الجمهوريـــــة الجزائريـــــة الديمقراطيـــــة الشعبيـــــة
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة التـــعـليـم العـــالي والبـحث العـلـمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
جـــامعة سعيدة – د. مولاي الطاهر
UNIVERSITÉ DESAÏDA – Dr MOULAY TAHAR

Faculté des Sciences et de Technologie

Département d'Electronique

PROJET DE FIN D'ÉTUDE

Présenté Pour l'Obtention du Diplôme de Master en Electronique

Spécialité : Instrumentation

Conception et Simulation d'un réseau local d'entreprise avec Cisco Packet Tracer

---

Présenté par :

Bouanani Ahmed

Soutenu le …/06/2026, devant le jury composé de :

Dr ARBOUCHE Omar	Pr	Président
Dr DINE Khaled	MCA	Encadreur
Dr CHERIFI Abdelhamid	Pr	Examinateur

Année universitaire 2025/2026

Dédicace

C'est avec profonde gratitude et sincères mots que je dédie ce modeste travail de fin d'étude à mes chers parents, qui ont sacrifié leur vie pour notre réussite.

A mes chères sœurs.

A mes chers frères Abdenour et Mourad, qui m'ont également encouragé tout au long de mes études.

A mes chers Ahmed, Otman, Fathi, Younes et toute ma famille et mes proches amis. Pour finir, je remercie mes enseignants et tous mes amis de la promotion.

Remerciements

Je remercie tout d'abord le grand Dieu pour l'achèvement de ce mémoire.

Je remercie Monsieur Dr. Dine Khaled, mon encadreur, pour ses conseils et suggestions avisés qui m'a aidé à mener à bien ce travail.

J'exprime mon gratitude à Monsieur le président de jury d'avoir accepté d'examiner ce mémoire.

Je remercie Messieurs les membres de jury, d'avoir accepté de prendre part à ce jury ainsi que pour l'intérêt qu'ils l'ont portés à ce travail.

Résumé

La gestion et l'amélioration des réseaux locaux au sein d'une entreprise répondent à tous ses besoins internes à haute disponibilité.
Ce travail vise à réaliser une étude globale et une simulation d'un réseau local de l'entreprise Naftal, unité GPL de Saïda. Il porte sur l'élaboration d'un réseau local (LAN), en utilisant des VLANs, et en incluant la gestion de la sécurité.

L'environnement de simulation Cisco Packet Tracer est un outil efficace et performant pour la création, la configuration et la validation des réseaux informatiques. IL est utilisé dans ce travail pour effectuer la création, la configuration et les tests de validation, permettant ainsi de concevoir et d'expérimenter, et de valider le réseau ainsi crée de façon virtuelle avant leur déploiement effectif.
Ce projet utilise le principe du routage inter-VLAN (Inter-VLAN Routing), qui facilite l'échange d'informations entre les divers VLAN, soit via un routeur (Router-on-a-Stick), soit au moyen d'un switch de couche 3 (Layer 3 Switch).
Ce travail souligne l'importance d'une conception anticipée des réseaux locaux et du rôle crucial de la simulation pour minimiser les erreurs et optimiser les performances avant leur mise en œuvre effective.

Les mots clés : Simulation, Réseau informatique, Réseau local (LAN), VLAN, routage inter-VLAN, Cisco Packet Tracer.

Abstract

Managing and improving local area networks (LANs) within a company addresses all its internal high-availability needs.

This work aims to conduct a comprehensive study and simulation of a LAN for Naftal, a GPL unit in Saïda. It focuses on developing a LAN using VLANs and incorporating security management.

The Cisco Packet Tracer simulation environment is an efficient and powerful tool for creating, configuring, and validating computer networks. It is used in this work to perform the creation, configuration, and validation tests, thus enabling the design, experimentation, and validation of the virtual network before its actual deployment.

This project utilizes the principle of inter-VLAN routing, which facilitates the exchange of information between different VLANs, either via a router (Router-on-a-Stick) or through a Layer 3 switch.

This work highlights the importance of early local area network design and the crucial role of simulation in minimizing errors and optimizing performance before actual implementation.

Keywords: Simulation, computer network, Local Area Network (LAN), VLAN, inter-VLAN routing, Cisco Packet Tracer.

الملخص

تُعدّ إدارة الشبكات المحلية داخل المؤسسات وتحسينها من المتطلبات الأساسية لتلبية مختلف الاحتياجات الداخلية وضمان توفر الخدمات بدرجة عالية من الاعتمادية. يهدف هذا العمل إلى إجراء دراسة شاملة ومحاكاة لشبكة محلية خاصة بمؤسسة نفطال، وحدة غاز البترول المميع (GPL) بسعيدة. ويرتكز المشروع على تصميم شبكة محلية (LAN) باستخدام الشبكات المحلية الافتراضية (VLANs)، مع دمج آليات إدارة الأمن والحماية.

يُعتبر برنامج Cisco Packet Tracer بيئة محاكاة فعّالة وقوية لإنشاء الشبكات الحاسوبية وتهيئتها والتحقق من صحتها. وقد تم استخدامه في هذا العمل لتنفيذ عمليات التصميم والإعداد واختبارات التحقق، مما أتاح إمكانية تصميم الشبكة وتجربتها والتحقق من كفاءتها بشكل افتراضي قبل الشروع في تنفيذها الفعلي.

يعتمد المشروع على مبدأ التوجيه بين الشبكات المحلية الافتراضية(Inter-VLAN Routing) ، الذي يسهّل تبادل المعلومات بين مختلف شبكاتVLAN ، سواءً عبر استخدام موجه (Router-on-a-Stick) أو من خلال مبدّل من الطبقة الثالثة (Layer 3 Switch).

ويبرز هذا العمل أهمية التخطيط المسبق للشبكات المحلية والدور المحوري للمحاكاة في تقليل الأخطاء وتحسين الأداء وضمان فعالية الشبكة قبل تطبيقها على أرض الواقع.

الكلمات المفتاحية: المحاكاة، الشبكات الحاسوبية، الشبكة المحلية(LAN) ، الشبكات المحلية الافتراضية(VLAN) ، التوجيه بين الشبكات الافتراضية (Inter-VLAN Routing) ، Cisco Packet Tracer.

Liste des abbreviations

LAN: Local Area Network

WAN: Wide Area Network

MAN: Metropolitan Area Network

PAN: Personal Area Network

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

NAT: Network Address Translation

STP: Spanning Tree Protocol

ARP: Address Resolution Protocol

ICMP: Internet Control Message Protocol

IP: Internet Protocol

VLAN: Virtual Local Area Network

VTP: Virtual Local Area Network

SVI: Switch Virtual Interface

OSI: Open Systems Interconnection

TCP: Transmission Control Protocol

MAC: Media access control

IEEE: Institute of Electrical and Electronics Engineers)

P2P: peer to peer

IPV6: internet protocol version 6

UTP: Unshielded Twisted Pair

S/FTP: Shielded/Foiled Twisted Pair

FTP: Foiled Twisted Pair

STP: Shielded Twisted Pair

ACL: Access Control List

SMTP: Simple Mail Transfer Protocol

Table des matières

Liste des tableaux

Liste des figures

Chapitre 01

Chapitre 02

Chapitre 03

Chapitre 04

Introduction Générale

Avec les technologies de l'information et de la communication, les réseaux informatiques sont devenus un pilier essentiel des entreprises modernes. Permettre de partager plus facilement les ressources, d'envoyer rapidement des données et de gérer au mieux les services et les utilisateurs. Le réseau local (LAN) occupe une place majeure parmi les différents types de réseaux, grâce à sa capacité à relier plusieurs appareils au sein d'un espace limité, tout en garantissant performances, sécurité et fiabilité.

Dans ce cadre, la segmentation du réseau à l'aide des VLAN (Virtual Local Area Network) représente une approche efficace pour optimiser l'organisation du réseau, accroître la sécurité et améliorer les performances des échanges entre les différents services d'une entreprise.

Ce travail porte sur la conception et simulation d'un réseau local destiné à l'entreprise Naftal (GLS) Unité du Saida, à l'aide du logiciel Cisco Packet Tracer. L'objectif principal est de mettre en place une infrastructure réseau efficace, sécurisée et capable de garantir la communication entre les différents services de l'entreprise, grâce à la création et à la configuration des VLAN.

Le logiciel Packet Tracer de la firme Cisco permet de concevoir, configurer et de simuler les réseaux, et d'implémenter les différentes fonctionnalités nécessaires au bon fonctionnement de l'infrastructure de ces réseaux ainsi conçus. Nous avons configuré les appareils réseau et implémenté les différentes fonctionnalités nécessaires au bon fonctionnement de l'infrastructure.

Dans ce mémoire de fin d'étude, nous avons d'abord exposé les concepts de base des réseaux informatiques en chapitre 1, suivi d'un exposé sur les réseaux locaux et les VLAN en chapitre 2. Ensuite, nous avons présenté l'entreprise Naftal en chapitre 3, et présenter brièvement le logiciel Packet Tracer et les outils utilisés pour la simulation. Dans ce travail, nous avons conçu, modélisé et simulé le réseau à l'aide du logiciel Cisco Packet Tracer, en configurant les équipements réseau et en mettant en œuvre les différentes fonctionnalités nécessaires au bon fonctionnement de l'infrastructure. Et ce en configurant les équipements réseau et en appliquant les diverses fonctionnalités requises. On a ensuite procéder à un ensemble de tests de validation et de vérification du bon fonctionnement du réseau local ainsi conçu et réalisé sous Packet Tracer. A la fin, nous pouvons garantir le bon fonctionnement de l'infrastructure réseau, et son efficacité.

Chapitre 01

Généralités sur les réseaux informatiques

1.1 Introduction

Les réseaux informatiques constituent aujourd'hui la base essentielle des systèmes d'information. Ils permettent de centraliser et/ou de partager efficacement les ressources matérielles et logicielles. Dans ce premier chapitre, nous présentons les concepts de base des réseaux, leurs types, topologies, modèles et technologies de transmission.

1.2 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'appareils ou de nœuds connectés entre eux et capables de communiquer, mais aussi de partager des ressources. Il permet aux ordinateurs de travailler ensemble, d'envoyer des données et d'accéder à des ressources partagées (fichiers, messagerie électronique, imprimantes, etc.) d'un appareil à l'autre [1].

1.3 Objectifs des réseaux informatiques

Les réseaux informatiques ont plusieurs objectifs plus ou moins importants. Ceux-ci peuvent être classés en deux catégories notamment [2] :

- **Partage des ressources matérielles et logicielles** : Les nœuds du réseau reliés en réseaux peuvent partager des ressources matérielles, telles que des imprimantes, des serveurs, des dispositifs de réseautage, etc., et ressources logicielles, telles que des fichiers, des bases de données, des messages, les applications, les jeux, etc. Ce partage permet alors un gain en coût énorme, ce qui permet de réduire les dépenses des personnes et des entreprises.
- **Connexion et communication entre utilisateurs et entre applications et entre processus** : Les réseaux permettent la connexion et la communication entre personnes et entre processus industriels, et entre applications. Les personnes peuvent alors s'échanger facilement des messages en quelque secondes (e-mail, forum, etc.), des fichiers, etc. les applications et les processus s'échangent des données, et des fichiers de taille différentes [1].

1.4 Les différents Types de réseaux

Les réseaux sont classés en différents types selon leur taille (nombre de machines), leur vitesse de transfert des données et leur étendue. On distingue habituellement trois sortes de réseaux [1]:

1.4.1. Réseaux personnels (PAN):

Les réseaux personnels ou PAN (Personal Area Networks) sont des réseaux qui permettent à des équipements de communiquer au niveau individuel. Un exemple fréquent est celui du réseau sans fil qui relie un ordinateur à ses périphériques. On trouve pratiquement sur tous les ordinateurs un moniteur, un clavier, une souris et une imprimante.

1.4.2. Les réseaux locaux (LAN):

Il s'agit d'un réseau informatique d'une portée géographique relativement limitée, destiné à relier entre eux les ordinateurs d'un domicile particulier, les ordinateurs d'une entreprise, les ordinateurs d'une salle informatique, les ordinateurs d'un bâtiment, etc. L'infrastructure est privée et gérée en local. A l'intérieur, ou « sur » le réseau local, il y a des ordinateurs fixes ou portables reliés par câble ou sans fil (Réseaux locaux sans fil : WLAN) (Figure 1.1).

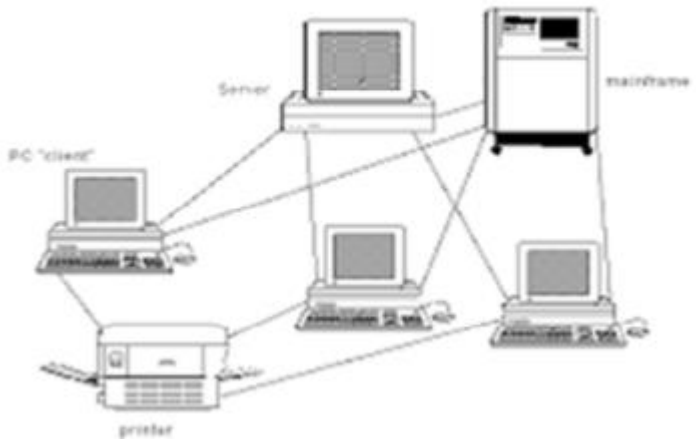


***Figure 1.1**: réseau LAW*

1.4.3. Les réseaux métropolitains (MAN):

Il s'agit d'un réseau métropolitain, c'est-à-dire un réseau constitué d'ordinateurs qui est généralement utilisé sur des campus ou dans des villes. Ainsi, un MAN permet à deux nœuds (ordinateurs) distants de communiquer comme s'ils appartenaient au même réseau local. Un MAN est constituée de commutateurs ou de routeurs reliés entre eux par des liens à haut débit qui font généralement usage de la fibre optique (Figure 1.2).

Figure 1.2 : *réseau MAN*

1.4.4. Réseau à grande distance (WAN):

Le réseau Internet (WAN) est un réseau d'une grande extension géographique, au niveau d'un pays, d'un continent ou même du monde entier. Il permet le raccordement d'un réseau local ou métropolitain à l'internet mondial. Infrastructure et généralement publique (Figure 1.3).

Figure 1.3 *: réseau WAN*

1.5 Topologies physiques et logiques :

1.5.1. Définition générale de la topologie réseau :

La topologie d'un réseau informatique correspond à la façon dont sont disposés et reliés entre eux les divers éléments du réseau. Elle permet de décrire à la fois la disposition matérielle des liaisons et le mode de circulation logique des données entre les nœuds du réseau. Pour un ingénieur, la topologie est un choix fondamental qui détermine les performances, la fiabilité, la sécurité et la capacité d'évolution du réseau. Il existe deux types principaux de topologies : la topologie physique et la topologie logique.

1.5.2. Définition de la topologie physique :

La topologie physique décrit la disposition matérielle réelle des équipements du réseau. Elle décrit le raccordement physique des ordinateurs, serveurs, commutateurs, routeurs et supports de transmission (câbles, fibres optiques, liaisons sans fil) [2].

1.5.2.1. Topologie en bus:

On appelle topologie en bus une architecture dans laquelle tous les équipements partagent un même support de transmission linéaire. Les données transmises par un équipement sont diffusées sur l'ensemble du bus et reçues par tous les autres équipements. Cette topologie est simple et peu coûteuse, mais elle offre une faible tolérance aux pannes et des performances limitées en cas d'augmentation du trafic (figure 1.4).

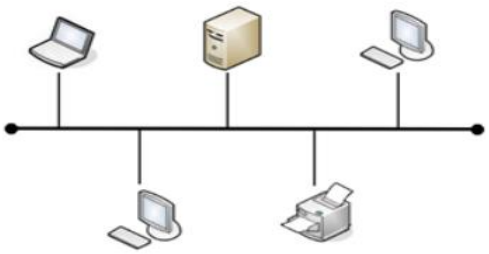


Figure 1. 4: *Topologie en bus*

1.5.2.2. Topologie physique en étoile :

Une topologie en étoile est une architecture où tous les équipements sont reliés à un nœud central, généralement un commutateur. Toutes les communications passent par ce centre. Cette topologie facilite la gestion, l'extension et le diagnostic du réseau. C'est aujourd'hui la plus employée dans les réseaux locaux modernes (Figure 1.5).

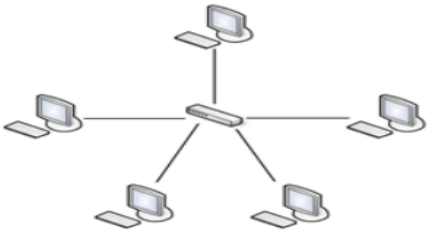


Figure 1.5: *Topologie en étoile*

1.5.2.3. Topologie physique en anneau :

Une topologie en anneau est une organisation dans laquelle chaque équipement est connecté à deux autres, créant ainsi une boucle fermée. Les données transitent séquentiellement autour de l'anneau. Cette topologie permet de contrôler strictement l'accès au média, mais elle est sensible aux pannes et complexité de maintenance (figure 1.6).

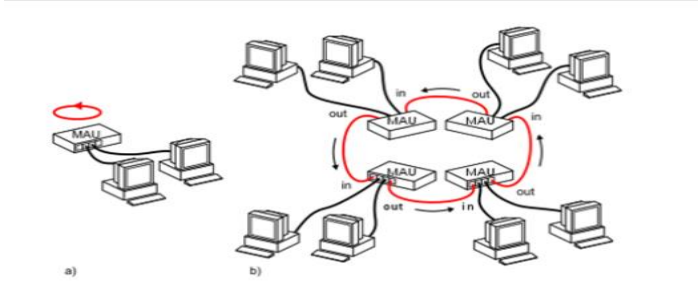


Figure 1.6: *Topologie en anneau*

1.5.2.4. Topologie physique maillée :

Une topologie maillée est une architecture où chaque équipement est connecté à plusieurs autres équipements du réseau. Il existe deux types de maillage : maillage partiel et maillage complet. Cette topologie permet une excellente redondance et une grande disponibilité, idéale pour les réseaux critiques, mais elle est coûteuse et sa mise en place est complexe (Figure 1.7).

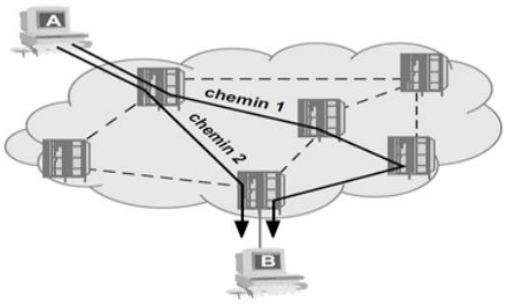
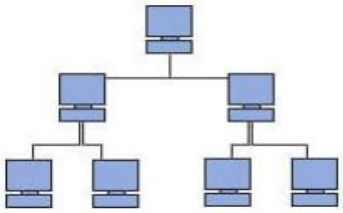


Figure 1.7 : *Topologie en maillé*

1.5.2.5. La topologie en arbre

La topologie arborescente, aussi appelée topologie hiérarchique, résulte de la combinaison des topologies en étoile et en bus. Elle est constituée d'une ligne centrale (bus) à laquelle sont reliés plusieurs réseaux en étoile. Chaque réseau en étoile fonctionne comme une branche indépendante du réseau en bus (Figure 1.8).



· ***Figure 1.8:*** *Topologie en arbre*

1.5.2.6. La topologie mixte:

C'est une topologie de réseau qui intègre deux ou plusieurs topologies de base (étoile, bus, anneau, arbre, etc.) au sein d'une même infrastructure. Elle est conçue pour tirer parti des avantages de chaque topologie tout en limitant leurs inconvénients, afin de répondre aux besoins spécifiques d'un réseau complexe ou étendu (Figure1.9).

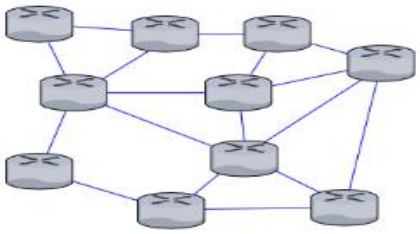


Figure 1.9 : *Topologie en mixte*

1.5.3 Définition de la topologie logique :

La topologie logique définit le flux des données dans le réseau, sans tenir compte de l'organisation physique. Elle définit le chemin logique de l'information ainsi que les règles

d'accès au support de transmission. La topologie logique dépend surtout des protocoles de communication utilisés.

Dans un réseau Ethernet moderne, par exemple, la topologie physique est le plus souvent de type étoile, alors que la topologie logique correspond à une diffusion de type bus. En outre, les technologies telles que les VLAN permettent de créer plusieurs topologies logiques distinctes au sein d'une même infrastructure physique.

1.6. Le modèle OSI

1.6.1 Définition de modèle OSI :

Le modèle OSI est un modèle de référence, normalisé par l'Organisation internationale de normalisation, qui vise à structurer et à normaliser les communications entre systèmes informatiques hétérogènes. C'est une architecture conceptuelle (pas une implémentation opérationnelle) utilisée pour l'analyse et la conception de réseaux. Son fonctionnement est basé sur une segmentation du processus de communication en sept niveaux fonctionnels, chacun jouant un rôle particulier et ne communiquant qu'avec les niveaux voisins, permettant ainsi une meilleure interopérabilité, une facilité de maintenance et une capacité d'évolution pour les réseaux (Figure 1.10) [4].

Figure 1.10 : *les sept couches du modèle OSI*

1.6.2. Présentation et rôle des sept couches du modèle OSI:

- **Couche 1 : Couche physique**

La couche physique assure la transmission brute des bits sur le support de communication. Elle précise les caractéristiques électriques, mécaniques et fonctionnelles de l'interface physique entre les équipements. Cette couche définit entre autres les niveaux de tension, les types de connecteurs, la synchronisation des signaux et les débits binaires.

- **Couche 2 : Couche liaison de données**

  La couche liaison de données permet une transmission fiable des trames entre deux équipements directement connectés. Elle assure l'adressage physique (adresse MAC), la détection et éventuellement la correction des erreurs, et le contrôle d'accès au support de transmission.

  Cette couche est très importante dans les réseaux locaux, car elle assure une bonne transmission des données entre les différents nœuds d'un même segment réseau.

- **Couche 3 : La couche réseau**

  La couche réseau a pour rôle d'assurer la transmission de paquets de données entre différents réseaux. Elle gère l'adressage logique, le routage et le choix de l'itinéraire optimal vers la destination. Pour l'ingénieur réseau, cette couche est très importante puisqu'elle permet l'interconnexion de réseaux hétérogènes et sert de base aux réseaux étendus tels que l'Internet.

- **Couche 4 : couche transport**

  La couche transport assure la communication de bout en bout entre les applications des systèmes distants. Elle assure la segmentation des données, le contrôle de flux, la gestion des erreurs et la fiabilité de la transmission.

  Cette couche assure que les données arrivent complètes, sans duplication et dans le bon ordre, conformément aux exigences de l'application.

- **Couche 5 : Couche session**

  La couche session assure l'établissement, la maintenance et la terminaison des sessions de communication entre les applications. Elle synchronise les échanges et permet de reprendre la communication en cas d'interruption. Bien qu'elle soit souvent intégrée à d'autres couches dans les implémentations modernes, cette couche conserve son importance sur le plan conceptuel.

- **Couche 6 : Couche présentation**

  La couche présentation assure la représentation des données. Elle assure le formatage, la conversion, la compression et le chiffrement des données. Il a pour fonction de s'assurer que les données transmises soient compréhensibles par le système récepteur.

  Cette couche est essentielle pour la sécurité et l'interopérabilité des applications réseau.

- **Couche 7 : couche application**

  La couche application est celle qui est la plus proche de l'utilisateur. Elle assure les services réseau directement accessibles par les applications, comme l'accès aux fichiers, la messagerie électronique ou la navigation web.

  Elle est le point de contact entre les applications de l'utilisateur et les services de communication du réseau.

1.7 Le modèle TCP/IP

1.7.1. Définition du modèle TCP/IP:

Le modèle TCP/IP est un modèle de communication utilisé comme base opérationnelle des réseaux modernes, en particulier du réseau Internet. Il a été développé initialement par le département de la Défense des États-Unis dans le cadre du projet ARPANET. Contrairement au modèle OSI, qui est essentiellement théorique, le modèle TCP/IP est directement issu de l'implémentation réelle des protocoles de communication.

Le modèle TCP/IP a pour objectif principal d'assurer l'interconnexion de réseaux hétérogènes de manière fiable et robuste, même en cas de défaillance partielle du réseau. Il repose sur une architecture plus simple que celle du modèle OSI et se compose de quatre couches fonctionnelles (Figure 1.11) [2].

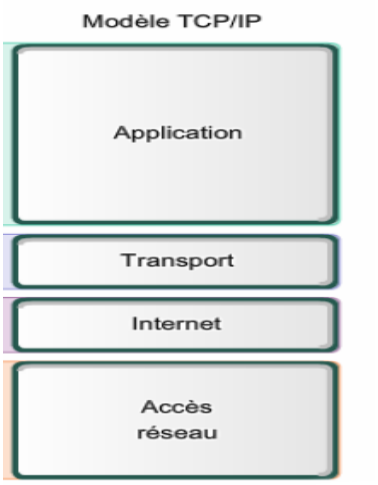


Figure 1.11 : *les quatre couches du modèle TCP/IP*

1.7.2. Architecture et couches du modèle TCP/IP

- **Couche 1 : Accès réseau**

  La couche d'accès réseau regroupe les fonctions relatives à la transmission physique et à la liaison de données. Elle assure la communication entre un équipement et le réseau auquel il est directement connecté. Cette couche définit les méthodes d'accès au support, l'encapsulation des données et l'adressage physique.

  Elle correspond approximativement aux couches physiques et liaison de données du modèle OSI. Les technologies telles qu'Ethernet, Wifi opèrent à ce niveau.

- **Couche 2 : Internet**

  La couche Internet est le cœur du modèle TCP/IP. Elle est responsable de l'adressage logique et du routage des paquets à travers des réseaux interconnectés. Son rôle principal est d'acheminer les données de la source vers la destination, indépendamment du chemin emprunté.

  Le protocole fondamental de cette couche est le protocole IP (Internet Protocol). Cette couche assure une transmission dite « non fiable », ce qui signifie qu'elle ne garantit ni la livraison ni l'ordre des paquets.

- **Couche 3 : Transport**

  La couche transport assure la communication de bout en bout entre les applications des systèmes distants. Elle est responsable de la segmentation des données, du contrôle de flux et de la gestion des erreurs. Deux protocoles majeurs opèrent à ce

niveau. Le protocole TCP fournit un service fiable, orienté connexion, garantissant l'intégrité et l'ordre des données. Le protocole UDP offre un service non fiable, sans connexion, privilégiant la rapidité et la simplicité.

- **Couche 4 : Application**

  La couche application regroupe l'ensemble des protocoles permettant aux applications utilisateur d'accéder aux services réseau. Elle fournit directement les fonctionnalités nécessaires aux échanges de données entre applications.

  Parmi les protocoles les plus connus de cette couche figurent HTTP pour le web, FTP pour le transfert de fichiers, SMTP pour la messagerie électronique et DNS pour la résolution des noms de domaine.

1.8 Types de transmission et médias de communication :

Les modes de transmission utilisés et les médias de communication choisis influencent grandement les performances d'un réseau informatique. Pour l'ingénieur, il est indispensable de maîtriser parfaitement ces deux concepts afin d'adapter le réseau aux besoins applicatifs, aux contraintes techniques et à l'environnement d'exploitation.

1.8.1. Définition des types de transmission:

Les types de transmission décrivent comment l'information passe entre un émetteur et un récepteur. Leur définition dépend du sens et de la simultanéité des échanges [2].

1.8.1.1. Transmission simplex:

On parle de transmission simplex lorsqu'il s'agit d'un mode de communication unidirectionnel, dans lequel les données ne circulent que dans un seul sens, de l'émetteur vers le récepteur. Le récepteur ne peut pas communiquer d'informations à l'émetteur. Dans des systèmes simples comme la diffusion radio ou la transmission de signaux par des capteurs, on utilise ce type de transmission (Figure 1.12).

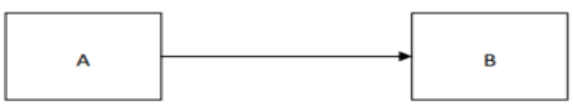


Figure 1.12: *mode de transmission simplex*

1.8.1.2. Transmission half-duplex :

La transmission semi-duplex est un mode de communication bidirectionnel non simultané. Les deux équipements sont capables d'émettre et de recevoir des données, mais pas simultanément. Ce mode est souvent employé dans les systèmes où le support de transmission est partagé, par exemple les réseaux sans fil (Figure 1.13).

.

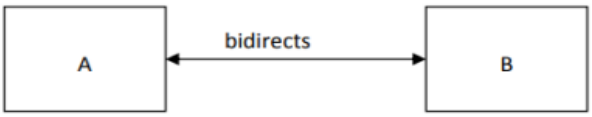


Figure 1.13: *mode semi-duplex (half-duplex)*

1.8.1.3. Transmission full-duplex:

Le mode full-duplex permet de communiquer dans les deux sens en même temps. Les deux équipements peuvent s'envoyer et se recevoir des données simultanément. Ce mode permet d'avoir de meilleures performances et moins de latence. Il est très employé dans les réseaux Ethernet modernes et les liaisons téléphoniques numériques (Figure 1.14).

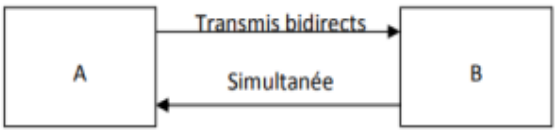


Figure 1.14*: mode duplex (full duplex)*

1.8.2. Définition des médias de communication

Les médias de communication sont les supports physiques ou radioélectriques qui assurent le transport de l'information entre les équipements du réseau. On les classe en médias filaires et médias sans fil.

1.8.2.1. Médias de communication filaires :

Les médias filaires utilisent un support physique pour la transmission des signaux [1].

1.8.2.1.1. La paire torsadée :

Le support de transmission le plus utilisé dans les réseaux locaux (LAN) est la paire torsadée. Elle est formée de paires de fils en cuivre tordus, ceci afin de réduire les interférences électromagnétiques. Économique et simple à mettre en place, elle fournit des débits adaptés aux besoins des réseaux locaux. On en distingue quatre types principaux, selon le degré de blindage (figure15).

- **UTP (Unshielded Twisted Pair) :** câble non blindé, très utilisé grâce à son faible coût et à sa simplicité, mais sensible aux interférences.
- **STP (Shielded Twisted Pair) :** câble dans lequel chaque paire est entourée d'un blindage métallique, ce qui améliore son immunité face aux perturbations.
- **FTP (Foiled Twisted Pair) :** câble disposant d'un blindage global en feuille métallique, qui offre une protection intermédiaire contre les interférences.
- **S/FTP (Shielded/Foiled Twisted Pair)** : câble combinant un blindage individuel et un blindage global pour une protection maximale et de hautes performances.

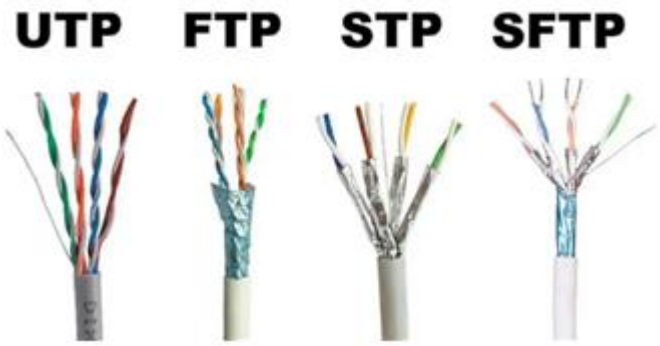


Figure 1.15: *Les différents Types de paires torsadées*

1.8.2.1.2. Le câble coaxial:

Le câble coaxial est un moyen de transmission filaire employé pour acheminer des signaux électriques, en particulier au sein des réseaux de télévision, des réseaux informatiques ainsi que des systèmes de télécommunication. Il se compose d'un conducteur central en cuivre, entouré d'une couche isolante, puis d'un blindage métallique (sous forme de tresse et/ou de feuille) destiné à diminuer les interférences électromagnétiques. L'ensemble est entouré d'une

gaine isolante extérieure. Cette structure permet au câble coaxial de transmettre le signal de façon stable et fiable sur de longues distances, tout en réduisant les pertes de signal et les perturbations externes (figure 1.16).

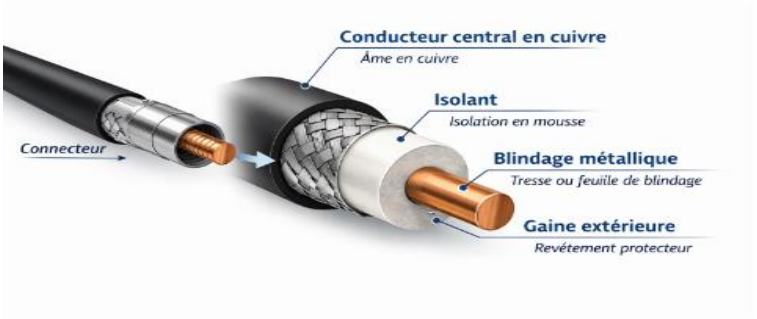


***Figure 1.16** : la structure d'un câble coaxial*

1.8.2.1.3. La fibre optique:

La fibre optique est le support de transmission filaire le plus avancé technologiquement dans les réseaux informatiques modernes. Elle est faite de très fins fils de verre ou de plastique, appelés fibres, qui peuvent transporter des signaux sous forme de lumière.

Le fonctionnement de la fibre optique s'appuie sur le phénomène de réflexion interne totale, qui permet à la lumière de parcourir de longues distances avec de très faibles pertes.

En général, une fibre optique comprend trois éléments principaux :

- **Cœur (core) :** partie centrale où circule le signal lumineux.
- **La gaine:** couche qui entoure le cœur et assure la réflexion de la lumière.
- **Le revêtement :** protection externe contre les agressions mécaniques.

L'utilisation de la fibre optique offre plusieurs avantages majeurs :

- Très grande largeur de bande, ce qui permet d'avoir des débits extrêmement élevés (plusieurs térabits par seconde).
- Faibles pertes de signal, permettant des transmissions sur de très longues distances sans amplification fréquente.
- Une immunité totale aux interférences électromagnétiques, contrairement aux câbles en cuivre.
- Haute sécurité, car les données sont difficiles à intercepter (Figure 1.17).

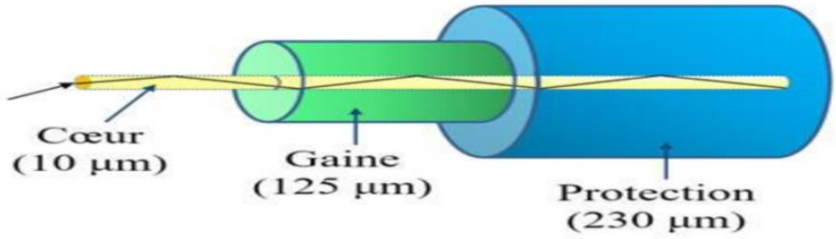


Figure 1.17 : *la structure d'une fibre optique*

1.8.2.2. Médias de communication sans fil:

Les médias sans fil sont des ondes électromagnétiques qui permettent de transmettre l'information sans support physique (Figure 18).

Figure 1.18 : *Médias de communication sans fil*

- Les réseaux Wifi, Bluetooth et les réseaux cellulaires utilisent les ondes radio. Elles sont très souples et permettent aux utilisateurs de se déplacer.
- Les micro-ondes servent à la liaison point à point et aux communications sur de longues distances. Elles demandent une ligne de vue directe entre les émetteurs.
- Les liaisons par satellite permettent de communiquer sur de très longues distances, en particulier dans les régions isolées. Elles ont toutefois une forte latence et un coût élevé.

Conclusion :

Ce chapitre a permis de poser les bases des réseaux informatiques en présentant leur définition, leurs différents types selon l'étendue géographique et les principales topologies physiques et logiques. L'analyse des modèles de référence, en particulier le modèle OSI et le modèle TCP/IP, a permis de mieux comprendre le fonctionnement des communications réseau et l'organisation des protocoles. Enfin, l'analyse des types de transmission et des médias de communication a montré leur rôle essentiel dans la performance et la fiabilité des échanges de données.

Chapitre 02
Les réseaux LAN et VLAN

2.1 Introduction :

Dans ce deuxième chapitre les notions fondamentales relatives aux réseaux locaux et aux réseaux virtuels sont présentées d'une manière simple. On a va définir ces deux concepts essentiels, leurs différents types de réseaux LAN, et les méthodes de fonctionnement, et modes de fonctionnement des VLAN, les méthodes de routage en relation, etc.

2.2 Les réseaux locaux (LAN)

Un réseau local ou LAN (Local Area Network) est un ensemble d'ordinateurs et d'autres équipements reliés entre eux sur une zone géographique limitée, comme un bureau, une entreprise, une école ou un bâtiment. Il permet de partager les ressources – fichiers, imprimantes, connexion Internet – entre les différents utilisateurs.

Le réseau local permet une vitesse de transmission élevée, et un faible taux d'erreurs grâce à des technologies adaptées telles que le Wifi ou Ethernet. En général, il n'est géré que par une seule organisation, ce qui facilite son administration, sa maintenance et sa sécurisation.

2.3 Architecture réseau

2.3.1 L'architecture poste à poste :

C'est un modèle où tous les ordinateurs du réseau jouent un rôle équivalent et peuvent échanger directement des ressources entre eux, sans passer par un serveur central. Chaque poste peut fonctionner à la fois en tant que client et serveur. Ce le type d'architecture est simple à déployer et convient bien aux petits réseaux. Mais, son L'administration se complique et sa sûreté reste bornée lorsque le réseau s'étend (Figure 2.1).

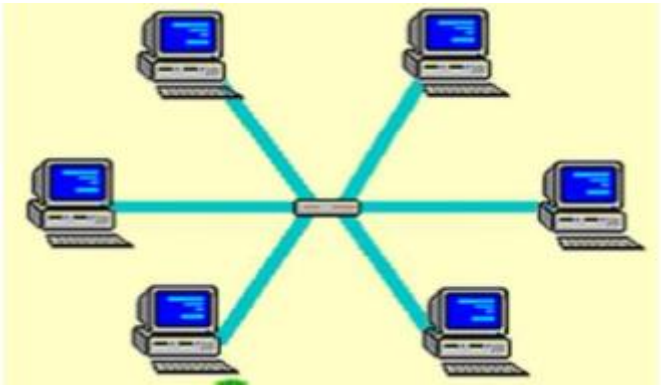


Figure 2.19 : *Le réseau poste à poste*

2.3.2 L'Architecture client-serveur :

L'architecture client-serveur repose sur la présence d'un serveur central qui fournit des services et des ressources aux machines clientes. Les clients envoient des requêtes et le serveur y répond de façon centralisée. Ce modèle améliore la gestion, renforce la sécurité et administre le réseau de façon plus efficace. Il est couramment employé dans les réseaux d'entreprise et les milieux professionnels (Figure 2.2)

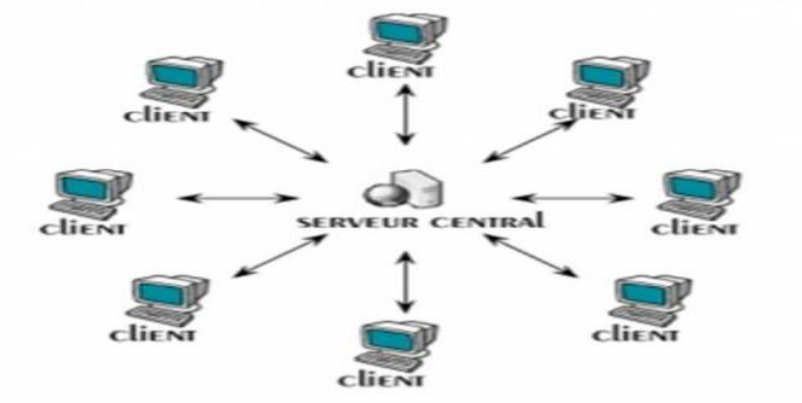


Figure 2.20: *réseau client-serveur*

2.4 Équipements d'un réseau

Les équipements réseau sont des dispositifs matériels qui permettent d'assurer la connectivité, la communication et la gestion des flux de données entre les différents nœuds d'un réseau.

2.4.1 La carte d'interfaçage réseau (NIC)

Un ordinateur ne peut pas se connecter à un réseau sans une carte réseau, qui est un composant matériel essentiel. Elle assure l'interface entre le système informatique et le support de transmission. Une carte possède une adresse physique unique, appelée adresse MAC, qui permet d'identifier l'équipement sur le réseau.

2.4.2 Le modem

Le modem (modulateur-démodulateur) est un appareil qui permet de convertir des signaux numériques en signaux analogiques et vice-versa. Il sert à transmettre des données par les lignes téléphoniques, les réseaux câblés ou les liaisons fibre optique.

2.4.3 Serveur

Un serveur est un ordinateur ou un système qui assure la gestion des ressources d'un réseau. Il offre des services aux autres appareils, dits clients, tels que le stockage, les applications ou l'accès aux données. Il peut être spécialisé (serveur web, serveur de fichiers…) ; Il occupe une place centrale dans l'organisation du réseau.

2.4.4 Pare- feu

Un pare-feu est un système de sécurité qui protège un réseau informatique contre les accès non autorisés. Il trie les données qui arrivent et qui partent selon des règles qu'il a définies. Il peut être matériel, logiciel ou les deux. C'est indispensable pour assurer la confidentialité et l'intégrité des données sur un réseau.

2.5 Équipements d'interconnexion de réseau :

2.5.1 Répéteur

Le répéteur est un dispositif utilisé pour amplifier ou régénérer un signal afin d'augmenter la distance de transmission dans un réseau. Il reçoit un signal affaibli et le retransmet avec une meilleure qualité. Il fonctionne au niveau physique du modèle OSI et ne filtre pas les données.

2.5.2. Hub (Concentrateur)

Le hub est un équipement qui permet de connecter plusieurs appareils dans un réseau local. Il diffuse les données reçues vers tous les ports sans distinction. Il fonctionne au niveau physique du modèle OSI. Il est aujourd'hui peu utilisé car remplacé par le switch.

2.5.3. Bridge (Pont)

Le bridge est un dispositif qui relie deux segments de réseau et filtre les données selon les adresses MAC. Il permet de réduire les collisions en séparant les domaines de collision. Il fonctionne au niveau liaison de données (couche 2). Il améliore les performances du réseau.

2.5.4. Switch (Commutateur)

Le switch est un équipement qui connecte plusieurs appareils au sein d'un réseau local. Il transmet les données uniquement vers le destinataire grâce à l'adresse MAC. Il fonctionne principalement au niveau 2 du modèle OSI. Il offre de meilleures performances que le hub.

2.5.5 Routeur

Le routeur est un dispositif qui permet de relier plusieurs réseaux différents entre eux. Il choisit le meilleur chemin pour acheminer les données en utilisant les adresses IP. Il fonctionne au niveau réseau (couche 3). Il est essentiel pour l'accès à Internet.

2.5.6. Passerelle (Gateway)

La passerelle est un équipement qui permet la communication entre des réseaux utilisant des protocoles différents. Elle traduit les données pour assurer la compatibilité entre systèmes. Elle peut fonctionner à plusieurs niveaux du modèle OSI.

2.6. Les protocoles de réseau (DHCP, DNS, NAT, STP, ARP, ICMP, IP)

- **Le protocole DHCP :** permet de simplifier la configuration des machines sur un réseau local. D'affecter automatiquement à chaque appareil une adresse IP ainsi que les autres paramètres nécessaires, comme le masque de sous-réseau, la passerelle par défaut et le serveur DNS. Système permet à l'administrateur de ne pas avoir à configure chaque machine manuellement, ce qui permet de gagner du temps et d'éviter des erreurs, notamment des conflits d'adresses IP.
- **DNS (Domain Name System)** autorise les utilisateurs à accéder aux ressources du réseau à l'aide de noms faciles à mémoriser plutôt que d'adresses IP complexes. Par

exemple, on peut utiliser un nom simple au lieu de saisir une suite de chiffres, le DNS se chargeant alors de trouver l'adresse correspondante. Réseau plus pratique, particulièrement lorsqu'il y a plusieurs équipements ou services.

- **NAT (Network Address Translation)** sert à ce que les équipements d'un réseau local puissent accéder à Internet en utilisant une seule adresse IP publique. L'extérieur, il convertit l'adresse privée en une adresse publique. Plus de conserver des adresses IP, il procure un certain niveau de sécurité grâce à la dissimulation des détails du réseau interne.
- **STP (Spanning Tree Protocol)** permet d'éviter la création de boucles dans un réseau où plusieurs commutateurs sont interconnectés entre eux. Être à l'origine de problèmes tels que des ralentissements ou des pannes du réseau.
- **ARP (Address Resolution Protocol**) établit le lien entre une adresse IP et une adresse physique (MAC) sur un réseau local. Lorsqu'un appareil veut envoyer des données à un autre, il doit connaître son adresse MAC ; ARP permet de trouver cette adresse à partir de l'adresse IP. Il s'agit d'une étape importante pour garantir une bonne transmission des données.
- **ICMP (Internet Control Message Protocol)** Le protocole ICMP sert à contrôler l'état du réseau et à repérer d'éventuels problèmes. Il permet d'envoyer des messages pour connaître l'accessibilité d'un appareil. Par exemple, le protocole utilisé par la commande Ping permet de tester la connexion entre deux machines.
- **IP (Protocole Internet)** L'adresse IP (Internet Protocol) est un identifiant numérique unique attribué à chaque appareil connecté à un réseau informatique. Identifier et localiser un équipement afin d'assurer la bonne transmission des données. L'adressage est au cœur de toute communication sur Internet, permettant d'acheminer les paquets vers leur destination. C'est donc un élément essentiel du fonctionnement des réseaux. Ce protocole comporte deux versions principales :
  - **IP4 (Protocole version 4)** : c'est la première version du protocole IP à être utilisée à grande échelle. Il repose sur un format de 32 bits, généralement représenté par quatre nombres décimaux séparés par des points. Il permet de générer quelque 4, 3 milliards d'adresses uniques.
  - **IPv6 (Internet Protocol version 6)** est une version récente conçue pour succéder à l'IPv4. Format de 128 bits, ce qui permet un nombre d'adresses extrêmement élevé. La capacité d'IPv6 permet de répondre à l'augmentation

massive des appareils connectés, mais elle renforce aussi la sécurité et l'efficacité du routage.

2.7. Réseau local virtuel

2.7.1. Définition

Les VLANs se situent au niveau 2 du modèle OSI. Les VLANs (Virtual Local Area Network) permettent de segmenter un support physique en plusieurs segments logique (nous entendons par support physique un ensemble de matériels : Hub, commutateurs, et de liens constituant le support physique d´un protocole de niveau deux). Il est ainsi possible de se dédouaner de l´architecture physique du réseau afin de réaliser la segmentation de celui-ci. Un VLAN Ethernet spécifique a le comportement d´un LAN Ethernet aux vues de couches supérieures.

2.7.2 Avantages des VLAN

- **Amélioration des performances** : Les VLAN réalisent une segmentation qui diminue la taille des domaines de broadcast et donc le nombre de collisions dans ces domaines. Les VLAN reposent par ailleurs sur la commutation (et non le routage) pour segmenter les domaines de diffusion ce qui permet un traitement bien plus rapide.
- **Réduction des coûts :** les VLAN simplifient l'administration du réseau. L'utilisation des VLAN entraînent souvent la réduction du nombre de routeurs nécessaires, ou les routeurs sont plus onéreux que les commutateurs ;
- **Formation de groupes virtuels :** On trouve concrètement, dans les entreprises, des groupes de développement, de travail sur un projet spécifique, dont les membres appartiennent à des départements différents.

  Cela permet de créer des groupes de travail de façon transparente par rapport à l'architecture physique du réseau ;
- **Gain de sécurité** : les groupes contenant des données sensibles sont séparés du réseau. Ces groupes sont le plus souvent constitués pour une durée brève et déterminée. Dans ce cas de figure, un VLAN pourrait être mis en place (sans déplacer les individus) en fonction des besoins ponctuels de ce groupe [5].

2.7.3 Les types d'association (comment le réseau identifie l'appareil)

Il existe trois types de VLAN **[6]:**

Les réseaux VLAN fondés sur les ports ;

- Les réseaux VLAN fondés sur les adresses MAC ;
- Les réseaux VLAN fondés sur les protocoles.

Différents types de VLAN sont établis en fonction du critère de commutation ainsi que du niveau auquel celle-ci est réalisée :

2.7.3.1. VLAN de niveau 1

Un VLAN de niveau 1, également désigné VLAN par port (Port-Based VLAN en anglais), constitue un réseau virtuel déterminé en fonction des ports de connexion sur le commutateur (figure 2.3).

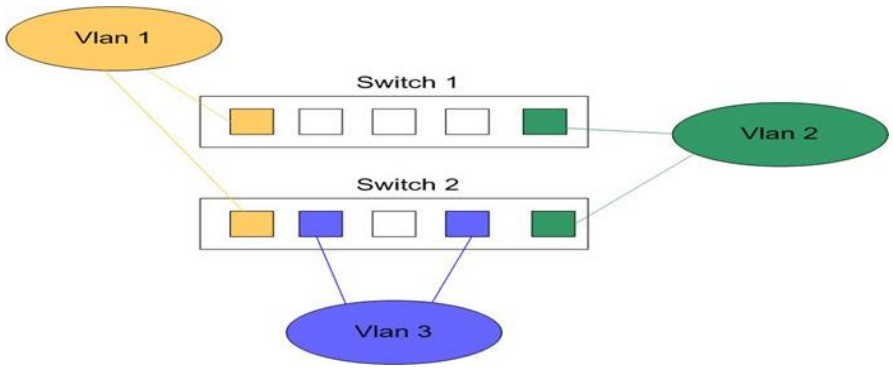


***Figure 2.21** : VLAN fondés sur les ports*

Avantage :

- Le principal avantage du VLAN par port est qu'il permet une étanchéité maximale des VLANs. Le PC pirate ne pourra être attaqué de l'extérieur qu'en le connectant à un port taggé. Ainsi, le pirate a besoin d'accéder à la machine physique pour pénétrer le VLAN

- L'administrateur peut aisément choisir les ports à taguer sans avoir d'information de la part des machines auxquelles sont reliés les ports.

Inconvénients :

- Le principal inconvénient du VLAN par port réside dans la nécessité d'une configuration lourde et contraignante sur chaque Switch. À chaque changement de poste, il est nécessaire d'adapter les commutateurs correspondants afin de conserver une qualité de service.
- Le mécanisme de VLAN par port n'offre pas d'architecture centralisée qui permettrait de pallier la lourdeur de la configuration. Chaque Switch a sa propre table de correspondance, sans tenir compte des autres commutateurs.

2.7.3.2. VLAN de niveau 2

Aussi appelé VLAN MAC, VLAN par adresse IEEE ou, en anglais, MAC Address-Based VLAN. Il consiste à définir un réseau virtuel d'après les adresses MAC des postes. Ce type de VLAN est beaucoup plus souple que le VLAN par port, car le réseau ne dépend pas de l'emplacement de la station (figure 2.4).

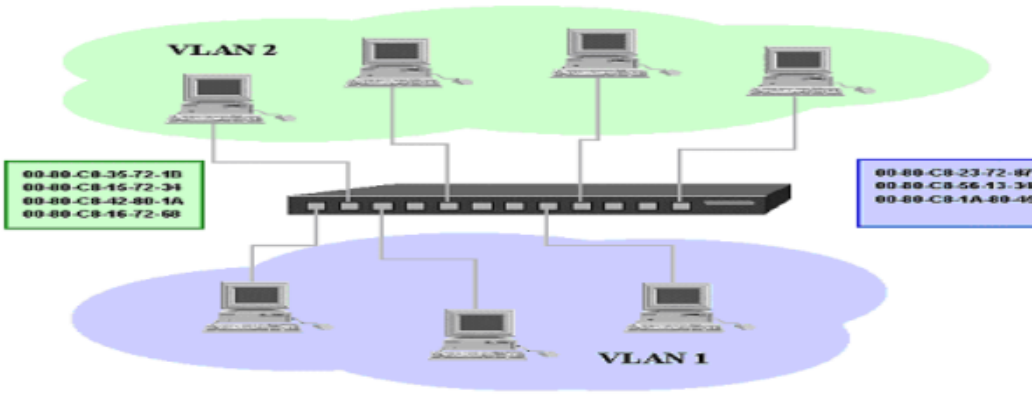


Figure 2.22: *les VLAN fondés sur les adresses MAC*

Avantages

- Les VLANs de niveau 2 offrent une sécurité au niveau de l'adresse MAC. En effet, un pirate qui voudrait se connecter au VLAN devrait d'abord obtenir une adresse MAC du VLAN pour pouvoir y accéder.

- Les VLANs de niveau 2 permettent de centraliser les tables VLANs d'adresses MAC. Chaque Switch interroge ensuite cette table afin d'obtenir les informations requises pour une adresse MAC donnée.

Inconvénients :

- Le VLAN de niveau 2 n'est pas aussi sécurisant que le VLAN par port car il est possible de spoofférer l'adresse MAC. Par ailleurs, il n'y a pas de contrôle de flux prévu, ce qui nécessite un bon dimensionnement du réseau.

2.7.3.3. VLAN niveau trois (VLAN par sous-réseau)

Les VLAN de niveau 3 permettent de regrouper plusieurs machines suivant le sous-réseau auquel elles appartiennent. La mise en place d'un VLAN de niveau 3 nécessite l'utilisation d'un protocole routable (IP, autres protocoles propriétaires, etc.). L'attribution des VLANs se fait automatiquement en décapsulant le paquet jusqu'à l'adresse source. Cette adresse va déterminer à quel Vlan appartient la machine (Figure 2.5).

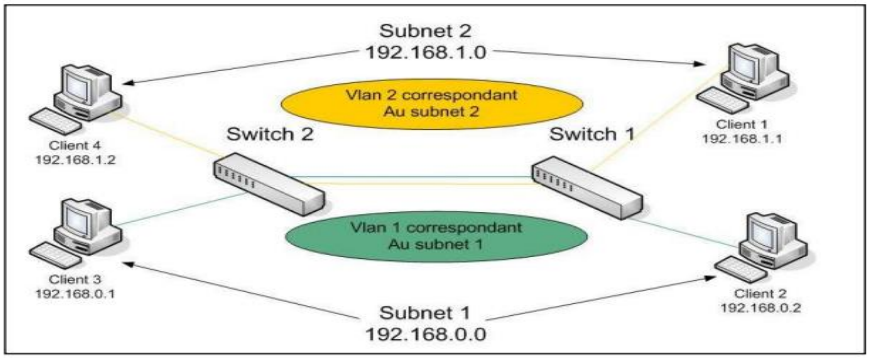


***Figure 2.23**: VLAN fondés sur les protocoles*

Avantage :

- Le principal avantage du VLAN de niveau 3 réside dans le fait qu'il autorise l'affectation automatique à un VLAN suivant une adresse IP. Ainsi, il suffit de configure les clients afin de les joindre aux groupes souhaités. On peut également dissocier les protocoles par VLAN.

Inconvénients :

- Les VLANs de niveau 3 sont plus lents que les VLANs de niveau 1 et 2. En effet, le switch doit décapsuler le paquet jusqu'à l'adresse IP afin de déterminer à quel VLAN il appartient.
- Les VLANs de niveau 3 sont limités par l'utilisation d'un protocole de routage afin d'obtenir l'identifiant de niveau 3 et de rejoindre ainsi le VLAN correspondant.

2.8 Différents Types de VLAN

Il existe différents types de VLAN utilisés dans les réseaux modernes. Certains types de VLAN sont définis par les classes de trafic. D'autres types de VLAN sont définis par leur VLAN sont définis par leur fonction spécifique (ou rôle).

2.8.1 VLAN de données

Un VLAN de données est un réseau local virtuel configuré pour transmettre le trafic généré par l'utilisateur. Dans ce type de VLAN, les postes et les appareils partagent le même segment logique et peuvent communiquer entre eux. Cela permet de regrouper les utilisateurs en fonction de leurs besoins spécifiques, tels que les départements, les équipes ou les services, tout en les isolant du trafic d'autres VLAN. Les VLAN de données sont également appelés VLAN utilisateur.

2.8.2 VLAN par défaut

Tous les ports de commutateur font partie du VLAN par défaut après le démarrage initial d'un commutateur chargeant la configuration par défaut. Les ports de commutateur qui participent au VLAN par défaut appartiennent au même domaine de diffusion. Cela permet à n'importe quel périphérique connecté à n'importe quel port du commutateur de communiquer avec d'autres périphériques sur d'autres ports du commutateur.

2.8.3 VLAN natif

Un réseau local virtuel natif (VLAN natif) est associé à un port trunk 802.1Q. Les ports trunk sont les liaisons entre les commutateurs qui permettent la transmission du trafic associé à plusieurs VLAN. Un port trunk 802.1Q prend en charge le trafic provenant de nombreux VLAN, qu'il s'agisse de trafic étiqueté ou de « tagged traffic ». Le VLAN natif est essentiel pour gérer correctement les trames non étiquetées et faciliter la communication initiale entre les appareils avant toute configuration VLAN spécifique.

2.8.4 VLAN de gestion

Un VLAN est un VLAN aux fonctionnalités de gestion du commutateur, telles que la configuration, la surveillance et la maintenance. Pour créer le VLAN de gestion, l'interface virtuelle spécifiquement configuré pour gérer et administrer un commutateur réseau. Il est souvent utilisé pour accéder du commutateur (SVI) de ce VLAN se voit attribuer une adresse IP et un masque de sous-réseau. Cela permet de gérer le commutateur via des protocoles tels que HTTP.

2.8.5 VLAN de voix

Le VLAN de voix est configuré pour acheminer le trafic vocal. Les VLAN vocaux bénéficient pour la plupart d'une priorité de transmission élevée par rapport aux autres types de trafic réseau. Pour garantir la qualité de la voix sur IP (VoIP) (délai inférieur à 150 millisecondes (ms) sur le réseau), nous devons disposer d'un VLAN voix séparé car cela préservera la bande passante pour les autres applications.
Les VLAN dynamiques prennent en charge la mobilité instantanée des périphériques finaux. Lorsque nous déplaçons un périphérique d'un port à un autre d'un commutateur, les VLAN dynamiques configurent automatiquement l'appartenance au VLAN.

2.9 Agrégation de VLAN :

L'agrégation de VLAN, aussi appelée trunking, est une technique qui permet de regrouper plusieurs VLAN sur une seule liaison physique entre deux commutateurs (ou entre un commutateur et un routeur).

Le trunking est souvent utilisé pour relier les commutateurs de niveau d'accès aux commutateurs de niveau de distribution ou aux routeurs. Il permet de transporter avec efficacité le trafic de plusieurs VLAN sur une connexion unique. Les protocoles des plus utilisés sont IEEE 802.1Q et ISL (Inter-Switch Link).

2.9.1 IEEE 802.1Q :

La norme IEEE 802.1Q définit le contenu de la balise de VLAN (VLAN tag). Il ne s'agit pas d'une nouvelle encapsulation, mais plutôt de l'ajout d'une étiquette, ou TAG, dans l'en-tête de la trame (un ensemble de champs placé juste après le champ d'adresse MAC d'origine). Comme le cadre sera modifié, le commutateur recalculera la valeur du champ FCS. Cette étiquette occupe 4 octets, soit 32 bits (Figure 2.6).

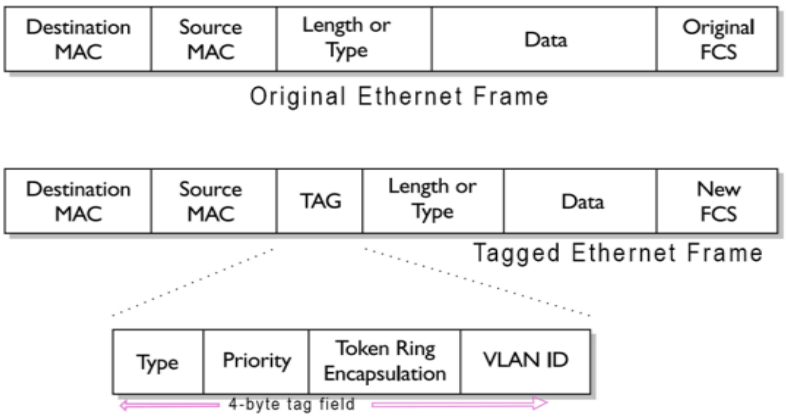


Figure 2.24: *IEEE 802.1Q*

2.9.2. ISL (Inter-Switch Link)

Le protocole ISL (Inter-Switch Link) est une méthode de trunking qui permet de faire passer les VLANs dans le réseau. Ce protocole a été créé par Cisco pour aider les commutateurs à identifier les différents VLAN sur la liaison trunk (figure 2.7).

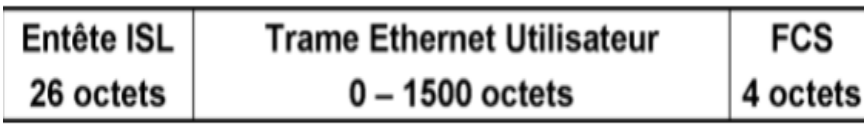


Figure 2.25: *ISL (Inter-Switch Link)*

2.10 VTP (Protocole de Trunking Virtuel)

Le protocole VTP (VLAN Trunking Protocol) sert à configure et à gérer les VLAN sur les appareils CISCO [6]. Il permet d'ajouter, de renommer ou de supprimer un ou plusieurs réseaux locaux virtuels sur un seul switch, et cette nouvelle configuration est diffusée à tous les autres commutateurs du réseau. Le VTP aide à éviter les problèmes de configuration de VLAN dans tout un réseau local.

Les modes VTP Le switch possède 3 modes VTP : client, transparent ou server (actif par défaut) :

- En mode client : il est rattaché à un domaine VTP. Les VLAN sont déclarés sur le serveur. Il met à jour la liste des VLAN déclarés et la diffusée à tous les clients ;
- En mode transparent : Il transmet les informations VTP aux autres switchs mais ne les traite pas. Ces switchs sont indépendants et ne prennent pas partie aux VTP ; Il est rattaché à un domaine VTP. Il reçoit la liste des VLAN, la propage aux autres clients connectés et met à jour sa propre liste.
- En mode serveur : il diffuse ses informations VTP à tous les autres switchs du même domaine VTP. Ces informations sont enregistrées en NVRAM et sur un tel commutateur, on peut créer, modifier ou supprimer un VLAN du domaine VTP.
  Aucun domaine VTP ne lui est associé. Sa liste de VLAN est locale et ne se met pas à jour lorsqu'il reçoit une trame VTP. IL propage toutefois les listes de VLAN qu'il reçoit.

2.11 Mode Access et Mode trunk

Dans un réseau local commuté, la gestion du trafic entre les différents VLANs nécessite des mécanismes adaptés afin d'assurer une communication efficace et sécurisée [5]. Les commutateurs utilisent principalement deux modes de configuration des ports : le mode access et le mode trunk. Ces deux modes jouent un rôle essentiel dans l'organisation et le transport des données au sein d'une architecture VLAN, en permettant soit l'affectation d'un seul VLAN à un port, soit la transmission simultanée de plusieurs VLANs sur un même lien.

2.11.1 Mode trunk

Pour relier plusieurs réseaux locaux virtuels et les répartir sur différents équipements, il faut créer une méthode de partage des réseaux entre ces équipements. Cette La technique sert à marquer les trames pour reconnaître le trafic des différents réseaux locaux sur un même canal. Ainsi, les réseaux locaux sont répartis sur les différents appareils par des connexions logiques spéciales appelées lignes réseau.

Le trunk est une seule connexion physique qui transporte le trafic de plusieurs réseaux virtuels. Passer par le tronc est complété avec un identifiant de réseau local virtuel (VLAN id). Grâce à cette identification, les trames restent dans le même VLAN (Figure 2.8).

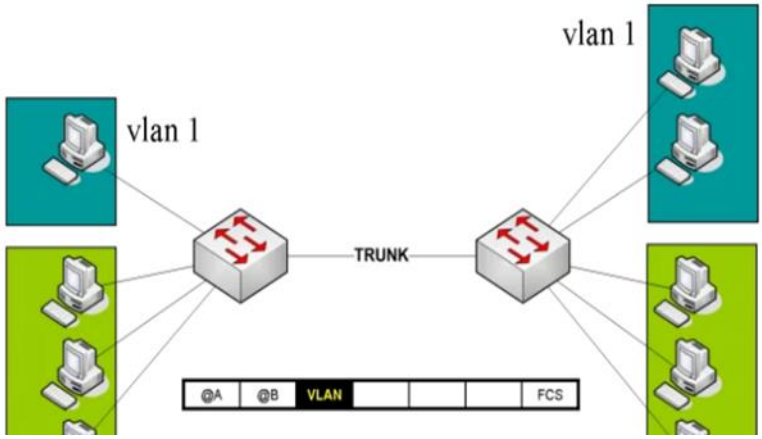


Figure 2.26: *mode trunk*

Les trunks peuvent être utilisés :

- Entre deux commutateurs : C'est le mode de connexion le plus courant dans les réseaux locaux. En utilisant des trunks entre deux commutateurs, on fait passer le trafic de plusieurs VLAN sur une seule connexion, ce qui simplifie la gestion et la répartition du trafic dans le réseau local.
- Entre un switch et un ordinateur : C'est un fonctionnement à suivre de près. Lorsqu'un hôte prend en charge le trunking, il peut analyser le trafic. De tous les réseaux locaux virtuels ils auxquels il est connecté. Il est relié. Cela peut créer des problèmes de sécurité ou de confidentialité si le trafic n'est pas bien séparé ou filtré.

- Entre un switch et un routeur : C'est le fonctionnement qui permet d'accéder aux fonctions de routage, notamment pour connecter les réseaux virtuels par routage inter-VLAN. En En dépendant d'un commutateur sur un routeur avec un trunk, le routeur peut acheminer le trafic entre les différents VLAN, permettant ainsi leur connexion. Cela règle le premier problème, qui est l'interconnexion des VLAN.

2.11.2 Mode Access

Le mode Access est le mode par défaut des ports d'un commutateur. Il est principalement utilisé pour connecter des équipements terminaux tels que les ordinateurs, les imprimantes, les serveurs ou les téléphones IP.

Dans ce mode, le port est associé à un seul VLAN (appelé VLAN d'accès). Toutes les trames qui entrent ou sortent de ce port appartiennent à ce VLAN unique. Lorsque le commutateur reçoit une trame provenant d'un équipement connecté à un port Access, cette trame est **non taguée** Le switch ajoute en interne l'identifiant du VLAN correspondant avant de la transmettre dans le réseau (Figure 2.9).

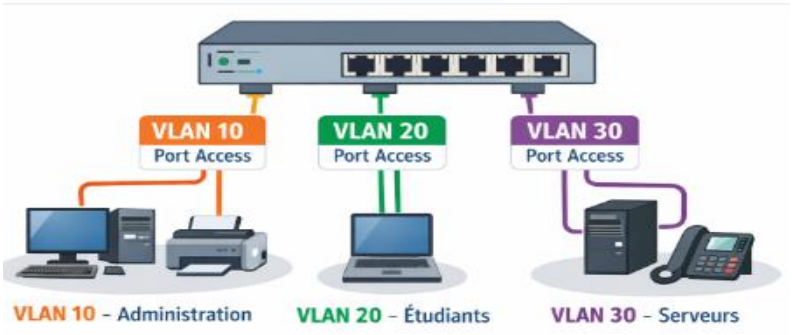


Figure 2.27 : Affectation des ports access aux VLANs

2.12 Routage entre VLAN

Le routage inter-VLAN permet de faire passer le trafic d'un VLAN à un autre avec un appareil de couche 3 comme un routeur ou un commutateur multicouche. Chaque VLAN est un domaine de diffusion à part, et chaque VLAN a une adresse IP. Si un ordinateur veut communiquer avec une adresse IP en dehors de son réseau, il doit passer par sa passerelle par défaut, qui permet de relier plusieurs réseaux différents.

2.13 Importance du routage entre les VLANs

Le routage entre les VLAN est très important dans les réseaux informatiques. Il permet de diviser le trafic réseau selon les besoins de chaque VLAN, ce qui améliore les performances et la sécurité du réseau. Avec le routage inter VLAN, les utilisateurs peuvent accéder aux ressources partagées et communiquer, même s'ils sont dans des VLAN différents. Cette méthode permet d'organiser et de gérer le réseau plus facilement, ce qui aide à mieux contrôler les données et à utiliser les ressources de manière optimale.

2.14 Les façons de router entre les VLAN.

Il y a 3 façons de router entre les VLAN.

- Routage inter-VLAN hérité : Il s'agit d'une solution ancienne.
- Router-on-a-Stick : C'est une solution acceptable dans le cas d'un réseau de petite et moyenne taille.
- Switch de couche 3 avec des interfaces virtuelles commutées (SVI) : il s'agit d'une solution adéquate pour un réseau de petite et moyenne taille.

2.14.1 Routage inter-VLANS hérité

La première solution de routage inter-VLAN utilisant des routeurs disposant de plusieurs interfaces Ethernet. Chaque interface devait être connectée à un port de commutateur dans des VLAN différents. Les interfaces du Le routeur a été utilisé comme passerelle par défaut vers les hôtes locaux du sous-réseau VLAN. Par exemple, prenez la topologie où R1 a deux interfaces connectées au commutateur S1 (figure 2.10).

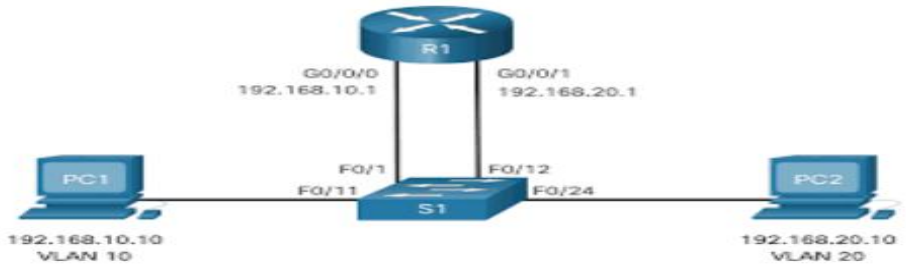


Figure 2.28 : *exemple de routage inter-VLAN*

Il convient de noter que, dans l'exemple, la table des adresses MAC de S1 est renseignée de la manière suivante :

- Le port Fa0/1 est attribué au VLAN 10 et relié à l'interface G0/0/0 du routeur R1.
- Le port Fa0/11 est attribué au VLAN 10 et relié au PC1.
- Le port Fa0/11 est attribué au VLAN 20 et relié à l'ordinateur PC2.
- Le port Fa0/12 est attribué au VLAN 20 et relié à l'interface R1 G0/0/1

Port	**Adresse MAC**	**VLAN**
F0/1	R1G0/0/0MAC	10
F0/11	PC1MAC	10
F0/12	R1G0/0/1MAC	20
F0/24	PC2MAC	20

***Tableau 2.1** : Table d'adresses MAC pour S1*

Lorsqu'un paquet est envoyé de PC1 à PC2 situé sur un réseau différent, il est transféré vers la passerelle par défaut 192.168.10.1. R1 réceptionne le paquet via son interface G0/0/0 et analyse l'adresse de destination associée. R1 transmet ensuite le paquet via son interface G0/0/1 au port F0/12 du VLAN 20 sur S1. Enfin, S1 relais la trame vers PC2.

La méthode traditionnelle de routage inter-VLAN reposant sur des interfaces physiques demeure opérationnelle, mais elle comporte une contrainte majeure. Il ne présente pas une évolutivité raisonnable en raison du nombre restreint d'interfaces physiques disponibles sur les routeurs. L'obligation de Le fait de disposer d'une interface physique de routeur par VLAN épuise rapidement la capacité du routeur.

2.14.2 Routage inter-VLAN avec la méthode router-on-a-stick

La configuration « router-on-a-stick » est un type de configuration de routeur dans lequel une seule interface physique sert à acheminer le trafic entre plusieurs VLAN d'un réseau. Le routeur est connecté au commutateur S1 par le biais d'une seule liaison physique (un tronc). L'interface du routeur est configurée pour fonctionner en mode tronçon et est connectée à un port du commutateur configuré en mode tronçon. Le routeur réalise le routage inter-VLAN en recevant le trafic portant l'étiquette VLAN sur l'interface trunk du commutateur voisin. Il effectue ensuite le routage interne entre les VLAN grâce à des sous-interfaces. Le routeur transfère alors le trafic acheminé, étiqueté VLAN vers le VLAN de destination, depuis la même interface physique qui a reçu le trafic. Les sous-interfaces sont des interfaces virtuelles créées par logiciel, qui sont liées à une seule interface physique. Le logiciel permet de configure les sous-interfaces sur un routeur. Chaque sous-interface est configurée séparément avec une adresse IP et une affectation VLAN. Les sous-interfaces sont configurées pour différents sous-réseaux correspondant à leur affectation VLAN afin de permettre le routage logique. Dés qu'une décision de routage a été prise en fonction de la destination VLAN, les trames de données sont étiquetées VLAN et renvoyées depuis l'interface physique (Figure 2.11).

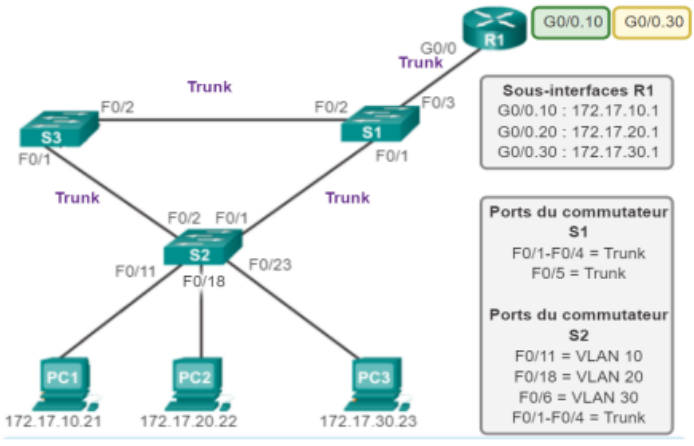


Figure 2.29 : *routage inter vlan de type router-on-a-stick*

- Le PC1 qui se trouve dans le VLAN 10 veut échanger avec le PC3 qui appartient au VLAN 30. Cette la communication est faite par le routeur R1 avec une seule interface physique qui est configurée avec des sous-interfaces.

- Le PC1 envoie les trames au commutateur S2 en premier lieu.

- Le commutateur S2 associe ces trames au VLAN 10 en leur ajoutant une étiquette VLAN, puis les transmet au commutateur S1 par le biais d'une liaison trunk.
  Une fois les trames reçues

- le commutateur S1 les transmet vers le routeur R1 à travers le port trunk F0/5.

- Le routeur R1 reçoit les trames du VLAN 10, réalise le routage inter-VLAN, et oriente le trafic vers le VLAN 30 grâce aux sous-interfaces configurées.
  Avant de rediriger les trames vers le réseau .le routeur y ajoute l'étiquette correspondante au VLAN 30.

- Le commutateur S1 reçoit alors les trames marquées VLAN 30 et les transmet vers S2 à travers la liaison trunk.

- le commutateur S2 enlève l'étiquette VLAN et transmet les trames au PC3 qui est connecté sur le port F0/6.

2.14.3 Commutateur de couche 3 utilisant des interfaces virtuelles commutées (SVI) :

La méthode moderne d'exécution du routage inter-VLAN consiste à utiliser des commutateurs de couche 3 et des interfaces virtuelles commutées (SVI). Une interface SVI est une interface virtuelle configurée dans un commutateur de couche 3 (Figure 2.12).

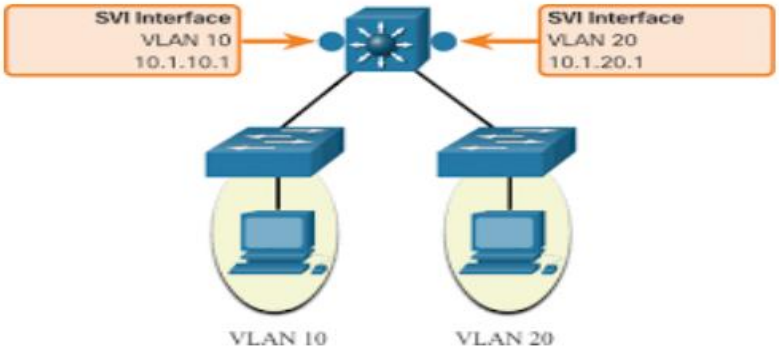


Figure 2.30 : *exemple de routage inter VLAN de communication de couche 3*

Conclusion :

Ce chapitre nous a permis de présenter les notions essentielles des réseaux locaux et des VLAN. Ces deux concepts pratiques sont très fondamentales théocratiquement et pratiquement. On a présenté alors leurs définitions, types, avantages et inconvénients, méthodes de fonctionnement, ainsi que les notions en relation (mode Access, mode trunk), les différents types de routage employés, etc.

Chapitre 03

Présentation de l’entreprise et du logiciel Cisco Packet Tracer

Introduction :

Ce troisième chapitre est réservé à l'étude de réseau existant dans l'entreprise Naftal Saida GPL et sa configuration. Tout d'abord nous allons présenter un bref aperçu de Naftal pour mieux connaitre sa structure et son organigramme des départements et services. Ensuite nous allons donner un aperçu sur le simulateur Cisco Packet Tracer utilisé pour faire la simulation de ce réseau.

3.1 Historique de NAFTAL :

NAFTAL est une entreprise nationale qui a été fondée en 1999 à la suite de la fusion de plusieurs entreprises algériennes spécialisées dans la distribution des produits pétroliers. Cette initiative visait à rationaliser et à centraliser la gestion de la distribution des produits énergétiques dans tout le pays [7]. Depuis sa création, NAFTAL est devenue un acteur majeur dans le secteur de l'énergie en Algérie. L'entreprise gère une vaste infrastructure de stations-service, de réservoirs de stockage et de réseaux de distribution pour assurer l'approvisionnement du pays en essence, gasoil, GPL (gaz de pétrole liquéfié), et autres produits dérivés du pétrole.

Dans ce cadre, les unités GPL qui lui sont rattachées occupent une place stratégique dans l'approvisionnement énergétique des citoyens et des différents secteurs économiques, en particulier dans les régions fortement dépendantes de cette source d'énergie.

Parmi ces unités figure l'unité GPL de Saïda, intégrée au réseau de Naftal, qui assure des missions essentielles de stockage et de distribution du GPL à l'échelle de la wilaya de Saïda ainsi que des régions limitrophes. Cette unité contribue ainsi à garantir la continuité du service public et à répondre de manière efficace et régulière à la demande locale en gaz de pétrole liquéfié.

3.2 Présentation de l'unité Naftal- GPL de Saida :

L'unité GPL de Saïda, relevant de la société Naftal, constitue une structure opérationnelle importante au sein du réseau national de distribution du gaz de pétrole liquéfié en Algérie. Sa mission principale consiste à réceptionner, stocker et distribuer le GPL afin d'assurer

l'approvisionnement du marché local au niveau de la wilaya de Saïda ainsi que des régions avoisinantes.

L'unité GPL de Saïda a été créée dans le cadre de l'expansion du réseau de Naftal au cours des années ayant connu le développement du secteur de distribution du gaz de pétrole liquéfié en Algérie

Cette unité est implantée au niveau de la ville de Saïda, dans la zone industrielle (Figure 3.1).

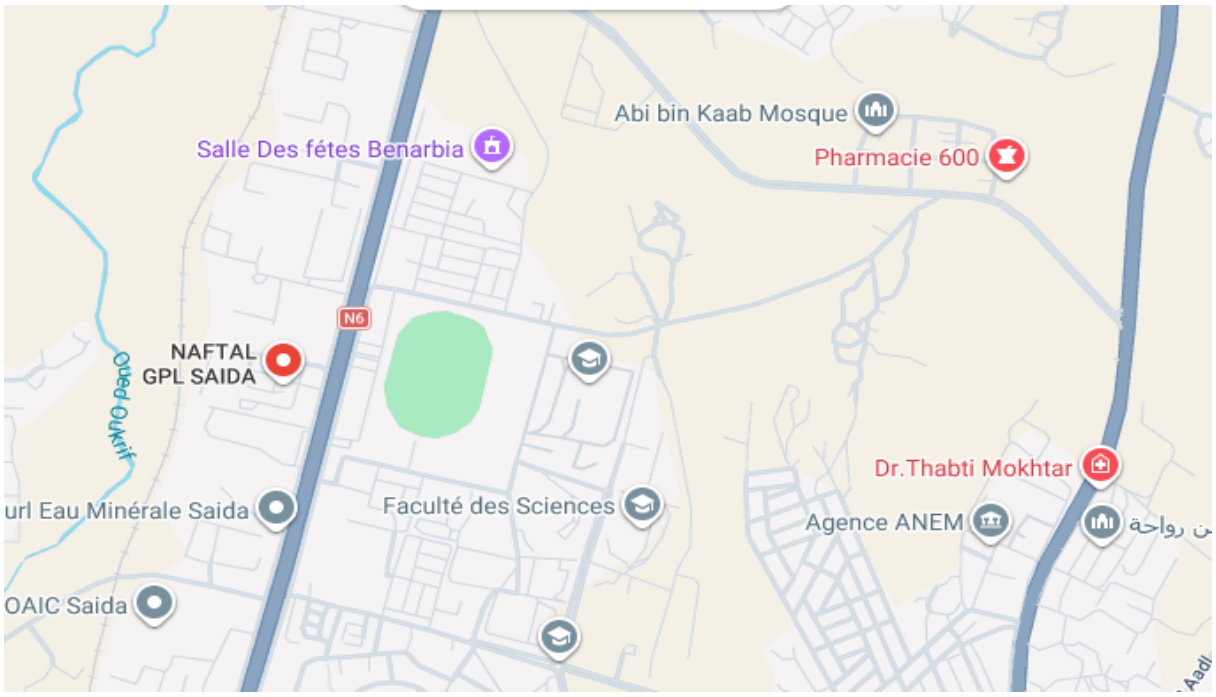


***Figure** 3.31: localisation du l'unité Naftal GPL Saida*

3-3 Organisation générale de la branche GPL :

(Source NAFTAL, branche GPL - Saida)

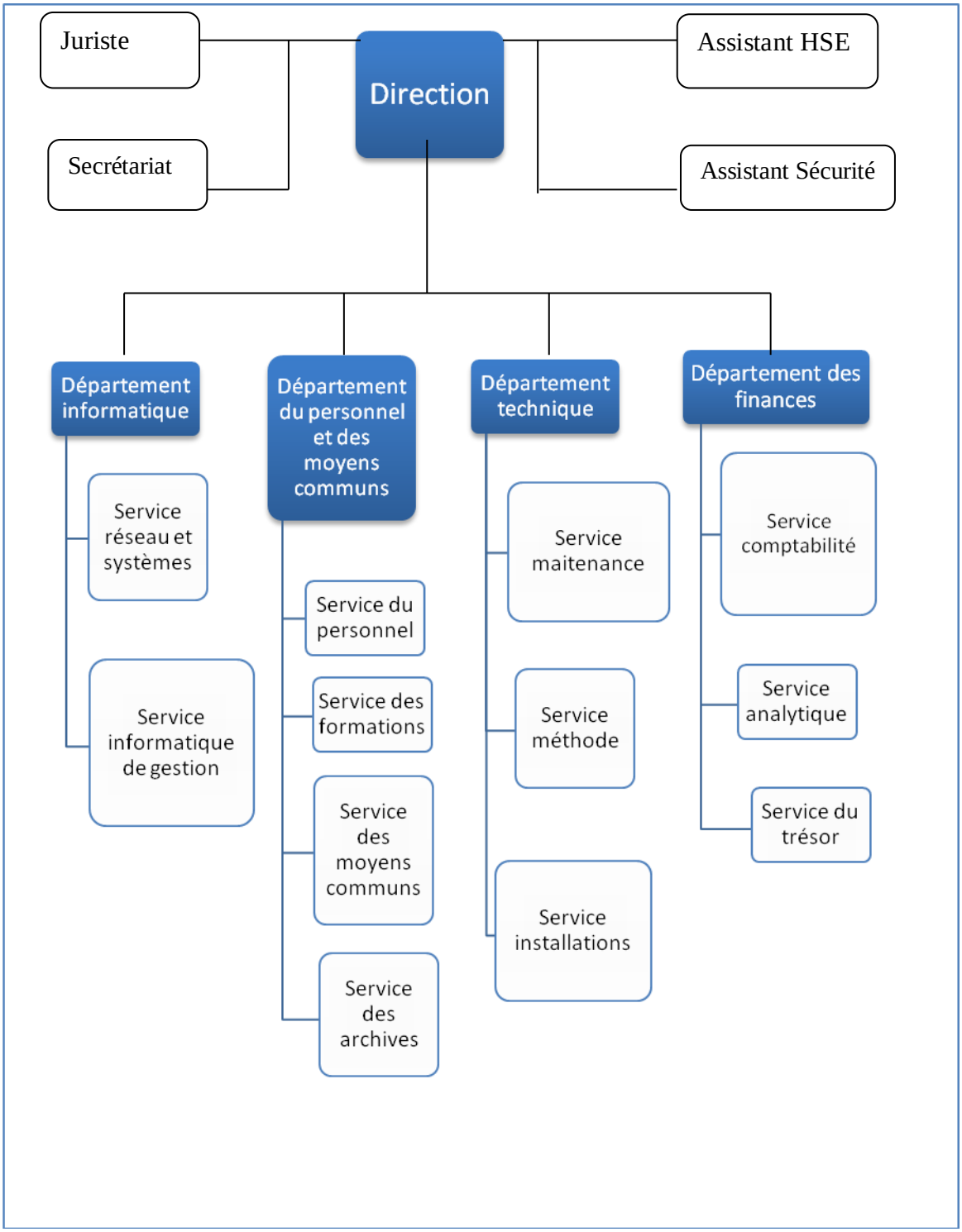


Figure 3.32 : organigramme de NAFTAL Saida GPL

3.4 Présentation des départements

*** Département du personnel et des moyens communs** :

Ce département assure la gestion administrative, paie, prestations sociales et des Moyens généraux du district confirmeront aux procédures et réglementation en vigueur.

*** Département des finances et comptabilité** :

Il coordonne toutes les activités de comptabilité, trésorerie et budget du patrimoine. Il assure ainsi la gestion financière, comptable et fiscale du district conformément à la réglementation et procédures en vigueur

*** Département informatique** :

Ce département a comme finalité de garantir la continuité du service des systèmes informatiques déployés au niveau des districts et centres opérationnels ; d'assurer le support aux utilisateurs des systèmes installés et la sécurité des données et systèmes informatiques. Il veille aussi à la mise à disposition des informations de gestion vers les structures du district, les branches et structures centrales

*** Département technique & maintenance** :

Ce département assure la réalisation des objectifs de la maintenance des installations fixes et du matériel roulant du district conformément aux procédures et réglementation en vigueur.

3.5 Missions et fonctions de l'entreprise

Les missions principales de Naftal sont directement liées à son rôle dans le secteur énergétique. Elles peuvent être regroupées en plusieurs fonctions essentielles :

- **Gestion commerciale :**

Elle consiste à assurer la vente et la distribution des produits pétroliers. Cette fonction inclut la gestion des clients, le traitement des commandes et le suivi des transactions.

- **Gestion logistique :**

Cette fonction est responsable du suivi des stocks, du transport des produits et de la gestion des dépôts. Elle garantit la disponibilité des produits sur tout le territoire.

- **Gestion administrative et financière :**

Elle englobe la comptabilité, la gestion des ressources humaines et le suivi financier des opérations de l'entreprise.

- **Communication interne et externe :**

Elle assure la circulation de l'information entre les différents services et avec les partenaires externes.

- **Gestion des bases de données :**

Toutes les informations sont centralisées dans des bases de données permettant un accès rapide et sécurisé.

Ces missions nécessitent un réseau informatique performant capable de supporter un grand volume d'échanges de données.

Dans ce contexte, le système d'information joue un rôle essentiel pour assurer la communication entre les services, la gestion des données et l'accès aux applications métiers.

3.6 Analyse des besoins

3.6.1 Besoins fonctionnels

Les besoins fonctionnels représentent les services que le réseau doit fournir aux utilisateurs :

- Connexion réseau pour tous les employés de l'entreprise.
- Accès sécurisé à Internet pour les opérations professionnelles.
- Partage de fichiers et d'imprimantes pour faciliter la collaboration.
- Accès aux applications métiers (gestion commerciale, bases de données).
- Mise en place d'un système de communication pour les appels internes.

Ces besoins permettent d'assurer la continuité du travail et d'améliorer la productivité.

3.6.2 Besoins non fonctionnels

Les besoins non fonctionnels concernent les performances et la qualité du réseau :

- Haute disponibilité du réseau
- Sécurité des données sensibles
- Performance et rapidité de transmission
- Évolutivité pour répondre à l'augmentation du nombre d'utilisateurs

3.7 Type de réseau utilisé

Le réseau proposé est un réseau local d'entreprise (LAN) basé sur une architecture hiérarchique. Cette architecture est composée de trois couches principales :

- Couche d'accès Elle permet de connecter directement les utilisateurs (PC, imprimantes, téléphones IP). Elle constitue le point d'entrée du réseau.
- Couche de distribution Elle joue un rôle intermédiaire en assurant : le routage entre VLAN, la gestion des politiques de sécurité et le contrôle du trafic réseau.
- Couche cœur (Core) Elle représente la partie centrale du réseau. Elle est responsable du transport rapide des données avec une très faible latence.

3.8. Sécurité du réseau

La sécurité est un élément fondamental dans la conception du réseau de Naftal, car les données manipulées sont sensibles.

*** Pare-feu (Firewall)**

Le pare-feu permet de filtrer le trafic entrant et sortant afin de bloquer les accès non autorisés.

*** VLAN (Virtual Local Area Network)**

Les VLAN permettent de segmenter le réseau en plusieurs zones logiques (administration, finance, technique), ce qui améliore la sécurité et réduit les risques de propagation d'attaques.

*** ACL (Access Control List)**

Les ACL définissent des règles d'accès précises pour contrôler les communications entre les différents réseaux.

3.9 Matériel utilisé :

Dans le cadre de la conception de ce réseau local d'entreprise, un ensemble d'équipements réseau professionnels a été sélectionné afin de garantir la performance, la sécurité et la fiabilité de l'infrastructure.

Equipement	**type**	**nombre**
Routeur	Cisco1900	01
Firewall	Cyberoam CR750	01
Switch fédérateur	4507 R-E	01
Switchs	Switch 24 ports Catalyst2960	03
PC		25
Câble fibre optique		2000 m
Imprimante		08

***Tableau 3.2**: listes des équipements utilisés*

3.10 Présentation du logiciel Packet Tracer :

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

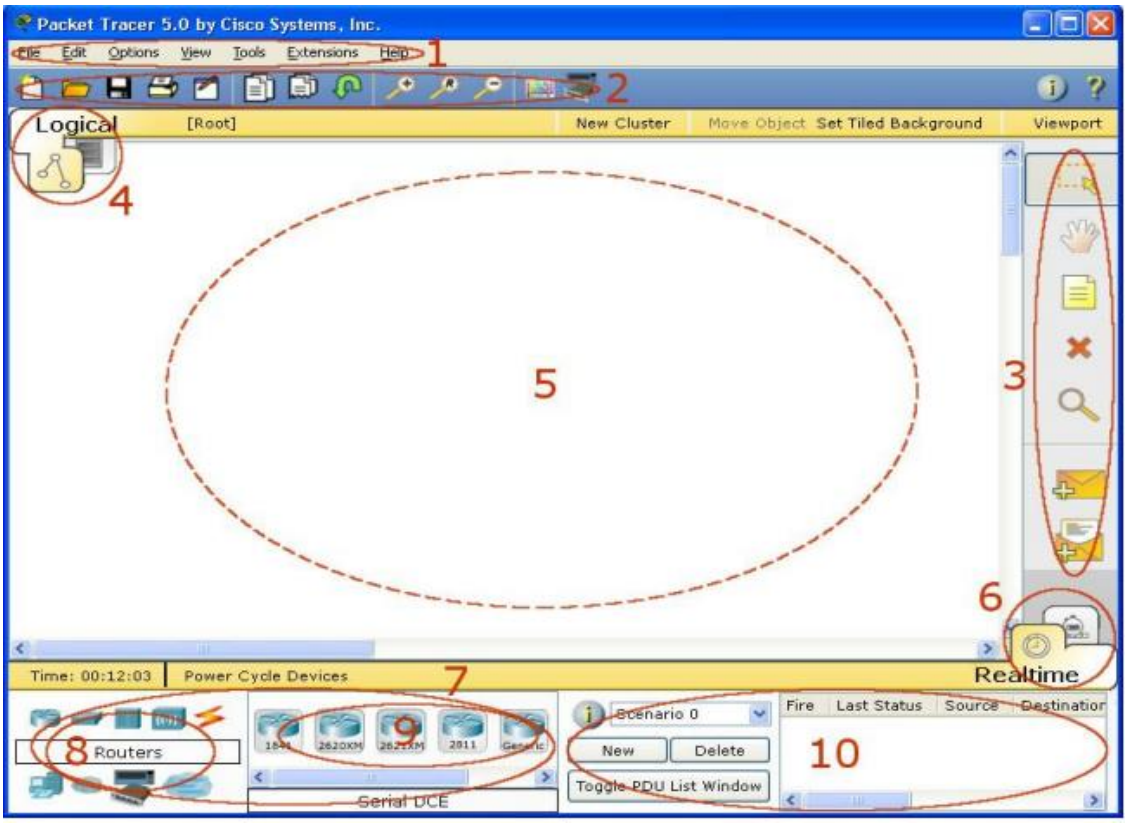


Figure 3.33: *Fenêtre de démarrage de Packet Tracer*

01	Barre de menu	Cette barre fournit le dossier, l'édite, d'option, de vue, d'outils, de prolongements, et d'aide. on trouve des commandes de base telles qu'ouvrir, sauvegarder, imprimer, et les préférences dans ces menus. On peut également accéder au magicien d'activité du menu de prolongements.
2	Barre Principale d'outils	Cette barre fournit des icônes de raccourci au dossier et édite des commandes de menu. Cette barre fournit également des boutons pour le Zoom, la palette de dessin, et le directeur de calibre de dispositif. Du côté droit, on trouve également le bouton de l'information de réseau, qu'on peut utiliser pour écrire une description pour le réseau courant.
3	Barre courante d'outils	Cette barre permet d'accéder à ces outils couramment utilisés de zone de travail : Choisir, déplacer, placer la note, supprimer, ajouter la PDU simple, et ajouter la PDU complexe.
4	Zone de travail logique et physique et barre de navigation	On peut basculer entre la zone de travail physique et la zone de travail logique avec les languettes sur cette barre. Dans la zone de travail logique, cette barre permet de grouper des éléments en un seul groupe pour alléger le schéma. Dans la zone de travail physique, cette barre permet de produire une ville neuve, produire une construction neuve, construire une armoire pour les équipements, appliquer la grille du fond.
5	Espace de travail	C'est la zone où on créera notre réseau, observeras des simulations, et visualiseras beaucoup de genres d'information et de statistiques
6	Barre du mode temps réel/ simulation	On peut basculer entre le mode en temps réel et le mode de simulation avec les tabulateurs sur cette barre et des boutons de contrôle de jeu et le bouton de basculeur de liste d'événement en mode de simulation. En outre, elle contient une horloge qui affiche le temps relatif en mode en temps réel et mode de simulation.
7	Cadre des composants de Réseau	On y trouvera les différents éléments du réseau (câbles, routeurs, switchs, etc.), il contient les dispositifs types et les dispositifs réseaux.
8	Dispositif-type	Ce cadre contient le type des dispositifs et de connexions disponibles dans le logiciel. Le cadre Dispositif-Particulier changera selon le type de dispositif qu'on choisit.

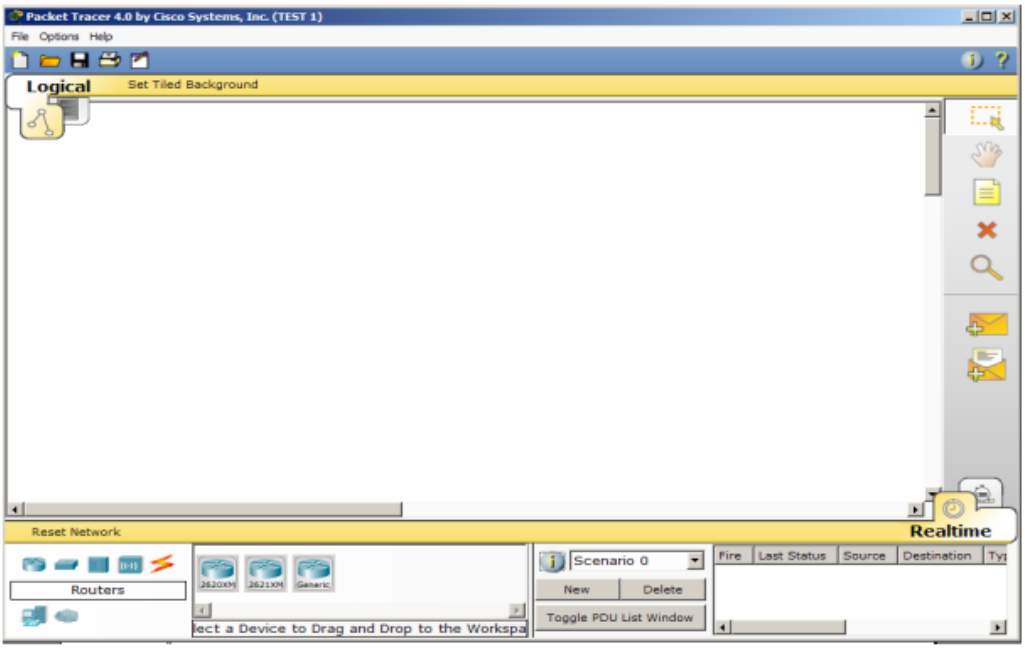
9	Dispositif particulier	Une fois le dispositif-type choisit, on a les différents types du dispositif choisit.
10	Fenêtre de contrôle des paquets	Cette fenêtre contrôle les paquets que tu mets dans le réseau pendant les scénarios de simulation.

3.11 Utilisation de Packet Tracer :

Pour utiliser Packet Tracer il suffit de suivre les étapes suivantes :

3.11.1 Lancement de Packet Tracer :

La fenêtre de démarrage apparaît comme suit :



3.11.2 Sélection des équipements:

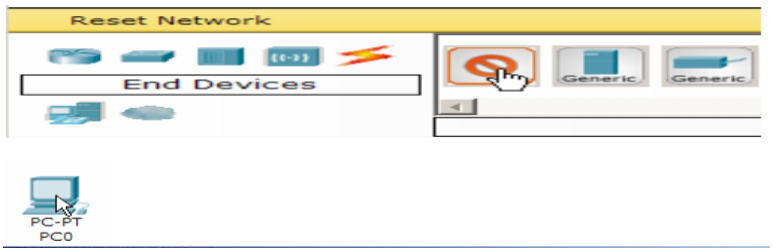
Routeurs

switches

Connexions

Pour utiliser un appareil ou une connexion, il suffit de le choisir et de le positionner dans l'espace de travail.

Exemple : choix d'un ordinateur.



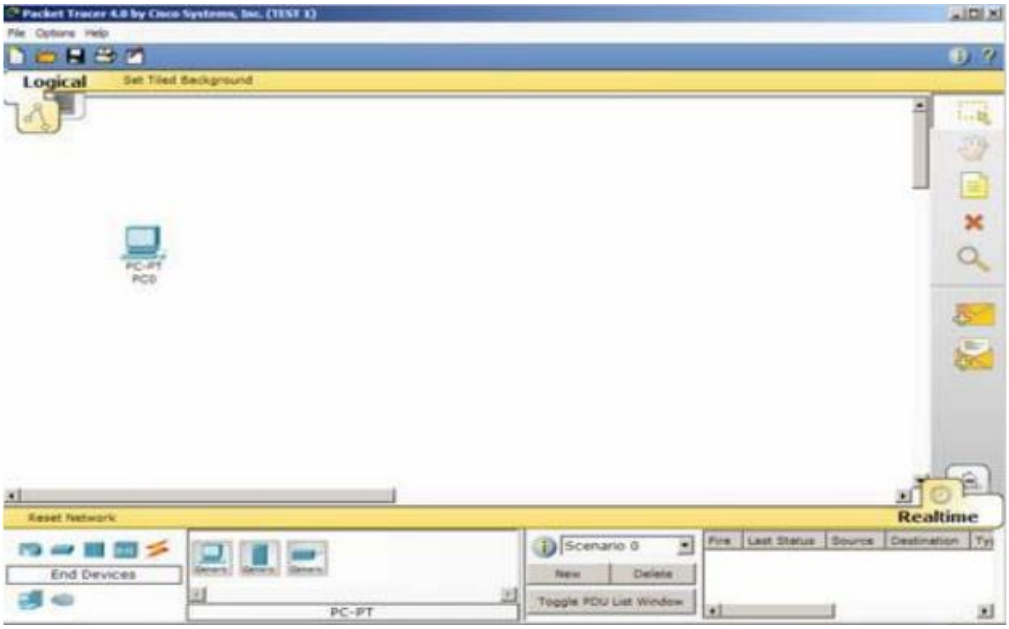
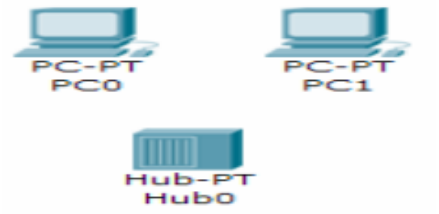


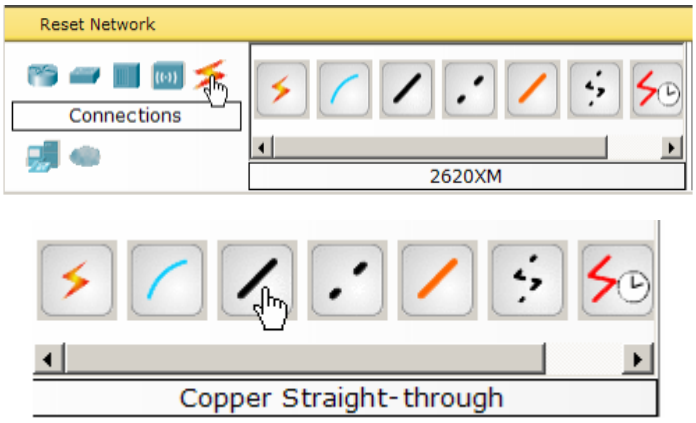
Figure 3.34 : *sélection d'un PC sur Packet Tracer*

3.11.3 Sélection des Connexions :

On va réaliser un exemple de connexion entre un HUB et un PC :

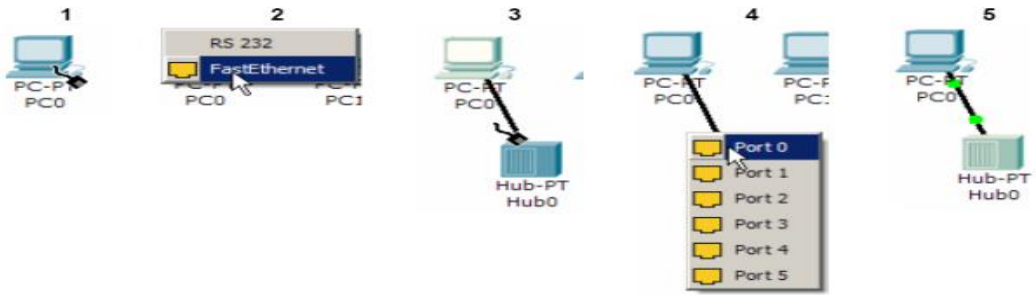


On sélectionne la partie connexion

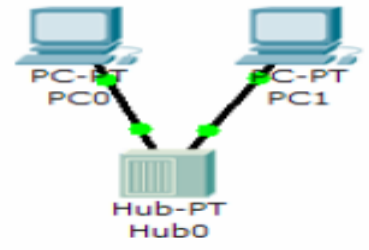


1. Cliqueter une fois sur **PC0**
2. Choisir Fast Ethernet
3. Traîner le curseur jusqu'au **Hub0**
4. Cliqueter une fois sur **Hub0** et choisir le port **0**

5. L'apparence des lumières vertes de lien sur le NIC de l'Ethernet **PC0** et **Hub0** montre qui le lien est en activité.



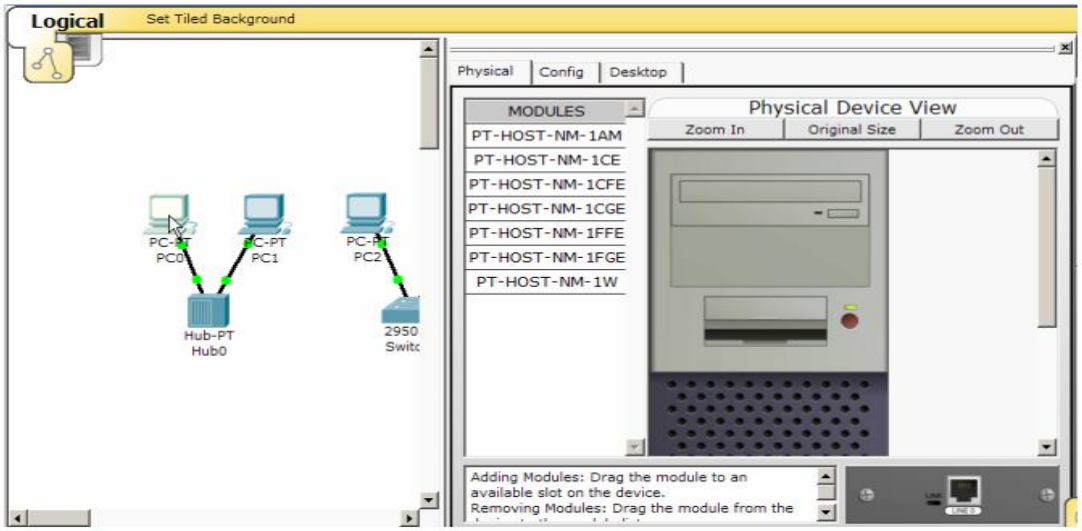
Il faut refaire les mêmes opérations pour connecter le deuxième PC.



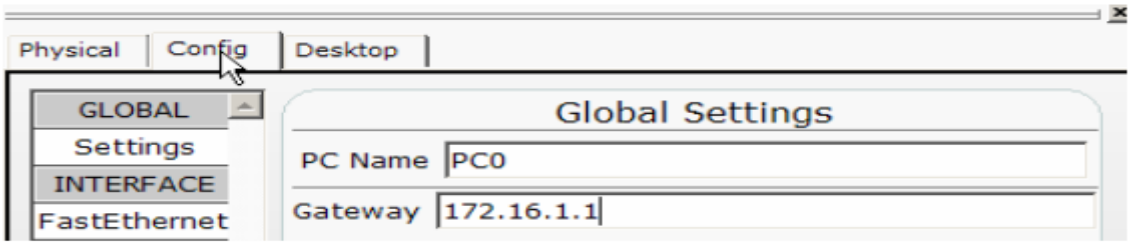
3.11.4 Configuration des adresses IP, et les masques de sous réseaux :

Avant que nous puissions communiquer entre les centres serveurs nous devons configure des adresses d'IP et des masques de sous réseau en fonction des équipements :

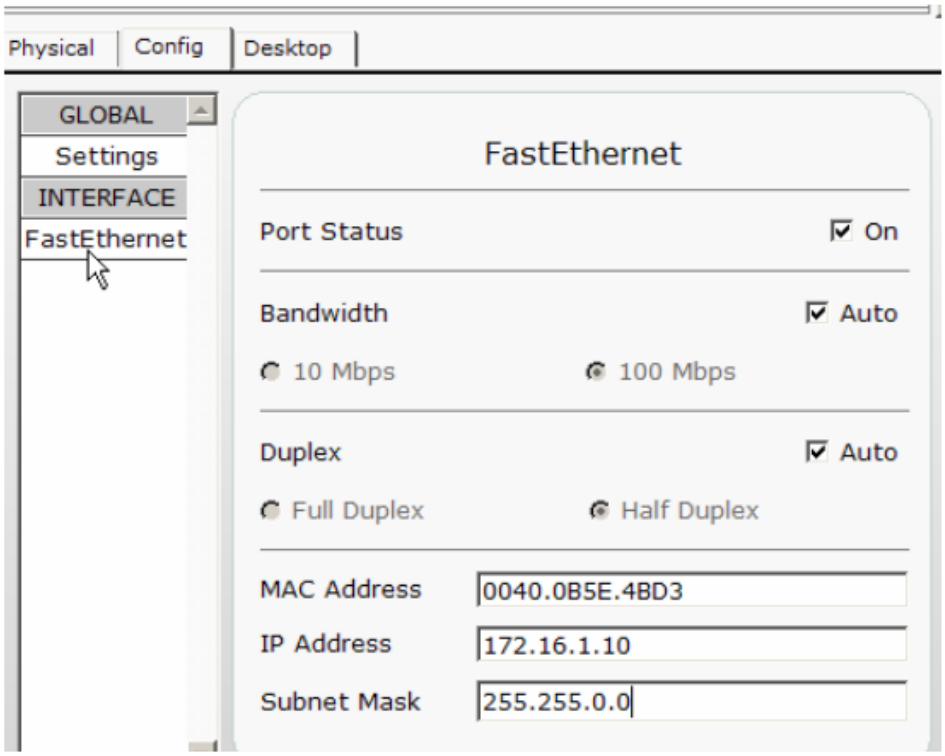
Cliquer sur PC0 :



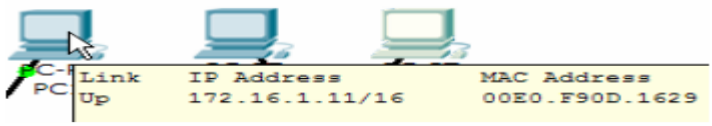
Choisir le bouton de config, c'est ici qu'on peut changer le nom de PC0.On peut également écrire une IP ADDRESS de Gateway, également connu sous le nom de Gateway de défaut. Nous discuterons ceci plus tard, mais ceci doit être l'IP Address du réseau local, exemple on peut écrire l'IP Address 172.16.1.1



Cliquer sur FastEthernet. Bien que nous n'ayons pas encore discuté des adresses IP, ajouter l'IP Address 172.16.1.10 puis cliquer une fois dans le domaine de subnet mask pour écrire le subnet mask de défaut.



Pour vérifier les informations il suffit de placer le curseur sur le PC :



3.11.5 Vérification des connexions :

Il existe deux modes de vérification :

♠ Le mode en temps réelle.

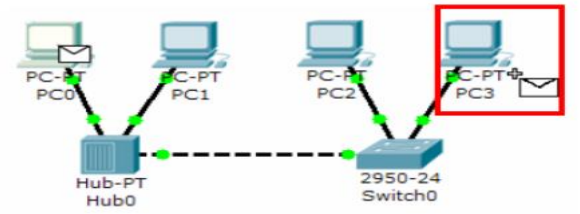
♠ Le mode Simulation.

3.11.5.1 Mode en temps réel :

Réaliser un réseau qui comporte : 4 PC, un Hub, un Switch.

Sélectionner l'outil simple de PDU utilisé pour pinguer les machines.

Cliquer une fois sur PC0, puis une fois sur PC3.



L'envoi de PDU devrait montrer comme réussi

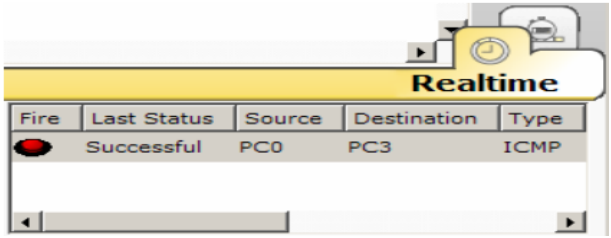


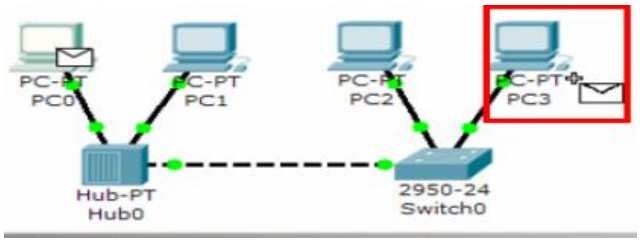
Figure 3.35 : *réussite de l'envoi de PDU*

3.11.5.2 Mode Simulation :

Réaliser un réseau qui comporte : 4 PC, un Hub, un Switch.

Sélectionner l'outil simple de PDU utilisé pour pinguer les machines.

Cliquer une fois sur PC0, puis une fois sur PC3.



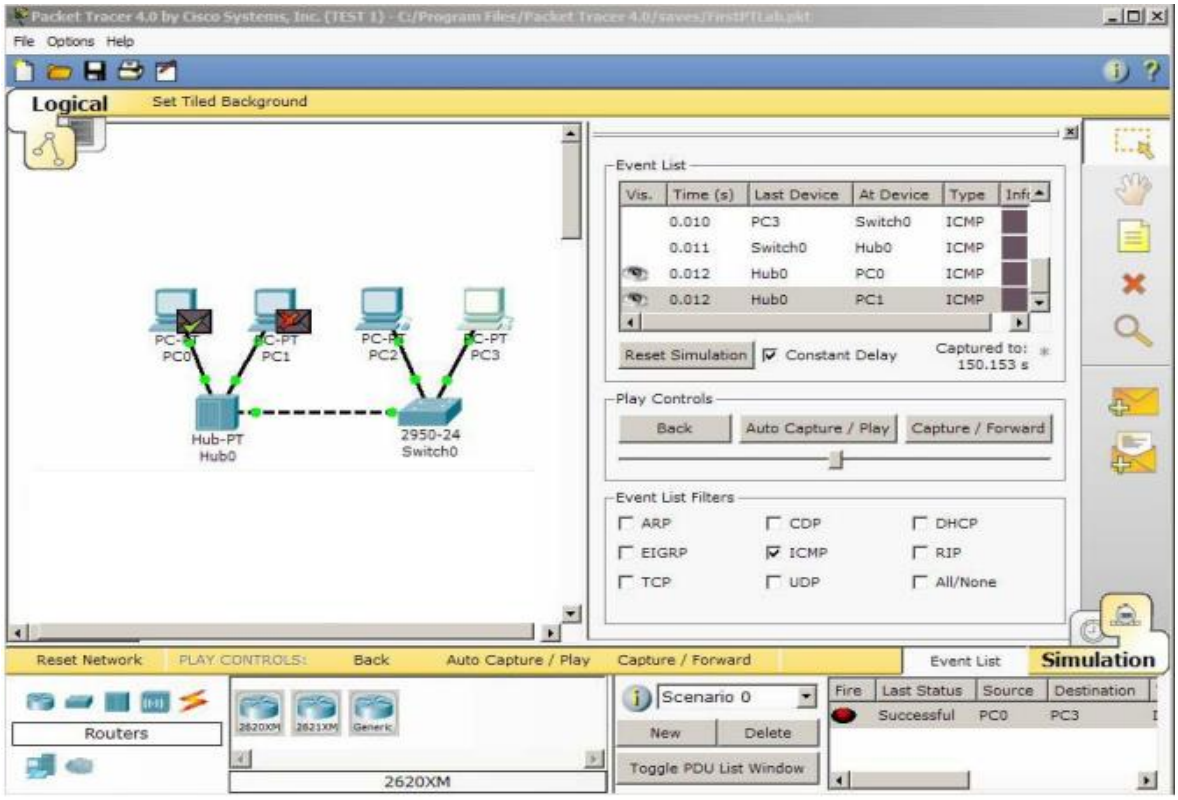


Figure 3.36: *visualisation de l'envoi des paquets de données*

Si on veut analyser les trames, on clique sur le paquet de données (enveloppe) et on visualise le détail des trames au niveau des protocoles.

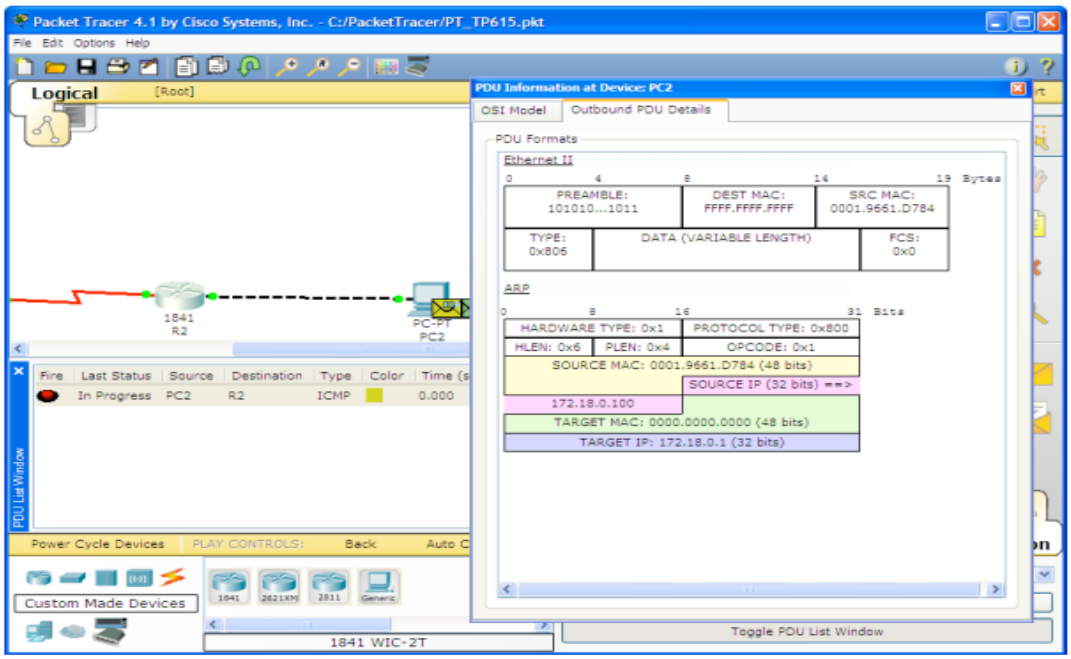


Figure 3.37 : *analyse de la trame au niveau des protocoles*

Conclusion :

Dans la première partie de ce chapitre nous avons présenté l'unité GPL de Saida relevant de l'entreprise Naftal. Et exposer son organigramme fonctionnel des départements et services. Aussi, nous avons détaillé les missions de chaque département et service dans le but de comprendre les missions, prérogatives et besoins de chacun deux. Dans la deuxième partie, nous avons présenté brièvement le logiciel de simulation utilisé, qui est le logiciel Packet Tracer de l'entreprise pionnière CISCO.

Chapitre 04

Conception et Simulation d’un réseau local d’entreprise

4.1 Introduction

Ce travail pratique consiste à concevoir et à simuler un réseau local d'entreprise destiné à l'unité Naftal (GPL) de Saïda à l'aide du logiciel Cisco Packet Tracer. Le réseau est conçu selon l'architecture VLAN, permettant ainsi de séparer les différents services de l'entreprise et d'optimiser l'organisation et la gestion du trafic réseau. Cinq commutateurs ont été utilisés pour modéliser les départements de l'entreprise, auxquels s'est ajouté un commutateur multicouches se chargeant du routage inter-VLAN. Un routeur ainsi qu'un pare-feu ont également été intégrés pour assurer la connectivité, la sécurité et la protection du réseau contre les accès non autorisés. Ce travail de simulation permettra de concevoir l'architecture de la société de manière à se rapprocher le plus possible de la réalité, tout en testant la connexion du réseau, la communication entre les VLAN et le fonctionnement des différentes sécurités mises en place.

4.2 Présentation de l'architecture réseau existante

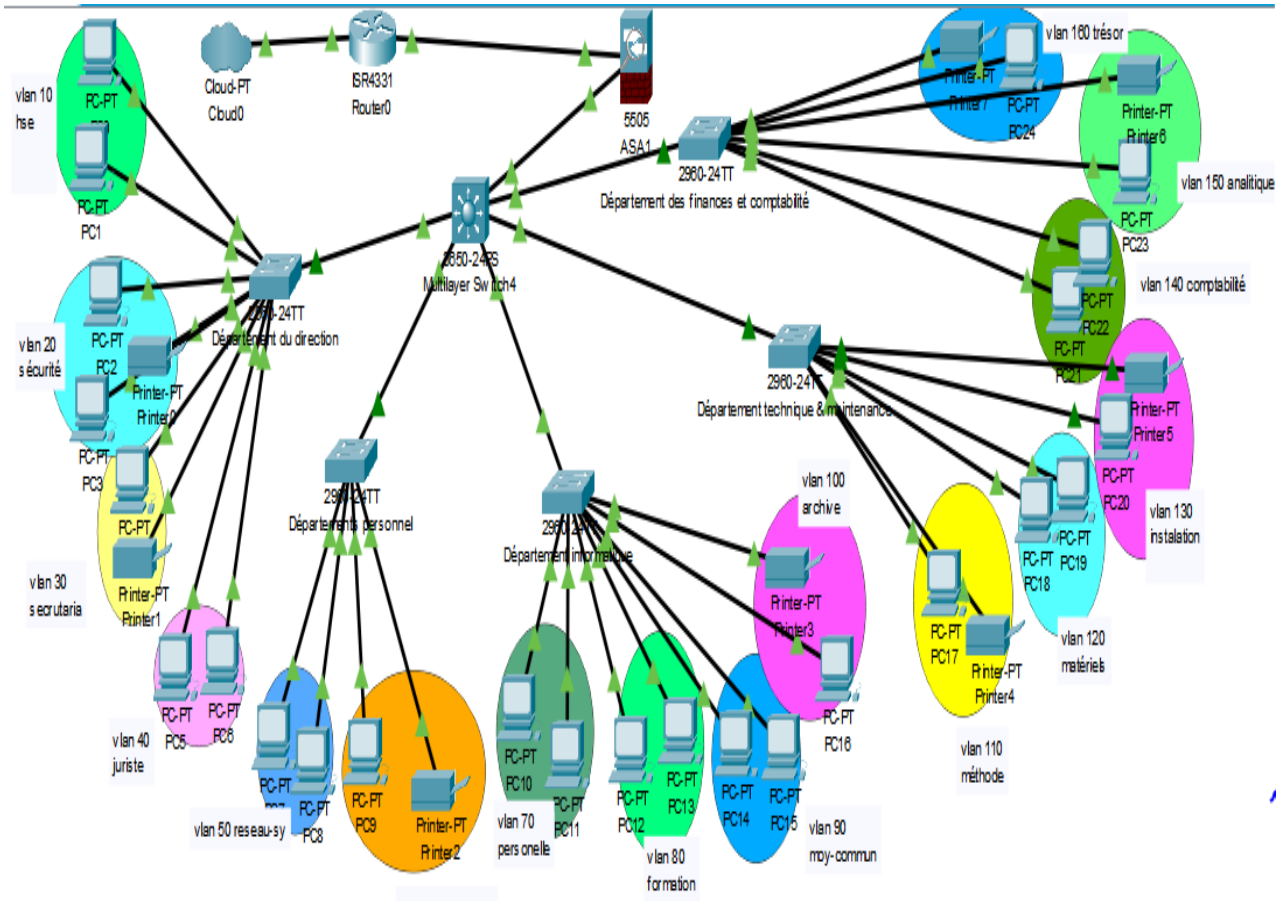


Figure 4.38:*l'architecture du réseau local de l'unité Naftal GPL Saida*

Remarque :

La simulation de ce réseau intègre deux ou trois équipements par service uniquement afin de vérifier la connectivité ainsi que le bon fonctionnement du réseau. Nous avons procédé à une configuration statique réalisée manuellement ainsi qu'à une configuration dynamique effectuée au moyen du protocole DHCP.

4.3 Configuration des équipements

4.3.1 Configuration du commutateur central :

Le commutateur central représente le composant fondamental de l'architecture des réseaux d'entreprise ; il joue un rôle principal dans la gestion et la distribution du trafic réseau entre les différents commutateurs et VLAN.

Dans un premier temps, le commutateur principal se voit attribué un nom comme montré dans la figure 4.2.

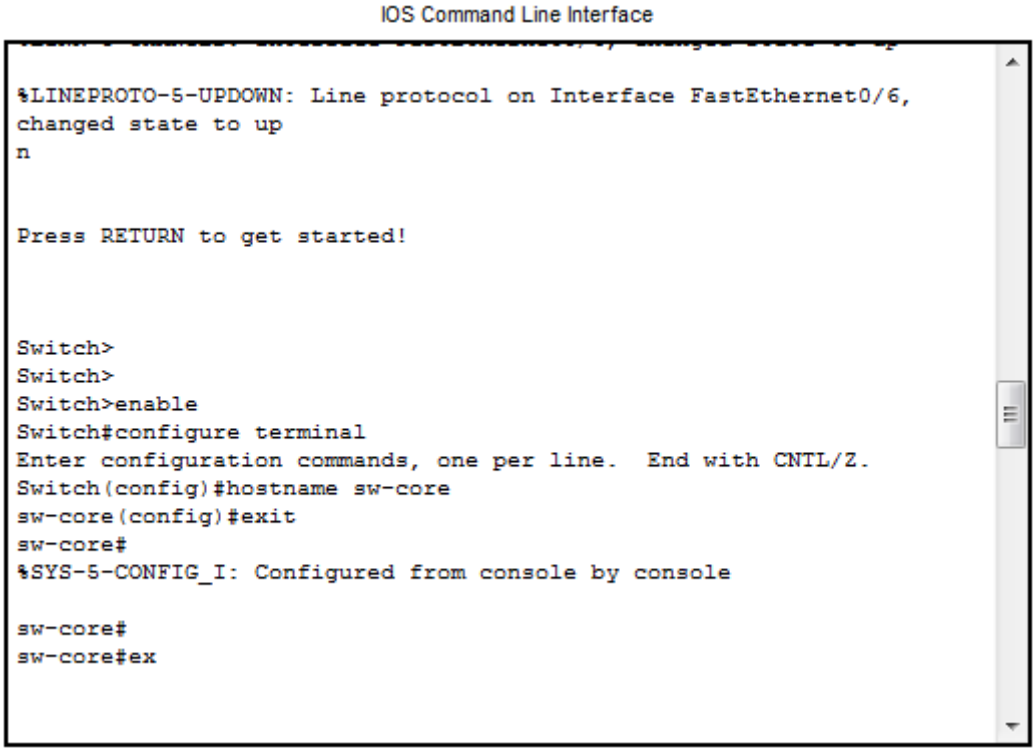


Figure 4.39: *Configuration du nom du commutateur principal*

4.3.2 Sécurisation du commutateur principal

La sécurisation du commutateur principal constitue une étape cruciale pour garantir la protection de l'infrastructure réseau contre les accès non autorisés ainsi que les attaques internes. Dans ce contexte, on a plusieurs mécanismes de sécurité, comme la sécurité par mot de passe, qui permet de limiter l'accès administratif au commutateur principal et la sécurité de la console permet l'administration locale du commutateur (Figure 4.3).

IOS Command Line Interface

```
sw-core(config-line)#
sw-core(config-line)#
sw-core(config-line)#
sw-core(config-line)#
sw-core(config-line)#
sw-core(config-line)#exit
sw-core(config)#ex
sw-core#
%SYS-5-CONFIG_I: Configured from console by console

sw-core#
sw-core#
sw-core#
sw-core#enable
sw-core#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw-core(config)#line vty 04
sw-core(config-line)#password admin
sw-core(config-line)#login
sw-core(config-line)#exit
sw-core(config)#line consol 0
sw-core(config-line)#password admin
sw-core(config-line)#login
sw-core(config-line)#exit
sw-core(config)#
```

Figure 4.40: Sécurisation du commutateur principal

4.3.3 Configuration du protocole VTP

Le protocole VTP autorise la centralisation de la gestion des VLAN au sein du réseau .Le commutateur central est configuré en mode serveur afin de distribuer automatiquement les VLAN aux autres commutateurs configurés en mode client. Par conséquent, le mode Server est attribué au commutateur central (figure 4.4).

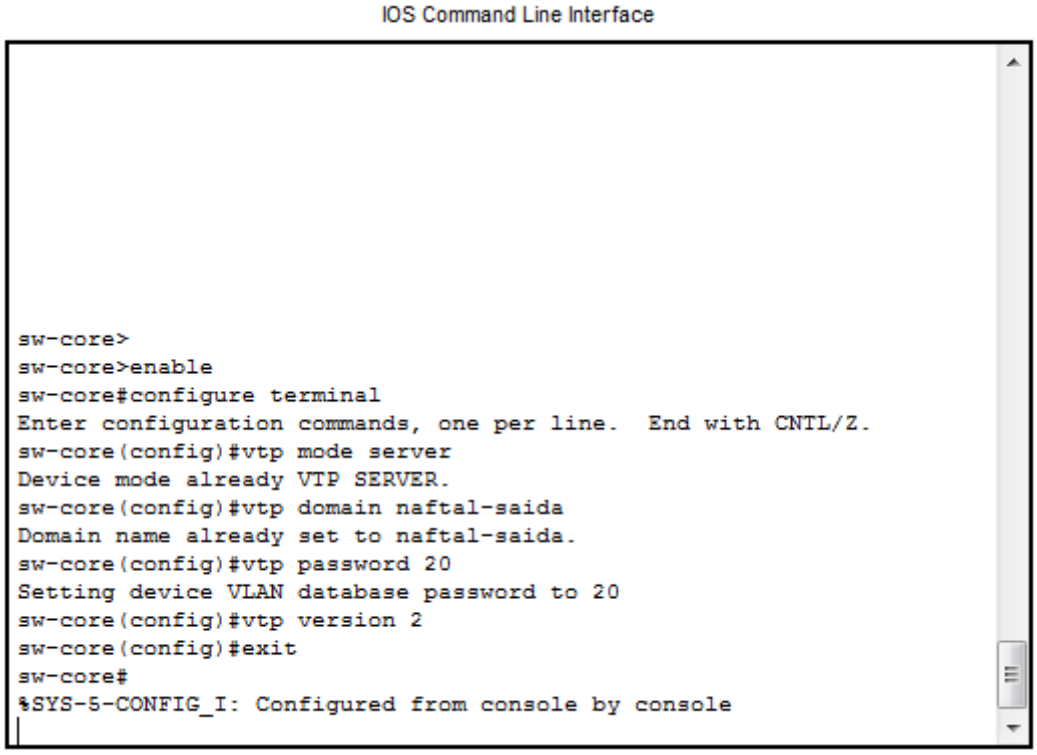
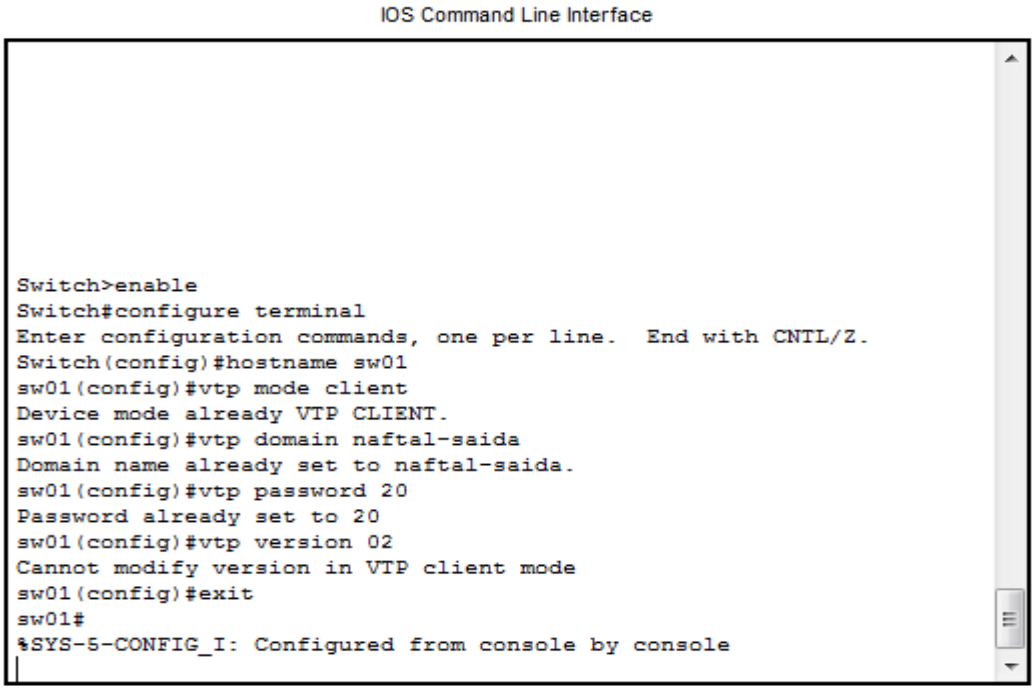


Figure 4.41 : *Configuration du protocole VTP (mode server)*

Les commutateurs secondaires fonctionnent en mode client afin de recevoir automatiquement les VLAN transmis par le commutateur principal (Figure 4.5).



IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up


Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname sw02
sw02(config)#vtp mode client
Setting device to VTP CLIENT mode.
sw02(config)#vtp domain naftal-saida
Changing VTP domain name from NULL to naftal-saida
sw02(config)#vtp password 20
Setting device VLAN database password to 20
sw02(config)#vtp version 02
Cannot modify version in VTP client mode
sw02(config)#exit
```

IOS Command Line Interface

```
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up


Switch>
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname sw03
sw03(config)#vtp mode client
Setting device to VTP CLIENT mode.
sw03(config)#vtp domain naftal-saida
Changing VTP domain name from NULL to naftal-saida
sw03(config)#vtp password 20
Setting device VLAN database password to 20
sw03(config)#vtp version 02
Cannot modify version in VTP client mode
sw03(config)#exit
sw03#
%SYS-5-CONFIG_I: Configured from console by console
```

IOS Command Line Interface

```
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up


Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname sw04
sw04(config)#vtp mode client
Setting device to VTP CLIENT mode.
sw04(config)#vtp domain naftal-saida
Changing VTP domain name from NULL to naftal-saida
sw04(config)#vtp password 20
Setting device VLAN database password to 20
sw04(config)#vtp version 02
Cannot modify version in VTP client mode
sw04(config)#exit
sw04#
%SYS-5-CONFIG_I: Configured from console by console
```

IOS Command Line Interface

```
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up


Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname sw05
sw05(config)#vtp mode client
Setting device to VTP CLIENT mode.
sw05(config)#vtp domain naftal-saida
Changing VTP domain name from NULL to naftal-saida
sw05(config)#vtp password 20
Setting device VLAN database password to 20
sw05(config)#vtp version 02
Cannot modify version in VTP client mode
sw05(config)#exit
sw05#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 4.42: *Configuration du protocole VTP (mode client) dans le commutateur secondaire*

4.3.4 Création des VLAN

La création des VLAN s'effectue au niveau du commutateur principal après la mise en place du protocole VTP. Chaque VLAN correspond à un service spécifique au sein de l'entreprise (Figure 4.6).

IOS Command Line Interface

```
sw-core#
sw-core#en
sw-core#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw-core(config)#vlan 10
sw-core(config-vlan)#name hse
sw-core(config-vlan)#vlan 20
sw-core(config-vlan)#name securite
sw-core(config-vlan)#vlan 30
sw-core(config-vlan)#name secrutaire
sw-core(config-vlan)#vlan 40
sw-core(config-vlan)#name jurist
sw-core(config-vlan)#vlan 50
sw-core(config-vlan)#name reseau-systeme
sw-core(config-vlan)#vlan 60
sw-core(config-vlan)#name inf-gestion
sw-core(config-vlan)#vlan 70
sw-core(config-vlan)#name personnelle
sw-core(config-vlan)#vlan 80
sw-core(config-vlan)#name formation
sw-core(config-vlan)#vlan 90
sw-core(config-vlan)#name moyene-commun
sw-core(config-vlan)#vlan 100
sw-core(config-vlan)#name archive
sw-core(config-vlan)#
sw-core(config-vlan)#vlan 110
sw-core(config-vlan)#name methode
sw-core(config-vlan)#vlan 120
sw-core(config-vlan)#name materiels
sw-core(config-vlan)#vlan 130
sw-core(config-vlan)#name instalation
sw-core(config-vlan)#vlan 140
sw-core(config-vlan)#name comptabilite
sw-core(config-vlan)#vlan 150
sw-core(config-vlan)#name analitique
sw-core(config-vlan)#vlan 160
sw-core(config-vlan)#name tresor
sw-core(config-vlan)#exit
sw-core(config)#exit
sw-core#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 4.43 : *Création des VLAN*

4.3.5 Attribution des ports des commutateurs au VLANs

Les ports d'accès assurent la connexion des postes utilisateurs à un VLAN spécifique. Chaque port est attribué à un VLAN unique, ce qui facilite la structuration des utilisateurs en fonction de leur service. Cette opération est faite au niveau de chaque commutateur (mode client) (figure 4.7).

IOS Command Line Interface

```
sw01>enable
sw01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw01(config)#interface range f0/1-2
sw01(config-if-range)#switchport mode access
sw01(config-if-range)#switchport access vlan 10
sw01(config-if-range)#exit
sw01(config)#interface range f0/3-5
sw01(config-if-range)#switchport mode access
sw01(config-if-range)#switchport access vlan 20
sw01(config-if-range)#exit
sw01(config)#interface range f0/6-7
sw01(config-if-range)#switchport mode access
sw01(config-if-range)#switchport access vlan 30
sw01(config-if-range)#exit
sw01(config)#interface range f0/8-9
sw01(config-if-range)#switchport mode access
sw01(config-if-range)#switchport access vlan 40
sw01(config-if-range)#exit
sw01(config)#
```

```
sw02>
sw02>enable
sw02#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw02(config)#interface range f0/1-2
sw02(config-if-range)#switchport mode access
sw02(config-if-range)#switchport access vlan 50
sw02(config-if-range)#exit
sw02(config)#interface range f0/3-4
sw02(config-if-range)#switchport mode access
sw02(config-if-range)#switchport access vlan 60
sw02(config-if-range)#exit
sw02(config)#
```

IOS Command Line Interface

```
sw03>
sw03>enable
sw03#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw03(config)#interface range f0/1-2
sw03(config-if-range)#switchport mode access
sw03(config-if-range)#switchport access vlan 70
sw03(config-if-range)#exit
sw03(config)#interface range f0/3-4
sw03(config-if-range)#switchport mode access
sw03(config-if-range)#switchport access vlan 80
sw03(config-if-range)#exit
sw03(config)#interface range f0/5-6
sw03(config-if-range)#switchport mode access
sw03(config-if-range)#switchport access vlan 90
sw03(config-if-range)#exit
sw03(config)#interface range f0/7-8
sw03(config-if-range)#switchport mode access
sw03(config-if-range)#switchport access vlan 10
sw03(config-if-range)#exit
```

```
sw04>enable
sw04#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw04(config)#interface range f0/1-2
sw04(config-if-range)#switchport mode access
sw04(config-if-range)#switchport access vlan 110
sw04(config-if-range)#exit
sw04(config)#interface range f0/3-4
sw04(config-if-range)#switchport mode access
sw04(config-if-range)#switchport access vlan 120
sw04(config-if-range)#exit
sw04(config)#interface range f0/5-6
sw04(config-if-range)#switchport mode access
sw04(config-if-range)#switchport access vlan 130
sw04(config-if-range)#exit
sw04(config)#
```

```
sw05>enable
sw05#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw05(config)#interface range f0/1-2
sw05(config-if-range)#switchport mode access
sw05(config-if-range)#switchport access vlan 140
sw05(config-if-range)#exit
sw05(config)#interface range f0/3-4
sw05(config-if-range)#switchport mode access
sw05(config-if-range)#switchport access vlan 150
sw05(config-if-range)#exit
sw05(config)#interface range f0/5-6
sw05(config-if-range)#switchport mode access
sw05(config-if-range)#switchport access vlan 160
sw05(config-if-range)#exit
sw05(config)#
```

Figure 4.44 : *Attribution des ports des commutateurs (mode client).*

4.3.6 Configuration des liens Trunk entre les commutateurs

4.3.6.1 Configuration des liens Trunk entre les commutateurs et le commutateur principal

Les interfaces des équipements d'interconnexion devant être configurées en mode Trunk se situent exclusivement entre l'ensemble des commutateurs d'accès et le commutateur cœur. Les commandes suivantes permettent d'attribuer un port à un VLAN en mode Trunk en utilisant la commande range, qui autorise la configuration simultanée de plusieurs interfaces (Figure 4.8).

IOS Command Line Interface

```
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#
sw01#enable
sw01#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw01(config)#interface gig0/1
sw01(config-if)#switchport trunk allowed vlan 10-160
sw01(config-if)#switchport mode trunk
sw01(config-if)#exit
sw01(config)#
```

```
sw02>
sw02>enable
sw02#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw02(config)#interface gig0/1
sw02(config-if)#switchport trunk allowed vlan 10-160
sw02(config-if)#switchport mode trunk

sw02(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
exit
sw02(config)#
```

IOS Command Line Interface

```
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>
sw03>enable
sw03#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw03(config)#interface gig0/1
sw03(config-if)#switchport trunk allowed vlan 10-160
sw03(config-if)#switchport mode trunk
sw03(config-if)#exit
sw03(config)#
```

```
sw04>
sw04>enable
sw04#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw04(config)#interface gig0/1
sw04(config-if)#switchport trunk allowed vlan 10-160
sw04(config-if)#switchport mode trunk
sw04(config-if)#exit
sw04(config)#
```

```
sw05>
sw05>
sw05>ENABLE
sw05#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw05(config)#interface gig0/1
sw05(config-if)#switchport trunk allowed vlan 10-160
sw05(config-if)#switchport mode trunk
sw05(config-if)#exit
sw05(config)#
```

***Figure 4.45**: Configuration des liens Trunk entre les commutateurs et le commutateur principa*l

4.3.6.2: Configuration des liens Trunk entre le commutateur principal et les autres commutateurs

Dans ce contexte, le protocole IEEE 802.1Q est utilisé pour l'encapsulation des trames Ethernet, ce qui autorise l'identification des VLAN transportés sur les liaisons trunk par l'insertion d'un identifiant VLAN dans chaque trame. Ce mécanisme permet de prévoir une transmission fiable, efficace et sécurisée des données entre les différents commutateurs du réseau d'entreprise. Grâce à l'ajout d'une étiquette VLAN dans chaque trame (Figure 4.9).

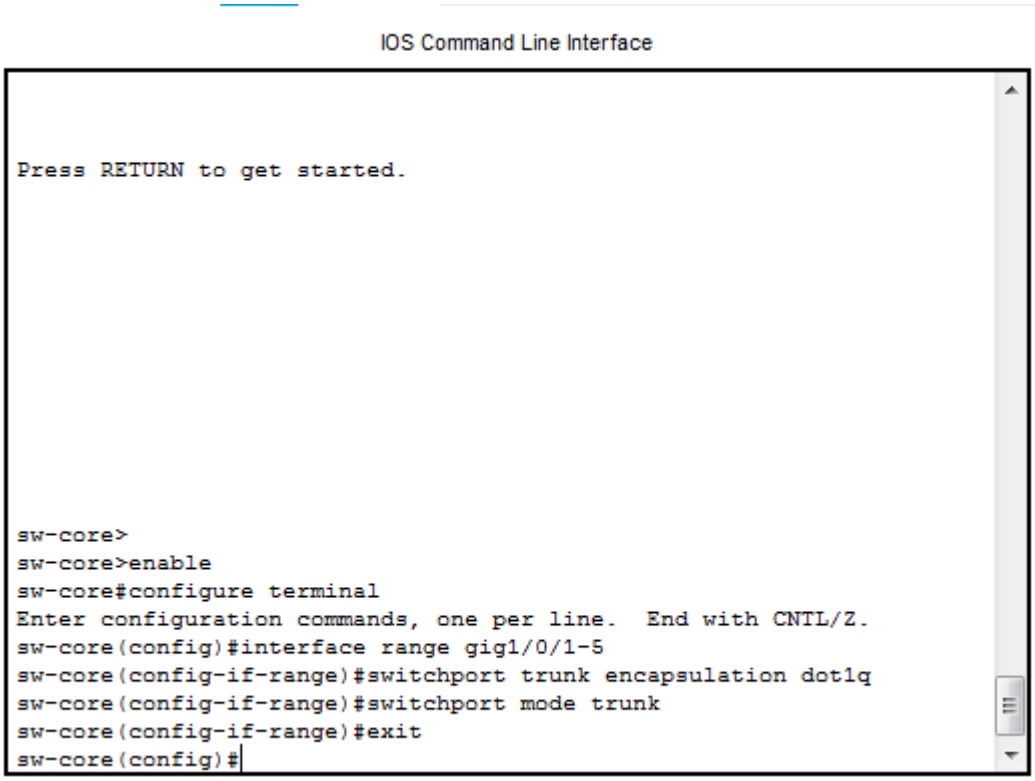


Figure 4.46: *Configuration des liens Trunk entre le commutateur principal et les autres commutateurs.*

4.3.7 Configuration des interfaces VLAN

Pour assurer l'interconnexion des VLAN, il est nécessaire de créer des interfaces virtuelles (SVI) sur le commutateur principal (commutateur server). Cette L'interface est configurée avec une adresse IP qui constitue la passerelle par défaut pour les dispositifs du VLAN (Figure 4.10).

IOS Command Line Interface

```
sw-core#
sw-core#enable
sw-core#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw-core(config)#interface vlan 10
sw-core(config-if)#ip address 192.168.10.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 20
sw-core(config-if)#ip address 192.168.20.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 30
sw-core(config-if)#ip address 192.168.30.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config-if)#exit
sw-core(config)#interface vlan 40
sw-core(config-if)#ip address 192.168.40.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 50
sw-core(config-if)#ip address 192.168.50.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 60
sw-core(config-if)#ip address 192.168.60.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 70
sw-core(config-if)#ip address 192.168.70.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 80
sw-core(config-if)#ip address 192.168.80.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 90
sw-core(config-if)#ip address 192.168.90.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 100
sw-core(config-if)#ip address 192.168.100.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 110
sw-core(config-if)#ip address 192.168.110.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#
```

```
sw-core(config-if)#interface vlan 120
sw-core(config-if)#ip address 192.168.120.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 130
sw-core(config-if)#ip address 192.168.130.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 140
sw-core(config-if)#ip address 192.168.140.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 150
sw-core(config-if)#ip address 192.168.150.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#interface vlan 160
sw-core(config-if)#ip address 192.168.160.1 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#exit
sw-core#
```

Figure 4.47 : *Configuration des interfaces VLAN*

4.3.8 Activation du routage inter-VLAN

Le routage entre VLANs est réalisé au sein du commutateur principal .Ce commutateur occupe une fonction cruciale au sein de l'infrastructure réseau, car il facilite les échanges entre les divers VLANs (Figure 4.11).

```
sw-core#
sw-core#enable
sw-core#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw-core(config)#ip routing
sw-core(config)#exit
sw-core#
%SYS-5-CONFIG_I: Configured from console by console

sw-core#
```

Figure 4.48 : *routage inter-VLAN*

4.3.9 Configuration DHCP :

Le DHCP simplifie la gestion des adresses IP dans l'entreprise. Les utilisateurs reçoivent automatiquement leurs paramètres réseau sans intervention manuelle de l'administrateur. La figure 4.12 montre les plages d'adresses utilisées et le sous- réseau approprié pour chaque VLAN.

IOS Command Line Interface

```
sw-core#en
sw-core#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw-core(config)#ip dhcp pool vlan10
sw-core(dhcp-config)#network 192.168.10.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.10.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan20
sw-core(dhcp-config)#network 192.168.20.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.20.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan30
sw-core(dhcp-config)#network 192.168.30.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.30.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan40
sw-core(dhcp-config)#network 192.168.40.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.40.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan50
sw-core(dhcp-config)#network 192.168.50.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.50.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan60
sw-core(dhcp-config)#network 192.168.60.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.60.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan70
sw-core(dhcp-config)#network 192.168.70.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.70.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#
```

```
sw-core(config)#ip dhcp pool vlan80
sw-core(dhcp-config)#network 192.168.80.0 255.255.255.0
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan90
sw-core(dhcp-config)#network 192.168.90.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.90.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan100
sw-core(dhcp-config)#network 192.168.100.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.100.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan110
sw-core(dhcp-config)#network 192.168.110.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.110.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan120
sw-core(dhcp-config)#network 192.168.120.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.120.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
```

```
sw-core(dhcp-config)#network 192.168.120.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.120.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan130
sw-core(dhcp-config)#network 192.168.130.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.130.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan140
sw-core(dhcp-config)#network 192.168.140.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.140.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan150
sw-core(dhcp-config)#network 192.168.150.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.150.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
sw-core(config)#ip dhcp pool vlan160
sw-core(dhcp-config)#network 192.168.160.0 255.255.255.0
sw-core(dhcp-config)#default-router 192.168.160.1
sw-core(dhcp-config)#dns-server 8.8.8.8
sw-core(dhcp-config)#exit
```

Figure 4.49 : *Configuration DHCP*

4.3.10 Configuration du port du commutateur principal connecté au Pare-feu :

La liaison entre le commutateur principal et le pare-feu garantit simultanément le routage ainsi que la sécurisation du trafic réseau.

Le lien connectant le commutateur principal au pare-feu est généralement configuré comme port de couche 3 et, par défaut, les ports de commutateur principal fonctionnent comme des ports de couche 2. Ainsi, il est possible de transformer un port classique en port routé fonctionnel au niveau de la couche 3 du modèle OSI. Et ceci avec la commande **no Switchport** (Figure 4.13).

IOS Command Line Interface

```
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#
sw-core#enable
sw-core#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw-core(config)#interface gig1/0/6
sw-core(config-if)#no switchport
sw-core(config-if)#ip address 192.168.1.2 255.255.255.0
sw-core(config-if)#no shutdown
sw-core(config-if)#exit
sw-core(config)#
```

***Figure 4.50**: Configuration du port connecté au Pare-feu sur Le commutateur principal*

4.4 Configuration du pare-feu :

4.4.1 Configuration de l'interface interne et externe du pare-feu :

L'interface d'entrée du pare-feu est raccordée directement au commutateur principal pour recevoir le trafic des VLANs internes : C'est le réseau interne de l'entreprise. Et l'interface des sorties représente le réseau externe du réseau il est connecté avec le routeur (Figure 4.14).

IOS Command Line Interface

```
Type help or '?' for a list of available commands.

ciscoasa>
ciscoasa>
ciscoasa>
ciscoasa>
ciscoasa>
ciscoasa>enable
Password:
ciscoasa#
ciscoasa#
ciscoasa#configure terminal
ciscoasa(config)#interface vlan1
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)#interface vlan2
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address 200.0.0.1 255.255.255.0
ciscoasa(config-if)#exit
ciscoasa(config)#
```

Figure 4.51 : *Configuration de l'interface interne et externe du pare-feu*

4.4.2 Attribution des ports physiques au VLAN1 et VLAN2

Cette opération permet d'organiser le trafic du réseau d'entrée et le réseau de sortie (Figure 4.15).

IOS Command Line Interface

```
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#
ciscoasa(config-if)#ex
ciscoasa(config)#
ciscoasa(config)#ex
ciscoasa#
ciscoasa#enable
         ^
% Invalid input detected at '^' marker.

ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#configure terminal
ciscoasa(config)#interface ethernet 0/0
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#interface ethernet 0/1
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#exit
ciscoasa(config)#
ciscoasa(config)#
```

Figure 4.52: *Attribution des ports physiques au VLAN1 et VLAN2*

4.4.3 Configuration du protocole NAT :

Cette configuration est réalisée au niveau du pare-feu. Ce protocole permet de convertir les adresses IP privées du réseau interne en adresses publiques afin de permettre l'accès à Internet (Figure 4.16).

IOS Command Line Interface

```
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#
ciscoasa(config-network-object)#ex
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#
ciscoasa#configure terminal
ciscoasa(config)#object network inside-net
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic
interface
ciscoasa(config-network-object)#exit
ciscoasa#
```

***Figure 4.53**: Configuration de protocole NAT*

4.5 Configuration du routeur

4.5.1 Configuration du nom de routeur

Pour démarrer la configuration de base du routeur, nous allons commencer par assigner un nom à l'aide de la commande suivante (figure 4.17):

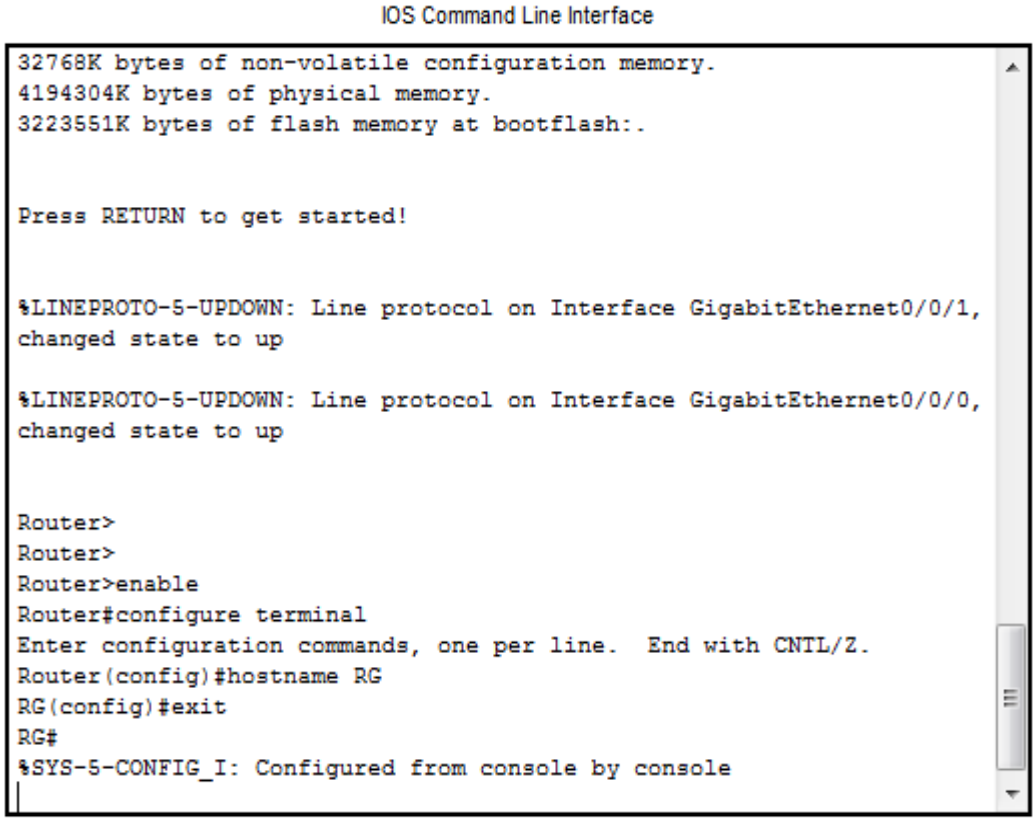


Figure 4.54 : *Configuration du nom de routeur*

4.5.2 Sécurisation du routeur

Lorsqu'il est nécessaire de sécuriser un routeur, il convient d'ajouter un mot de passe en mode privilégié, correspondant au mot de passe d'accès enable (Figure 4.18).

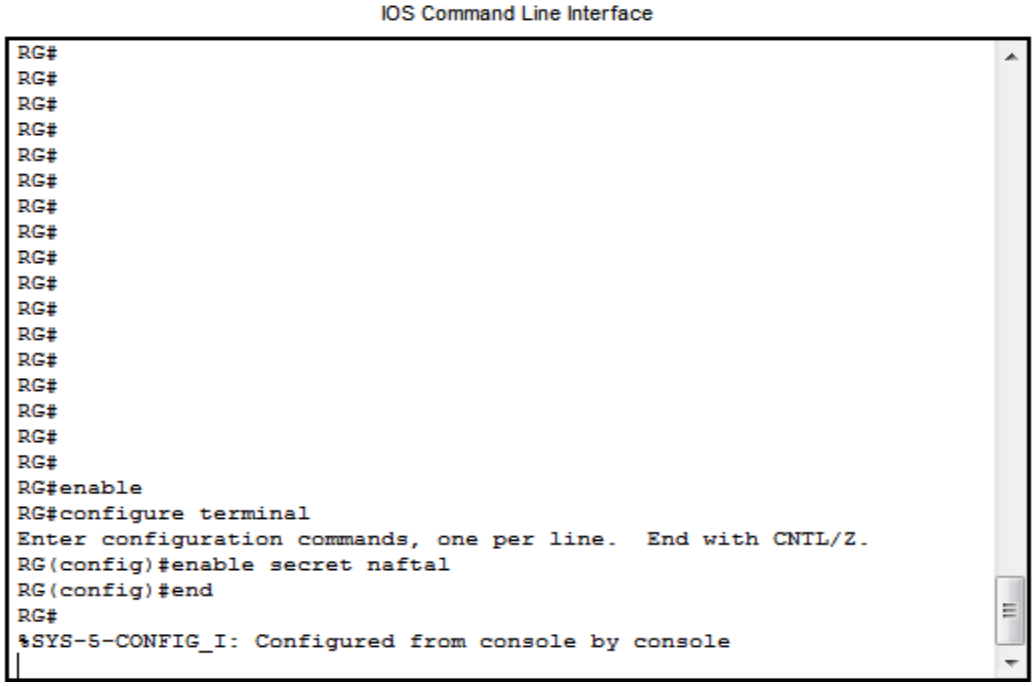


Figure 4.55 : *Sécurisation du routeur*

4.5.3 Configuration des interfaces du routeur :

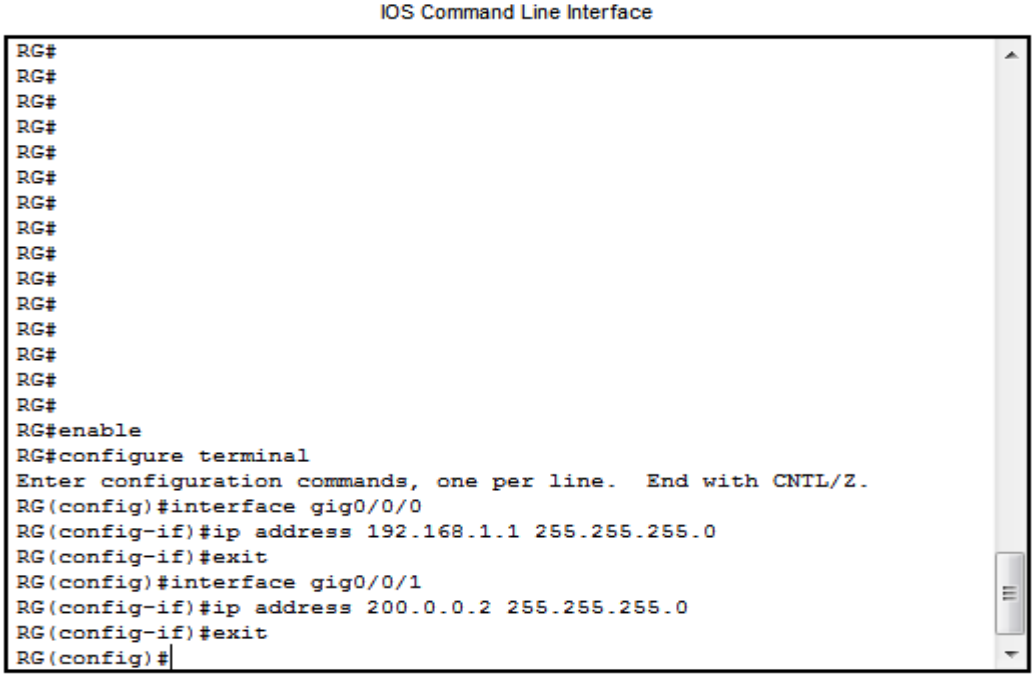


Figure 4.56: *Configuration des interfaces du routeur*

4.5.4 Utilisation de la liste de contrôle d'accès ou ACL

Une liste de contrôle d'accès (ACL) appliquée entre deux VLANs permet le filtrage du trafic circulant d'un réseau virtuel vers un autre.

Par exemple interdire au VLAN 10 (HSE) de communiquer avec le VLAN 120 (comptabilité), mais autoriser le reste du trafic (Figure 4.20).

IOS Command Line Interface

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Rg
Rg(config)#exit
Rg#
%SYS-5-CONFIG_I: Configured from console by console

Rg#
Rg#
Rg#
Rg#
Rg#
Rg#
Rg#
Rg#enable
Rg#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Rg(config)#access-list 101 deny ip 192.168.10.0 0.0.0.255
192.168.140.0 0.0.0.255
Rg(config)#access-list 101 permit ip any any
Rg(config)#interface vlan 10
Rg(config-if)#ip access-group 101 in
Rg(config-if)#exit
Rg(config)#
```

Figure 4.57 : *exemple de l'utilisation des ACL*

4.6 Vérifications et tests de validation

4.6.1 Vérification dans commutateurs

4.6.1.1 Vérification des VLAN

Après la création des VLAN, ceux-ci seront affichés à l'aide de la commande **show VLAN bref** (Figure 4.21).

IOS Command Line Interface

```
                                                Gig1/0/19, Gig1/0/20,
Gig1/0/21, Gig1/0/22
                                                Gig1/0/23, Gig1/0/24,
Gig1/1/1, Gig1/1/2
                                                Gig1/1/3, Gig1/1/4
10   hse                              active
20   securite                         active
30   secrutariat                      active
40   jurist                           active
50   reseau-systeme                   active
60   inf-gestion                      active
70   personelle                       active
80   formation                        active
90   moyene-commun                    active
100  archive                          active
110  methode                          active
120  materiels                        active
130  instalation                      active
140  comptabilite                     active
150  analitique                       active
160  tresor                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
 --More--
```

Figure 4.58: *Vérification de l'état des VLANs*

4.6.1.2 Vérification du lien Trunk

Nous vérifions le mode Trunk dans le commutateur principal par la commande **show inter trunk** (Figure 4.22).

IOS Command Line Interface

```
sw-core#
sw-core#
sw-core#show inter trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig1/0/1    on           802.1q         trunking      1
Gig1/0/2    on           802.1q         trunking      1
Gig1/0/3    on           802.1q         trunking      1
Gig1/0/4    on           802.1q         trunking      1
Gig1/0/5    on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig1/0/1    1-1005
Gig1/0/2    1-1005
Gig1/0/3    1-1005
Gig1/0/4    1-1005
Gig1/0/5    1-1005

Port        Vlans allowed and active in management domain
Gig1/0/1    1,10,20,30,40,50,60,70,80,90,100,110,120,130,140,150,160
Gig1/0/2    1,10,20,30,40,50,60,70,80,90,100,110,120,130,140,150,160
Gig1/0/3    1,10,20,30,40,50,60,70,80,90,100,110,120,130,140,150,160
Gig1/0/4    1,10,20,30,40,50,60,70,80,90,100,110,120,130,140,150,160
Gig1/0/5    1,10,20,30,40,50,60,70,80,90,100,110,120,130,140,150,160

Port        Vlans in spanning tree forwarding state and not pruned
```

Figure 4.59 : *Vérification du lien Trunk*

4.6.1.3 Vérification des interfaces VLAN

Dans le commutateur principal nous visualisons ses interfaces VLAN par la commande **show ip interface brief** (Figure 4.23).

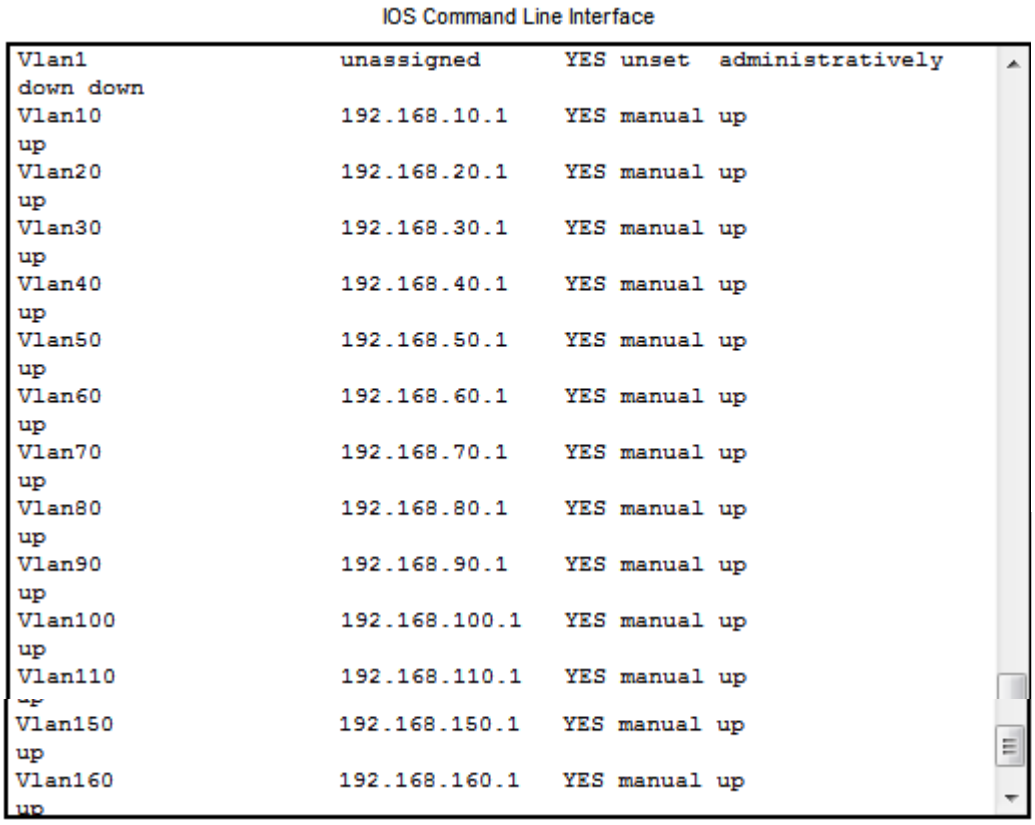


Figure 4.60 : *Vérification des interfaces VLAN*

4.6.2 Test de connectivité entre le PC1 et le PC2 sur le même VLAN 20

Nous testons l'accessibilité des équipements d'un même VLAN situés sur un réseau local commun. Depuis le PC 1, nous essayons d'accéder au PC 2 et écrire la commande **ping** comme présenté dans la figure 4.24.

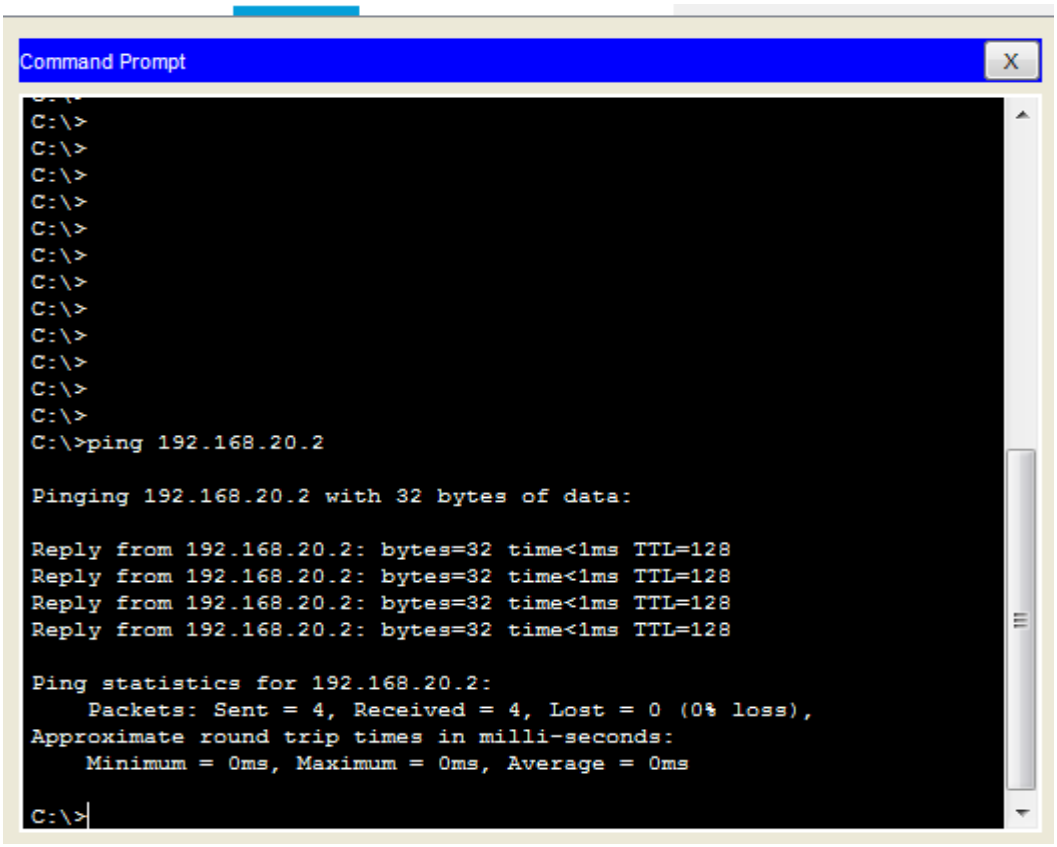


Figure 4.61: *Vérification de la connectivité entre PC1 et PC2 dans le VLAN 20*

4.6.3 Vérification de la connectivité entre PC1 de VLAN10 et PC2 de VLAN150

On peut tester la communication entre les différents équipements dans un même réseau mais dans deux VLANs différents à partir du PC 1 du VLAN 10 en essayant d'accéder au PC 2 du VLAN 150 (figure 4.25).

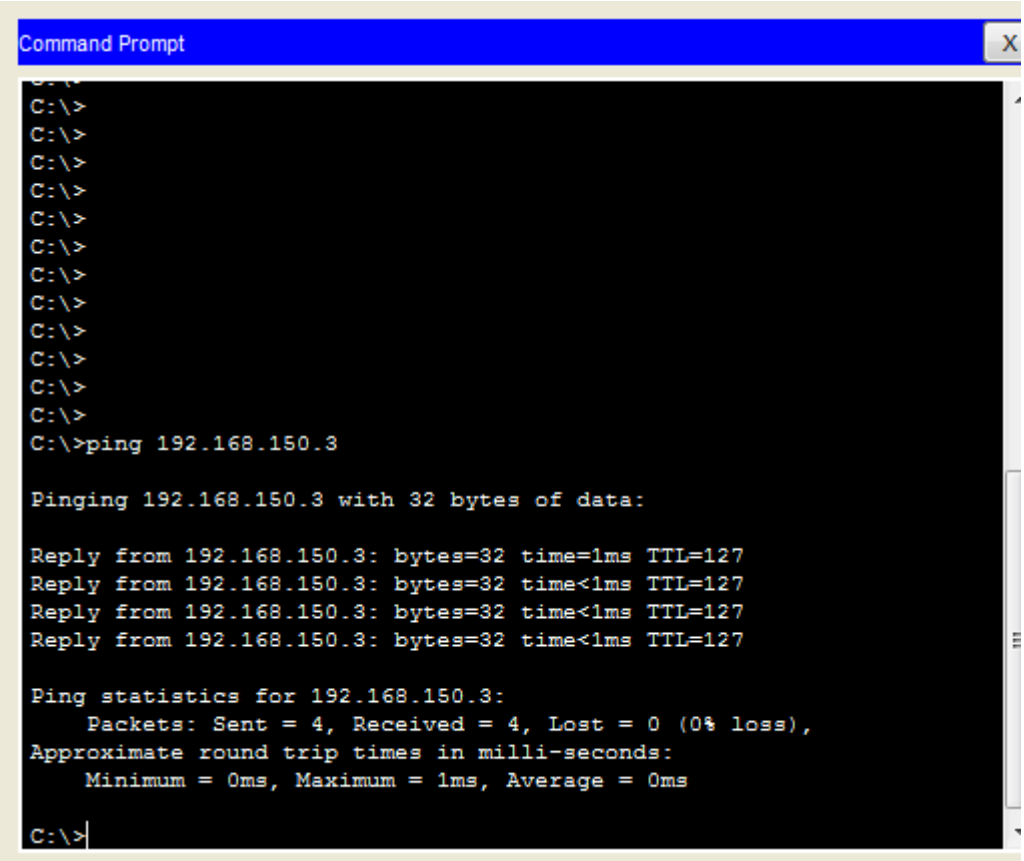


Figure 4.62 : *Vérification de la connectivité entre PC1 de VLAN10 et PC2 de VLAN150*

Conclusion

Dans ce chapitre, nous avons procédé à la création du réseau local, la configuration de l'ensemble des équipements présents dans ce réseau, notamment les commutateurs, le routeur et les ordinateurs, à l'aide du simulateur Cisco Packet Tracer. Puis nous avons réalisé une série de tests de validation visant à démontrer le fonctionnement correcte, l'efficacité et la performance du réseau conçu pour l'entreprise Naftal-GPL de Saida.

Conclusion générale

Ce travail de mémoire portant sur la conception et la simulation d'un réseau local pour l'entreprise Naftal nous a permis d'étudier les différentes étapes à suivre pour mettre en place une infrastructure réseau fiable et organisée. L'objectif principal de ce travail était de concevoir une architecture permettant une communication efficace entre les différents services de l'entreprise NAFTAL tout en assurant une meilleure gestion du trafic et un niveau de sécurité satisfaisant. Pour cela, nous avons utilisé le logiciel Cisco Packet Tracer afin de concevoir et tester l'ensemble de la solution réseau. La mise en œuvre des VLAN a été essentielle pour segmenter le réseau et pour optimiser les échanges de données. L'organisation a permis de réduire les diffusions inutiles, de faciliter la gestion du réseau et d'améliorer la sécurité des ressources informatiques de l'entreprise. Ailleurs L'organisation, le routage inter-VLAN et les mécanismes de contrôle d'accès ont permis une circulation contrôlée des informations entre les différents départements. Ce travail également permis d'approfondir nos compétences théoriques et pratiques dans le domaine des réseaux informatiques, notamment sur la configuration des commutateurs, le routage et les techniques de sécurisation. La simulation a été un passage obligé pour s'assurer que le réseau fonctionnait correctement avant toute mise en œuvre concrète. Cette étude montre donc qu'une conception réseau optimale est indispensable pour assurer la performance, la stabilité et la sécurité du système d'information d'une entreprise telle que Naftal. Dans le futur, l'enrichissement de ce projet pourrait passer par l'intégration de nouvelles technologies telles que les réseaux sans fil, les systèmes avancés de surveillance ou des solutions de haute disponibilité afin de garantir une infrastructure plus performante et évolutive encore.

Bibliographie

[1] A. Tanenbaum and D. J. Wetherall, Computer networks, Prentice Hall, 5th edition.

[2] Jean-François Pillou, tout sur les réseaux et Internet, Ed. Dunod, 3eme édition, 2012.

[3] José Dordoigne, Les réseaux, Nantes : ENI, 5eme édition, 2013.

[4] G. Pujolle, Initiation aux réseaux, Editions Eyrolles, 2014.

[5] https://www.cisco.com/.

[6] Cours Cisco CNNA.

[7] https://www.naftal.dz/.

Annexe

VLAN	Nom	IP	Masque	Passerelle
VLAN 10	HSE	192.168.10.0	255.255.255.255	192.168.10.1
VLAN 20	Sécurité	192.168.20.0	255.255.255.255	192.168.20.1
VLAN 30	Secrétariat	192.168.30.0	255.255.255.255	192.168.30.1
VLAN 40	Justus	192.168.40.0	255.255.255.255	192.168.40.1
VLAN 50	Réseau et système	192.168.50.0	255.255.255.255	192.168.50.1
VLAN 60	Informatique de la gestion	192.168.60.0	255.255.255.255	192.168.60.1
VLAN 70	Personnelle	192.168.70.0	255.255.255.255	192.168.70.1
VLAN 80	formation	192.168.80.0	255.255.255.255	192.168.80.1
VLAN 90	Moyenne commun	192.168.90.0	255.255.255.255	192.168.90.1
VLAN 100	Archive	192.168.100.0	255.255.255.255	192.168.100.1
VLAN 110	Méthode	192.168.110.0	255.255.255.255	192.168.110.1
VLAN 120	Matériels	192.168.120.0	255.255.255.255	192.168.120.1
VLAN 130	Installation	192.168.130.0	255.255.255.255	192.168.130.1
VLAN 140	Comptabilité	192.168.140.0	255.255.255.255	192.168.140.1
VLAN 150	analytique	192.168.150.0	255.255.255.255	192.168.150.1
VLAN 160	Trésor	192.168.160.0	255.255.255.255	192.168.160.1

Tableau 2 : la liste des adresses IP des VLAN

Pc	**IP adresse**	**Le masque**	**passerelle**	**VLAN**
PC 0	192.168.10.2	255.255.255.0	192.168.10.1	VLAN 10
PC 1	192.168.10.3	255.255.255.0	192.168.10.1	
PC 2	192.168.20.2	255.255.255.0	192.168.20.1	VLAN 20
PC 3	192.168.20.3	255.255.255.0	192.168.20.1	
Imprimante 0	192.168.20.4	255.255.255.0	192.168.20.1	
PC 4	192.168.30.2	255.255.255.0	192.168.30.1	VLAN 30
Imprimante 1	192.168.30.3	255.255.255.0	192.168.30.1	
PC 5	192.168.40.2	255.255.255.0	192.168.40.1	VLAN 40
PC 6	192.168.40.3	255.255.255.0	192.168.40.1	
PC 7	192.168.50.2	255.255.255.0	192.168.50.1	VLAN 50
PC 8	192.168.50.3	255.255.255.0	192.168.50.1	
Imprimante 2	192.168.60.2	255.255.255.0	192.168.60.1	VLAN 60
PC 9	192.168.60.3	255.255.255.0	192.168.60.1	
PC 10	192.168.70.2	255.255.255.0	192.168.70.1	VLAN 70
PC 11	192.168.70.3	255.255.255.0	192.168.70.1	
PC 12	192.168.80.2	255.255.255.0	192.168.80.1	VLAN 80
PC 13	192.168.80.3	255.255.255.0	192.168.80.1	
PC 14	192.168.90.3	255.255.255.0	192.168.90.1	VLAN 90
PC 15	192.168.90.2	255.255.255.0	192.168.90.1	
PC 16	192.168.100.2	255.255.255.0	192.168.100.1	VLAN 100
Imprimante 3	192.168.100.3	255.255.255.0	192.168.100.1	
PC 17	192.168.110.3	255.255.255.0	192.168.110.1	VLAN 110
Imprimante 4	192.168.110.2	255.255.255.0	192.168.110.1	
PC 18	192.168.120.3	255.255.255.0	192.168.120.1	VLAN 120
PC 19	192.168.120.2	255.255.255.0	192.168.120.1	
PC 20	192.168.130.2	255.255.255.0	192.168.130.1	VLAN 130
Imprimante 5	192.168.130.3	255.255.255.0	192.168.130.1	
PC 21	192.168.140.2	255.255.255.0	192.168.140.1	VLAN 140
PC 22	192.168.140.3	255.255.255.0	192.168.140.1	
PC 23	192.168.150.2	255.255.255.0	192.168.150.1	VLAN 150
Imprimante 6	192.168.150.3	255.255.255.0	192.168.150.1	

PC 25	192.168.160.3	255.255.255.0	192.168.160.1	VLAN 160
Imprimante 3	192.168.160.4	255.255.255.0	192.168.160.1	

Tableau 3 : la liste des adresses IP des PC