République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Djilali Bounaama Khemis Miliana

Faculté des Sciences et de la Technologie
Département de Technologie

Mémoire du Projet de Fin d'Etudes
Pour l'obtention du diplôme de

Master

En
« Télécommunications »
Option :
« Systèmes de Télécommunications »

Titre :

Etude et simulation d'un réseau LAN développé en utilisant Cisco Packet Tracer

Réalisé par :

Ouazani Amel

Benaichouba Hadjer

Encadré par :

Dr Kaddeche Mourad

Année Universitaire: 2019/2020

Dédicace 01

A mes très chers parents, la lumière de ma vie

Aucun mot ne pourra exprimer mes sentiments envers vous

A mes très chers frères Amin, Yacine et Ishak

A mes petites sœurs Malak et Meriem

A Toutes mes fidèles amies et bien sur mon binôme Amel

A toute la famille Benaichouba et Bellounes

A tous ceux qui j'aime, tous ceux qui m'aiment

Et tous ceux qui me sont chers

A tous mes enseignants et mes camarades de promotion

2020

Je dédie ce travail

Hadjer

Dédicace 02

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

A mes chères sœurs Linda, Kaouthar, Amina et Abir

A mes chers frères Maamar, Khaled, Walid et Mohamed

Qui m'ont également encouragé tout au long de mes études.

A mon fiancé Aissa source d'espoir et de motivation. Et A ma belle mère.

A mes chers Abed elrezak, Hamdido, Silin, Younes et ma princesse Racha.

A Hadjer chère amie avant d'être binôme

A toute mes cousines, toute ma famille et mes proches amies.

Pour finir je remercie mes enseignants et toutes mes amies de la promotion.

Amel

Remerciements

Nous remercions tout d'abord le grand Dieu pour l'achèvement de ce mémoire.

Nous remercions Monsieur Dr. Mourad Kaddeche notre encadreur pour ces conseils et suggestions avisés qui nous a aidés à mener à bien ce travail et l'ingénieur Farouk Bouyahyaoui d'avoir rapporté à ce mémoire ces remarques et conseils.

Nous exprimons nos gratitudes à Monsieur le président de jury d'avoir accepté examiné ce mémoire.

Nous remercions 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

L'organisation et l'optimisation des réseaux locaux d'une entreprise permettent de satisfaire tous les besoins internes de cette entreprise à haute disponibilité.

L'objectif de ce travail c'est de faire une étude générale et simulation d'un réseau local d'entreprise, il s'agit du réseau de notre université Djilali Bounaama.

Ce projet s'intéresse au développement des réseaux LAN avec une prise en charge de la sécurité réseaux et la création des VLANs.

Les configurations et les tests de validation sont conduits sous l'environnement de simulation Cisco Packet Tracer 6.2.

Mots clés : Réseaux locaux, **S**imulation, **C**isco Packet Tracer, **V**LAN

Abstract

The organization and optimisation of the local networks of a company allows to satisfy all the internal needs of this company by high dispnibility.

The objective of this work is to do a general study and simulation of a local network of entreprise of our university Djilali Bounaama.

This project is intersted in the development of LAN networks with security and the creation of VLANs.

Configurations and validation tests are carried out under the Cisco Packet Tracer simulation environment.

Keywords : Local networks, **S**imulation, **C**isco Packet Tracer, **V**LAN

Liste des abréviations

ATM : **A**synchronous **T**ransfer **M**ode

BUS : Broadcast and **U**nknown **S**erver

CD : **C**ompact **D**isk

CLI : Command **L**ine **I**nterface

CSMA/CD : **C**arrier **S**ence **M**ultiple **A**ccess with **C**ollision **D**etection

CSMA/CA : **C**arrier **S**ence **M**ultiple **A**ccess with **C**ollision **A**voidance

DCE : Data **C**ircuit **T**erminating **E**quipment

DHCP : **D**ynamic **H**ost **C**onfiguration **P**rotocol

DTE : Data **T**erminating **E**quipment

DNS : Domain **N**ame **S**ystem

DOS : Denial **O**f **S**ervice

FDDI : **F**iber **D**istributed **D**ata **I**nterface

FTP : **F**ile **T**ransfer **P**rotocol

ICMP ECHO : Internet **C**ontrol **M**essage **P**rotocol

IEEE : **I**nstitue of **E**lectrical and **E**lectronic **E**ngineers

IPV6 : **I**nternet **P**rotocol **V**ersion **6**

LAN : **L**ocal **A**rea **N**etwork

LANE : Local **A**rea **N**etwork **E**mulation

LEC : **LAN E**mulation **C**lient

LECS : LAN Emulation **C**onfiguration **S**erver

LES : LAN Emulation **S**erver

LLC : **L**ogical **L**ink **C**ontrol

LMD : Licence-**M**aster-**D**octorat

MAC : **Media A**ccess **C**ontrol

MAN : **M**etropolitan **A**rea **N**etwork

MITM : Man in **T**he **M**iddle

MODEM : **MO**dulateur-**DEM**odulateur

OSI : **O**rganization **S**ystem **I**nterconnexion

P2P : **P**eer **T**o **P**eer

PC : **P**ersonel **C**omputer

RN4 : Route **N**uméro 4

RNIS : Réseau **N**umérique à **I**ntégration de **S**ervice

SNA : **S**ystem **N**etwork **A**rchitecture

TCP/IP : **T**ransmission **C**ontrol **P**rotocol/ **I**nternet **P**rotocol

UDBKM : Université **D**jilali **B**ounaama **K**hemis **M**iliana

VLAN : Virtual **L**ocal **A**rea **N**etwork

VPN : Virtual **P**rivate **N**etwork

VTP : Virtual **T**runk **P**rotocol

WAN : **W**ide **A**rea **N**etwork

Liste des figures

Chapitre I

Chapitre II

Chapitre III

Liste des tableaux

Table de Matière

Introduction générale

Les réseaux locaux ont été utilisés pour la première fois par les collèges et les universités dans les années 1960. Ces réseaux informatiques ont été utilisés pour cataloguer les collections des bibliothèques, planifier les cours, enregistrer les notes des élèves et partager les ressources matérielles.

Les réseaux locaux ne sont devenus populaires auprès des entreprises qu'après que Xerox PARC ai développé Ethernet en 1976. la Chase Manhattan Bank à New York a été la première utilisation commerciale de cette nouvelle technologie Au début des années 1980, de nombreuses entreprises disposaient d'un réseau Internet (Intranet) composé de centaines d'ordinateurs qui partageaient des imprimantes et des fichiers sur même site.

Après la sortie d'Ethernet, des sociétés telles que Novell et Microsoft ont développé des produits logiciels pour gérer ces réseaux LAN Ethernet. Au fil du temps, ces outils de réseautage sont devenus partie intégrante des systèmes d'exploitation informatiques populaires Microsoft Windows 10 dispose d'outils pour configurer un réseau domestique.

Durant ces dernières années et avec le développement technologique actuel les réseaux locaux sont connus une évolution remarquable et très importante dans divers domaines car le réseau LAN est le cœur de chaque entreprise, le principal but de ce développement n'est plus de proposer un moyen de connecter les gens, mais plutôt de fournir la meilleure connexion et le meilleure service possible et d'augmenter les volumes et les vitesses de transfert des données au moindre coût.

L'objectif principal de notre travail consiste à une contribution à l'étude et la simulation de l'architecture réseau de notre université Djilali Bounaama- khemis miliana en utilisant le logiciel Cisco Packet Tracer 6.2.

Notre travail est divisé en trois chapitres principaux :

Dans Le premier chapitre nous allons établir une description générale sur les réseaux el les éléments indispensables qui contribuent à la réalisation de ce dernier.

Le deuxième chapitre concerne le développement et la sécurité dans les réseaux locaux : nous commençons par une brève étude sur les notions de base des réseaux LAN puis les principaux domaines de développement actuel et nous présenterons quelques concepts de base sur la sécurité réseau.

Dans le troisième et dernier chapitre nous avons faire deux parties : la première partie concernant le réseau de notre université Djilali Bounaama que nous avons étudié, la deuxième partie concernant la simulation de ce réseau à l'aide de logiciel Cisco Packet tracer 6.2.

A la fin de ce mémoire, nous donnerons une conclusion générale avec les perspectives.

Chapitre I

Généralités sur les réseaux informatiques

I.1. Introduction

L'objectif de ce chapitre introductif est de comprendre quelques notions de base sur les réseaux informatiques et plus particulièrement sur les réseaux locaux.

D'abord, un réseau informatique est un ensemble des ordinateurs et des périphériques relies entre eux par des canaux électroniques (filaire ou sans fil) pour le but d'échanger des informations (partage des ressources, envoie des fichiers et des messages).

I.2. Réseaux informatiques

La technologie des réseaux informatique constitué l'ensemble des outils qui permettent à des ordinateurs de partager des informations et de ressources.

Un réseau est constitué d'équipement appelé nœuds .ces réseaux sont catégorisés en fonction de leur étendue et de leur domaine d'application.

Pour communiquer entre eux, les nœuds utilisent des protocoles, ou langages, compréhensibles par tous. [1]

I.3. Types des réseaux

Nous distinguons le type de réseau selon plusieurs critères tel que : la taille de réseau, la vitesse de transfert des données et leur étend.

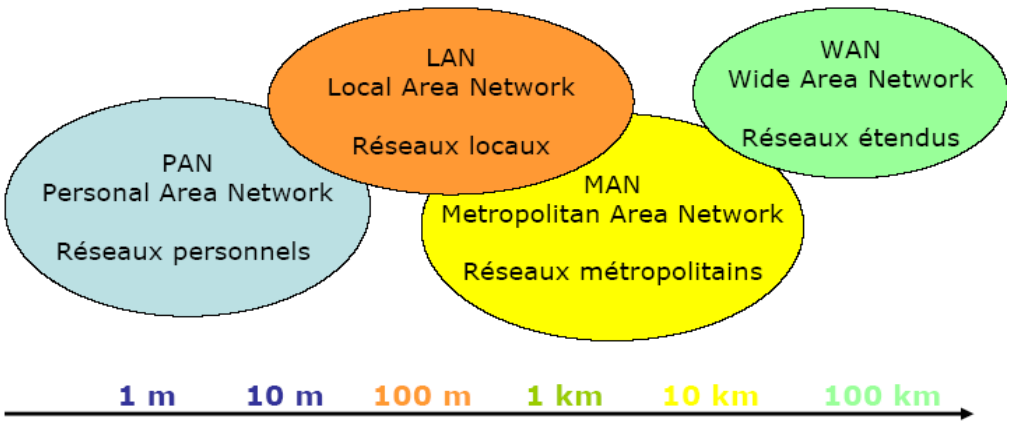


Figure I.1 : Schéma montrant l'échelle de type des réseaux informatique

I.3.1 Réseau LAN

LAN signifie Local Area Network (en français Réseau Local). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

Un réseau local est donc un réseau sous sa forme la plus simple.

La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (pour un réseau Ethernet par exemple) et 1 Gbps (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs. [2]

I.3.2. Réseau MAN

Les MAN (Metropolitan Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local.

Un MAN est formée de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique). [2]

I.3.3. Réseau WAN

Les étendues des réseaux les plus conséquentes sont classées en Wide Area Network(WAN), constitué de réseaux de types LAN, voire MAN, les réseaux étendus sont capable de transmettre les informations sur les milliers de kilomètres à travers le monde entier .le WAN le plus célèbre est le réseau public internet dont le nom provient de cette qualité : inter Networking ou interconnexion de réseaux. [1]

I.4. Topologies des réseaux

I.4.1. Topologie en bus

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câbles,

Généralement de type coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau. Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté. [3]

I.4.2. Topologie en Etoile

Dans un réseau en étoile, la forma physique de réseau ressembleà une étoile. N'importequelappareil (routeur, commutateur, concentrateur,…) peut être au centre d'un réseau en étoile. L'important, c'est que pour parler à uneautre entité en passe par le matériel centrale (qui peut être le hub, le Switch,…).

En pratique, dans un réseau d'entreprise en étoile, au centre en trouve un Switch.

Le principale défaut de cette topologie, c'est que si l'élément centrale ne fonctionne plus, plus rien ne fonctionne : toute communication est impossible. Cependant il n'y a pas de risque de collision de données. [4]

I.4.3. Topologie en Anneau

Dans un réseau possédant une topologie en anneau, les ordinateurssont théoriquement situés sur une boucle et communiquent chacun à leur tour. Ils sont en réalité reliés à un répartiteur (MAU) qui va gérer la communication entre eux en impartissant à chacun un « temps de parole ». [3]

I.4.4. Topologie en Arbre

Dans l'architecture en arbre, les photos sont reliées entre eux de manièrehiérarchique, à l'aide concentrateurs cascadables. Cette connexion doit être croisée. [1]

I.4.5. Topologie en Maille

Le principe de la topologie maillée est de relier tous les ordinateurs entre eux (au du moins, un maximum). Commença, aucune risque de panne général si la machine tombe en rade, mais si vous vous prenez les pieds dans des câbles, étant donnée qu'il y en a partout c'est la cata, vous faits tous tomber.

Cette topologie reste peut utiliser vu la difficulté à mettre au place tell infrastructure. [4]

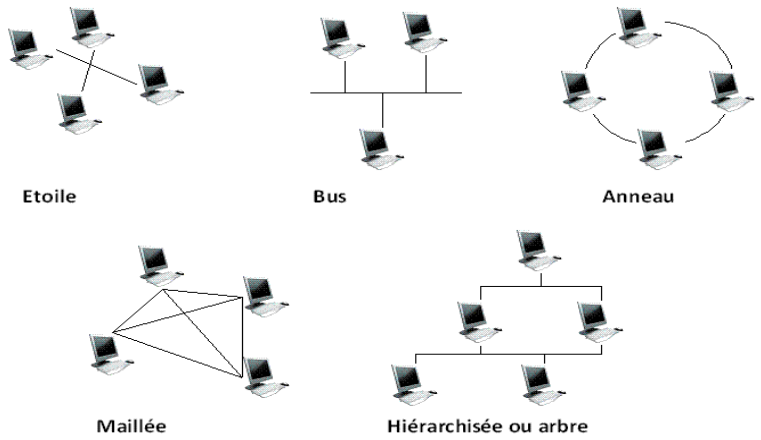


Figure I.2 : Schéma général montrant les topologies des réseaux informatiques

I.5. Classification des réseaux selon l'architecture

Nous distinguons également deux catégories de réseaux :

- Réseaux poste à poste (Peer to Peer=P2P).
- Réseaux client/serveur.

I.5.1. Réseaux poste à poste

Contrairement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié. Ainsi chaque ordinateur dans un tel réseau joue à la fois le rôle de serveur et de client. Cela signifie notamment que chacun des ordinateurs du réseau est libre de partager ses ressources.

Les réseaux poste à poste ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés. Tous les systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste à poste.

Dans un réseau poste à poste typique, il n'y a pas d'administrateur. Chaque utilisateur administre son propre poste. D'autre part tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent (données dans des répertoires partagés, imprimantes, cartes fax etc.). [2]

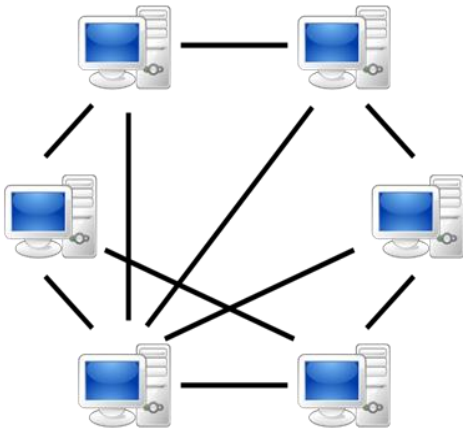


Figure I.3 : Schéma montrant le réseau poste à poste

I.5.2. Réseau Server/Client

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine Généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services. Ces Services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, etc. Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. On parle ainsi de client (client FTP, client de messagerie, etc.) lorsque l'on désigne un programme tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès d'un serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client de messagerie il s'agit de courrier électronique). [2]

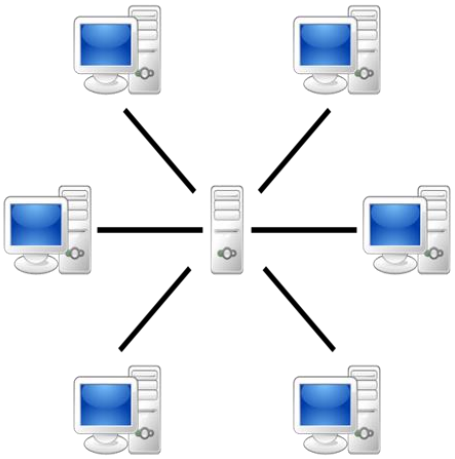


Figure I.4 : Schéma montrant le réseau Server/Client

I.6. Modèle OSI

I.6.1. Principe du Modèle OSI

L'organisation ISO a défini en 1984 un modèle de référence, nommé open system interconnexion(OSI) destiné à normaliser les échanges entre deux machines, il définit ce que doit être une communication réseau complète, l'ensemble du processus est ainsi découpé en sept couche hiérarchiques.

Ce modèle définit précisément les fonctions associées à chaque couche. Chacune d'entre elle se comporte comme un prestataire de service pour la couche immédiatement supérieure. Pour qu'une couche puisse envoyer une commande ou des données au niveau équivalent du correspondant, elle doit constituer une information et lui faire traverser toutes les couches inferieure, chacune d'elle ajoutant un en-tête spécifique à ce qui devient une sorte de train, cette information est décodée, la commande ou les données sont libérées. [1]

I.6.2. Description des couches du modèles OSI

- **Couche physique**

La couche physique assure un transfert de bit sur le canal physique (support). A cette effet, elle définit les supports et les moyennes d'y accéder : spécification mécaniques (connecteurs), spécification électriques (niveaux des tensions), spécification fonctionnaire des éléments de raccordement nécessaire à l'établissement, au maintien et a libération de la ligne. Elle détermine aussi les moyennesd'adaptation.

- **Couche liaison de données**

La couche de la liaisons de données assure sur la ligne un service de transfert de bloc de données (trame) entre deux systèmes adjacents on assurant le contrôle , l'établissement, le maintien et la libération du lien logique entre les entités .

- **Couche réseau**

La couche réseau assure lors d'un transfert à travers un système relais, l'acheminement de données (paquets) à travers des différents nœuds d'un sous réseau (routage). Les protocoles de ce niveaux fournissent les moyennes d'assurer l'acheminement de l'appel, le routage, le contrôle de congestion, l'adaptation de la taille des blocs de données aux capacités de sous réseau physique utilisée. Elle offre en outre un service de facturation de la présentation fournit par le ce réseau de transport.

- **Couche transport**

La couche transport est la couche pivot du modèle OSI. Elle assure le contrôle du transfert de bout en bout des informations (messages) entre les deux systèmes d'extrémités .la couche transport est la dernière couche de contrôle des informations, elle doit assurer aux couche supérieure un transfert faible quelle que soit la qualité du sous réseau de transport utilisés.

- **Couche session**

La couche session gère l'échange de données (transaction) entre les applications distantes. La fonction essentielle de la couche session est la synchronisation des échanges et la définition de points de reprises.

- **Couche présentation**

Interface entre les couches qui assurent l'échanges de données et celle qui les manipules, cette couche assure la mise en forme des données, les conversions des codes nécessaires pour délivrer a la couche supérieure un message dans une syntaxe compréhensible par celle-ci .on outre, elle peut, éventuellement, réalisée des transformations spéciales, comme la compression de données.

- **Couche application**

La couche application, la dernière du modèles de référence, fournit au programme utilisateur, l'application proprement dite un ensemble de fonctions (entités d'application) permettant le déroulement correcte des programmes communicant (transfert de fichiers, courrier électronique…). [6]

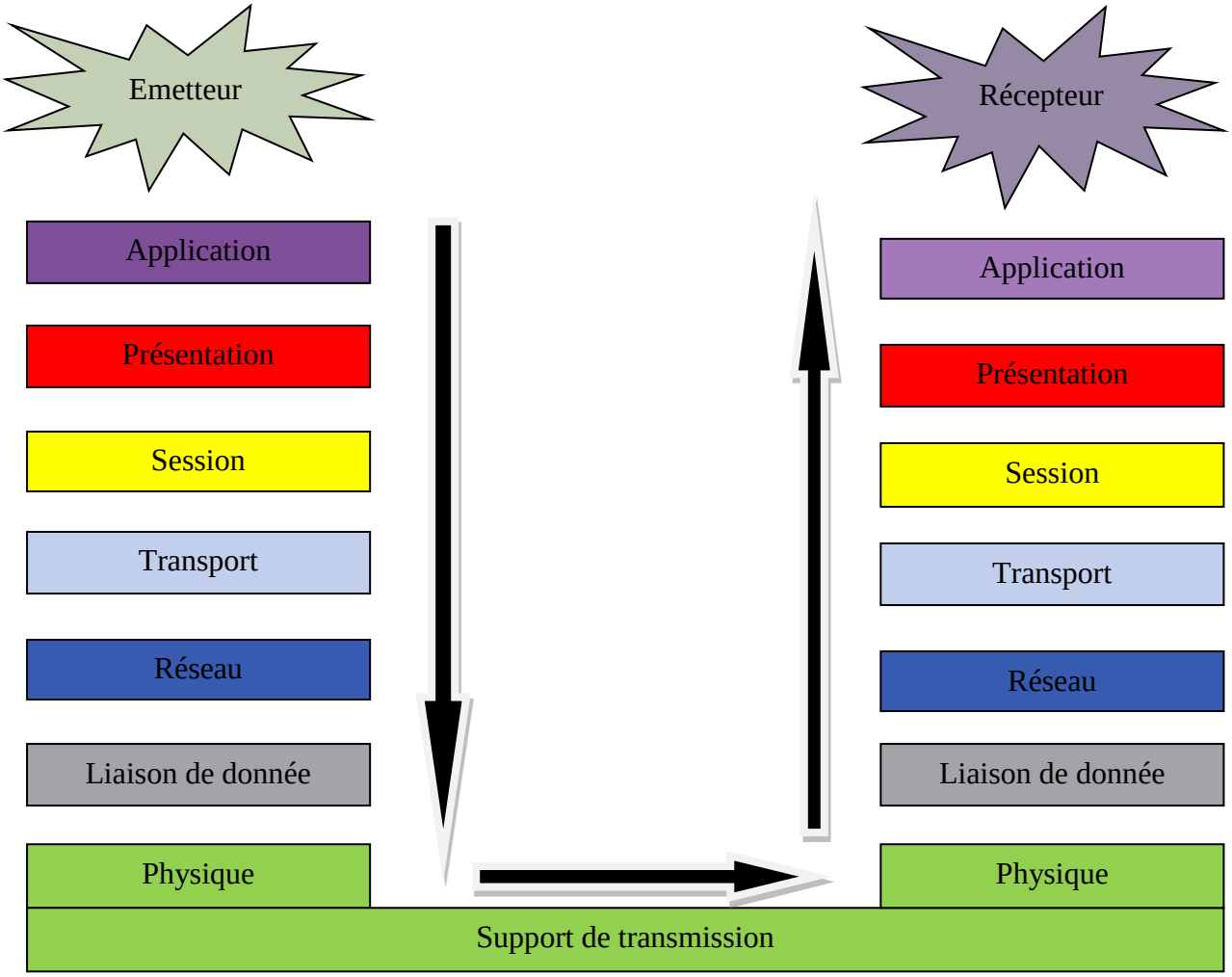


Figure I.5 : Modèle OSI en détail

I.7. Modèle TCP/IP

I.7.1. Principe du modèle TCP/IP

Le modèle TCP/IP est l'ensemble des protocoles utilisées pour le transfert ou la transmission des données sur internet, son nom est l'abréviation de (Transmission Control Protocole/Internet Protocole), ce modèle et la pile de protocole TCP/IP rendent possible l'échange des données entre deux machines partout le monde.

I.7.2. Description des couches du modèle TCP/IP

Le modèle TCP/IP comporte quatre couches, à chaque couche une information est ajoutée au paquet des données il s'agit d'un en-tête :

- **Couche accès réseau**

Il regroupe les couches liaisons des données et les couches physiques du modèle OSI.

- **Couche internet**

La couche internet, correspondant à la couche réseau du modèle OSI.

- **couche transport**

Son rôle est le même que celui de la couche transport du modèle OSI, permettre à des entités paires de soutenir une conversation.

- **Couche Application**

La couche application, similaire à la couche homonyme du modèle OSI.

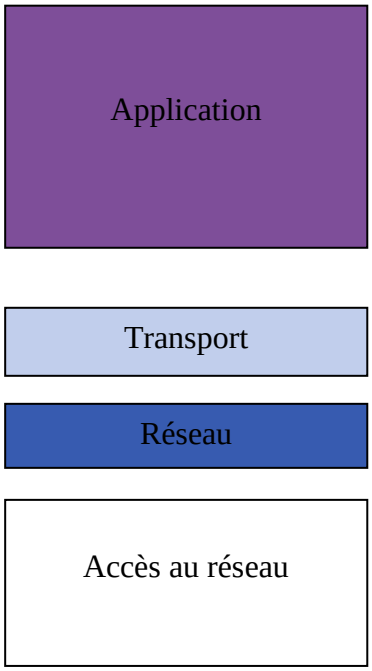


Figure I.6 : Modèle TCP/IP.

1.8. Supports de transmission

- **Paires torsadées**

La paire torsadée ou symétrique de deux conducteurs identiques torsadés. Les torsades réduisent l'inductance de la ligne (L) généralement plusieurs paires sont regroupées sous une enveloppe protectrice appelée gaine pour former un câble. Les câbles contiennent 1

paire (desserte téléphonique), 4paires (réseaux locaux), oùplusieursdizaines de paires (câble téléphonique). [5]

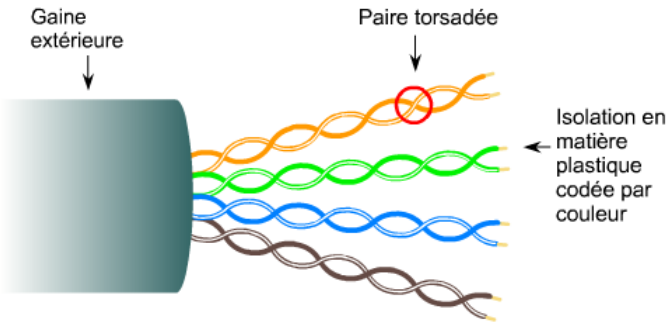


Figure I.7 : Câble paire torsadée

- **Câble coaxial**

Une paire coaxial ou câble coaxial est constituée de deux conducteurs concentriques maintenus à distance constante par un diélectrique. Le conducteur extérieurtressemétallique en cuivre recuit appelée blindage est mis à la terre. L'ensemble est protégé par une gaine isolante.

Le câble coaxial possède des caractéristiquesélectriques supérieures à celles de la paire torsadée. Il autorise des débits plus élevés et est peu sensible aux perturbations électromagnétiques extérieures. Le taux d'erreur sur un tel câble est d'environs10^{-9}. [5]

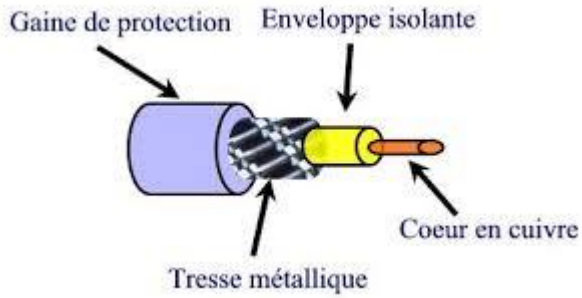


Figure I.8 : Câble coaxial

- **Fibre optique**

La fibre optique est un guide d'onde optique à section circulaire constitué de plusieurs couches de matériaux électriques (plastique, verre), le cœur d'indice de réfraction n1 dans lequel la lumière se propage, la gaine optique d'indice de réfraction n2 qui réalise le confinement optique, et la gaine de protection.

La fibre est transfère des données numérique sous forme d'impulsion lumineuses modulées .une diode laser émet le signal lumineux qui est récupéré à l'autre extrémité par une photodiode qui transfère le signal en signal électrique. [1]

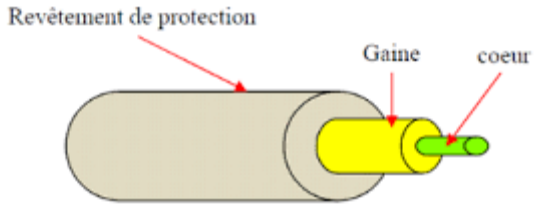


Figure I.9 : Câble fibre optique

I.9. Équipements de base d'un réseau

- **Carte réseau**

La carte réseau est le composant le plus important de base indispensable. C'est par elle que transitent toutes les données à envoyer et à recevoir du réseau dans un ordinateur. [4]

- **Commutateur (Switch)**

Est un périphérique de mise en réseau multicast fonctionne dans la couche liaison de données de modèle OSI, il utilise un table de commutation qui lui permettre de faire une correspondance entre les adresses MAC et les ports qui lui permettre de bien envoyer les paquets aux destinataires.

- **Concentrateur (hub)**

Est un dispositif de diffusion de réseau simple qui fonctionne dans la couche physique du modèle OSI qui lui connecte plusieurs ordinateurs dans un réseau, il envoie les données d'un PC vers tous les autres PC.

- **Routeur**

Est un périphérique réseau, fonctionne dans la couche réseau du modèle OSI, il utilise pour relier deux réseaux différents. Ou plus il travaille avec les adresses IP seulement il utilise une table de routage pour savoir ou transfère les paquets IP.

- **Répéteur**

Il agit au niveau de la couche physique de modèle OSI. Il permet d'étendre la longueur maximale d'un segment, en amplifiant le signal en même temps qu'il permet d'interconnecter deux supports physiques différents. [1]

- **Ponts**

Les ponts ou bridges sont des éléments d'interconnexion de niveau 2(couche liaison des données), Ils permettent d'interconnecterdeux ou plusieurs réseaux (ponts multiports) dont les couches physiques sont dissemblables, Les ponts sont transparents aux protocoles de niveau supérieur. [5]

- **Passerelle**

Il s'agit d'une machine, en général un serveur dédié, qui opère au niveau des couches 3 à 7 en tant que traducteur des couches moyennes et hautes, notamment pour la mise en forme des données.

Avec la généralisation de l'usage de TCP/IP, les passerelles sont moins utilisées. On en retrouve surtout pour l'interconnexion entre ces protocoles et des grands environnements, exploitants system network architecture(SNA). [1]

Conclusion

Tout a long de ce chapitre ,nous a permis de mieux comprendre des notions sur les réseaux informatiques à partir de leurs définitions, leurs types et leurs topologies et une description du modèle OSI et TCP /I . Ainsi que nous avons donné une vue sur les équipements d'interconnexions dans un réseau local.

Chapitre II

Développement et sécurité dans les réseaux locaux

II.1. Introduction

Ce chapitre sera réservé à l'étude des réseaux locaux, ses besoins, ses caractéristiques … puis nous allons passer aux développements des réseaux LAN qui sont notamment connu un large succès. Ensuite nous allons étudier la sécurité qui est caractérisée comme un concept très important dans tous les réseaux, nous parlons sur les différentes techniques des attaques réseau ainsi que les moyens et les technologies qui permettent de faire face à ces attaques.

II.2. Rappel sur les réseaux LAN

Les réseaux locaux, également appelé LAN (Local Area Network), correspondent par leur taille aux réseaux intra-entreprise. Ils servent au transport de toutes les informations numériques de l entreprise. En règle générale, les bâtiments à câbler s étendent sur plusieurs centaines de mètres. Les débits de ces réseaux vont aujourd'hui de quelques mégabits à plusieurs centaines de mégabits par second [8].

Un LAN est un réseau limité à un espace géographique comme un bâtiment. Par exemple, l'ensemble des ordinateurs dans une école forme un LAN. Ce type de réseau utilise généralement une configuration de type domaine [4].

II.3. Besoins du réseau LAN

Le réseau local à pour but :

- De mettre en commun des données communes à plusieurs utilisateurs (fichiers comptable par exemple...)
- De partage des périphériques (FAX, MODEM, imprimantes lecture de CD ROM...)
- De partager un accès à Internet
- De partager des applications ex : partage d'un logiciel d'application
- De partager des documents (classeur Excel, textes Word, base de données partagée)
- D'accéder à un site d'intranet

De plus, les matériels les plus anciens peuvent être connectés au réseau et bénéficier des ressources du serveur.

Chaque utilisateur peut travailler en autonomie avec ses propres logiciels tout en bénéficiant des données d'autres utilisateurs, stockées au niveau du serveur(ou d'un poste faisant office de serveur).

- Le partage de ressources matérielles permet de réaliser des économies substantielles (achat d'une seule imprimante pour plusieurs postes)
- Le développement des intranets améliore considérablement la communication (les informations d'entreprise sont consultable sur le site web Intranet, les échanges entre les services peuvent avoir lieu en utilisant la messagerie locale,...) [9].

II.4. Caractéristiques des réseaux locaux

Les caractéristiques principales permettant sur le plan physique de définir un réseau local sont :

II.4.1. Topologie

Dans un réseau local, on distingue deux types de topologie ;

La topologie physique concerne la façon dont les machines sont connectés c'est-à-dire le câblage (Bus, anneau, étoile …) comme nous avons vu dans le chapitre précédent (chapitre 01).

La topologie logique qui indique comment les informations circulent dans un réseau. (L'adressage).

II.4.2. Méthode d'accès au Support

Chaque type de réseau local possède une méthode d'accès au support. Elle concrétise la manière dont chaque nœud peut envoyer des trames sur le réseau sans créer de conflit avec des trames émises par d'autres nœuds. La méthode d'accès est souvent conditionnée par la topologie utilisée. Ainsi, sur un bus série 2 stations ne peuvent émettre en même temps sans provoquer une interférence entre les 2 signaux électriques émis. Cette interférence est appelée «collision » [10].

a- CSMA/CD (Carrier Sence Multiple Access with collision Détection)

Est une méthode d'accès utilisée sur les bus séries. Elle a pour but d'éviter les collisions et de les détecter si elles se produisent.

Dans un premier temps, la station qui désire émettre, 'écoute' si un signal est émis par un autre nœud du réseau. Cette fonction est assurée par une mesure physique de signal électrique sur le bus.

Si le réseau semble non occupé, le nœud émet sa trame qui est diffusée sur l'ensemble du réseau.

Cependant, suite au temps de propagation du signal électrique sur le support, il se peut qu'au moment de « l'écoute », le réseau semblait libre alors qu'un autre nœud était déjà en train d'émettre. Il se produit alors une collision. La transmission des 2 trames est perturbée. Chaque

station détecte cette collision par un moyen physique (mesure du signal électrique). L'émission des trames est arrêtée.

Une procédure de retransmission est alors entamée dans chacun des nœuds après un délai qui fixé de façon différente (T1 et T2) dans chaque nœud [10].

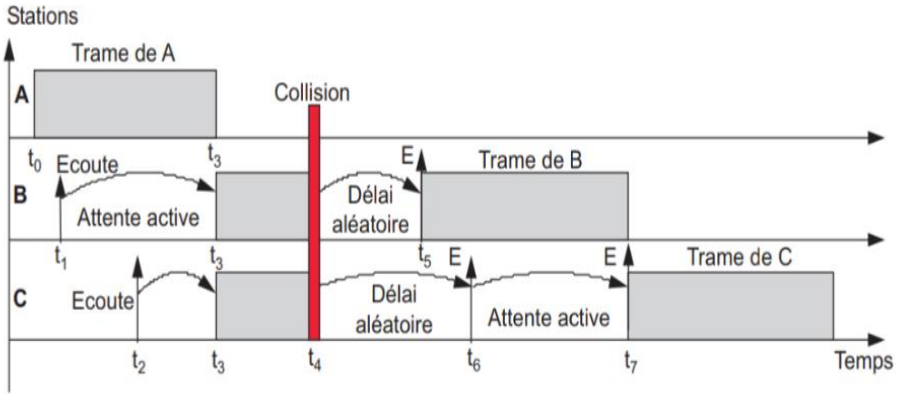


Figure II.1 : Principe du CSMA /CD [5]

Explication

La station a diffusé son message (t0 à t3). La station B, avant d'émettre, se met à l'écoute (t1). Le support est occupé elle diffère son émission, mais reste à l'écoute (attente active). De même C en t2 se porte à l'écoute et retarde son émission. En t4 chacune des stations détecte que son message est altéré, la collision est détecté. B et C cessent leur émission de déclenchent une temporisation aléatoire. En t5, le timer de B arrive à échéance. Le canal étant libre, B émet. En t6, C détecte le support occupé et diffère son émission jusqu'au temps t7. [5]

b-CSMA/CA (Carrier Sence Multiple Access with collision Avoidance)

Cette méthode reprend les principes de CSMA/CD en ce qui concerne « l'écoute ».mais la détection des collisions n'est pas assurée par un moyen physique, mais par une procédure logicielle [9].

c-Jeton(Token)

En fonction de la topologie physique, il existe deux variantes de cette méthode :

-Jeton sur anneau (Token Ring)

Une trame comportant un bit spécial appelé jeton tourne en permanence sur l'anneau. Les stations reçoivent et expient tour à tour cette trame. La station qui veut émettre modifie la valeur du jeton, la trame est considère occupée et les données sont placées dans le champ

approprié. La trame ayant fait un tour complet après passage dans toutes les stations, le jeton est repositionné à sa valeur de départ. La trame considère alors comme vide. Avec ce système une seule station peut émettre des données à la fois, ce qui élimine tous les risques de conflit. Cette méthode d'accès est dite déterministe, car on peut calculer en tenant compte du nombre de stations, le temps qui s'écoute entre 2 accès d'une station au réseau. [10]

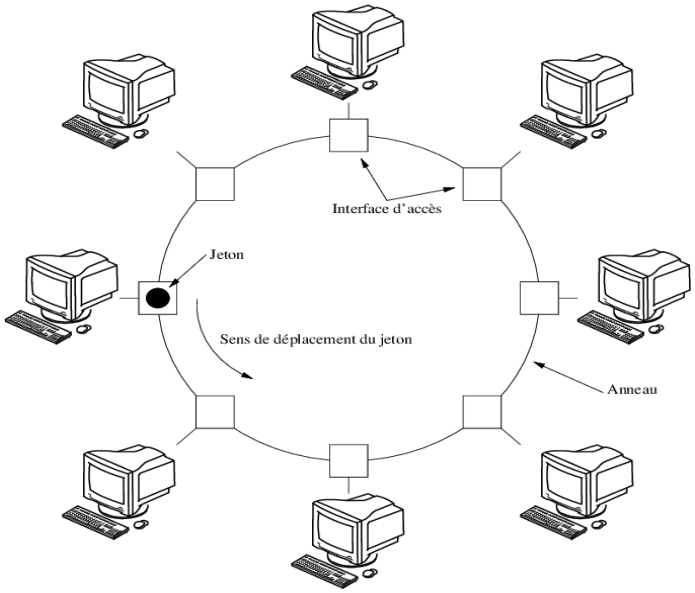


Figure II.2 : principe de jeton sur anneau

- Jeton sur Bus (Token Bus)

Dans la technique d'accès « jeton adressé sur bus », le jeton circule de la station de plus faible à celle de plus forte adresse, formant ainsi un anneau virtuel sur le bus (anneau logique/bus physique). Dans le système représenté **(figure II.2)**, chaque station à tour de rôle reçoit le jeton. Si elle a des données en attente d'émission, elle les émet puis passe le jeton à la station suivante (celle dont l'adresse suit la sienne).

Toutes les stations en fonctionnement sur le réseau perçoivent le message (bus), mais seule celle dont l'adresse est contenue dans le jeton, considère l'avoir reçu (jeton adressé). Si elle n'a rien à émettre, elle transfère immédiatement le jeton à la station suivante [5].

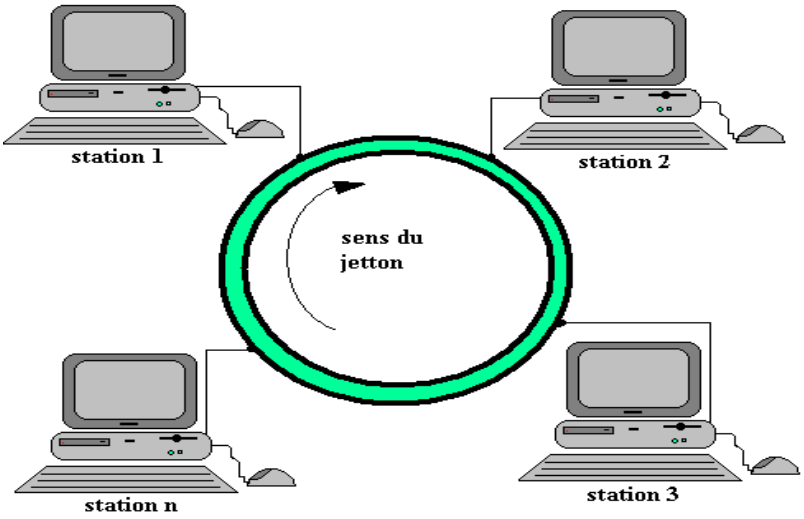


Figure II.3 : Principe de jeton sur bus

II.4.3. Technique de transmission

Il existe 2 méthodes de transmission possibles sur les réseaux locaux :

La méthode Large Bande (signal analogique)

La méthode Bande de base (signal numérique)

Pour des raisons pratiques, seule cette dernières est vraiment utilisée. Les données sont envoyées en mode série et sous forme numérique sur le support. Pour des raisons tenant à la synchronisation du récepteur et à la largeur de bande du signal à transmettre les données sont toujours envoyées de façon codée sur le support [10].

II.4.4. Support de transmission

Le signal représentant les données doit disposer d'un support pour être véhicule. Le signal électrique utilise des supports à base cuivre (pires torsadées ou câbles coaxiaux).le signal lumineux utilise les différents types de fibre optiques ou l'air (infrarouge, rayon laser) [10].
Nous avons vu leurs explications en détails dans le chapitre précédent (chapitre 1).

II.4.5. Débit binaire

Le premier réseau local vraiment répondu dans les années 80 fut le réseau AppleTalk. Sa partie physique est nommée Local Talk. Le débit est de 230.4 Kbps.

Un autre réseau, starlan, annonciateur d'Ethernet fonctionnant à 1 Mbps.

Les 2 versions de Token-Ring fonctionnent respectivement à 4 et 16 Mbps.

Ethernet fonctionne actuellement à 10 Mbps et tend vers 100 Mbps [10].

II.5. Normalisation

II.5.1. Modèle OSI

Nous avons vu leurs explications dans le chapitre précédent (chapitre1)

II.5.2. Normalisation IEEE

L'Institute of Electrical and electronic Engineers (IEEE) est une organisation professionnelle qui définit les normes touchant les réseaux. Les normes de l'IEEE (dont IEEE 802.3 et IEEE 802.5) sont actuellement les normes prédominantes et les plus connues dans le monde en matière de réseau local. La norme IEEE 802.3 définit la couche physique, ou couche 1 et la portion d'accès au canal de la couche liaison de données, ou couche 2.

Le modèle OSI comporte sept couches. Les normes de l'IEEE ne concernent que les deux couches inférieures ; par conséquent, la couche liaison de données se devise en deux parties :

- La norme LLC 802.2, non tributaire de la technologie
- Et des éléments tributaires de la technologie, qui intègrent la connectivité de la couche

L'IEEE divise la couche liaison OSI en deux sous-couches distinctes. Elle connait les sous-couches suivantes

-Media Access Control (MAC) (transitions vers le bas jusqu'au média)

-Logical Link Control (LLC) (transitions vers le haut jusqu'à la couche réseau). [11]

II.5.3. Couches MAC et LLC

a. Sous couches MAC

La sous-couche MAC concerne les protocoles que doit suivre un ordinateur hôte pour accéder au média physique.

Sans adresse MAC, votre réseau local comporterait un groupe d'ordinateur sans nom.

Chaque ordinateur a une façon unique de s'identifier. Tout ordinateur qu'il soit relié à un réseau ou non comporte une adresse physique. Il n'y a jamais deux adresses physiques identiques. L'adresse physique appelée adresse MAC, se trouve sur la carte réseau [11].

b. Sous-couche LLC

L'IEEE a créé la sous-couche LLC afin de permettre à une partie de la couche liaison de données de fonctionner indépendamment des technologies existantes.

La sous-couche LLC de la couche liaison de donnée gère les communications entre les dispositifs sur une liaison particulière d'un réseau. Cette sous-couche est définit dans la norme

IEEE 802.2 et autorise tant les services sans connexions que les services orientés connexion qui sont utilisée par les protocoles de couche supérieure. La norme IEEE 802.2 définit un certain nombre de champs dans les trames de couche liaison de donnée, qui permet à plusieurs protocoles de couche supérieure de partager une liaison de données physique [11].

II.6. Notions sur le développement dans un réseau LAN

De nos jours, l'information et les télécommunication occupent une place prépondérante dans notre vie ; donc avec l'évolution de la technologie l'avenir des réseaux informatiques soit de grandir et de se développer, ce développement peut répondre aux besoins des générations présente qui est appliquer à la croissance surtout dans les entreprises et les sociétés .Aujourd'hui, nous pouvons partager des applications, échanger des informations, consulter des bases des données et effectuer des transferts de la parole ,des photos, de la vidéo ou des fichiers entre plusieurs poste à distance ;toutes ces applications sont possible grâce aux développements des réseaux informatiques.

Maintenant, la tendance dans les réseaux d'entreprises est la transmission numérique et à l'utilisation de la communication sans fils ; de plus la technologie actuelle permet d'accroitre les volumes et les vitesses de transfert des données tout en diminuant les couts.

A l'heure actuelle, tous les entreprises et l'utilisateur cherchent à se protéger leurs données et comme des informations confidentielle circulent dans les réseaux, la sécurité des communications est devenue une préoccupation très important contre des utilisateurs frauduleuse et des intrusions malveillantes dans les systèmes informatique.

Dans tout les cas ; un réseau local utilise un support de transmission était initialement réalisées par des câbles en cuivre (coaxial ou paire torsadée) ; on trouve aussi maintenait des liens en fibre optique.

Enfin, on dit qu'avec l'évolution de la technologie les réseaux locaux cannaient un large développement dans tous leurs domaines.

II.7. Domaines de développement

Les évolutions récentes dans le domaine des réseaux locaux ont pour but l'augmentation du taux de transfert utile, l'amélioration de la flexibilité, la simplification de l'administration et l'homogénéisation des supports. Le taux de transfert peut être augmenté par un changement technologique (passage d'Ethernet à Fast Ethernet, Gigabit Ethernet ou ATM) ainsi que, dans certains cas, par une amélioration des techniques d'interconnexion entre les stations (segmentation d'un réseau Ethernet, remplacement des concentrateurs par des commutateurs). L'amélioration de la flexibilité et la simplification de l'administration (tout en restant

compatible avec l'exigence d'augmentation du taux de transfert) impliquent en général la définition de réseaux locaux virtuels. L'homogénéisation des supports signifie souvent le passage à ATM (technologie développée au départ pour WAN ou MAN) sur le réseau local [16].

II.7.1. Évolution d'IP : IPv6

Actuellement, l'internet mondial utilise encore majoritairement le protocole IPv4, ou internet Protocol 4. Cependant, un problème majeur va se poser dans les années à venir : toutes les adresses IPv4 seront bientôt attribuées. Un nouveau protocole, nommées IPv6 à commencer à être déployé pour palier à ce problème. En plus de fournir une infinité d'adresse IP supplémentaire, cette technologie comporte quelque différences et avantages par rapport à son ancêtre l'IPv4.

L'IPv6 à celle été créé en 1990. Elle compte 16 octets, au format hexadécimal qui sont séparés par deux points. Cela donne donc une taille d'adresse de 128 bits, correspondant à 340 sextillions d'adresses uniques. Donc cette quantité d'adresses et une meilleure agrégation des routes dans la table de routage d'internet.

II.7.2. Augmentation du débit

a. Support de transmission

Le choix du câblage effectué a un grand important dans toutes les sociétés car une erreur dans le choix peut être payée très cher. Aujourd'hui , de nombreuses entreprises de télécommunications utilisent la fibre optiquepour remplacer le fil de cuivre ; parce que ce dernier est moins efficace et sa vitesse de transmission relativement faible et son inconvénient majeur est une forte atténuation mais le guide optique sa vitesse de transmission plus rapide avec moins d'atténuation et une grande capacité de transfert d'information comme il caractérise par un avantage très utile c'est l'aspect sécurité : il est très difficile de brancher une écoute sur câble optique .

b. Evolution Ethernet vers le haut débit

La décision suivante concerne le débit du réseau, c'est-à-dire la vitesse de transmission des trames Ethernet, encore appelée bande passante ; Avec l'évolution d'Ethernet, Il existe actuellement trois déclinaisons d'Ethernet normalisées par l'IEEE (*Institute of Electrical and ElectronicsEngineers*) : le **10bT** à 10 Mbit/s (norme 802.3), le **100bTx** alias Fast Ethernet à 100 Mbit/s (norme802.3u) et le **1000bT** alias Gigabit Ethernet (norme802.3ab).

Le premier chiffre qualifie le débit du réseau Ethernet, la lettre “ b ” signifie un codage des signaux en bande de base (ex : Manchester) et la lette “ T ” représente “ *Twisted Pair* ”, ce qui signifie que le réseau Ethernet fonctionne sur un câblage en cuivre paires torsadées.

Il existe également les mêmes déclinaisons fonctionnant sur fibre optique : **10bF**, **100bFx** et **1000bX** (norme 802.3z). Parmi cette dernière, on distingue le **1000bSX** (S pour *short wavelength*) opérant à 850 nmsur fibre optique multi mode et le **1000bLX** (L pour *long wavelength*) opérant à 1 300 nm sur les fibres multi mode et monomode [15].

Ethernet	Codage en ligne	Codage complet	Paires cuivre utilisées	Fréquence du signal / Longueur d'onde	Distance maximale
10bT	Manchester	---	1,2 / 3,6	10 MHz (±15%)	100 m
10bF (FL et FB)	Manchester	---	---	850 nm	2 000 m
100bTx	NRZI	4B/5B	1,2 / 7,8	62,5 MHz	100 m
100bFx	NRZI	4B/5B	---	850 nm	2 000 m
1000bT	PAM5	8B1Q4	Toutes	125 MHz	100 m
1000bSX	NRZ	8B/10B	---	850 et 1 300 nm	220 à 550 m*
1000bLX	NRZ	8B/10B	---	1 300 et 1 550 nm	550 à 5 000 m*

Tableau II.1 : quelques notions sur l’Ethernet [15]

II.7.3. Émulation LAN sur ATM(LANE)

a. Description ATM

ATM (*Asynchronous Transfer Mode*) est une technique de transport asynchrone utilisant des paquets de 53 octets, développée pour servir de support au réseau numérique à intégration de services (RNIS) large bande (*Broadband* ISDN). Ceci signifie que ATM devrait permettre de transporter à la fois des informations isochrones (voix, sons, images animées) et asynchrones (données) [16].

b. Principe de fonctionnement

L'intérêt de l'émulation LAN est de permettre l'utilisation avec une nouvelle technologie de transport, ATM, des logiciels développés pour un LAN IEEE 802, et d'assurer ainsi une (éventuelle2) transition par étapes vers le tout ATM. Les composantes essentielles d'un LANE sont : [15]

- Les LEC (*LAN Emulation Client*) sont des composants logiciels présents sur les machines connectées au réseau. Ces composants logiciels se situent dans la couche liaison du LAN émulé et permettent de garder l'interface avec les couches supérieures malgré le remplacement de la technologie support du LAN par l'ATM. Chaque LEC possède deux adresses, une adresse IEEE 802 MAC sur 48 bits et une adresse ATM sur 20 octets [16].

- Le LES (LAN Emulation Server) est un composant logiciel (situé sur une machine connectée au réseau ou sur un commutateur ATM) qui garde les associations adresse IEEE 802 « adresse ATM et qui répond donc à des requêtes LE-ARP (LAN Emulation AddressResolution Protocol) envoyées par les LEC [16].
- Le BUS (Broadcast and Unknown Server) est un composant logiciel (situé sur une machine connectée au réseau ou sur un commutateur ATM) qui permet d'effectuer des envois de type broadcast sur le LANE. Pour cela, le BUS maintient des circuits virtuels (CV) bidirectionnels avec chaque LEC (pour le transfert des demandes de broadcast) et un CV unidirectionnel sous forme d'arbre en direction des LEC (pour l'envoi des broadcaste) [16].
- Le LECS (LAN Emulation Configuration Server) est un composant logiciel (situé sur une machine connectée au réseau ou sur un commutateur ATM) qui garde les configurations des différents LANE présents sur le même réseau support ATM [16].

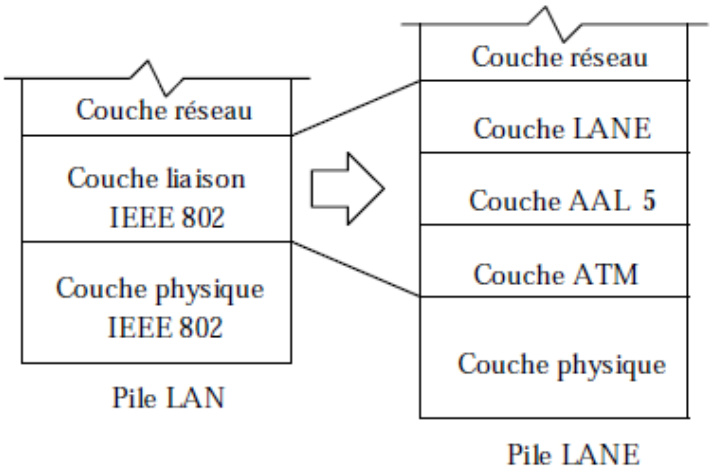


Figure II.4: déférence entre la Pile LAN et LANE [16]

II.8. Sécurité

II.8.1 Définition de la sécurité réseaux

La sécurité est aujourd'hui au cœur des soucis des entreprises. De nombreux événements récents, très médiatisés, ne font que renforcer cette affirmation. La plupart des ouvrages sur la sécurité des réseaux et des systèmes d'information insistent sur les connaissances nécessaires pour le développement de nouveaux algorithmes et systèmes de sécurité. [12]

La sécurité à mettre en œuvre dépend principalement des moyens qui seront mis en œuvre pour les attaques et donc principalement de ce qui à sécuriser. Il s'agit de trouver un juste équilibre entre le cout de la sécurité et les risques à assumer. [13]

Une politique de sécurité prend en compte non seulement la sécurisation de l'accès aux données mais aussi la protection des données et de l'outil de protection face à des événements éventuellement destructeurs comme le vol, l'incendie … [13]

D'une manière générale, la sécurité peut être décomposée en 2 types :

- ✓ Sécuriser l'accès physique au matériel
- ✓ Sécuriser les données et logiciels

II.8.2. Les attaque réseaux

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque, une attaque est l'exploitation d'une faille d'un système informatique.

II.8.3. Les techniques des attaques réseau

a. Attaque Ping de la mort (Ping of death)

Un Ping a normalement une longueur maximale de 65535 octets, incluant un entête de 20 octets. Un Ping of death c'est un Ping qui a une longueur de donnée supérieure à la taille maximale. Lors de son envoi, le Ping of death est fragmenté en paquets plus petits. L'ordinatrice victime qui reçoit ces paquets doit alors les reconstruire. Certains systèmes ne gèrent pas cette fragmentation, et se bloquent, ou crashent complètement. D'où le nom de cette attaque [6].

b. Attaque par réflexion (Smurf)

C'est un pingflooding un peu particulier. C'est une attaque axée réseaux, faisant partie de la grande famille des Refus De Service (DOS : Denial Of Service). Ce procédé est décomposé en deux étapes: La première est de récupérer l'adresse IP de la cible parspoofing. La seconde est d'envoyer un flux maximal de paquets ICMP ECHO (Ping) aux adresses de Broadcaste. Chaque Ping comportant l'adresse spoofée de l'ordinateur cible. Si le routeur permet cela, il va transmettre le broadcaste à tous les ordinateurs du réseau, qui vont répondre à l'ordinateur cible. La cible recevra donc un maximum de réponses au Ping, saturant totalement sa bande passante... Bien entendu, plus de réseau comporte de machines, plus c'est efficace [6].

c. Attaque man in the middle

L'attaque « man in the middle » (littéralement « attaque de l'homme au milieu » ou « attaques de l'intercepteur »), parfois notée MITM, est un scénario d'attaque dans lequel un pirate écoute une communication entredeux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties. La plupart des attaques de type « man in the middle » consistent à écouter le réseau à l'aide d'un outil appelé sniffer [7].

d. Attaque par rejeu

Les attaques par « rejeu » (en anglais « replay attaque ») sont des attaques de type « Man in the middle » consistant à intercepter des paquets de données et à les rejouer, c'est-à-dire les retransmettre tels quel (sans aucun déchiffrement) au serveur destinataire. Ainsi, selon le contexte, le pirate peut bénéficier des droits de l'utilisateur. Imaginons un scénario dans lequel un client transmet un nom d'utilisateur et un mot de passe chiffrés à un serveur afin de s'authentifier. Si un pirate intercepte la communication (grâce à un logiciel d'écoute) et rejoue la séquence, il obtiendra alors les mêmes droits que l'utilisateur. Si le système permet de modifier le mot de passe, il pourra même en mettre un autre, privant ainsi l'utilisateur de son accès [7].

e. Attaque par fragmentation

Une « attaque par fragmentation » (en anglais fragment attack) est une attaque réseau par saturation (déni de service) exploitant le principe défragmentation du protocole IP. En effet, le protocole IP est prévu pour fragmenter les paquets de taille importante en plusieurs paquets IP possédant chacun un numéro de séquence et un numéro d'identification commun. A réception des données, le destinataire réassemble les paquets grâce aux valeurs de décalage (en Anglais offset) qu'ils contiennent. L'attaque par fragmentation la plus célèbre est l'attaque Tear drop. Le principe de l'attaque Tear drop consiste à insérer dans des paquets fragmentés des informations de décalage erronées. Ainsi, lors duré assemblage il existe des vides ou des recoupements (over lapping), pouvant provoquer une instabilité du système.

A ce jour, les systèmes récents ne sont plus vulnérables à cette attaque [7].

II.8.3. Politique de la sécurité réseaux

La politique de sécurité réseau vise à satisfaire les critères suivants :

a. Authentification

Vérifier l'identité d'un utilisateur pour lui associer les droits d'accès.

b. Confidentialité

Consistant à assurer que les seules personnes autorisées aient accès aux ressources échangées.

c. Intégrité

Assurer que les informations ne peuvent être modifiées ou altérer que par les personnes autorisées.

d. Disponibilité

Assurer que l'information est disponible pour les personnes autorisées.

e. Non-répudiation

Permettant de garantir qu'une transaction ne peut être niée.

Solution de la sécurité

a. Pare-feu(firewall)

Les pare-feu est l'un des éléments très utile d'un système de sécurité des réseaux ; leur fonctionnement général est le filtrage statique et dynamique ainsi ils assurent la principale barrière de protection de l'architecture d'un entreprise.

Les pare-feu ont pour rôle de filtrer le trafic en fonction des informations contenues dans les couches 3 et 4 du modèle OSI [14].

Les pare-feu examinent tous les paquets entrants, choisissant de les accepter ou de les bloquer selon leur nature. On appelle cette fonction le filtrage en entrée [12].

Le filtrage en sortie s'applique aux paquets circulent de l'intérieur vers l'extérieur du réseau. Cette mesure de protection permet notamment d'empêcher les connexions non autorisées à des serveurs externes [12].

Les pare-feu assurent de nombreuses fonctions de protection, qui se caractérise essentiellement par trois catégories :

- ✓ Inspection de paquets
- ✓ Inspection d'application
- ✓ Translation d'adresse réseau

Les pare-feux se présentent à la fois sous forme de logiciels spécialisés et de matériels plus en moins dédiés [12]; on considère les types des pare-feux comme suite :

- ✓ Routeur filtrant
- ✓ Serveur pare-feu
- ✓ Boitier pare-feu
- ✓ Pare-feu individuel

A l'heure actuelle Les pare-feu est parmi les meilleurs outils disponible à pour déjouer les attaques lancé à l'extérieur si ca considère comme un avantage. Mais ils sont encore moins efficaces contre les attaques préparées à l'intérieur!!

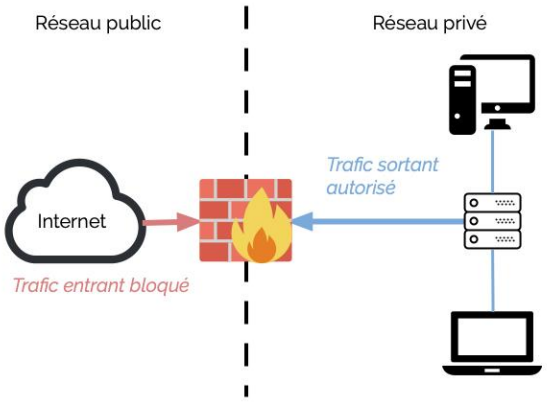


Figure II.5 : Principe de firewall

b-VPN : (Virtual private network)

Est un système permettant à crée un tunnel sécurisé entre deux entités. C'est-à-dire à l'intérieur d'un réseau. Pour l'objectif de l'isolation ou bien la sécurisation des échanges de données privées sensible sur les réseaux publics.

Le fonctionnement des VPN repose sur des technologies appelées protocoles de tunnelisation ou protocoles VPN.

c-Codes malicieux (virus)

Un virus est un programme « parasite » qui s'attache à un programme principal dont il modifie l'environnement de travail avec un objectif généralement destructeur.les programmes virus ont aussi la possibilité de ce propager de machine en machine directement avec le programme infecté (copie de programme),mais aujourd'hui de plus en plus par exploitation du carnet d'adresse de la machine infectée .

Des logiciels dits antivirus permettent de se protéger des virus connus. Cependant, malgré les mises à jour, les « pirates » ont toujours un virus d'avance. La seule parade efficace consiste à n'échanger des données avec personne et de ne jamais raccorder à un réseau ! [5]

d-Chiffrement des données

Le chiffrement est une technique destinée à rendre les données inintelligibles pour les tiers non autorisés. L'opération de brouillage du texte s'effectue à partir d'une clé (clé de chiffrement).le message est codé (chiffré) à l'aide d'une clé de chiffrement ; seul, le cryptogramme (message chiffré) est transmis sur le réseau. Le destinataire du message effectue le décryptage à l'aide d'une clé de déchiffrement.

Les techniques de cryptographie sont utilisée pour :

-assurer la confidentialité des données (algorithme de chiffrement),

-garantir l'intégrité des données (algorithme de hachage),

-authentifier l'émetteur des données (algorithme de signature numérique), [5]

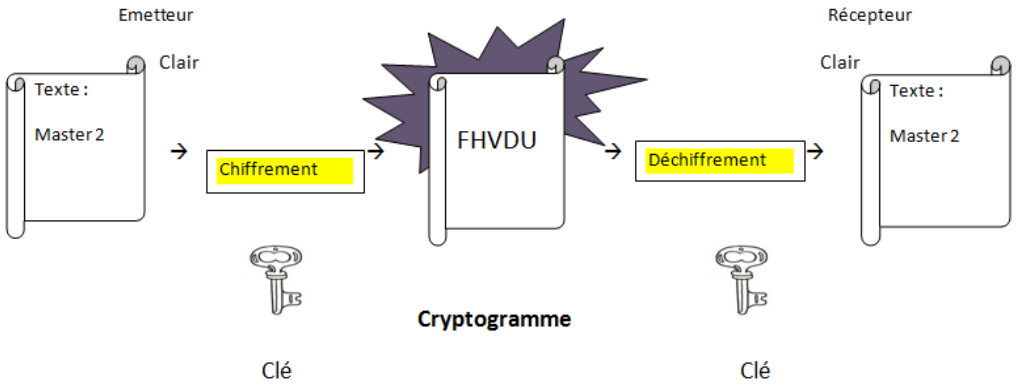


Figure II.6 : Principe de chiffrement

e- Les VLAN

Sur un Switch, un VLAN est un groupe de ports, les machines connectées à ces portes peuvent communiquer entre elle librement. En revanche, toute communication est impossible avec un port étranger au VLAN. On imagine aisément deux réseaux câblés isolés l'un de l'autre et qui le fait ne communiquent pas. Répartis sur un réseau Ethernet commuté, les VLAN offrent par exemple une solution pratique pour isoler les unes des autres des sociétés partageant infrastructure communes [14].

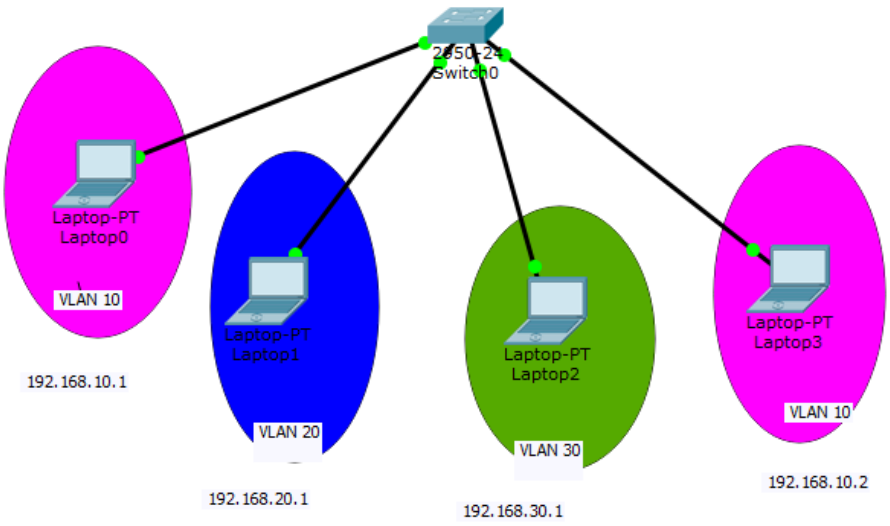


Figure II.7 : principe de VLAN

Conclusion

Nous avons vu tout au long de ce chapitre que le réseau LAN est le cœur des réseaux informatiques et nous avons vu le développement qui touche les réseaux LAN puis on passera à étudier les différents thermes de la sécurité des réseaux locaux. Le chapitre qui suit va se porter une étude de réseau existant au sein de l'université Djilali Bounaama.

Chapitre III
Etude et simulation du réseau de l’université Djilali Bounaama

III.1. Introduction

Ce chapitre sera réservé à l'étude de réseau existant dans l'université Djilali Bounaama et sa configuration, tous d'abord nous allons évoquer un bref aperçu de l'université pour mieux connaitre sa structure, ensuite nous allons utiliser le simulateur Cisco Packet Tracer pour faire la simulation de ce réseau.

III.2. Présentation générale d'université UDBK

III.2.1.Historique

La ville historique de Miliana a vu la genèse du premier établissement de l'enseignement supérieur au niveau de la wilaya d'Ain Defla (à 140 km à l'ouest d'Alger). En effet, c'est l'école nationale des mines de cette ville qui en devient l'établissement pionnier en 1991. Peu après, en 1995 et afin de permettre l'extension et l'ouverture de nouvelles filières, l'école est transférée vers l'institut technique agricole de la ville de Khemis Miliana où elle devient une antenne de l'université SAAD DAHLEB de Blida.

Après quelques années de travail et d'efforts considérables, les conditions sont réunies pour que cette antenne soit promue en un centre universitaire autonome le 18 septembre 2001. Réunissant ainsi quelques instituts pilotes, le centre a vu l'ouverture de plusieurs spécialités au cours des années qui suivent, dans le système classique comme dans le système LMD.

Cette dernière réforme a permis l'accélération de l'extension et l'épanouissement du centre universitaire, qui a dépassé rapidement les 10000 étudiants inscrits dans toutes les spécialités confondues. Offrant ainsi une formation de qualité, il a continué sa mission en concertation avec tous les secteurs socio-économiques locaux de la wilaya d'Ain Defla et autres, pour arriver à mettre en place un pôle universitaire et scientifique distingué. Ce centre est devenu par la suite Université, laquelle compte actuellement **6** facultés et **1** institut. [21]

III.2.2. localisation géographique

- **A partir de l'aéroport international d'Alger**

En prenant l'autoroute en direction d'Oran jusqu'à l'échangeur situé près du l'université (environ 1h30 de trajet).

- **A partir de la capitale Alger (par route)**

Soit par l'autoroute ou par la RN4 en direction d'Oran, au niveau de l'intersection à l'entrée Est de la ville de khemis Miliana prendre la direction qui mène vers Tissemsilt. L'université est visible de part et d'autre de la RN14.

- **A partir de l'autoroute Est-Ouest**

L'autoroute passe dans la partie Sud du territoire de la commune de khemis Miliana, près du l'université. Emprunter l'échangeur se trouvant juste à côté de cette structure universitaire.

- **A partir de la gare routière principale de khemis Miliana**

Prendre soit le bus universitaire (un arrêt fixe se trouve en face de cette gare) ou joindre l'université à pied en prenant la direction Est vers Alger jusqu'à l'intersection ensuite prendre la route de Tissemsilt (moins de 15 minutes de marche depuis la gare routière).

- **A partir de la wilaya de Médéa (par bus)**

Descendre prés de l'intersection de l'entrée Est de la ville de Khemis Miliana et joindre l'université à pied en prenant la direction de la route de Tissemsilt (quelques minutes de marche). Eviter de joindre la gare routière pour ne pas rebrousser le chemin

- **A partir de la wilaya de Tissemsilt et Tiaret**

L'université est sur la RN14 juste après l'intersection menant vers l'échangeur de l'autoroute.

- **A partir de la gare ferroviaire**

Cette gare se trouve dans la partie nord-ouest du tissu urbain de la ville de Khemis Miliana alors que l'université est située dans l'extrême partie sud-est. Vu l'éloignement de l'université, nous conseillons de prendre un taxi devant la gare. [21]

Figure III.1: Localisation géographique d'université Djilali Bounaama

III.2.3.Différents départements

- Faculté des sciences naturelles, de La Vie de La Terre.
- Collège des Sciences et Technologies.
- Faculté des Sciences Economiques, Commerciales et de Gestion.
- Faculté de Droit et de Science Politique.
- Collège des Sciences Sociales Et Humaines.
- Collège des Lettres et des Langues.
- Institut des Sciences et technologies des Activités Physiques et Sportives. [21]

III.2.4. Objectif d'université Djilali Bounaama

L'objectif principal de notre université est d'assurer une recherche scientifique efficace pour tous les niveaux.

III.2.5. Organigramme générale

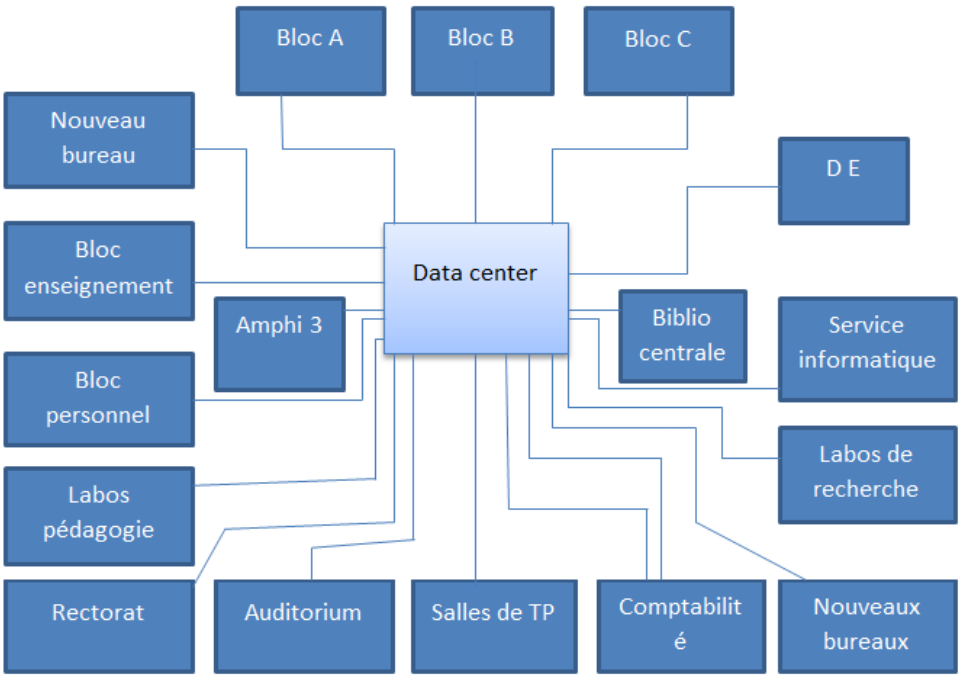


Figure III.2 : Organigramme d'université Djilali Bounaama

III.2.6.Présentation des équipements utilisés

Les équipements réseau sont illustrés dans le tableau III.1 :

Equipement	**Le type**	**Le nombre**
Routeur	Cisco1900	1
Firewall	Cyberoam CR750	1
Switch fédérateur	4507 R-E	1
Switch Catalyst2960 Ou Catalyst2950	Switch 48 ports+2 SFP	9
	Switch 48 ports	4
	Switch 24 ports	9
	Switch 48 ports+4 SFP	4
	Switch 24 ports+2 GBIC	3
	Switch 8 ports+ 1 SFP	2
	Switch 24 ports+2T /SFP	10
	Switch 10 ports GBIC	1
Câble fibre-optique	Monomode	1860 m
	Multi mode	Plus de 1670 m
Câble FTP	/	/

Tableau III.1 : listes des équipements utilisés

III.3. Présentation du simulateur Cisco Packet Tracer

III.3.1. Description générale du simulateur Cisco Packet Tracer

Packet Tracer est un logiciel de 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). Une fois l'ensemble des équipements reliés, il est possible de configurer chacun d'entre eux (les adresses IP, les services disponibles, etc.). [17]

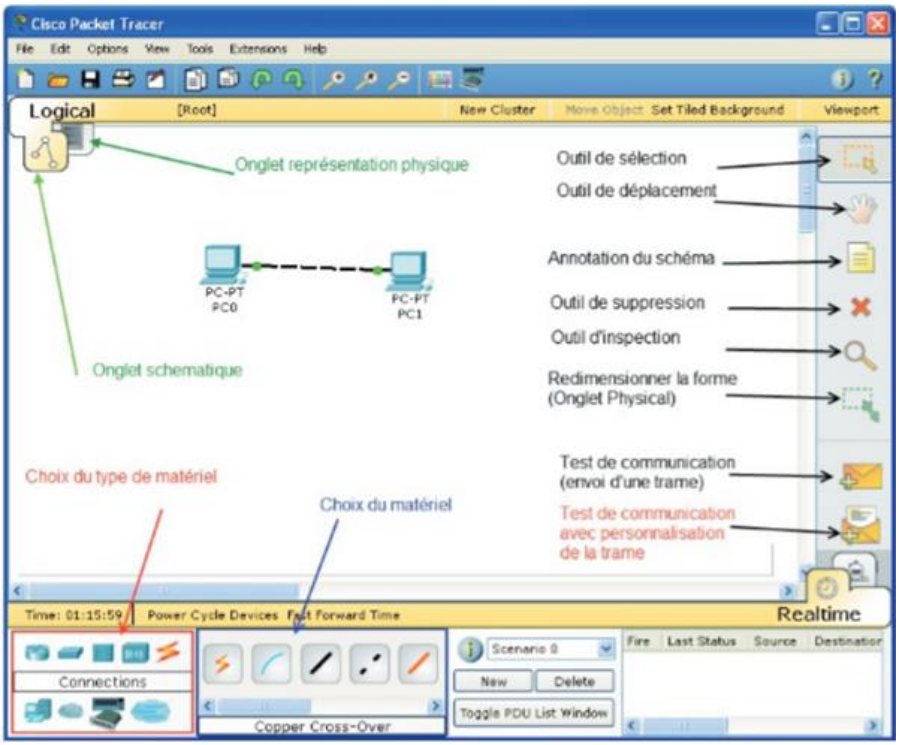


Figure III.3 : Interface Cisco Packet Tracer [17]

Trois éléments de la fenêtre de Packet Tracer seront nécessaires :

1. La zone de travail.
2. Les types d'appareillage.
3. Les différents modèles d'appareils du type sélectionné dans la zone 2[18]

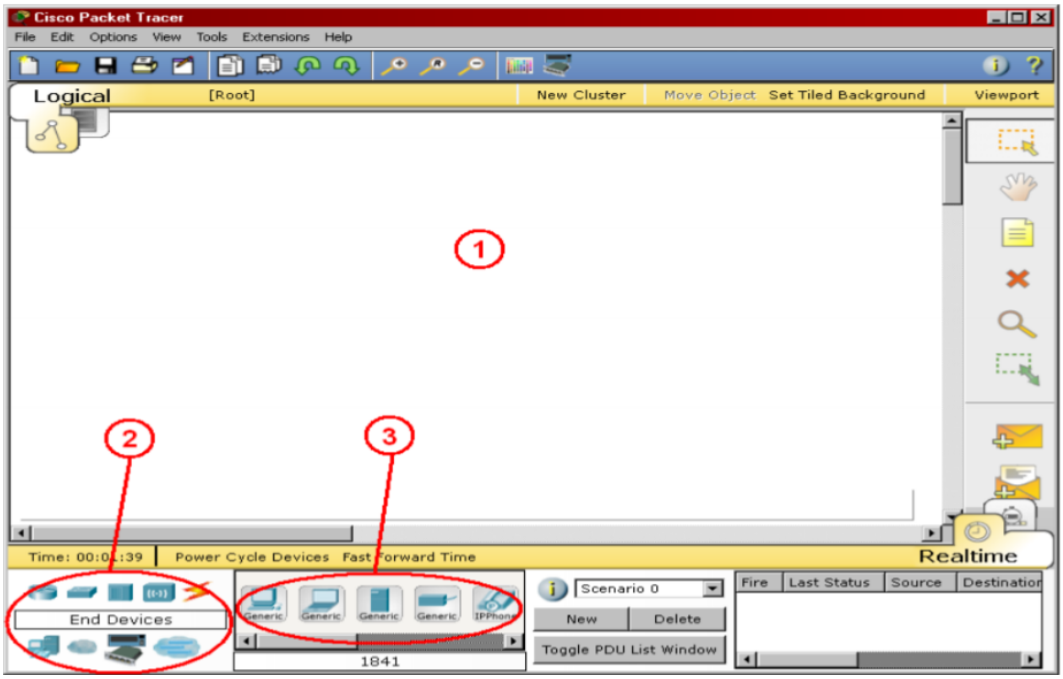


Figure III.4 : Eléments principaux dans l'interface Cisco Packet Tracer [18]

A. Spécification des équipements possibles

Les différents types d'appareils disponibles dans la boite à outils de la zone 2 :

1. Les routeurs
2. Les commutateurs (switches)
3. Les concentrateurs (hubs)
4. Les bornes sans fil (wifi)
5. Les connecteurs
6. Les ordinateurs
7. Les réseaux étendus (Wan)
8. Des appareils divers
9. Les connexions multi-usagers [17]

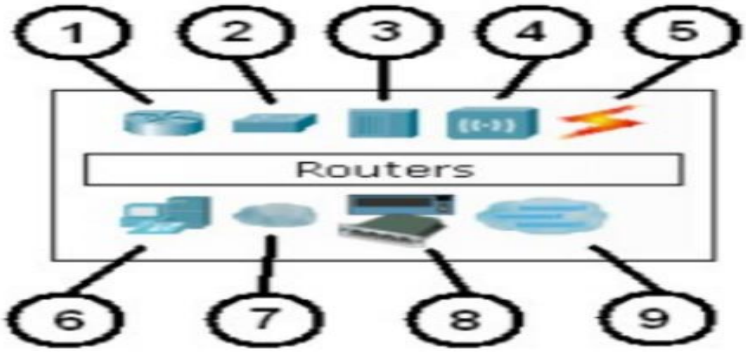


Figure III.5 : Équipements trouvés dans le simulateur Cisco Packet Tracer

B. Spécification des connecteurs possibles

Le simulateur Packet Tracer propose des principaux connecteurs possibles entre différents équipements réseaux

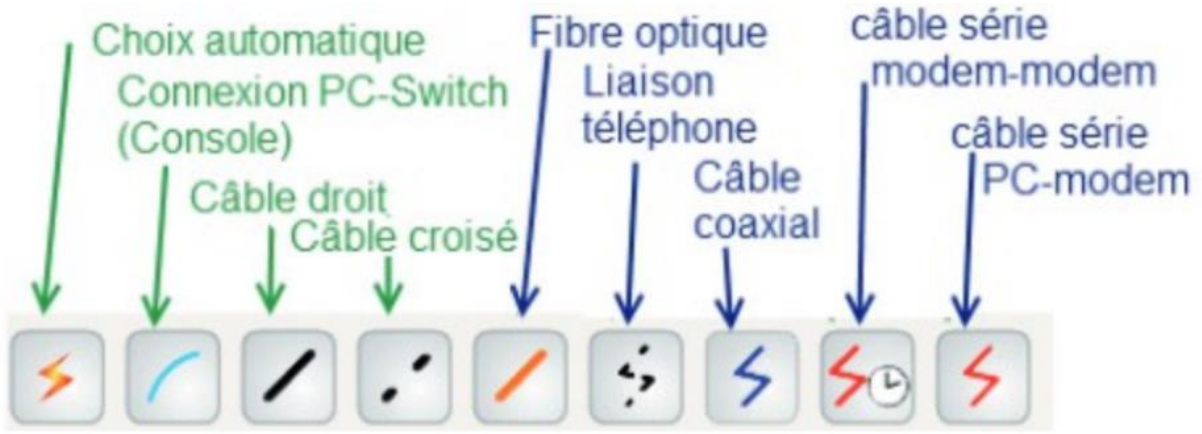


Figure III.6 : Câbles de connexion


Câble Console : les connecteurs console peuvent être établies entre PCs et routeurs ou commutateurs. Elles servent principalement à configurer les équipements.


Câble droit : standard Ethernet pour connecter les équipements opérant dans les différentes couches du modèle OSI. Packet Tracer supporte le 10,100 et 1000 Mbps.


Câble croisé : standard Ethernet pour connecter les équipements opérant dans les mêmes couches du modèle OSI. Packet Tracer supporte le 10, 100 et 1000 Mbps.


Fibre optique : les connecteurs fibres peuvent être établis si les équipements possèdent les portes fibres adéquates. Packet Tracer supporte le 100 et 1000 Mbps.


Ligne téléphonique : les connecteurs téléphoniques ne sont disponibles qu'entre les équipements possèdent des ports modem. Ces connexions se font généralement à travers un nuage réseau.


Câble Coaxial : Même chose que pour la ligne téléphonique, sauf que les ports utilisés sont des ports coaxiales.

 Câbles DCE et DTE : les connecteurs séries se font entre 2ports. Elles sont souvent utilisées pour simuler des liens WAN. Le doit être activé sur le câble DCE pour activer la connexion. En fonction du premier câble sélectionné (DTE ou DCE) le deuxième sera forcément de l'autre type afin d'assurer la connexion. [18]

III.3.2. Méthode de configuration des équipements

A. Construire un réseau

Pour construire un réseau. L'utilisateur doit choisir parmi les 8 catégories proposées par Packet Tracer, les routeurs, les switches, les hubs, les équipements sans fil, les connecteurs les équipements dits terminaux (ordinateurs, serveurs) des équipements personnalisée et enfin, une connexion multiutilisateurs. Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents.

Figure III.7: Outils pour construire un réseau

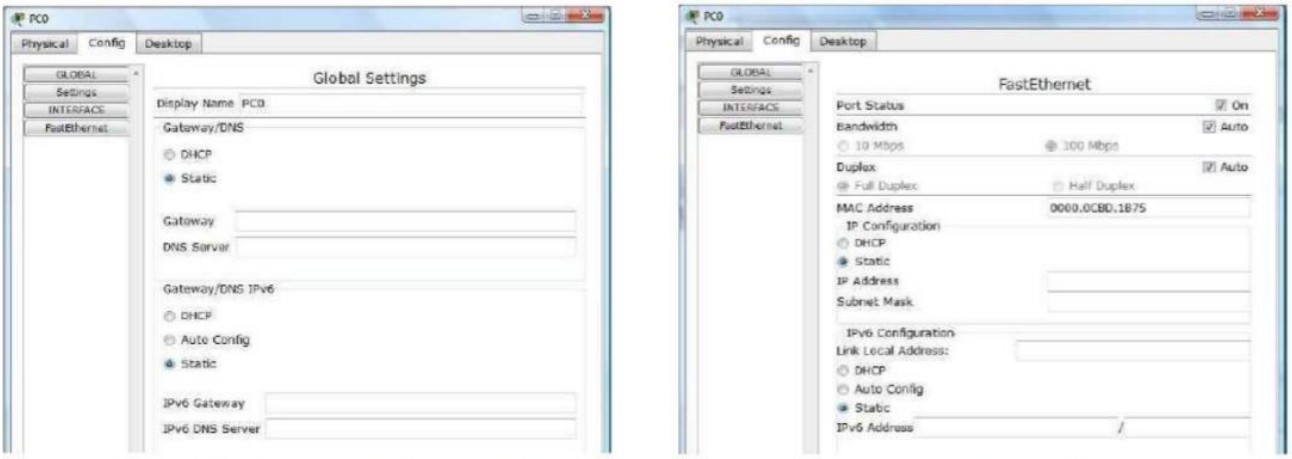
Pour relier deux équipements, il faut choisir la catégorie « connecteurs » puis cliquer sur la connexion désirée. Dans nos différents travaux pratiques nous n'utiliserons que 2 sortes de connexion : les câbles droits (Copper Straight-Through) et les câbles croisé (Copper Cross-Over). [19]

B. Configuration d'un équipement

Lorsqu'un ordinateur a été ajouté (appelé PC-PT dans Packet tracer), il est possible de la configurer en cliquant dessus, une fois ajouté dans le réseau.

Une nouvelle fenêtre s'ouvre comportant 3 anglet : Physical (aperçu réel de la machine et de ses modules), Config (configuration passerelle, DNS et adresse IP) et Desktop (ligne de commande ou navigateur web).

Dans l'onglet config, il est possible de configurer la passerelle par défaut, ainsi que l'adresse du serveur DNS (cliquer pour cela sur le bouton settings en-dessous du bouton global). Il est possible aussi de configurer l'adresse IP et le masque de sous-réseau (cliquer pour cela sur le bouton FastEthernet en-dessous du bouton INTERFACE). [19]



Configuration passerelle et DNS *Configuration IP*

Figure III.8 : Configuration d'un PC [19]

C. Interface CLI

La configuration des équipements fait par l'anglet CLI (commande line interface) on l'apercevra juste après dans la figure (figure **III.9**).

L'interface de ligne de commande de Cisco est la principale interface ou nous allons interagir avec les périphériques Cisco IOS, la CLI est accessible directement via un câble console ou à distance via des méthodes telles que Telnet/SSH à partir de là, nous pouvons effectuer des taches telles que la surveillance de l'état des périphériques ou la modification de la configuration Cisco a divisé son interface de ligne de commande en plusieurs modes différents, comprendre les modes de ligne de commande de Cisco IOS est essentiel car chaque mode possède son propre ensemble de commande. [22]

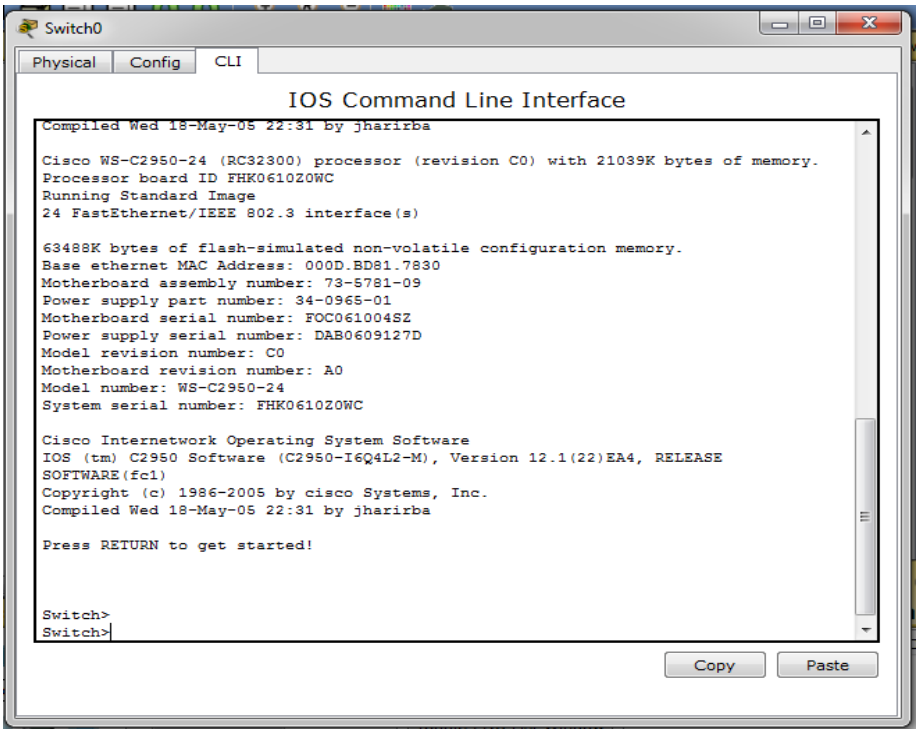


Figure III.9 : Interface CLI

D. Mode simulation

Une fois le réseau est créé il est prêt à fonctionner, il est possible de passer en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau. En mode simulation, la fenêtre principal est scindée en deux, la partie de droite permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulation, protocoles visibles. La partie gauche de la figure III.7, montre la partie simulation et sa partie droite montre les détails obtenus en cliquant sur un message (ici http). [19]

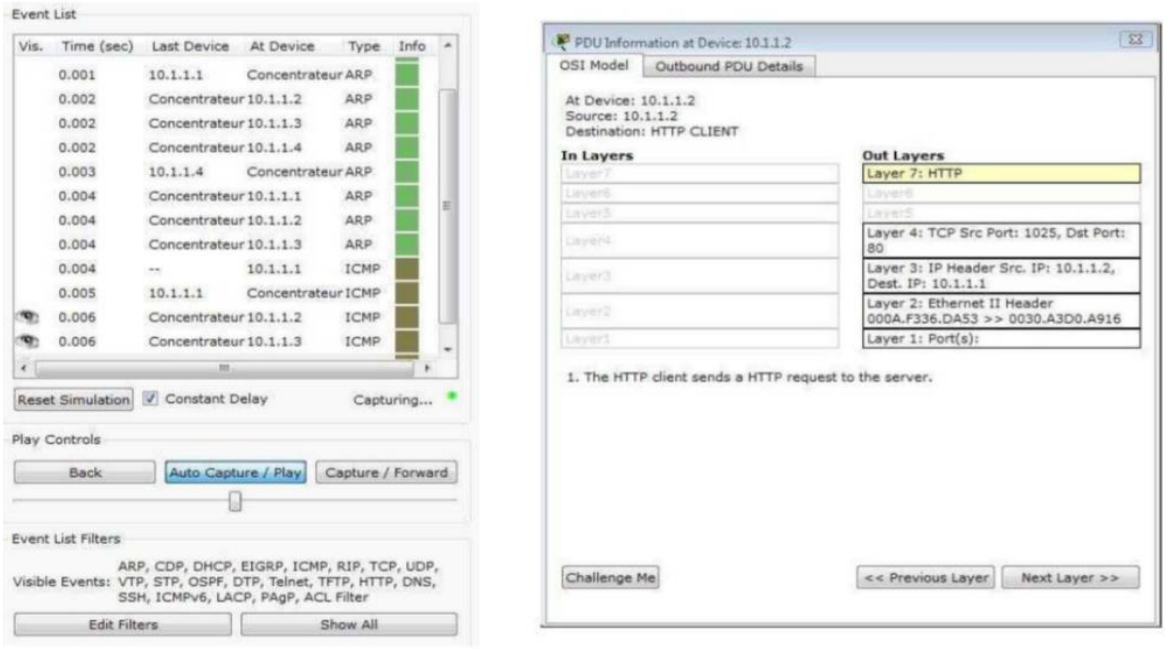


Figure III.10 : Partie simulation et le détail d'un paquet [19]

III.4. Réalisation et simulation de réseau de l'existant

III.4.1. Présentation d'architecture réseau de l'existant

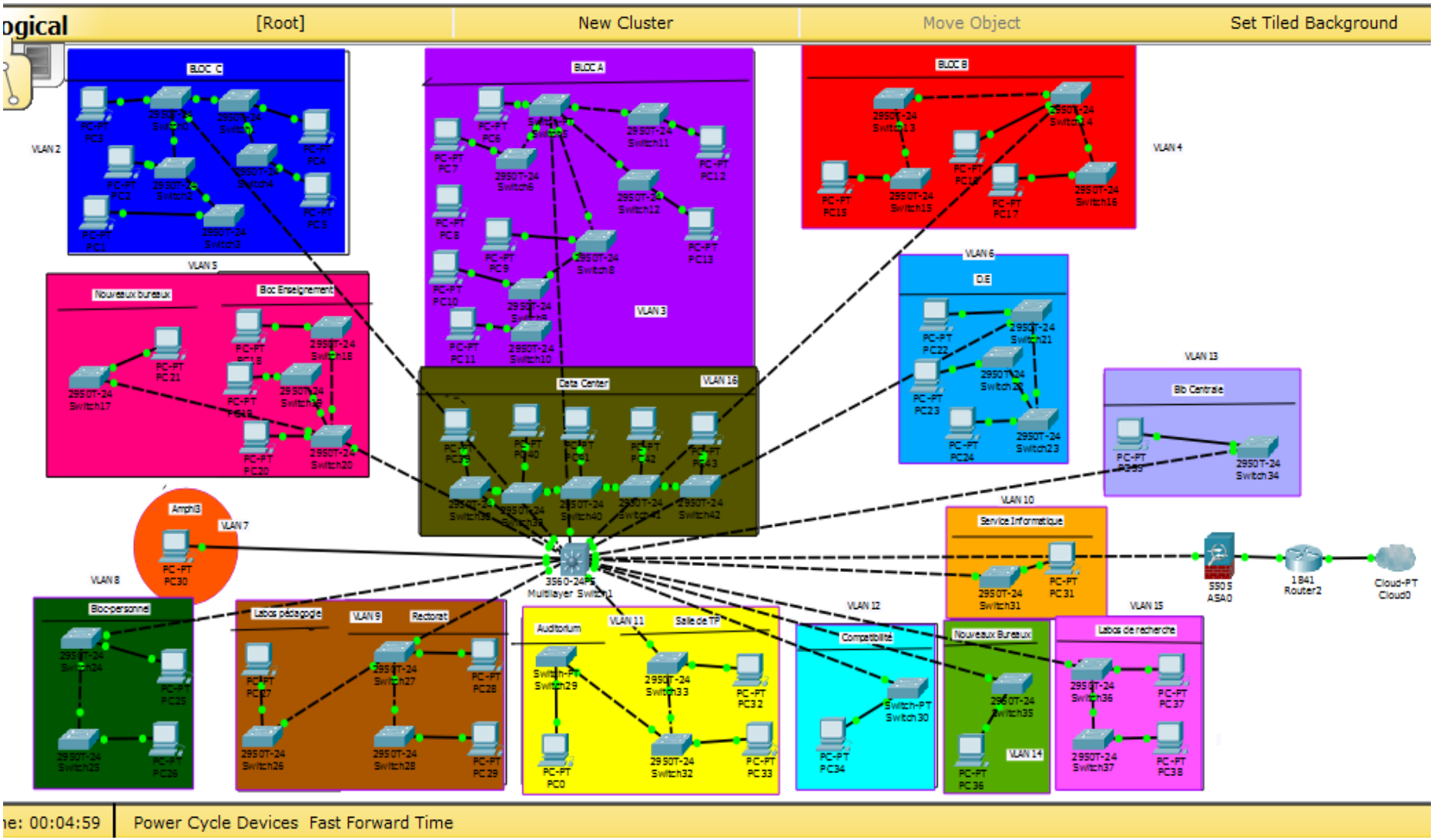


Figure III.11 : Architecture réseau de l'université djilali Bounaama

Notre université Djilali Bounaama est composée de deux pôles principaux l'ancien pôle et le nouveau pôle, les réseaux de ces pôles sont relies entre eux par la fibre optique.

La transmission des données se fait par la fibre optique, à l'entrée de réseau nous trouvons un routeur relié par un firewall qui est le responsable de la sécurité de ce réseau.

Dans chaque bloc de l'université nous trouvons de 2 jusqu'à 5 switch de types différents car les switch sont moins chère et facile d'installation par rapport aux routeurs c'est pour cela nous trouvons un seul routeur dans tous le réseau d'université.

Dans chaque switch nous trouvons entre 10 jusqu'au 35 postes.

Remarque : nous utilisons dans la simulation de ce réseau un seul PC dans chaque switch juste pour tester la connectivité et le bon fonctionnement du réseau.et nous avons réalisé une configuration statique (manuellement) et dynamique (à l'aide de protocole DHCP).

III.4.2.Configuration des équipements

III.4.2.1. Configuration de Switch

Au débit, nous commençons par l'attribution d'un nom au Switch fédérateur avec la commande suivante :

a. Configuration de nom de Switch

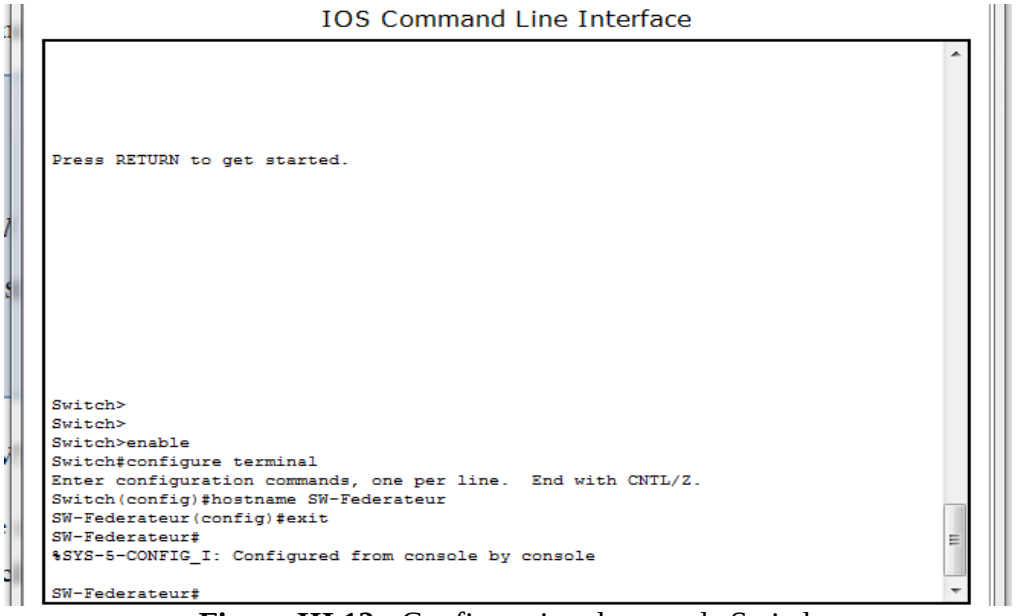


Figure III.12 : Configuration de nom de Switch

b. Sécurisation de l'accès aux périphériques

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

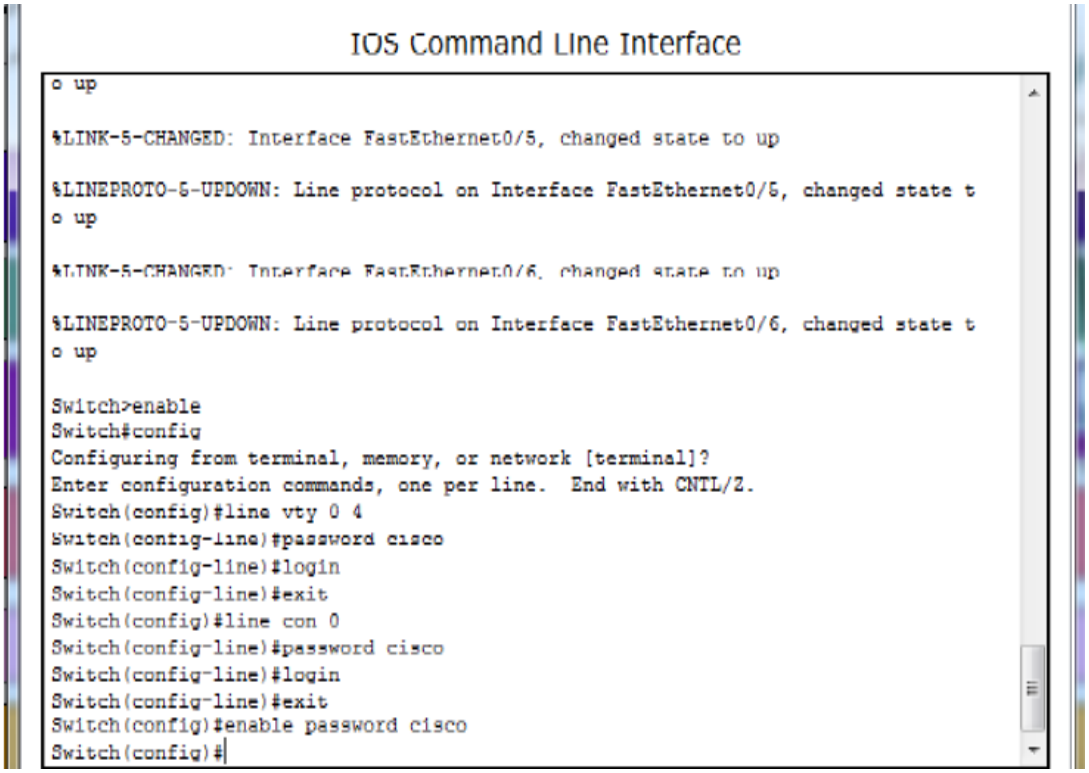


Figure III.13 : Sécurisation de switch fédérateur

c. Configuration du protocole VTP

VTP est l'abréviation de Virtual Trunk Protocol. Avec VTP, il est possible de communiquer automatiquement les changements d'un commutateur maître (mode server) vers tous les autres commutateurs réglés pour recevoir ces informations (mode client). Mais il est également possible de bloquer la communication sans appliquer les changements ou de véhiculer les informations sans les appliquer.

Donc nous associons le mode Server pour le Switch fédérateur :

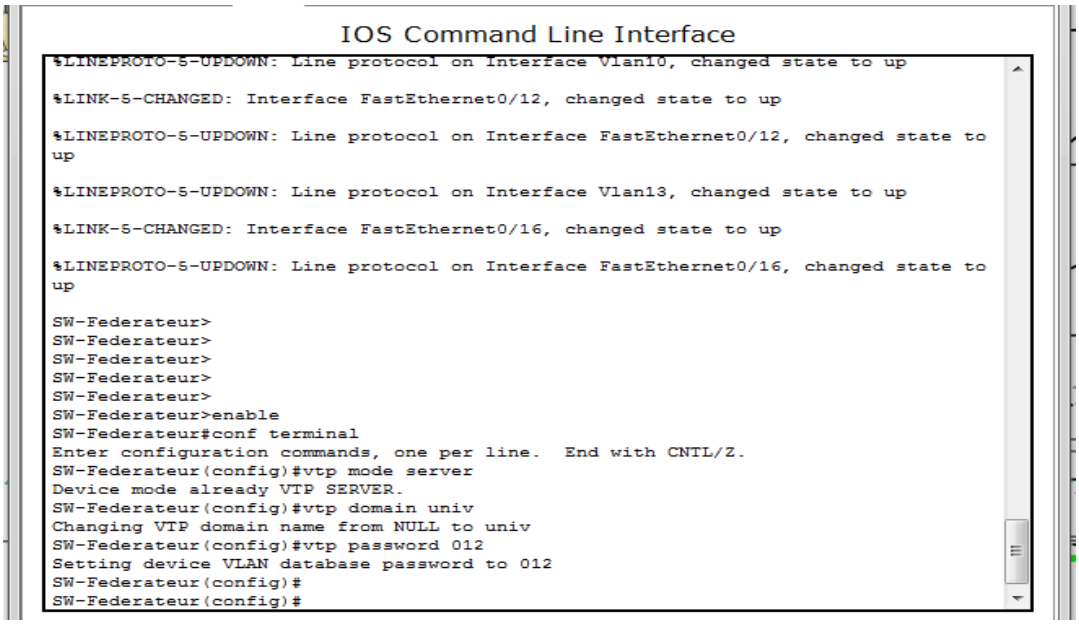


Figure III.14 : Configuration du protocole VTP (mode server)

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

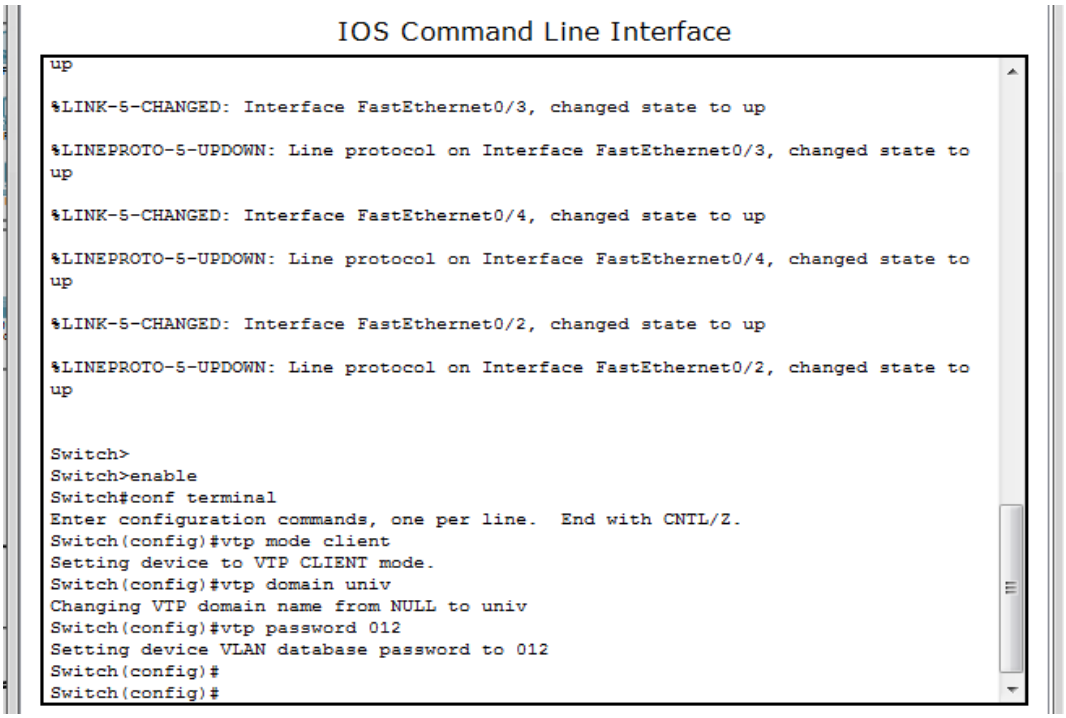


Figure III.15 : Configuration de protocole VTP (mode client)

d. Création des VLAN

La création des VLANs est faite au niveau de switch fédérateur après la configuration du protocole VTP.

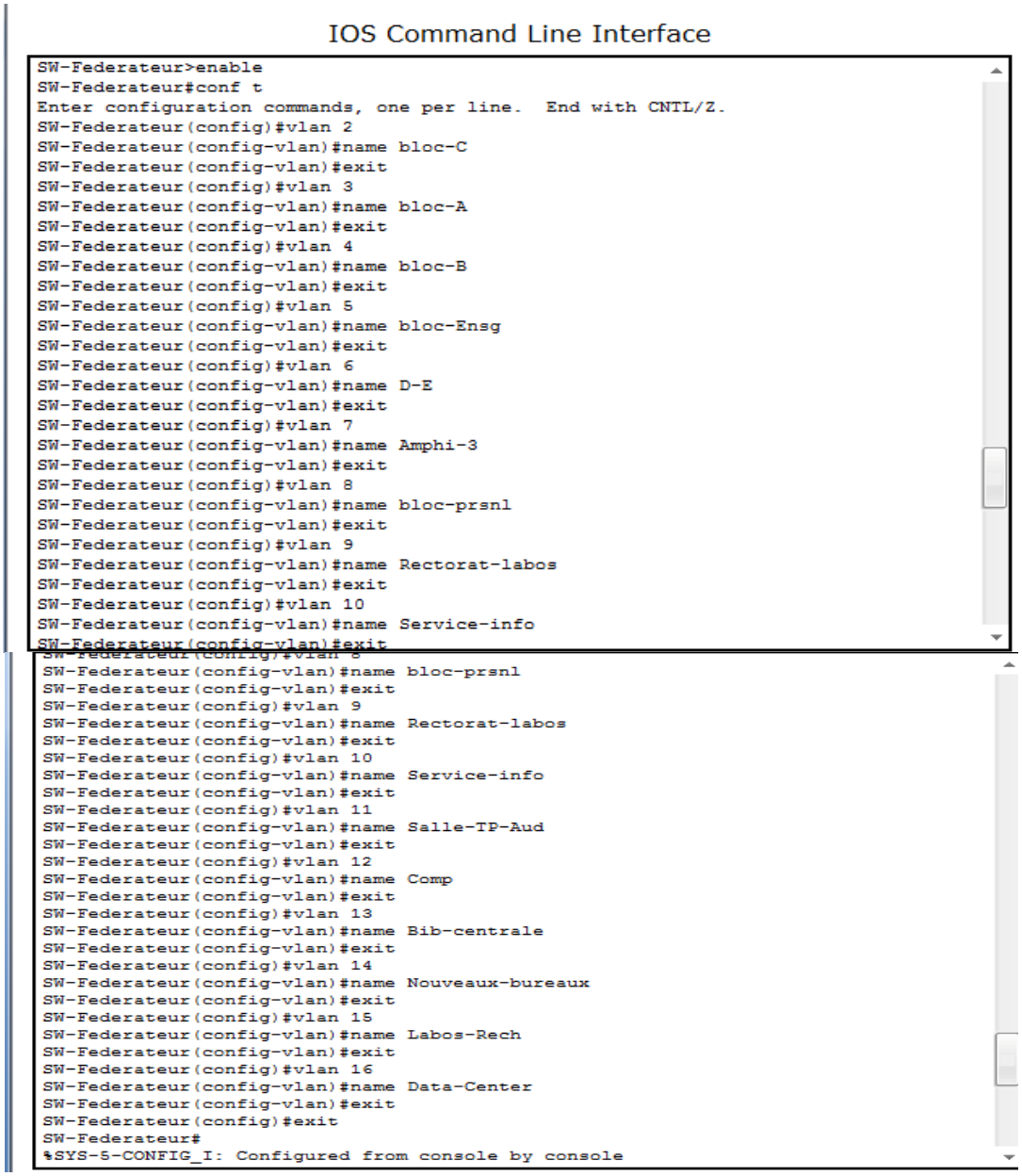


Figure III.16 : Créations des VLAN

e. Attribution des ports des commutateurs au VLAN

Par défaut tous les ports sont assignés au VLAN 1, mais nous voulons assigner chaque port du Switch fédérateur au VLAN convenable parmi les 15 que nous avions créé. Pour cela nous tapons les instructions montrées ci-dessous :

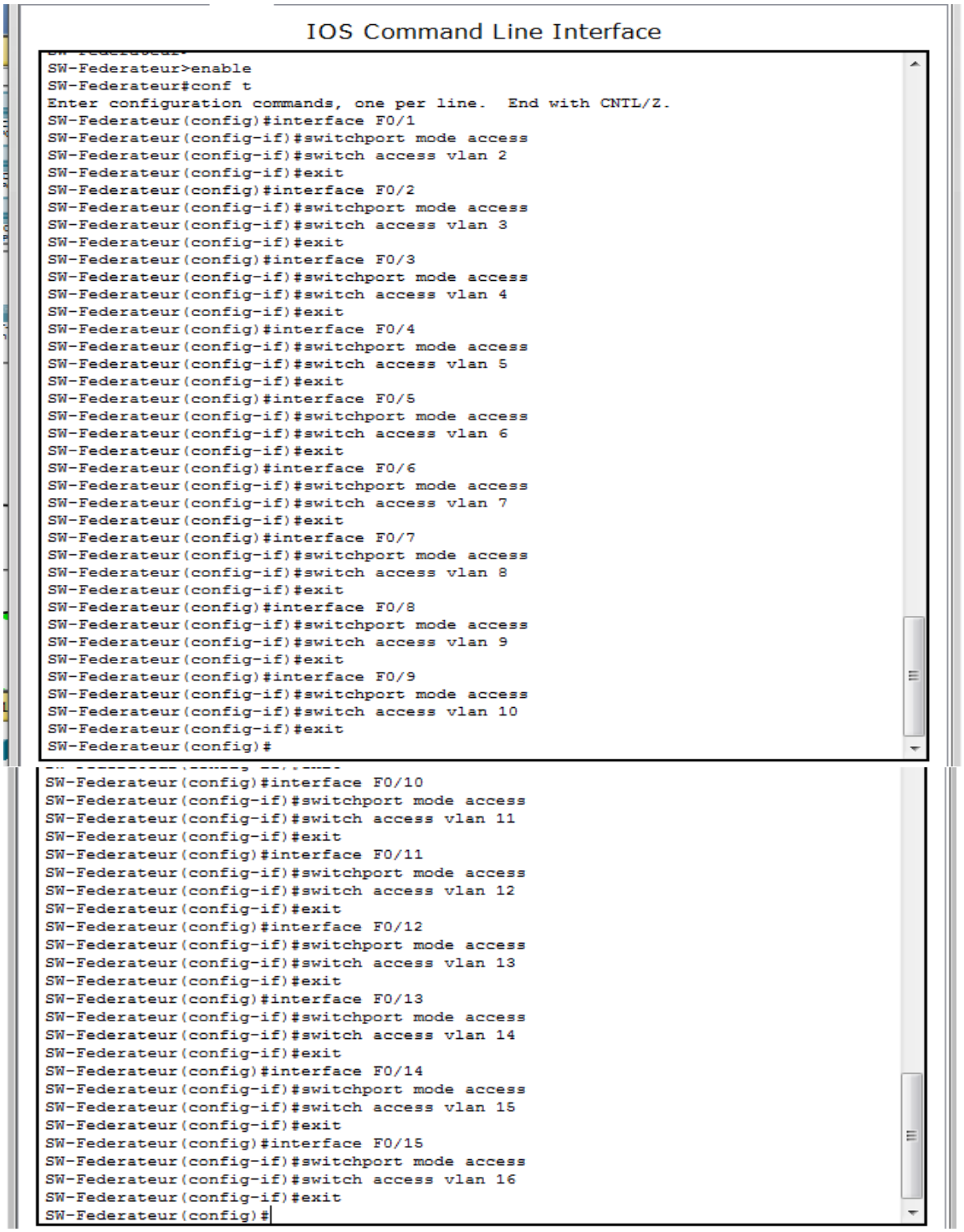


Figure III.17 : Attribution des ports des commutateurs aux VLAN

f. Configuration des liens Trunk

Les interfaces des équipements d'interconnexion à configurer en mode Trunk, existent toutes entre l'ensemble des commutateurs Accès et le commutateur cœur. Les commandes suivantes nous permettent d'associer un port à un vlan en mode Trunk en s'aidant de la commande range qui pourra réunir toutes les interfaces en une seule fois.

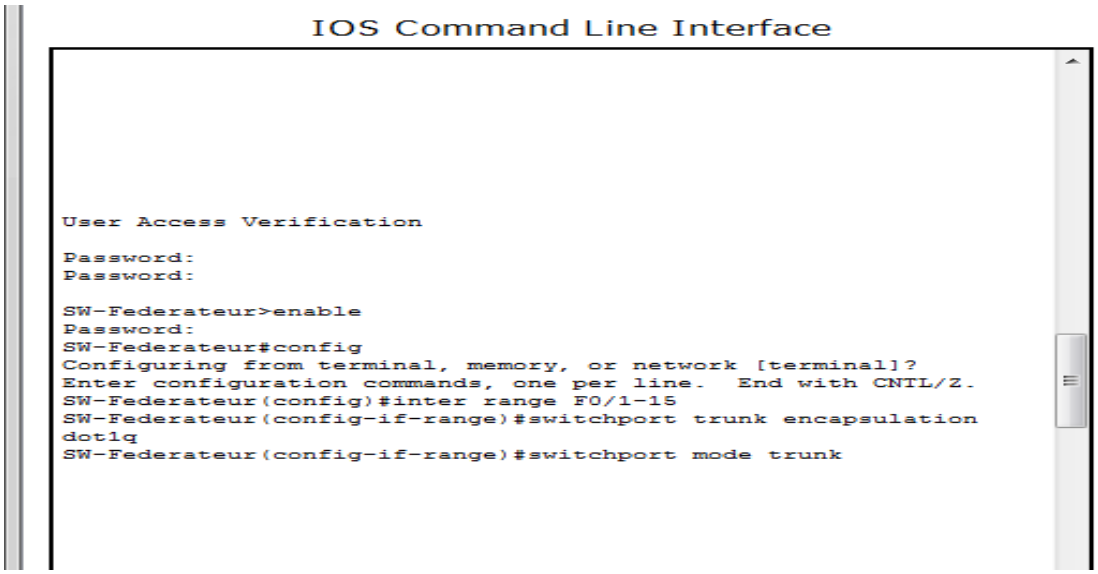
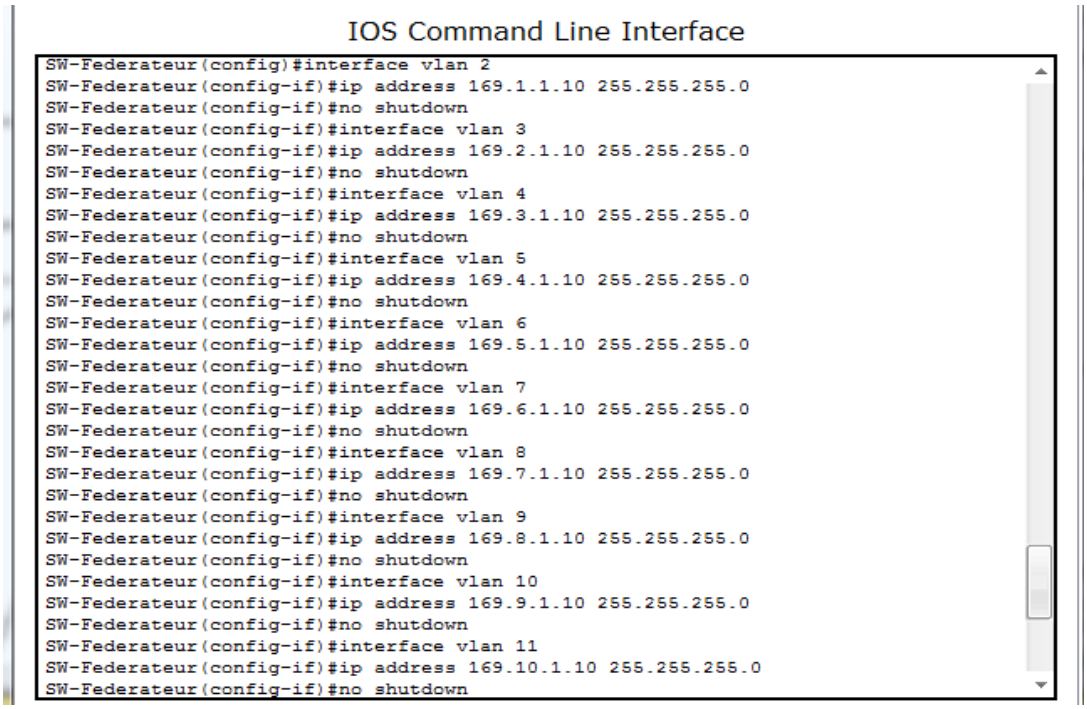


Figure III.18 : Configuration des liens Trunk

g. Configuration des interfaces VLAN

La configuration des interfaces VLANs est faite au niveau du switch fédérateur en donnant des adresses IP pour le VLAN, Pour cela nous tapons les instructions montrées ci-dessous :



```
SW-Federateur(config-if)#interface vlan 12
SW-Federateur(config-if)#ip address 169.11.1.10 255.255.255.0
SW-Federateur(config-if)#no shutdown
SW-Federateur(config-if)#interface vlan 13
SW-Federateur(config-if)#ip address 169.12.1.10 255.255.255.0
SW-Federateur(config-if)#no shutdown
SW-Federateur(config-if)#interface vlan 14
SW-Federateur(config-if)#ip address 169.13.1.10 255.255.255.0
SW-Federateur(config-if)#no shutdown
SW-Federateur(config-if)#interface vlan 15
SW-Federateur(config-if)#ip address 169.14.1.10 255.255.255.0
SW-Federateur(config-if)#no shutdown
SW-Federateur(config-if)#interface vlan 16
SW-Federateur(config-if)#ip address 169.15.1.10 255.255.255.0
SW-Federateur(config-if)#no shutdown
SW-Federateur(config-if)#exit
SW-Federateur(config)#
SW-Federateur(config)#
```

Figure III.19 : configuration des interfaces VLAN

h. Sauvegarde la configuration

Lorsque nous terminons la configuration nécessaire sur le Switch fédérateur il faut passer à une étape finale essentielle qui consiste à sauvegarder cette configuration à l'aide de la commande suivante :

IOS Command Line Interface

```
SW-Federateur con0 is now available



Press RETURN to get started.









SW-Federateur>enable
SW-Federateur#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-Federateur#
```

Figure III.20 : Sauvgarde de configuration

i. Sécurité des ports sur le switch fédérateur

Nous allons utiliser les 16 premiers ports, il nous reste les 8 ports derniers non utilisées, pour cela nous allons sécuriser ces 16 ports par l'intermédiaire de la commande suivante :

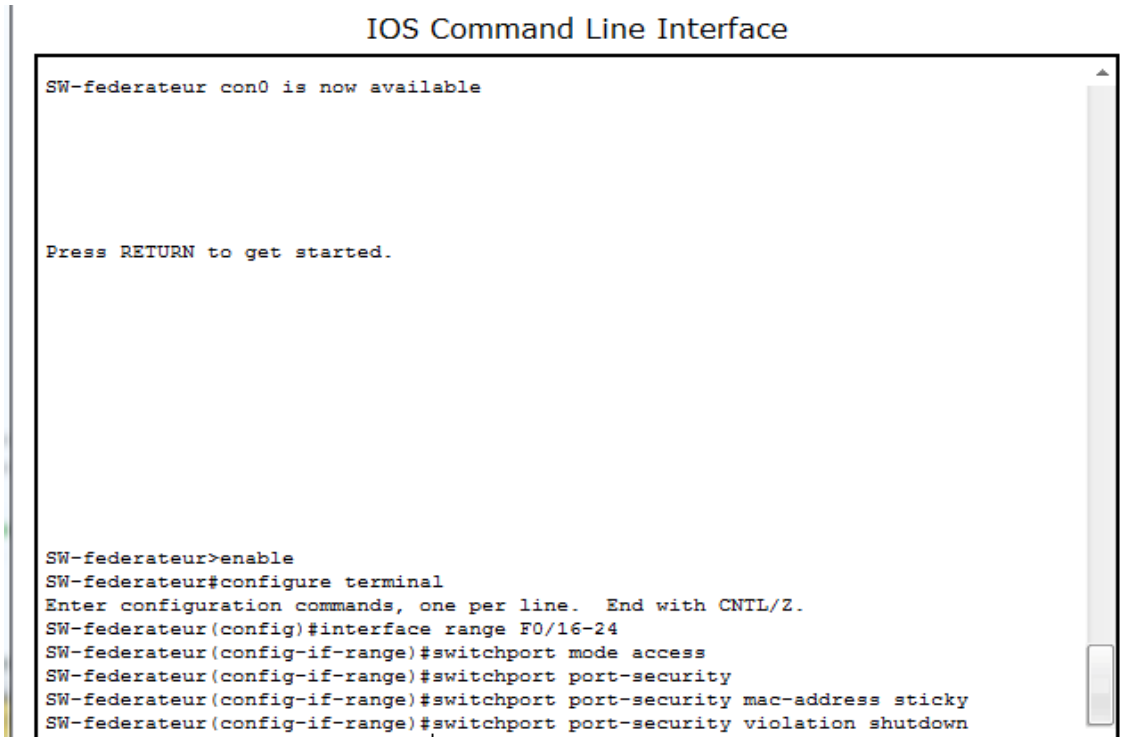


Figure III.21 : Sécurité des ports sur le switch fédérateur

III.4.2.2. Configuration de routeur

- ✓ **Routage statique et routage dynamique**

Dans le routage statique, les informations de routage sont mises à jour manuellement tandis que dans le routage dynamique, les informations sont automatiquement mises à jour à l'aide des protocoles, c'est-à-dire nous ajoutons un serveur DHCP au réseau permettant l'attribution automatique des adresses IP.

Lorsque nous faisons une petite comparaison entre les deux types nous trouvons que le routage dynamique est mieux que le routage statique grâce à :

L'avantage du routage dynamique est :

-Configuration sure, fiable et centralisée.

-Réduction de la gestion de configuration (surtout pour les réseaux de grande taille). [20]

L'inconvénient du routage statique est :

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

-A chaque fois quand le réseau évolue, il faut que chaque routeur soit au courant de l'évolution par une mise à jour manuelle de la part de l'administrateur qui doit modifier les routeurs selon l'évolution. [20]

1. Routage statique

a. Configuration de nom de routeur

Au début de configuration de base de routeur nous commençons par l'attribution du nom avec la commande suivante :

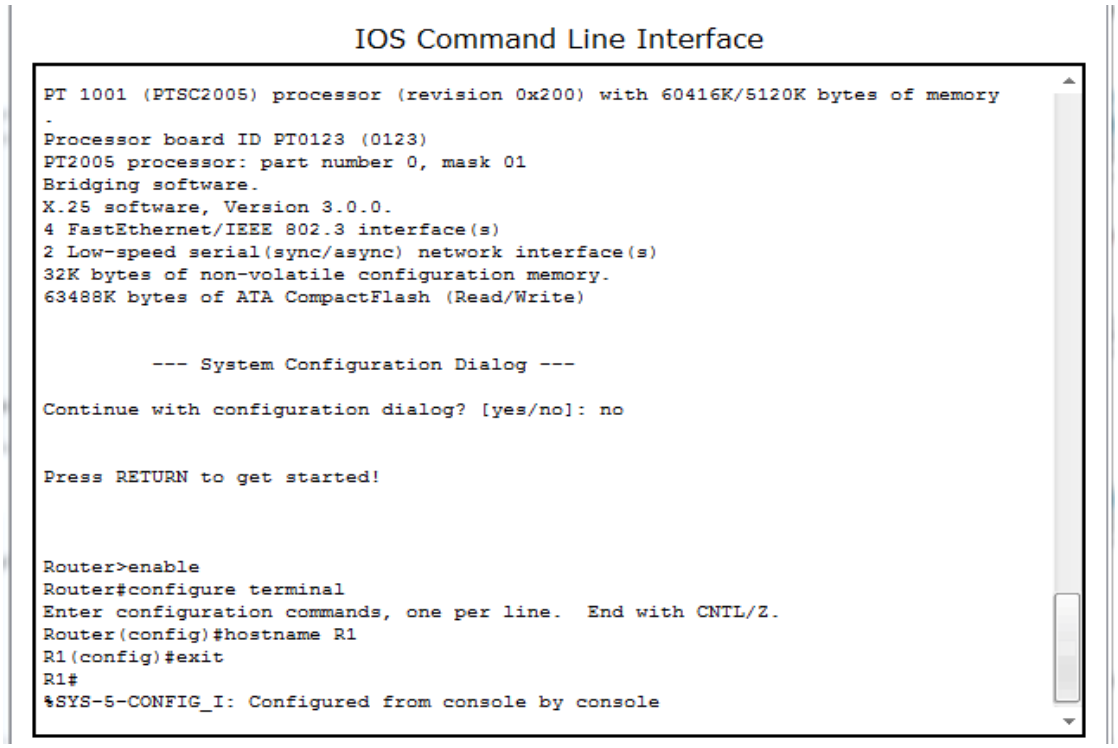


Figure III.22 : Configuration de nom de routeur

b. Sécurisation des routeurs

Lorsque nous voulons sécuriser mon routeur il faut ajouter un mot de passe en mode prévilligée c'est le mot de passe pour l'accès enable, nous considérons deux façons :

La première façon est enregistrer le mot de passe d'une façon claire dans le fichier de configuration et la deuxième façon est que le mot de passe va être enregistré d'une façon crypté.

✓ **La 1ère façon**

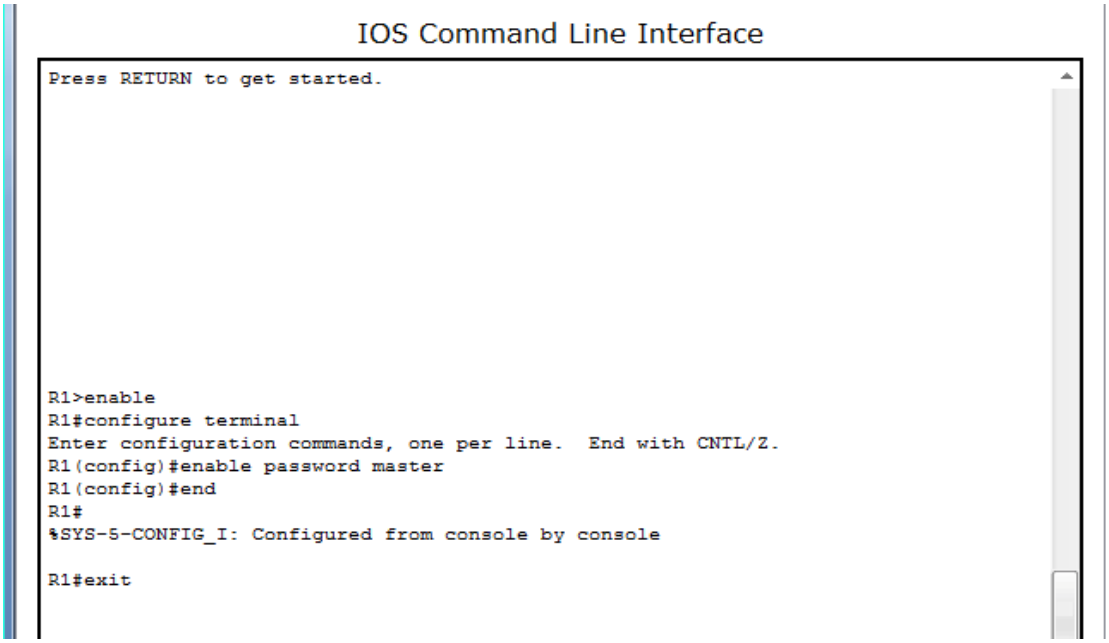


Figure III.23 : Sécurisation du routeur (claire)

✓ **La 2eme façon**

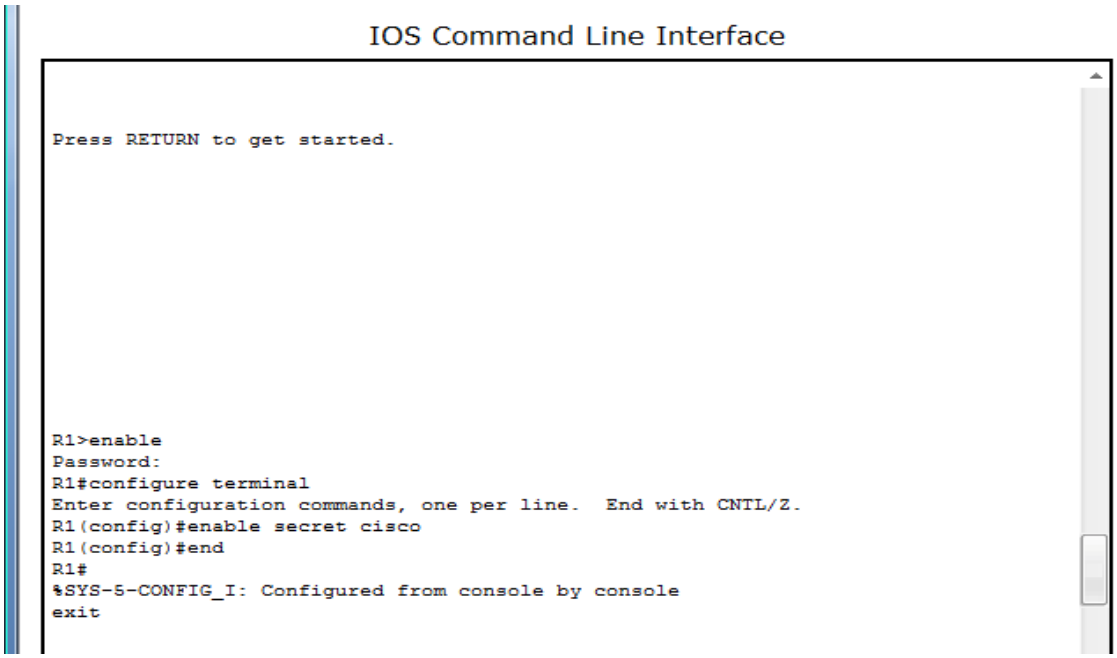


Figure III.24 : Sécurisation du routeur (crypté)

c. Configuration du routage RIP

Dans chaque routeur nous activions le routage RIP et nous déclarons les réseaux connectés directement au routeur.

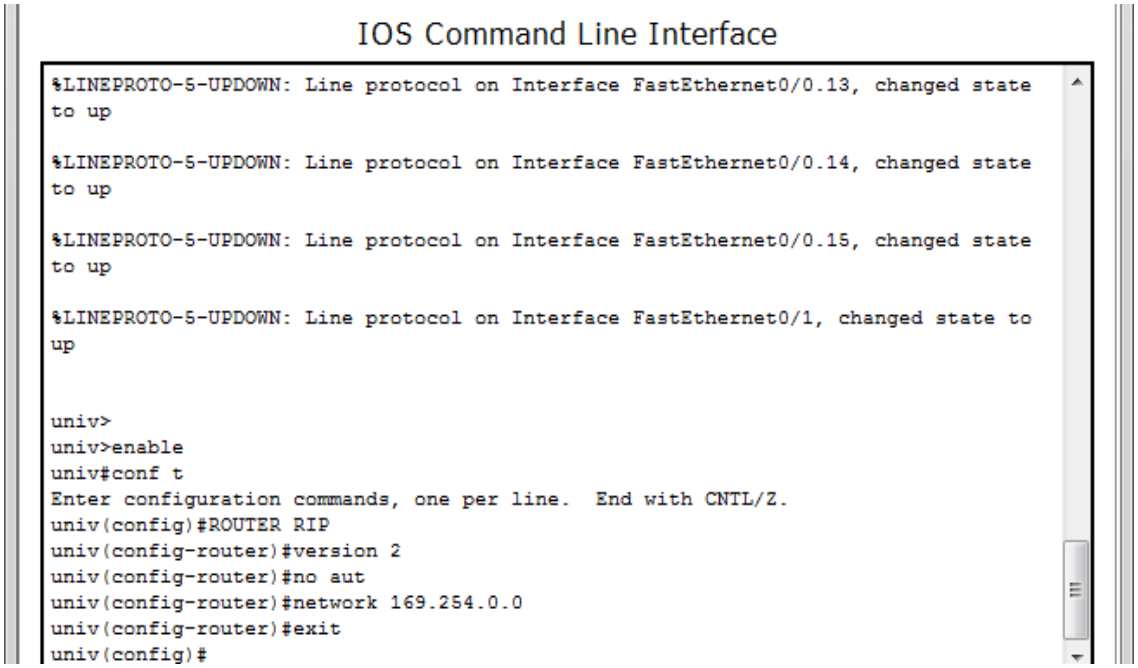


Figure III.25 : Routage RIP

d. Configuration des interfaces

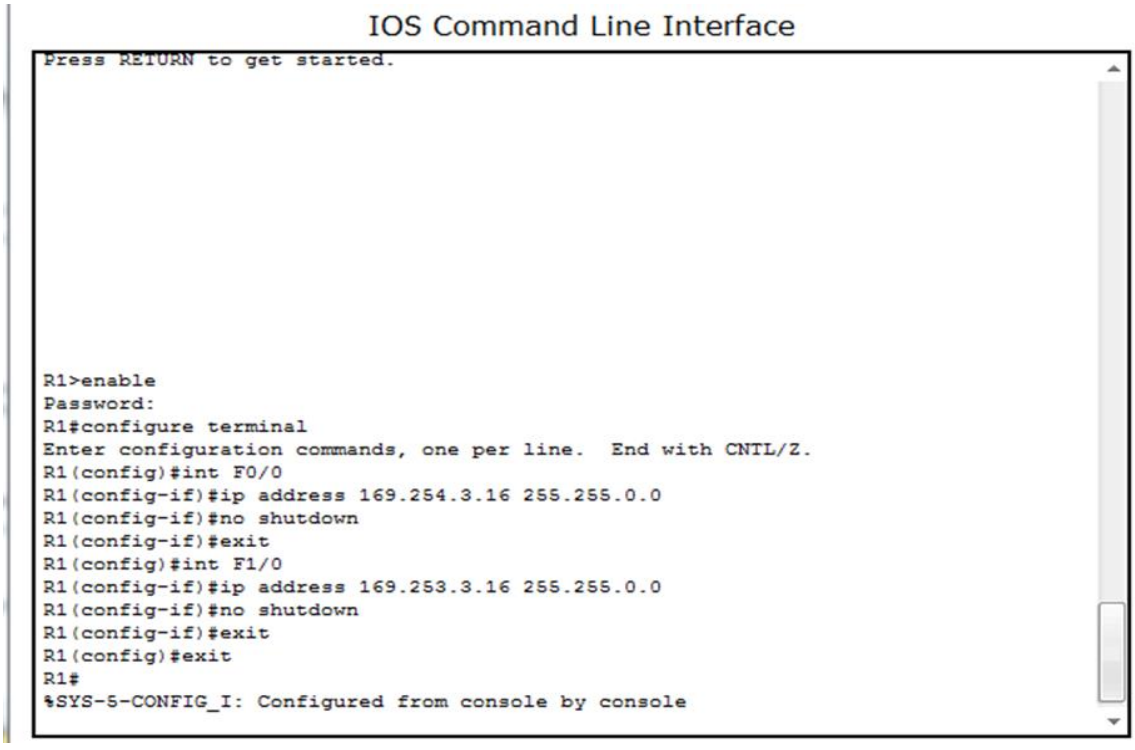


Figure III.26 : Configuration des interfaces

e. Routage inter VLAN

Pour relier des VLANs entre eux, il faut créer des interfaces virtuelles sur le routeur, la figure suivante (Figure III.27) illustre le routage inter-VLAN.

IOS Command Line Interface

```
univ>
univ>en
univ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
univ(config)#interface FastEthernet 0/0.1
univ(config-subif)#encapsulation dot1Q 2
univ(config-subif)#ip address 169.1.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.2
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state
to up

univ(config-subif)#encapsulation dot1Q 3
univ(config-subif)#ip address 169.2.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.3
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state
to up

univ(config-subif)#encapsulation dot1Q 4
univ(config-subif)#ip address 169.3.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.4
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.4, changed state
to up
```

```
univ(config-subif)#encapsulation dot1Q 5
univ(config-subif)#ip address 169.4.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.5
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.5, changed state
to up

univ(config-subif)#encapsulation dot1Q 6
univ(config-subif)#ip address 169.5.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.6
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.6, changed state
to up

univ(config-subif)#encapsulation dot1Q 7
univ(config-subif)#ip address 169.6.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.7
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.7, changed state to up
```

```
univ(config-subif)#encapsulation dot1Q 8
univ(config-subif)#ip address 169.7.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.8
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.8, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.8, changed state
to up

univ(config-subif)#encapsulation dot1Q 9
univ(config-subif)#ip address 169.8.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.9
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.9, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.9, changed state
to up

univ(config-subif)#encapsulation dot1Q 10
univ(config-subif)#ip address 169.9.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.10
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
```

```
univ(config-subif)#encapsulation dot1Q 11
univ(config-subif)#ip address 169.10.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.11
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.11, changed state
to up

univ(config-subif)#encapsulation dot1Q 12
univ(config-subif)#ip address 169.11.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.12
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.12, changed state to up
```

```
univ(config)#interface FastEthernet 0/0.13
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.13, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.13, changed state
to up

univ(config-subif)#encapsulation dot1Q 14
univ(config-subif)#ip address 169.13.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.14
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.14, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.14, changed state
to up

univ(config-subif)#encapsulation dot1Q 15
univ(config-subif)#ip address 169.14.1.10 255.255.255.0
univ(config-subif)#no shutdown
univ(config-subif)#exit
univ(config)#interface FastEthernet 0/0.15
univ(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.15, changed state to up
```

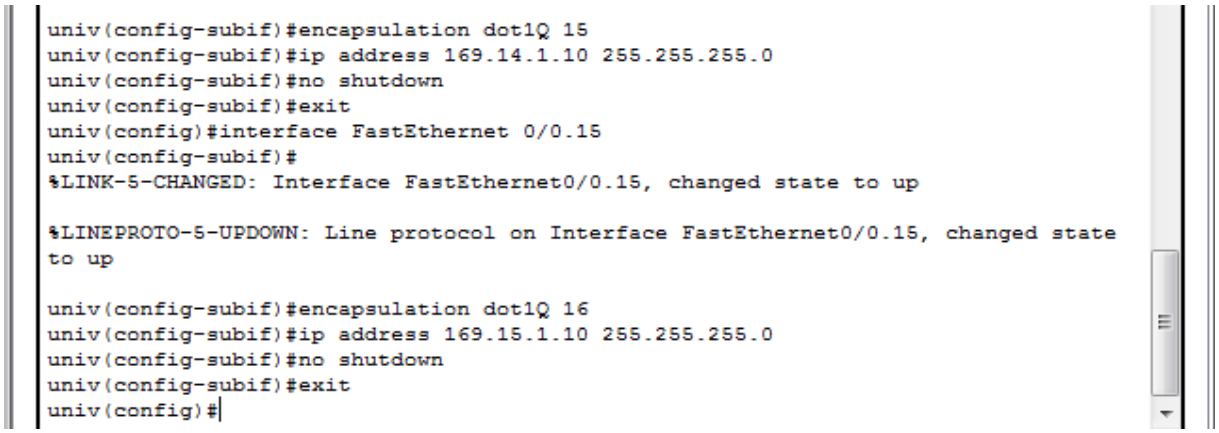


Figure III.27 : Routage inter-VLAN

Routage dynamique

Le Protocol DHCP (Dynamic Host Configuration Protocol) a pour rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine dans le réseau. Nous attribuons automatiquement avec le protocole DHCP les adresses à tous les PC existés dans le réseau et après nous faisions le Routage dynamique des VLAN dans le routeur.

f. Configuration DHCP

La figure suivante (Figure III.28) montre les plages d'adresses utilisées et le sous- réseau approprié pour chaque VLAN.

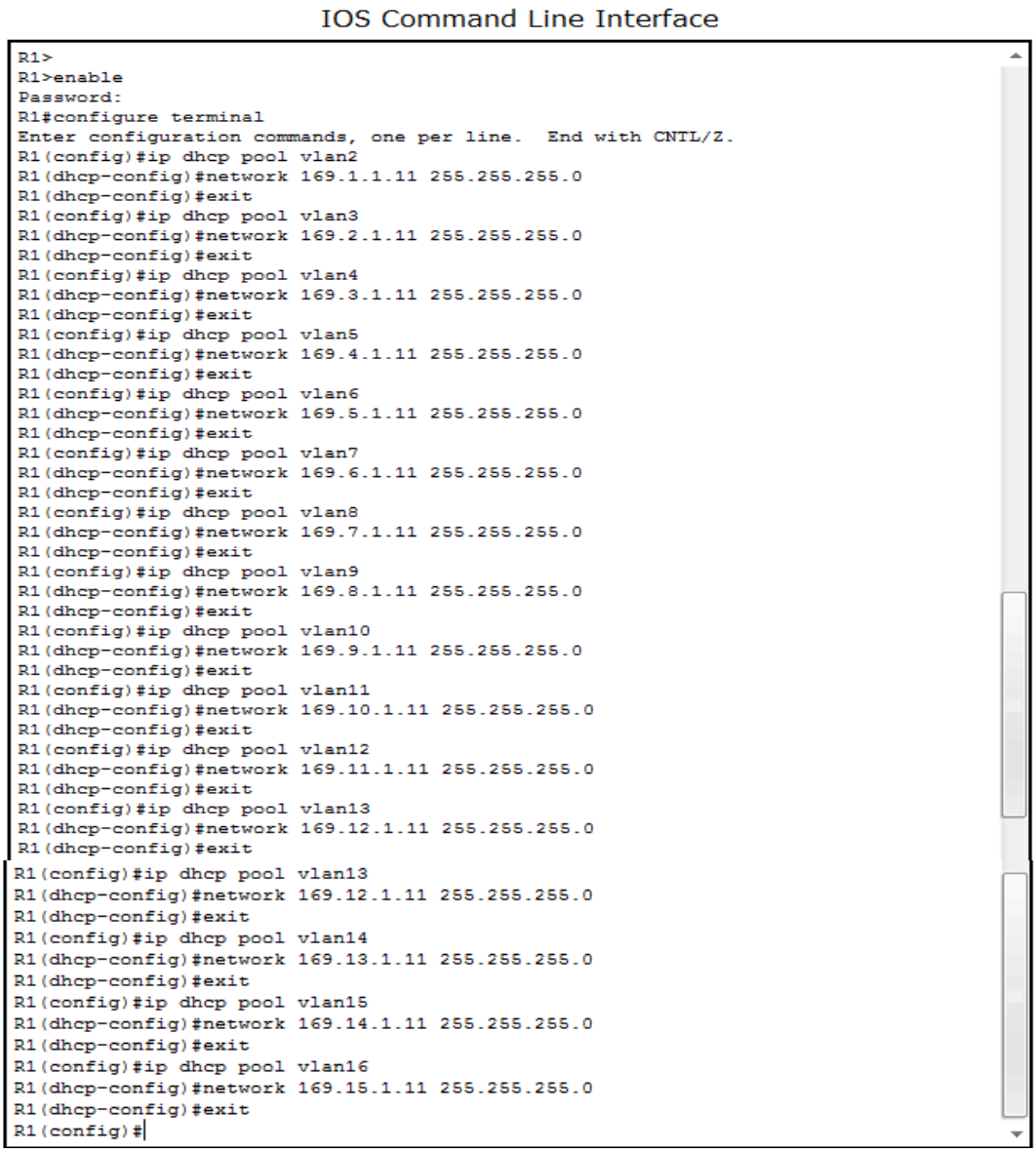


Figure III.28 : Configuration DHCP

III.4.3. Vérifications et test de validation

1/Vérification dans routeur

- **Vérification du mot de passe :**

Après la création du mot de passe nous allons l'afficher à l'aide de la commande « show run » comme suit :

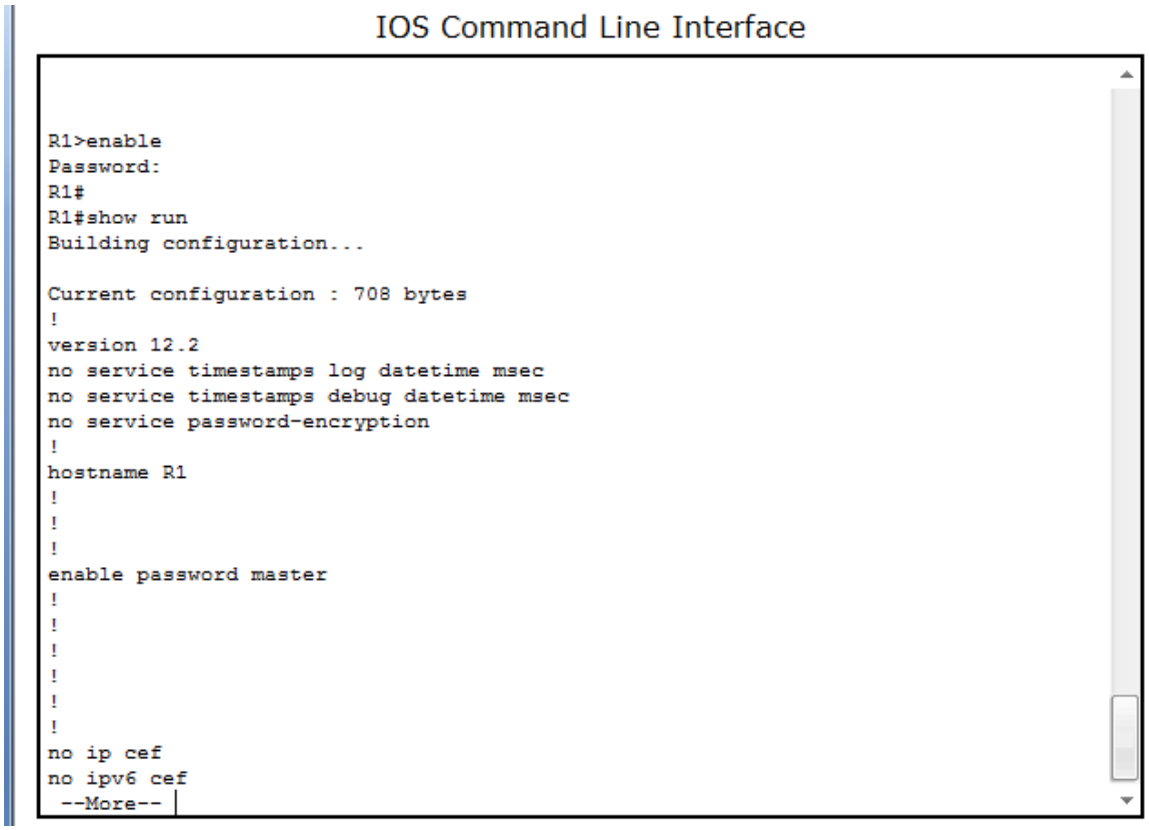


Figure III.29 : Vérification du mot de passe (claire)

- ✓ Le mot de passe est affiché clairement qui est master.

Après la création du mot de passe nous allons l'afficher à l'aide de la commande « show run » comme suit :

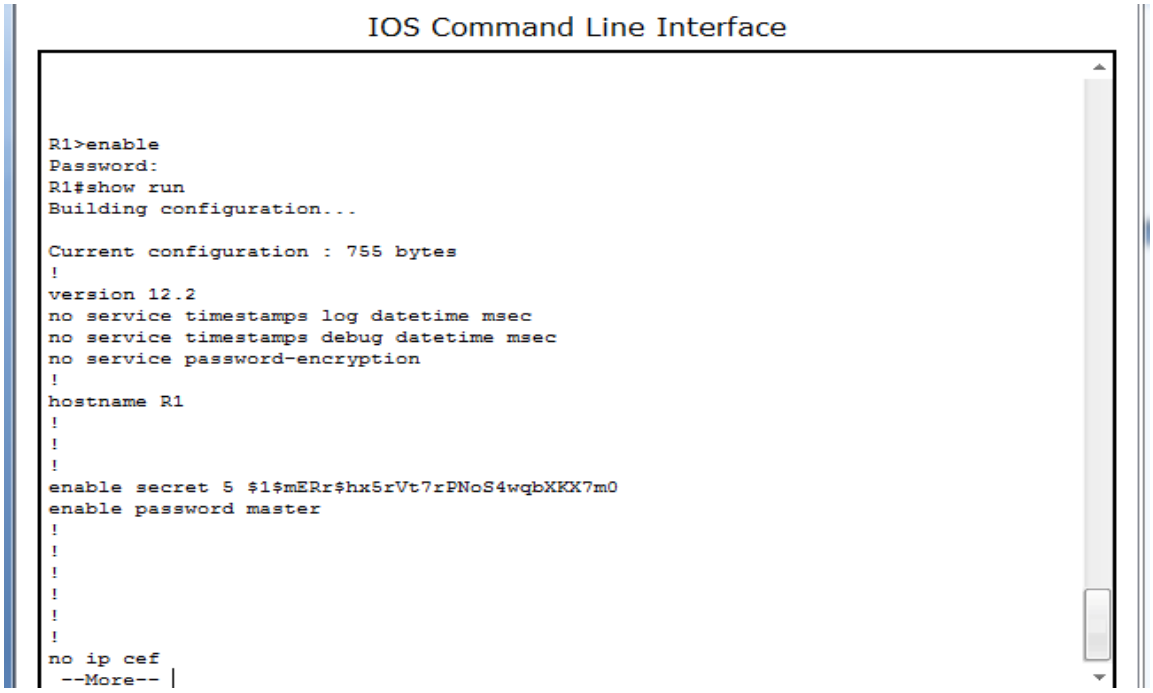


Figure III.30 : Vérification du mot de passe (crypté)

Nous avons affiché le mot de passe master et le mot de passe crypté Cisco

- .**Vérification inter vlan**

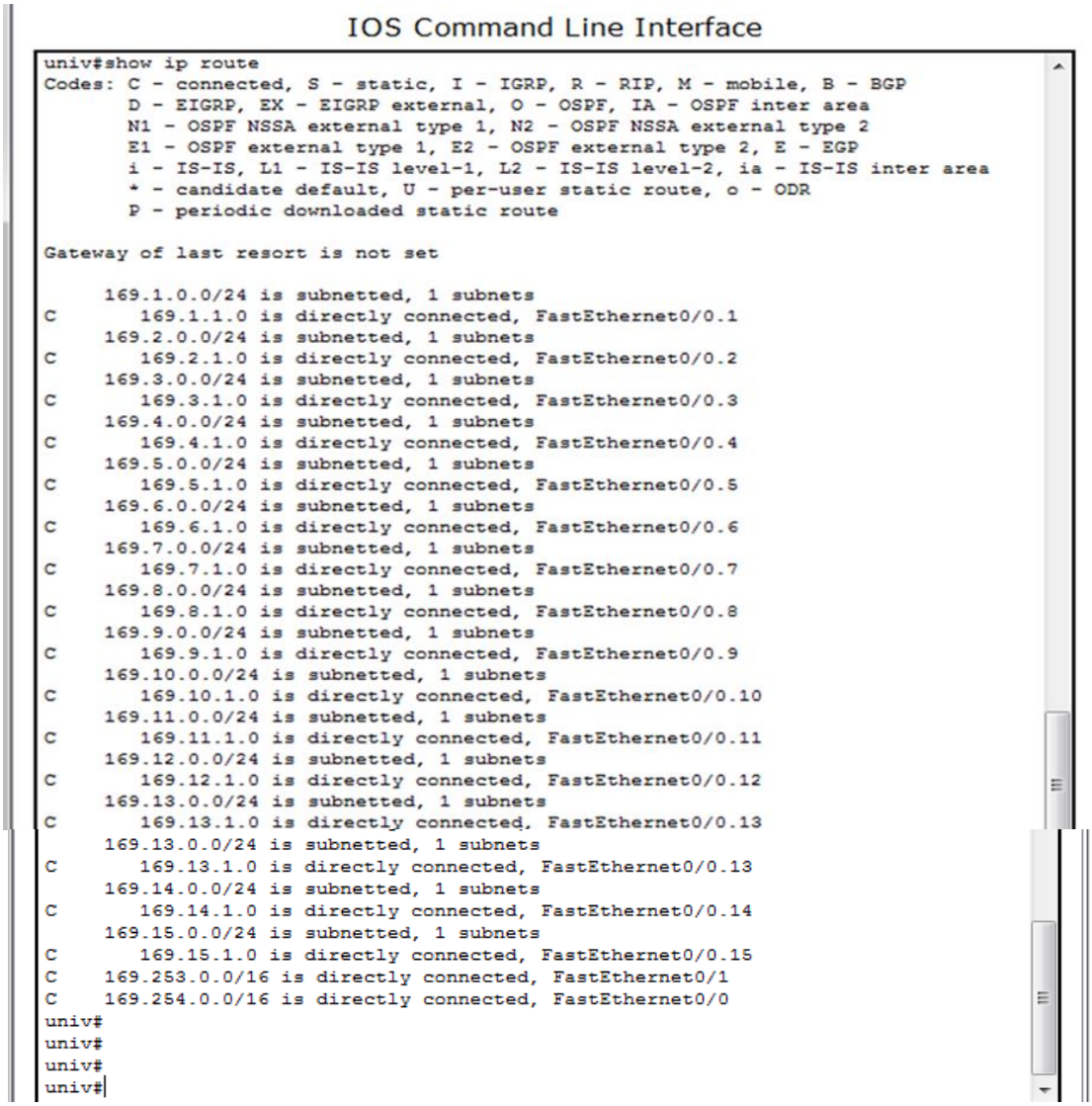
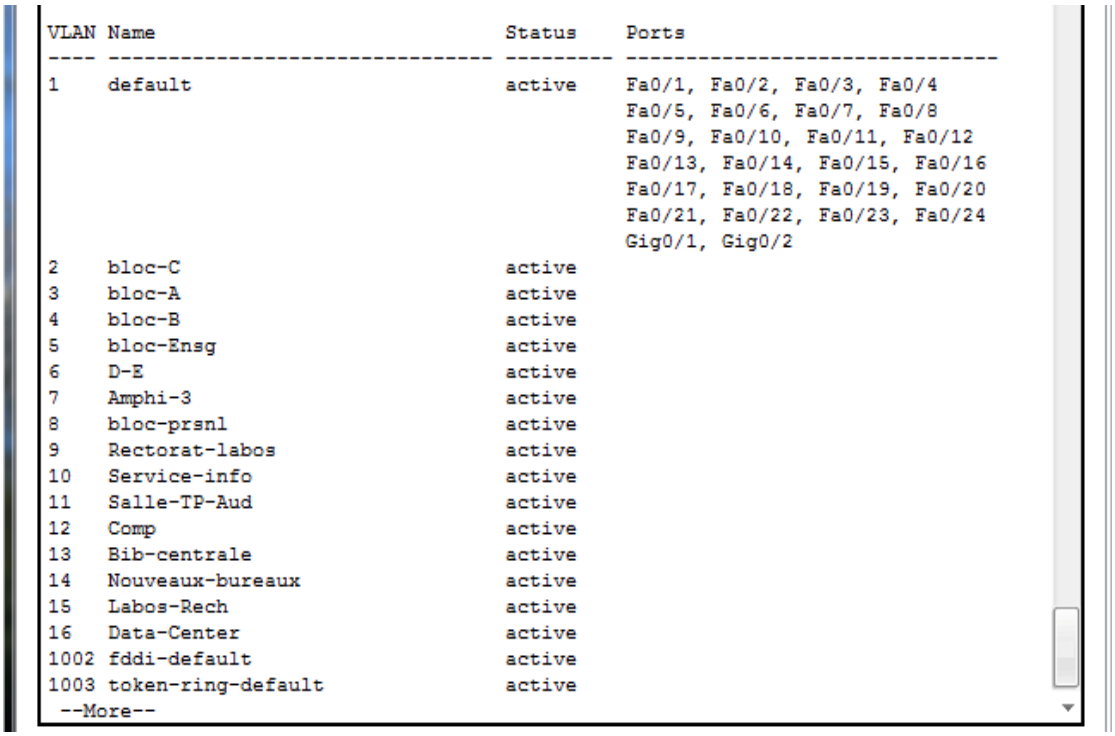


Figure III.31 : Vérification inter VLAN

2/Vérification dans les switch :

- **Vérification des VLAN :**

Après la création des VLAN nous allons les affichés en utilisant la commande (show vlan breif) :



```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
2    bloc-C                           active
3    bloc-A                           active
4    bloc-B                           active
5    bloc-Ensg                        active
6    D-E                              active
7    Amphi-3                          active
8    bloc-prsnl                       active
9    Rectorat-labos                   active
10   Service-info                     active
11   Salle-TP-Aud                     active
12   Comp                             active
13   Bib-centrale                     active
14   Nouveaux-bureaux                 active
15   Labos-Rech                       active
16   Data-Center                      active
1002 fddi-default                     active
1003 token-ring-default               active
 --More--
```

Figure III.32 : Vérification du VLAN

- **Vérification des interfaces VLAN dans le switch fédérateur**

Nous terminons la configuration des interfaces VLAN par la commande ip routing et après nous visualisons ces interfaces VLAN par la commande (show ip interface brief).

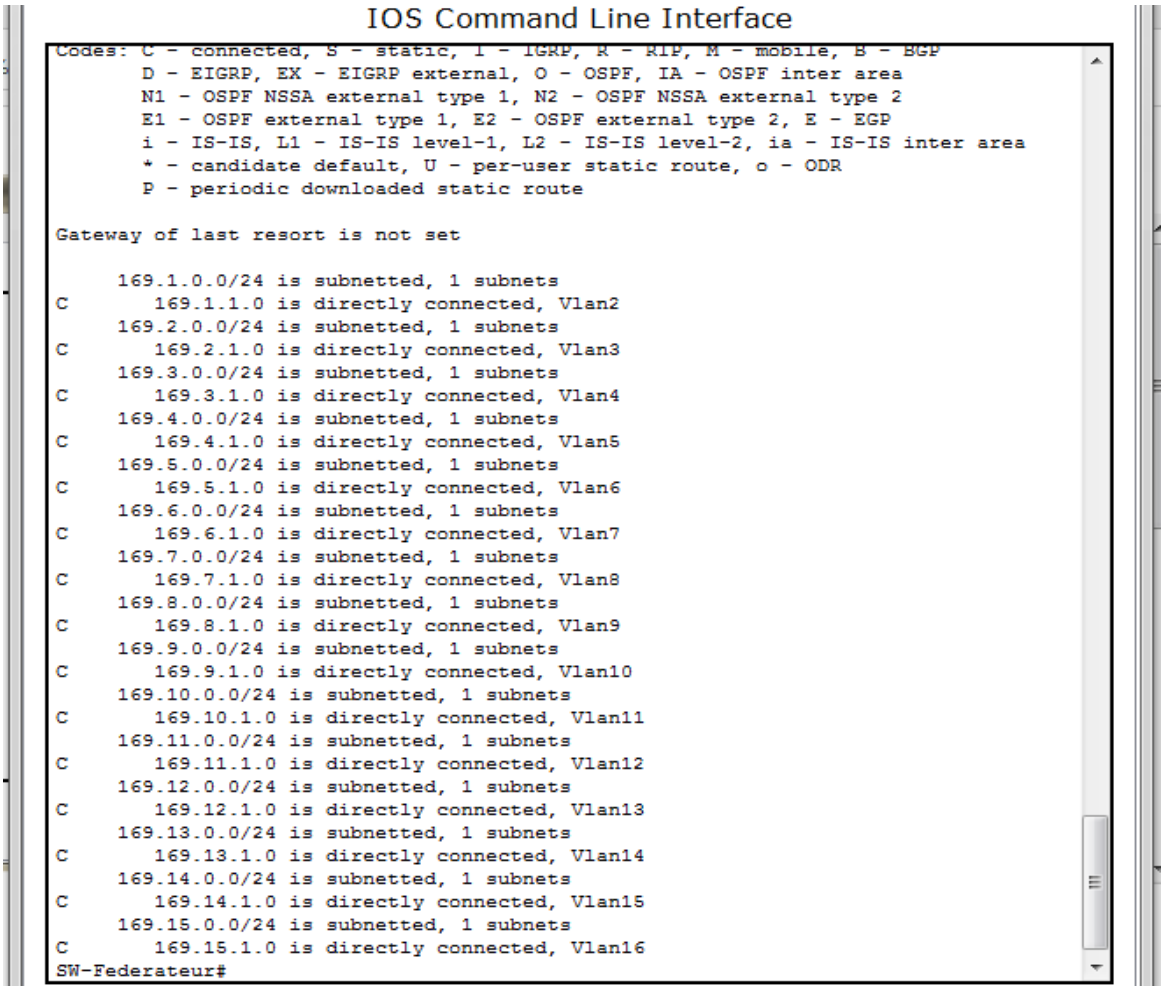


Figure III.33 : Vérification des interfaces VLAN dans le switch fédérateur

- **Vérification de lien Trunk**

Nous vérifions le mode Trunk dans le switch fédérateur par la commande « show inter trunk »

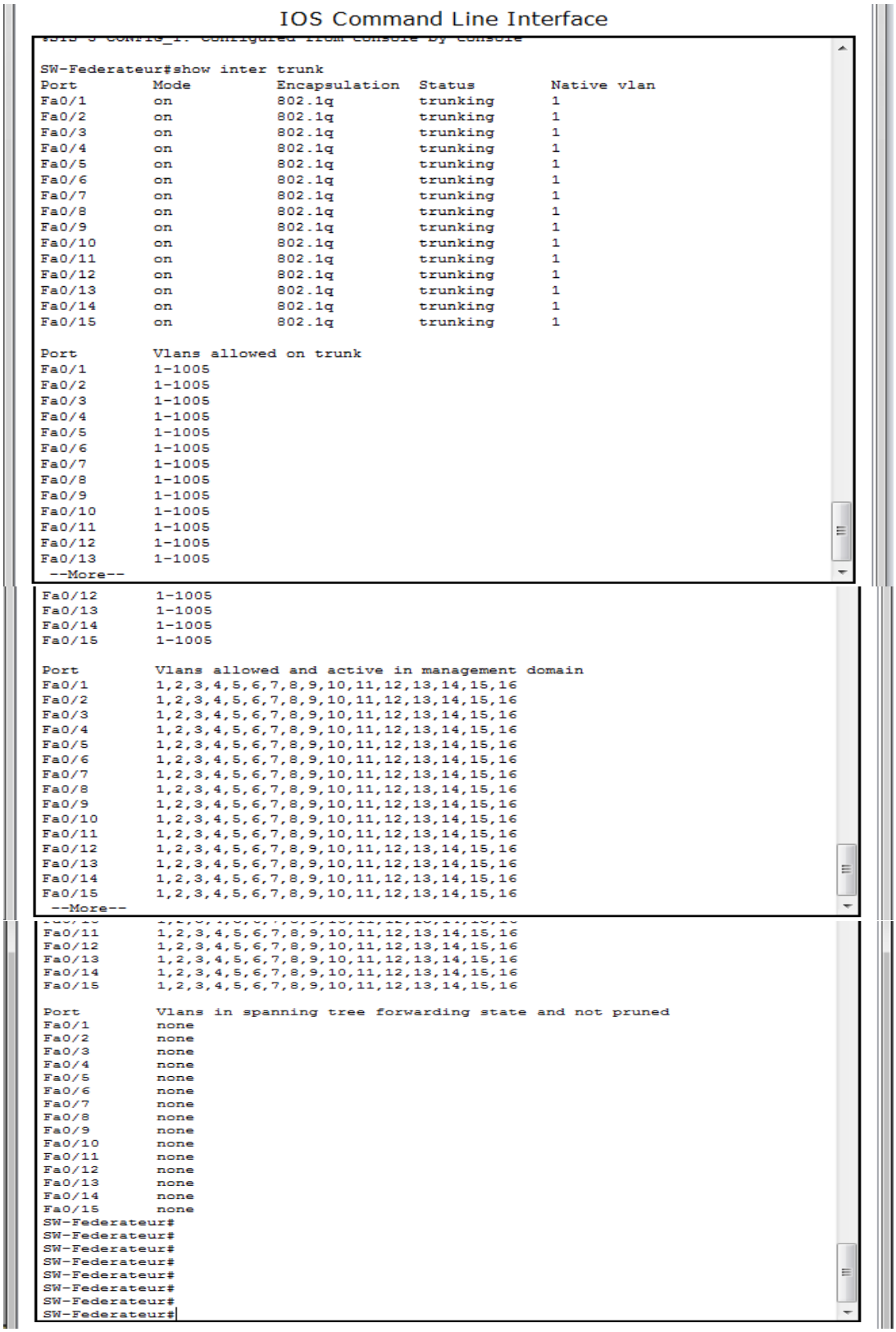


Figure III.34 : Vérification de lien Trunk

- **Vérification des ports de switch fédérateur**

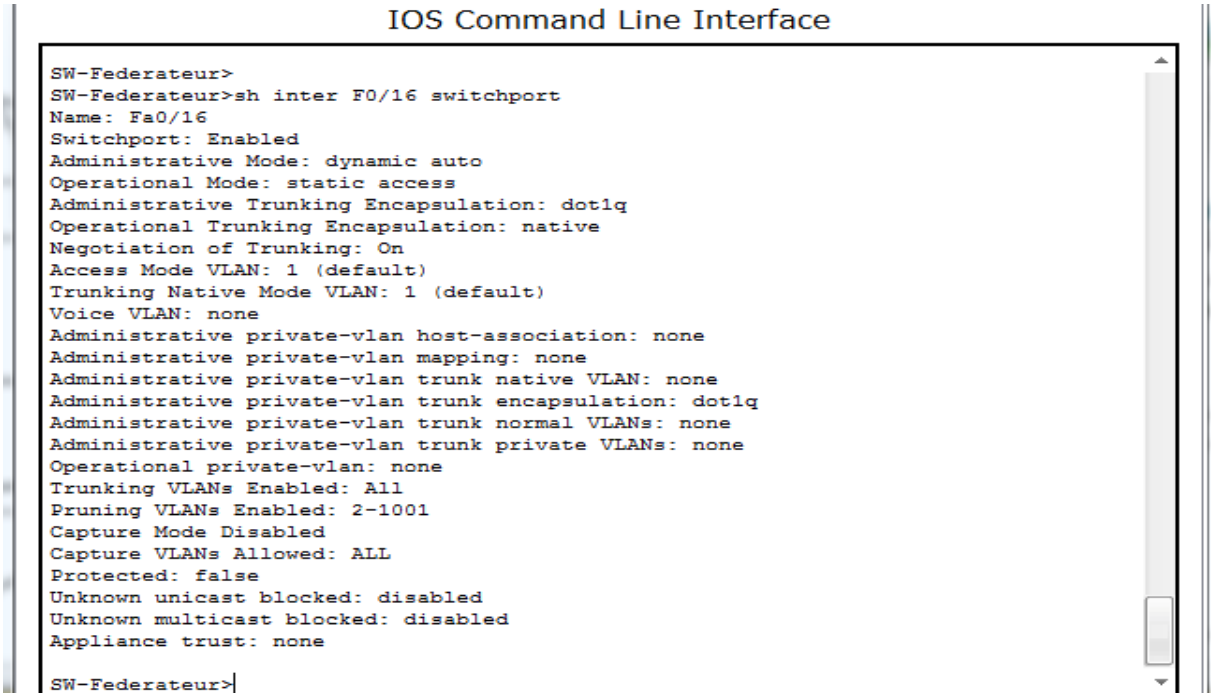


Figure III.35: Vérification des ports de switch fédérateur

- **Vérification de connectivité entre PC1 et PC2 de même VLAN2**

Nous vérifions l'accessibilité des équipements du même VLAN situé dans un réseau local commun. Depuis le PC 1, essayons d'accéder au PC 2, les deux se trouvent dans la même VLAN.

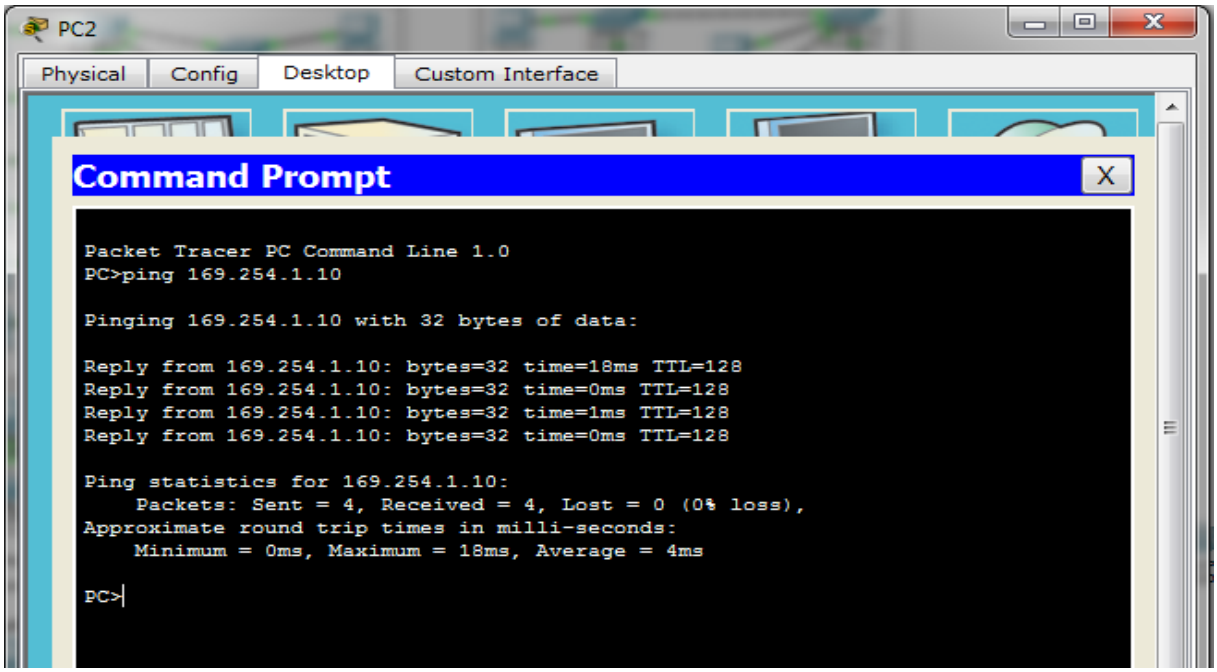


Figure III.36 : Vérification de connectivité entre PC1 et PC2

- **Vérification de connectivité entre PC1 de VLAN2 et PC6 de VLAN3**

A ce stade, nous pouvons vérifier l'accessibilité des différents équipements dans un même réseau mais dans deux VLANs distincts à partir du PC 1 en essayant d'accéder au PC 6.

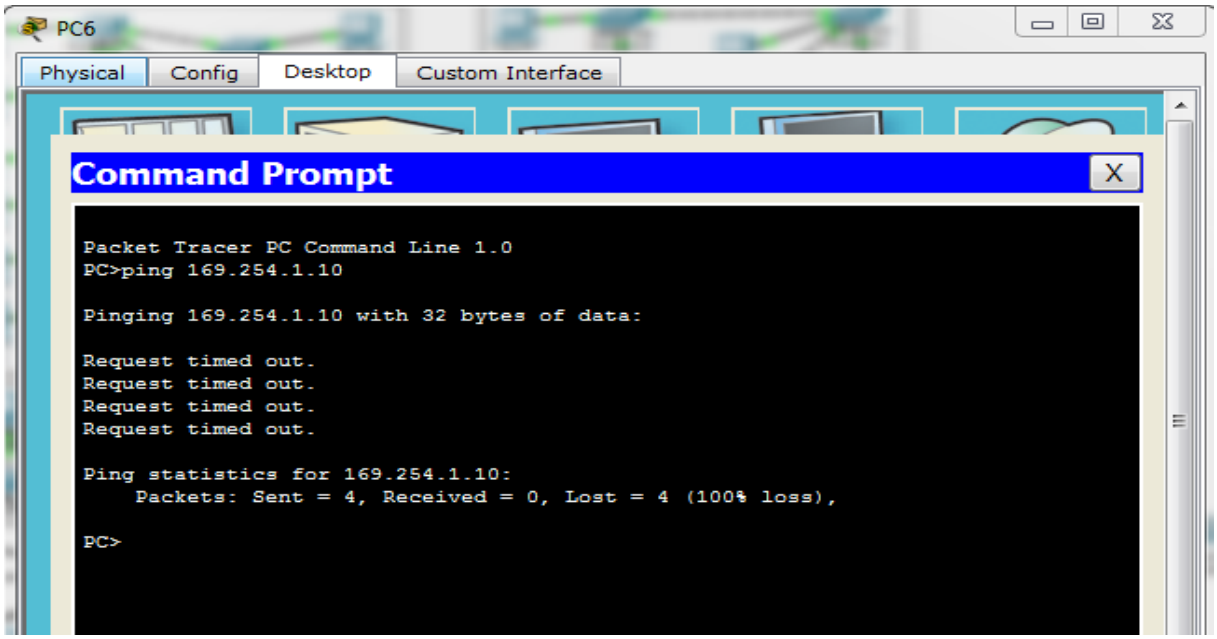


Figure III.37 : Vérification de connectivité entre PC1 et PC6

Conclusion

Dans ce chapitre nous avons essayé de faire la configuration de tous les équipements existés dans notre réseau : configuration des switch, routeur et PC par le simulateur Cisco Packet Tracer et nous avons ensuite effectué un ensemble de tests de validation afin de prouver l'efficacité du réseau.

Conclusion générale

Dans le but de mieux appréhender nos connaissances théoriques et les mettre en pratique, nous avons amenés à réaliser notre travail qui a pour objectif de l'étude et la simulation d'un réseau local au sein de notre université Djilali Bounaama sous l'environnement Cisco Packet Tracer 6.2.

Pour mettre en œuvre ce projet, nous avons acquis les connaissances nécessaires à la création d'un réseau local efficace et extensible. Nous Présentons ce projet en deux grandes parties. La première partie a porté de généralités sur les réseaux locaux et comment évolué ses dernies années ainsi que Nous avons donné aussi un aperçu sur les attaques réseaux et les mécanismes de la sécurité. La deuxième partie concerne la configuration de ce réseau, Nous Avons approfondi les fonctionnalités des commutateurs de niveau 2 et multi-niveaux tels que les VLANs, le protocole VTP, les trunks, le routage inter-VLAN, l'agrégation des ports, le routage dynamique et statique de routeur…etc. suivie par des tests et vérification de la validation qui assure le bien fonctionnement du notre réseau étudié.

Ce travail a pour but d'assurer le fonctionnement optimal des ressources réseaux de notre université et un partage facile des informations et effectuée un transfert des fichiers efficace entre plusieurs poste à distance, cet environnement permet aux administrateurs de bénéficier la sécurité et la facilité de la gestion au sein d'université

Finalement, nous avons le plaisir de traiter ce sujet qui nous a motivée à développer nos connaissances au domaine de réseau informatique et télécommunication et aussi a bien maîtrisée le logiciel Cisco Packet Tracer 6.2.

Bibliographie

[1] josé.DORDOIGNE, « réseaux informatique », 5eme Edition ENI, janvier 2013.

[2] www.ens-lyon.fr

[3] Jean-François PILLOU, «tous sur les réseaux et internet »,4eme Edition.

[4] junior0 et Vinc14, «les réseaux de zéro » ,14 octobre 2012.

[5] Jean-Pierre Arnaud, « Réseaux et Télécoms », Dunod, paris, 2003.

[6] http://www.securiteinfo.com

[7] Yousef chaiki douas, mémoire, les types des attaques informatiques, janvier 2010

[8]Guy Pujolle, « Les réseaux »,4éme édition, Groupe Eyrolles, 2004

[9] www.cours-gratuit.com--Coursréseau-id2815.pdf

[10]**GENE-96.DOC**, « cours sur les réseaux locaux », (www.cours-gratuit.com--Gene_lan.zip)

[11]JEBRI Elies-technologue, « Réseaux locaux »,(www.cours-gratuit.com--CoursInformatique-id3116.pdf)

[12]Raymond Panko, « Sécurité des systèmes d'information et des réseaux, 2004 Pearson Education France.

[13]Paul Pinault, « Administration d'un réseau local », 2003, (www.cours-gratuit.com--CoursInformatique-id31179.pdf)

[14] Vincent REMAZEILLES, « La sécurité des réseaux avec CISCO », Edition ENI-Février 2009

[15] Michel Crucianu, « réseaux locaux », SUPPORT DE COURS, E3i, 2001-2002, Université de Tours

[16] architecture des réseaux locaux. 622, PDF

[17] www.cours-gratuit.com--id-4304.pdf

[18]**KACED Kahina, Khelili Yasmina** « Etude sur la technologie MSAN et réalisation d'une plateforme VOIP simulée à base de la solution Vlan et le protocole DHCP », université MOULOUD MAMMERI DE TIZI-OUZOU, en 2015

[19]UtilisationPacketracer.pdf

[20] www.cours-gratuit.com--id-4235.pdf

[21] www.univ-km.dz

[22] https://flatfeefsbo.com/fr/cisco/17-understanding-cisco-ios-command-line-modes.html.com

{Annexe}

Switch	IP adresse
Switch 1	169.254.1.11
Switch 2	169.254.1.21
Switch 3	169.254.1.31
Switch 4	169.254.1.41
Switch 5	169.254.1.51
Switch 6	169.254.2.11
Switch 7	169.254.2.21
Switch 8	169.254.2.31
Switch 9	169.254.2.41
Switch 10	169.254.2.51
Switch 11	169.254.2.61
Switch 12	169.254.2.71
Switch 13	169.254.2.81
Switch 14	169.254.3.11
Switch 15	169.254.3.21
Switch 16	169.254.3.31
Switch 17	169.254.3.41
Switch 18	169.254.4.11
Switch 19	169.254.4.21
Switch 20	169.254.4.31
Switch 21	169.254.4.41
Switch 22	169.254.5.11
Switch 23	169.254.5.21
Switch 24	169.254.5.31
Switch 25	169.254.6.11
Switch 26	169.254.6.21
Switch 27	169.254.7.11
Switch 28	169.254.7.21
Switch 29	169.254.7.31
Switch 30	169.254.8.11
Switch 31	169.254.9.11
Switch 32	169.254.10.11
Switch 33	169.254.10.21
Switch 0	169.254.10.31
Switch 34	169.254.11.11
Switch 35	169.254.12.11

Switch 36	169.254.13.11
Switch 37	169.254.14.11
Switch 38	169.254.14.21
Switch 39	169.254.15.11
Switch 40	169.254.15.21
Switch 41	169.254.15.31
Switch 42	169.254.15.41
Switch 43	169.254.15.51

Tableau 1 : adresse des switch

Vlan	**Nom**	**@ IP**	**Masque**	**Passerelle**
Vlan 2	Bloc-C	169.1.1.11	255.255.255.0	169.1.1.10
Vlan 3	Bloc-A	169.2.1.11	255.255.255.0	169.2.1.10
Vlan 4	Bloc-B	169.3.1.11	255.255.255.0	169.3.1.10
Vlan 5	Bloc-Ensg	169.4.1.11	255.255.255.0	169.4.1.10
Vlan 6	D-E	169.5.1.11	255.255.255.0	169.5.1.10
Vlan 7	Amphi-3	169.6.1.11	255.255.255.0	169.6.1.10
Vlan 8	Bloc-prsnl	169.7.1.11	255.255.255.0	169.7.1.10
Vlan 9	Rectorat-labos	169.8.1.11	255.255.255.0	169.8.1.10
Vlan 10	Service-info	169.9.1.11	255.255.255.0	169.9.1.10
Vlan 11	Salle-TP-Aud	169.10.1.11	255.255.255.0	169.10.1.10
Vlan 12	Comp	169.11.1.11	255.255.255.0	169.11.1.10
Vlan 13	Bib-centrale	169.12.1.11	255.255.255.0	169.12.1.10
Vlan 14	Nouveaux-bureaux	169.13.1.11	255.255.255.0	169.13.1.10
Vlan 15	Labos-Rech	169.14.1.11	255.255.255.0	169.14.1.10
Vlan 16	Data-Center	169.15.1.11	255.255.255.0	169.15.1.10

Tableau 2 : adresse des VLAN

PC	**IP adresse**	**Le masque**	**Passerelle**	**Vlan**
Pc 1	169.254.1.10	255.255.0.0	169.254.1.252	VLAN 2
Pc 2	169.254.1.20	255.255.0.0	169.254.1.252	
Pc 3	169.254.1.30	255.255.0.0	169.254.1.252	
Pc 4	169.254.1.40	255.255.0.0	169.254.1.252	
Pc 5	169.254.1.50	255.255.0.0	169.254.1.252	
Pc 6	169.254.2.10	255.255.0.0	169.254.2.252	VLAN 3
Pc 7	169.254.2.20	255.255.0.0	169.254.2.252	
Pc 8	169.254.2.30	255.255.0.0	169.254.2.252	
Pc 9	169.254.2.40	255.255.0.0	169.254.2.252	
Pc 10	169.254.2.50	255.255.0.0	169.254.2.252	

Pc 11	169.254.2.60	255.255.0.0	169.254.2.252	
Pc 12	169.254.2.70	255.255.0.0	169.254.2.252	
Pc 13	169.254.2.80	255.255.0.0	169.254.2.252	
Pc 14	169.254.3.10	255.255.0.0	169.254.3.252	VLAN 4
Pc 15	169.254.3.20	255.255.0.0	169.254.3.252	
Pc 16	169.254.3.30	255.255.0.0	169.254.3.252	
Pc 17	169.254.3.40	255.255.0.0	169.254.3.252	
Pc 18	169.254.4.10	255.255.0.0	169.254.4.252	VLAN 5
Pc 19	169.254.4.20	255.255.0.0	169.254.4.252	
Pc 20	169.254.4.30	255.255.0.0	169.254.4.252	
Pc 21	169.254.4.40	255.255.0.0	169.254.4.252	
Pc 22	169.254.5.10	255.255.0.0	169.254.5.252	VLAN 6
Pc 23	169.254.5.20	255.255.0.0	169.254.5.252	
Pc 24	169.254.5.30	255.255.0.0	169.254.5.252	
Pc 25	169.254.6.10	255.255.0.0	169.254.6.252	VLAN 7
Pc 26	169.254.6.20	255.255.0.0	169.254.6.252	
Pc 27	169.254.7.10	255.255.0.0	169.254.7.252	VLAN 8
Pc 28	169.254.7.20	255.255.0.0	169.254.7.252	VLAN 8
Pc 29	169.254.7.30	255.255.0.0	169.254.7.252	
Pc 30	169.254.8.10	255.255.0.0	169.254.8.252	VLAN 9
Pc 31	169.254.9.10	255.255.0.0	169.254.9.252	VLAN 10
Pc 32	169.254.10.10	255.255.0.0	169.254.10.252	VALN 11
Pc 33	169.254.10.20	255.255.0.0	169.254.10.252	
Pc 0	169.254.10.30	255.255.0.0	169.254.10.252	
Pc 34	169.254.11.10	255.255.0.0	169.254.11.252	VLAN 12
Pc 35	169.254.12.10	255.255.0.0	169.254.12.252	VLAN 13
Pc 36	169.254.13.10	255.255.0.0	169.254.13.252	VLAN 14
Pc 37	169.254.14.10	255.255.0.0	169.254.14.252	VLAN 15
Pc 38	169.254.14.20	255.255.0.0	169.254.14.252	
Pc 39	169.254.15.10	255.255.0.0	169.254.15.252	VLAN 16
Pc 40	169.254.15.20	255.255.0.0	169.254.15.252	
Pc 41	169.254.15.30	255.255.0.0	169.254.15.252	
Pc 42	169.254.15.40	255.255.0.0	169.254.15.252	
Pc 43	169.254.15.50	255.255.0.0	169.254.15.252	

Tableau 3 : adresse des PC