le 802.1q aussi bien sur Ethernet que sur Token Ring.
- **Priorité :** 3bits utilisée pour coder 8 niveaux de priorité (de 0 à 7). On se sert de ces 8 niveaux pour fixer la priorité des trames d'un VLAN par rapport à d'autre.
- **VLAN ID :** le champ VID permet de fixer un identifiant sur 12bits, c'est le champ d'identification du VLAN auquel appartient la trame.

Résumé

De nos jours, l'organisation des réseaux locaux est primordiale, elle nécessite une bonne étude concernant sa segmentation afin de faciliter la communication entre les différents sous réseaux. L'objectif de ce projet est la configuration d'un réseau local d'une entreprise (réseau de campus) à l'aide du simulateur Packet Tracer, en proposant une bonne interconnexion entre les différents VLANs ainsi qu'une haute disponibilité (HSRP) pour faciliter la communication entre les différents réseaux locaux. En pratique, les LANs sont segmentés par des VLANs en adoptant la stratégie de VLAN fonctionnelle pour regrouper les utilisateurs. Nous avons en plus configuré un routage dynamique suivant le protocole EIGRP, pour l'ensemble des routeurs et switches multifonction pour l'interconnexion avec d'autres réseaux locaux.

Mots clés : Réseau de campus, Réseau locaux, VLAN, HSRP, EGRP.

Abstract

Today, the organization of local networks is paramount; it requires a good study on its segmentation to facilitate communication between different subnets. The objective of this project is setting up a local company network (campus network) using Packet Tracer simulator, offering a good interconnection between different VLANs and a high availability (HSRP) to facilitate communication between different LANs. In practice, the LANs are segmented by VLANs in VLAN adopting the functional strategy to group users. We have also set up a dynamic routing according EIGRP for all routers and switches multifunction for interconnection with other local networks.

Keywords: campus network, local network, VLANs, HSRP, EIGRP.