République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université Abderrahmane Mira Béjaia

Faculté des sciences exactes

Département d'informatique

Mémoire de fin de cycle

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

Option : Administration et Sécurité des Réseaux

Thème

Organisation du réseau en VLAN
Cas d'étude : Entreprise NAFTAL

Réalisé par :

- ✓ **Mr. AIT AMARA** Jugurta
- ✓ **Mr. AMEZZA** Lyes

Encadré par :

- ✓ **Mr. EL SAKAAN** Nadim
- ✓ **Pr. TARI** Alkamel

Devant le jury :

Président	**Mr. AMROUN** Kamel
Examinateur 1	**Mme. BATTAT** Nadia
Examinateur 2	**Mlle. BENNAI** Soufia

Promotion 2016-2017

Dédicaces

Ce modeste travail est dédié :

A nos chers parents

qui nous ont soutenus et encouragés durant toute notre scolarité

A nos frères

A nos enseignants

A nos amis(e)

A toutes les personnes qui nous ont apportés de l'aide…

Remerciements

Nos premiers remerciements s'adressent à Dieu le tout puissant qui par sa bonté et sa miséricorde nous a permis d'avoir le courage, la foi et la volonté de mener à bien ce travail. Nous tenons aussi à remercier nos encadreurs, le Professeur TARI et Monsieur EL SAKAAN qui ne nous ont lésé d'aucune information, qui ont été présent à tout moment de la réalisation de ce projet et surtout sans lesquels ce modeste travail n'aurait jamais vu le jour, ainsi que les membres du jury pour l'intérêt qu'ils ont portés à notre recherche en acceptant d'éxaminer notre travail et de l'enrichir par leurs propositions. Nous remercions également tous les enseignants qui ont contribués de près ou de loin à notre formation universitaire, sans oublier toute personne qui nous a aidés à mener à terme notre projet.

TABLE DES MATIÈRES

TABLE DES FIGURES

ABBREVIATIONS

ACL	Access Control List
ATM	Asynchronous Transfert Mode
CLI	Commande Langage Interface
CSMA/CD	Carrier Sence Multiple Access with Collision Detect
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
FTP	File Transfert Protocol
FDDI	Fiber Distributed Data Interface
HSRP	Host Standby Routing Protocol
HTTP	Hyper Text Transfer Protocol
IDS	Intrusion Detection System
ISO	International Standards Organisation
IP	Internet Protocol
IPX	Internetwork Packet eXchange
LAN	Local Area Network
MAN	Métropolitains Area Network
MAC	Media Acess Control
MAU	Multistaion Access Unit
OSI	Open Systems Interconnection
RSTP	Rapid Spanning Tree protocole
STP	Spanning Tree protocole
TCP	Transmission Control Protocol

VLAN	Virtual Local Area Network
VTP	Vlan Trunking Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

INTRODUCTION GÉNÉRALE

Au fil du temps les entreprises ont sentis le besoin de se confier a une solution réseau pour gérer leurs communications et partage de données sur le plan interne et externe. Mais la croissance de ces dernières s'est accompagné d'un certain nombres de contraintes résultant ainsi un nombre accru du trafic échangé et l'utilisation excessive de la bande passante, ce qui a provoqué une baisse de performances du réseau.donc une bonne organisation du réseau remédiera à ces problèmes.

L'évolution du réseau local a suivi une progression logique de l'amélioration de s'attaquer aux différentes contraintes posées au sein de l'entreprise. les commutateurs ont aussi subit une évolution par l'introduction d'un concept appelé VLAN(réseau local virtuel), qui a été introduit avec beaucoup de battage médiatique.

L'objectif de notre travail est d'étudier le réseau de NAFTAL (district béjaïa) avec une critique et une solution proposée.pour cela notre projet contiendra les chapitres suivants :

Le premier chapitre est consacré à la présentation de quelques généralités sur les réseaux et la sécurité informatique.

Le chapitre suivant contient deux parties la première présente une introduction aux réseaux locaux virtuels, les principales notions ainsi que les protocoles utilisés. Dans la deuxième partie nous avons présenter l'organisme d'accueil NAFTAL(district béjaïa) et l'étude de leurs existant.

Les problématiques rencontrées lors de notre stage au sein de cette entreprise feront l'objet de notre projet d'implémenter une solution VLAN .

Enfin nous allons conclure ce mémoire avec une conclusion générale et perspectives.

CHAPITRE 1

GENERALITES SUR LES RESEAUX ET LA SECURITE INFORMATIQUE

Introduction

Un réseau informatique permet de relier un ensemble de matériels par supports de transmission qui leur permettent d'échanger des informations entre eux. Pour bien mener notre projet, on doit comprendre les notions de bases sur les réseaux informatiques est très important de bien maitriser le sujet.

L'objectif de ce chapitre est de présenter quelques concepts de bases sur les réseaux informatiques, pour bien aider à mieux assimiler le fonctionnement des réseaux. Donc, toutes les notions nécessaires seront présentées, tirant exemple de la classification des réseaux, le modèle OSI et TCP/IP ainsi les moyens de sécurité.

1.1 Définition d'un réseau

Un réseau (network) est un ensemble des moyens matériels et immatériels mis en œuvre pour assurer les communications entre ordinateurs, stations de travail et terminaux informatiques.

Les réseaux informatiques permettent aux utilisateurs de communiquer entre eux et de transférer des informations. Ces transmissions de données peuvent concernées l'échange de messages entre utilisateurs, l'accès à distance aux bases de données ou encore le partage de fichiers .[1]

1.2 Les différents types de réseaux

On distingue différents types de réseaux selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. Les réseaux informatiques sont généralement classifiés en trois catégories de réseaux selon leur échelle géographique.[2]

1.2.1 LAN (Local Area Network)

Un réseau local est un réseau informatique à une échelle géographique relativement restreinte, il est utilisé pour relier entre les ordinateurs d'une habitation particulière, d'une entreprise, d'une salle informatique. L'infrastructure est privée et est gérée localement. Les LANs classiques offrent des débits de l'ordre de Mbps sur de courtes distances, les plus évolués permettent d'atteindre 100Mbps, les réseaux a 1Gbps sont même annoncés aujourd'hui.[2]

1.2.2 MAN (Metropolitan area network)

Les MANs 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 formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).[2]

1.2.3 WAN (Wide area network)

Un WAN (réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faible. Les WANs fonctionnent grâce à des routeurs qui permettent de ''choisir" le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet.[2]

1.3 Topologies des réseaux

Il existe deux types de topologies : topologie logique et topologie physique.[3]

1.3.1 Topologies physiques

la topologie physique est la façon dont les équipements sont connectés physiquement les uns aux autres grâce à des lignes de communication (câbles réseaux) et des éléments matériels (cartes réseau, etc.)

1.3.2 Topologies logiques

Elle représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet,Token ring et FDDI.

1.4 Les protocoles réseaux

1.4.1 NetBEUI

Développé par Microsoft et IBM à l'époque des premiers réseaux de PC, ce protocole simplissime fonctionne très bien sur des petits réseaux. Malheureusement, son efficacité décroit avec le nombre de postes. De plus, il n'est pas « routable », ce qui fait que l'on ne peut interconnecter des réseaux NetBEUI autrement que par des ports.[3]

1.4.2 IPX/SPX

Développé par la société NOVELL, qui s'est octroyé la part du lion dans les premiers réseaux de PC avant que Microsoft ne développe Windows NT. Plus efficace que NetBUEI pour les gros réseaux, ce protocole est plus routable ce qui augmente les possibilités, plus efficace que NetBUEI pour les gros réseaux, ce protocole est plus routable ce qui augmente les possibilités d'interconnexions.[3]

1.4.3 DNS

Les ordinateurs connectés à un réseau IP, comme Internet, possèdent une adresse IP. Ces adresses sont numériques afin d'être plus facilement traitées par une machine. Pour faciliter l'accès

Aux systèmes qui disposent de ces adresses, un mécanisme a été mis en place pour permettre d'associer un nom à une adresse IP, plus simple à retenir, appelé nom de domaine. Résoudre un nom de domaine consiste à trouver l'adresse IP qui lui est associée. Le Domain Name System (système de noms de domaine) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine,et plus généralement de trouver une information à partir d'un nom de domaine.[3]

1.4.4 HSRP (Hot Standby Routing Protocol)

Le protocole HSRP est un protocole propriétaire de « continuité de service » implémenté dans les routeurs Cisco pour la gestion des « liens de secours », il sert à augmenter la tolérance de panne sur le réseau en créant un router virtuel à partir de 2 (ou plus) routeurs physiques : un « actifs » et l'autre (ou les autres) « en attente » (ou « standby ») en fonction des priorités accordées à chacun de ces routeurs. HSRP est un protocole propriétaire aux équipements Cisco et il n'est pas activité par défaut.[3]

1.4.5 DHCP (Dynamic Host Configuration Protocol)

Le protocole DHCP est un standard IP conçu pour simplifier la gestion de la configuration d'IP hôte. Le standard DHCP permet d'utiliser des serveurs DHCP comme une méthode de gestion d'affectation dynamique d'adresse IP et d'autre détails de configuration correspondante pour les clients DHCP d'un réseau. [3]

1.4.6 STP (Spanning-Tree)

Le protocole Spanning Tree (STP) est un protocole de couche 2, conçu pour les commutateurs. Le standard STP est défini dans le document IEEE 802.1D-2004. Il permet de créer un chemin sans boucle dans un environnement commuté et physiquement redondant. STP détecte

et désactive ces boucles et fournit un mécanisme de liens de sauvegarde. Le standard a été amélioré en incluant IEEE 802.1w RSTP (Rapid Spanning Tree).

Le protocole STP a pour but d'éviter les cycles (et donc des trames qui se baladent) et doit être recalculé à chaque modification de la topologie d'un réseau. Un effet visible de l'utilisation de cette technologie est les blocages de quelques secondes voire dizaines de secondes que les utilisateurs peuvent observer lorsqu'une machine est insérée dans un réseau sur lequel il y a un arbre de recouvrement (débranchez une machine d'un commutateur, rebranchez-la et observez : si votre réseau se bloque quelques temps c'est peut-être que votre commutateur recalcule son arbre de recouvrement)[4].

1.5 Modèle OSI (Open System Interconnexion)

Pour faciliter l'interconnexion des systèmes, un modèle dit d'interconnexion des systèmes ouverts, appelé encore OSI a été défini par ISO (International Standards Organisation). Le modèle OSI décrit un ensemble de spécifications pour une architecture réseau permettant la connexion d'équipements hétérogènes. Le modèle OSI normalise la manière dont les matériels et les logiciels coopèrent pour assurer la communication réseau. Ce modèle est organisé en sept couches successives.[5]

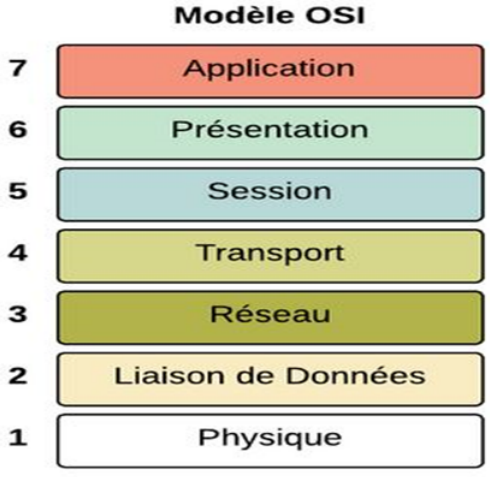

FIGURE 1.1: Le Modèle OSI[5]

1.5.1 Le rôle de ces couches

Chaque couche définie par le modèle a un rôle bien précis, qui va du transport du signal codant les données à la présentation des informations pour l'application du destinataire.[6]

1. **Couche physique :** cette couche gère la transmission des bits sur un support physique.
2. **Couche liaison de données :** cette couche assure le contrôle de la transmission des données, elle gère la fiabilité du transfert des bits d'un nœud à un autre du réseau, comprenant entre autres les dispositifs de détection et correction d'erreurs, ainsi que les systèmes de partage des supports. L'unité de données à ce niveau est appelée trames.
3. **Couche réseau :** cette couche assure la transmission des données sur les réseaux. c'est ici que la notion de routage intervient, permettant l'interconnexion de différents réseaux. En plus du routage, cette couche assure la gestion des congestions. L'unité de données à ce niveau est appelée paquet.
4. **couche transport :** cette couche gère le transport fiable des paquets de bout en bout.
5. **Couche session :**cette couche assure l'établissement, maintien et la terminaison des sessions de communication.
6. **Couche présentation :**conversion de données en un format standard. A ce niveau il y a la compression et cryptage de données.
7. **Couche application :** cette couche est source et destination de toutes les informations à transporter, elle rassemble toutes les applications qui ont besoin de communiquer par les réseaux : messagerie électronique, transfert de fichiers, gestionnaire de base de données.

1.6 Modèle TCP/IP

Même si le modèle de référence OSI est universellement reconnu, Historiquement et techniquement, la norme ouverte d'Internet est le protocole TCP/IP (pour Transmission Control Protocol/Internet Protocol). Le modèle de référence TCP/IP et la pille de protocoles TCP/IP rendent possible l'échange de données entre deux ordinateurs, partout dans le monde a une vitesse quasi équivalente à celle de la lumière.[5]

FIGURE 1.2: Le Modèle TCP/IP[5]

1.6.1 Le rôle de ces couche

1. **La couche application :** elle regroupe tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante .
2. **La couche transport :** chargée du contrôle de flux et la correction des erreurs et l'assurance d'un réseau de communication fiables avec un taux d'erreurs peu élevé.
3. **La couche internet :** elle assure la l'envoi des paquets d'un réseau quelconque et les faire parvenir à destination, indépendamment du trajet et les réseaux traversés pour y arriver.la commutations des paquets ainsi que l'identification du meilleur chemin ont lieu à ce niveau.
4. **La couche accès réseau :** elle se charge de tout ce qu'un paquet IP a besoin pour établir une liaison physique ainsi que tous les détails sur les technologies WAN, LAN et les autres détails dans les couches physiques et liaison de données du modèle OSI.

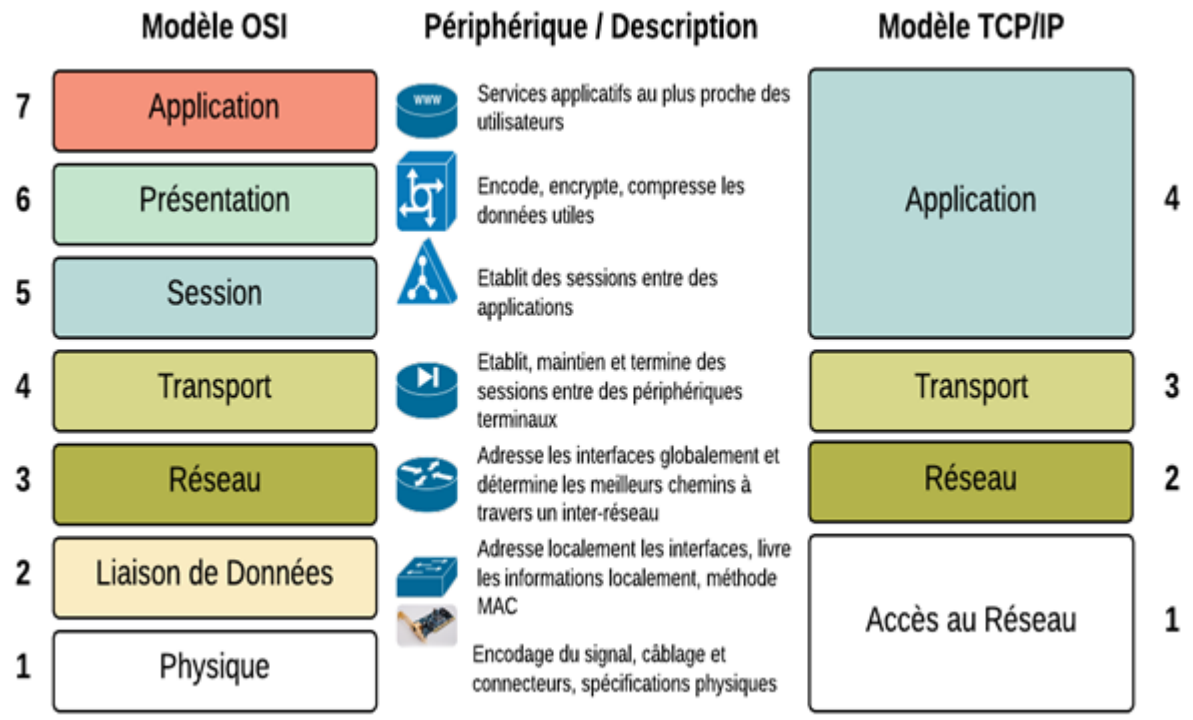

FIGURE 1.3: Correspondance des couches (TCP/IP et OSI)[5]

1.7 Sécurisation au niveau de la couche transport du réseau

Le paysage des attaques de sécurité au niveau de la couche de transport du réseau du modèle OSI est vaste. Celui-ci offre différentes opportunités d'effraction sur les communications. Cette couche a pour objectif de décrire la technologie utilisée pour le transport et l'acheminement des Datagrammes IP (paquets). C'est à ce niveau qu'interviennent les technologies Ethernet. Face à ces dangers, plusieurs techniques de protection et de prévention sont à la disposition des administrateurs réseau qui sont [7] :

1.7.1 Pare-feu

Le rôle du firewall est d'assurer un périmètre de protection entre le réseau interne à l'entreprise et le monde extérieur. Basé sur des technologies d'analyse des paquets à l'entrée et la sortie du périmètre protégé, le firewall permet ou interdit l'accès vers ou a partir de ce périmètre.

Composé d'équipements matériels et/ou logiciels, le firewall va réaliser les tâches suivantes :

- ✓ bloquer l'accès à des services non autorisés
- ✓ interdire l'accès à des systèmes
- ✓ protéger contre les attaques de type Dos (Déni de service)

Les firewalls peuvent intégrer des techniques de détection d'intrusions et peuvent envoyer des alertes afin de prévenir les équipes de surveillance technique. Ces équipements prennent en compte, un ensemble de règles qui doivent être définies en fonction des besoins d'une entreprise ou d'une administration.[7]

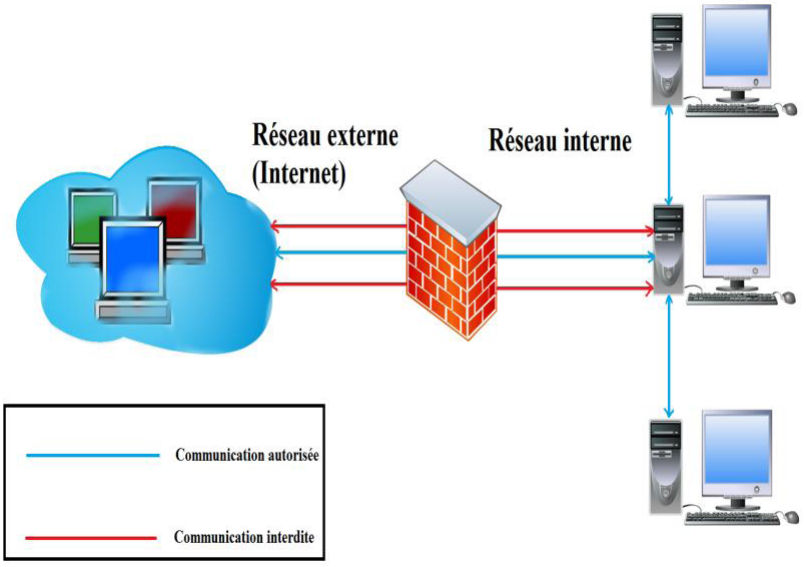

FIGURE 1.4: Pare-feu[7]

1.7.2 Proxy

Un système mandataire (Proxy) repose sur un accès à l'internet par une machine dédiée : le serveur mandataire ou Proxy server joue le rôle de mandataire pour les autres machines locales, et exécute les requêtes pour le compte de ces dernières [8].

Un serveur mandataire est configuré pour un ou plusieurs protocoles de niveau applicatif (HTTP, FTP, SMTP, etc.) et permet de centraliser, donc de sécuriser, les accès extérieurs (filtrage applicatif, enregistrement des connexions, masquage des adresses des clients, etc.).

Les serveurs mandataires configurés pour HTTP permettent également le stockage de pages web dans un cache pour accélérer le transfert des informations fréquemment consultées vers les clients connectés.

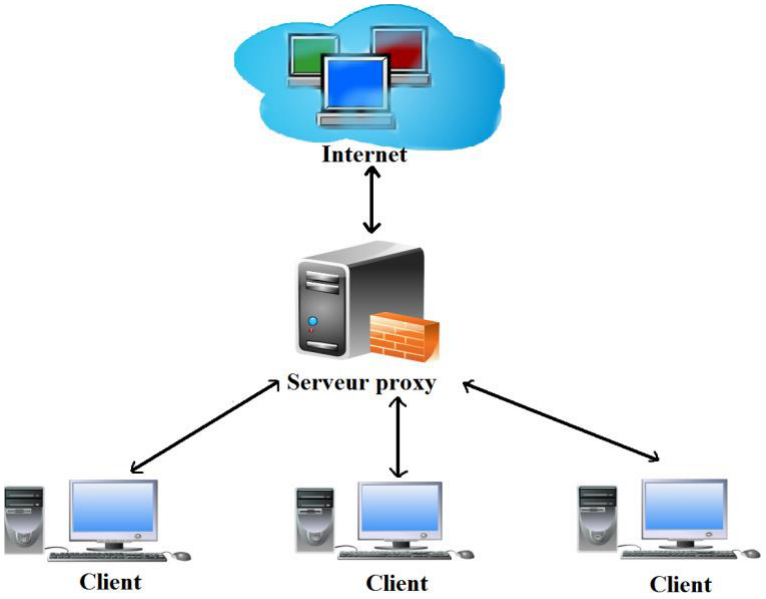

FIGURE 1.5: Proxy[8]

1.7.3 IDS/IDP/IPS

Les IDS/IDP/IPS, systèmes de détection d'intrusion et systèmes de détection et de prévention de l'intrusion, fournissent un complément technologique aux firewalls en leur permettant une analyse plus intelligente du trafic. Avec un firewall, on arrive à une bonne protection dans un périmètre délimité, Malheureusement, les hackers peuvent arriver à passer à travers les règles de sécurité des firewalls, notamment en exploitant les éventuelles failles des systèmes protégés. Les produits de détection d'intrusions (IDS ou Intrusion Detection System), développés parallèlement aux firewalls, permettent d'analyser plus finement les informations afin de détecter les véritables attaques et en évitant le plus possible les fausses alertes.
Les IDS sont chargés de distinguer les activités normales des activités parasites et/ou malveillantes. Il existe deux catégories d'évènements que les IDS doivent analyser :

1. **anomaly intrusion detection :**Il s'agit de la détection des comportements inhabituels de certains utilisateurs. Ce type de détection peut toutefois engendrer des fausses alertes, un comportement inhabituel n'étant pas forcément malveillant ou dangereux.
2. **misuse intrusion detection :** C'est la détection du mauvais fonctionnement d'un système informatique. La détection est basée sur des modèles prédéfinis d'attaques (signatures) qui exploitent les failles d'un système. Cette détection protège très bien contre les attaques connues, analysées et définies dans les modèles implémentés, mais ne réagit pas aux nouvelles attaques .

Puisque leur signature n'est pas encore connue. Il faudra donc prévoir d'apprendre à l'IDS ces nouvelles signatures.
La valeur des produits IDP/IPS réside dans leur capacité à bloquer immédiatement les attaques détectées, Un bon produit IDP/IPS, même s'il ne sera jamais parfait, devra :

- ✓ ne pas bloquer ou perturber le fonctionnement normal d'une entreprise ou d'une administration
- ✓ réagir immédiatement et bloquer l'attaque constatée
- ✓ agir complémentairement au firewall
- ✓ utiliser plusieurs algorithmes de lutte contre les attaques
- ✓ faire la différence entre un évènement normal et un évènement provoqué pour éviter les fausses alertes

1.7.4 Les Réseaux privés virtuels(VPN)

Le VPN (Virtual Private Network) permet d'établir des connexions sécurisées privées (un réseau privé) au travers d'un réseau public comme l'Internet. Ce dernier est réalisé avec les techniques d'encryptions et d'authentification, en assurant la qualité de services requise par les applications. Le VPN permet l'économie de connexions directes coûteuses entre les différentes implantations de l'entreprise, l'accès Internet lui servant à la fois pour la consultation classique de sites Web et pour son réseau privé.[9]

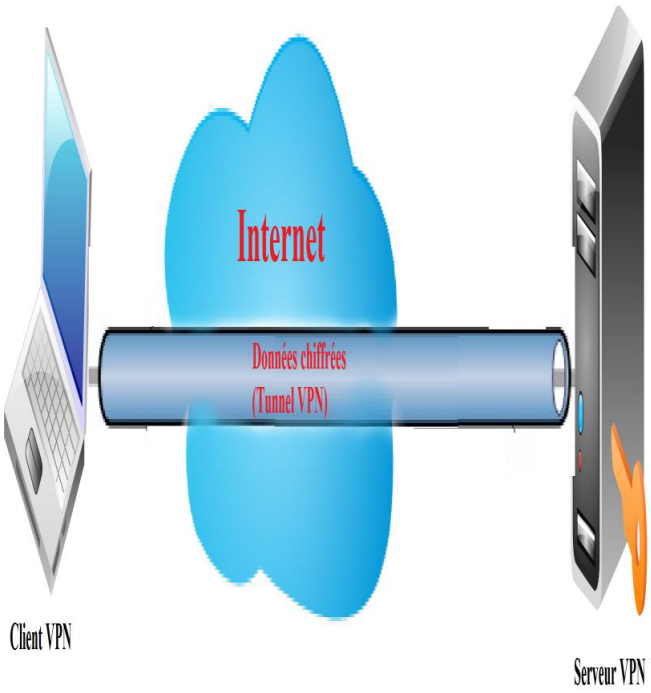

FIGURE 1.6: VPN[9]

1.7.4.1 Les cas d'utilisation des VPN

- ✓ réaliser des connexions à distance pour des utilisateurs mobiles ou télétravailleurs
- ✓ réaliser des interconnexions LAN to LAN
- ✓ contrôler l'accès dans un intranet

1.7.4.2 Les avantage des VPN

Les VPN présentent essentiellement deux avantages :

- ✓ les économies sur les budgets alloués à la connectivité. Ces économies sont obtenues en remplaçant les connexions longues distances via des lignes louées privées par une connexion unique à Internet sur laquelle on implémente des tunnels VPN afin de réaliser un réseau privé à travers Internet
- ✓ la flexibilité. Dans le cas d'une entreprise ou d'une administration ayant plusieurs localisations, l'ajout d'un nouveau site se fait simplement en le connectant à Internet et en l'incluant sur le VPN d'entreprise. Il sera ainsi très facilement intégré sur l'intranet d'entreprise.[9]

1.7.4.3 Les Inconvénients Des VPN

Parmi les désavantages des VPN, on peut citer :

- ✓ la disponibilité et les performances des VPN dépendent largement des fournisseurs de services et des sous-traitants.
- ✓ les standards ne sont pas toujours respectés et les technologies VPN restent dépendantes des équipements utilisés.
- ✓ la mise en route d'un VPN réclame une forte expertise, et notamment une bonne compréhension de la sécurité informatique et des technologies VPN spécifiques.[9]

1.7.5 Les Réseaux Locaux virtuels(VLAN)

L'évolution rapide de la connectivité Internet a poussé de nombreuses organisations à étendre leur installation informatique. La technologie LAN Ethernet (qui ne s'applique pas uniquement aux environnements Ethernets) apporte des solutions nouvelles dans la segmentation et la sécurisation des réseaux locaux, tout en augmentant leurs performances. Les VLAN Ethernet (réseau local virtuel) offrent de nouvelles solutions et opportunités en matière de gestion des réseaux informatiques des entreprises. Nous allons présenter plus de détails dans le chapitre suivant.

1.7.6 Les listes de contrôles d'accès (ACL)

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées généralement au trafic circulant via une interface de routeur.[10]

FIGURE 1.7: ACL[10]

Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter. L'acceptation et le refus peuvent être basés sur des conditions précises. Les ACL permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie. Des listes de contrôle d'accès peuvent être créées pour tous les protocoles routés, tels que les protocoles IP (Internet Protocol) et IPX (Inter network Packet Exchange). Des listes de contrôle d'accès peuvent également être configurées au niveau du routeur en vue de contrôler l'accès à un réseau ou à un sous-réseau.

1.7.6.1 l'intérêt d'utiliser des ACL

Voici les principales raisons pour lesquelles il est nécessaire de créer des listes de contrôle d'accès :

- ✓ Limiter le trafic réseau et accroître les performances. En limitant le trafic vidéo, par exemple, les listes de contrôle d'accès permettent de réduire considérablement la charge réseau et donc d'augmenter les performances
- ✓ Contrôler le flux de trafic. Les ACL peuvent limiter l'arrivée des mises à jour de routage. Si aucune mise à jour n'est requise en raison des conditions du réseau, la bande passante est préservée
- ✓ Fournir un niveau de sécurité d'accès réseau de base. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section
- ✓ Déterminer le type de trafic qui sera acheminé ou bloqué au niveau des interfaces du routeur. Il est possible d'autoriser l'acheminement des messages électroniques et de bloquer tout le trafic via Telnet.
- ✓ Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.
- ✓ Filtrer certains hôtes afin de leur accorder ou de leur refuser l'accès à une section de réseau. Accorder ou refuser aux utilisateurs la permission d'accéder à certains types de fichiers, tels que FTP ou HTTP.

1.7.6.2 les types des listes contrôles d'accès

Il existe trois types d'ACL que voici :

1. **Listes de contrôle d'accès standard :** Les listes d'accès standard vérifient l'adresse d'origine des paquets IP qui sont routés. Selon le résultat de la comparaison, l'acheminement est autorisé ou refusé pour un ensemble de protocoles complet en fonction des adresses réseau, de sous-réseau et d'hôte.
2. **Listes de contrôle d'accès étendues :** Les listes d'accès étendues sont utilisées plus souvent que les listes d'accès standard car elles fournissent une plus grande gamme de contrôle. Les listes d'accès étendues vérifient les adresses d'origine et de destination

du paquet, mais peuvent aussi vérifier les protocoles et les numéros de port. Cela donne une plus grande souplesse pour décrire ce que vérifie la liste de contrôle d'accès. L'accès d'un paquet peut être autorisé ou refusé selon son emplacement d'origine et sa destination, mais aussi selon son type de protocole et les adresses de ses ports.

3. **Listes de contrôle d'accès nommées :** Les listes de contrôle d'accès nommées IP ont été introduites dans la plate-forme logicielle Cisco IOS version 11.2, afin d'attribuer des noms aux listes d'accès standard et étendues à la place des numéros.

Conclusion

Au cours de ce chapitre, nous avons défini les réseaux informatiques, leurs différents types, ensuite nous avons donné une description globale du modèle OSI et TCP/IP ainsi que la sécurisation au niveau de la couche transport réseau.

CHAPITRE 2

SOLUTION

Introduction

Dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Ce qui donne sujet à divers problèmes affectant les performances du réseau, à savoir : Les collisions et la saturation du réseau.pour mener a bien notre chapitre Nous l'avons divisé en deux grandes parties.

Dans la première, nous allons aborder les concepts des réseaux locaux virtuels (VLAN), puis dans la deuxième partie nous passerons à la présentation de l'organisme d'acceuil et l'étude de leur existant pour pouvoir proposer une solution aux problèmes rencontrés.

Première partie

INTRODUCTION AUX RESEAUX LOCAUX VIRTUELS

Dans cette première partie, nous allons aborder quelques notions sur les réseaux locaux virtuels.

2.1 Généralités sur les réseaux locaux virtuels

L'idée de base des VLAN est de découper un seul réseau local (c'est à dire un ensemble cohérent d'infrastructures de niveau 2) en des réseaux logiques totalement disjoints : c'est comme si on avait plusieurs réseaux physiques totalement disjoints, un par VLAN. Ces réseaux partagent une même infrastructure. Nous nous situons bien ici au niveau de la couche liaison du modèle ISO, c'est à dire au niveau des trames (Ethernet, token-ring, FDDI pour citer quelques technologies). Pour utiliser des termes plus proches de la technologie Ethernet on peut dire que chaque VLAN correspond à un domaine de diffusion indépendant des autres. Les équipements modernes permettent à l'administrateur du réseau de construire des VLAN selon des critères techniques différents. Nous allons expliquer en quelques paragraphes à quoi correspondent les trois types de VLAN que l'on rencontre le plus fréquemment. [11]

2.1.1 L'interconnexion d'un réseau local

La mise en place d'un réseau soulève de nombreuses questions sur les contraintes d'utilisation. Comment faire si le réseau à créer dépasse les distances maximales imposées par le type de câble utilisé ? Comment faire parvenir les informations 'à d'autres réseaux que le sien ? Comment relier des réseaux utilisant des protocoles de communication différents ? Toutes ces questions peuvent ˆêtre résolue grâce 'à différents types de matériels qui sont [12] :

1. **Répéteur :** dispositif permettant d'étendre la distance de câblage d'un réseau local. Il amplifie et répète les signaux qui lui parviennent.
2. **Pont :** : Un pont (bridge) est un dispositif permettant de relier des réseaux de même nature.
3. **Routeur :** Un routeur (router) est un dispositif permettant de relier des réseaux locaux de telle façon 'à permettre la circulation de données d'un réseau 'à un autre de façon optimale.
4. **Passerelle :** Une passerelle (Gateway) est un dispositif permettant d'interconnecter des architectures de réseaux différentes .Elle assure la traduction d'un protocole d'un haut niveau vers un autre.

5. **Concentrateur :** Un concentrateur (hub) est un dispositif permettant de connecter divers élément de réseau.
6. **Commutateur :** Un commutateur (Switch) est un dispositif permettant de relier divers éléments tout en segmentant le réseau.
7. **Adaptateur :** les adaptateurs (adapter) sont destinés à être insérés dans un poste de travail ou un serveur afin de les connecter 'à un système de câblage.

2.1.2 Avantages des réseaux locaux virtuels

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants [13] :

- ✓ Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs.
- ✓ Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.
- ✓ Réduction de la diffusion du trafic sur le réseau.
- ✓ La réduction des messages de diffusion (notamment les requêtes ARP) limités à l'intérieur d'un VLAN. Ainsi les diffusions d'un serveur être limitées aux clients de ce serveur.
- ✓ La création de groupes de travail indépendants de l'infrastructure physique, possibilité de déplacer la station sans changer de réseau virtuel.
- ✓ L'augmentation de la sécurité par le contrôle des échanges inter-VLAN utilisant des routeurs (filtrage possible du trafic échangé entre les VLAN).
- ✓ L'indépendance entre infrastructure physique et groupe de travail implique qu'un commutateur puisse gérer plusieurs VLAN et qu'un même VLAN puisse être réparti sur plusieurs commutateurs. En conséquence, une trame qui circule dans un commutateur et entre les commutateurs doit pouvoir être associée à un VLAN.

Le principal avantage des VLAN est qu'ils permettent à l'administrateur réseau d'organiser le LAN de manière logique et non physique. Cela signifie qu'un administrateur peut effectuer toutes les opérations suivantes :

- ✓ Déplacer facilement des stations de travail sur le LAN.
- ✓ Ajouter facilement des stations de travail au LAN.
- ✓ Modifier facilement la configuration LAN.

- ✓ Contrôler facilement le trafic réseau.
- ✓ Améliorer la sécurité.
- ✓ Pour répondre aux objectifs des VLAN la règle suivante doit être impérativement respectée : ≪ une trame doit être associé à un VLAN et un Seul et ne peut pas sortir du VLAN, sinon l'étanchéité du niveau 2 n'est plus respecter. ≫

2.2 Définition d'un VLAN

Un VLAN (Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

Un VLAN est un réseau commuté qui est logiquement segmenté sur la base des fonctions, des équipes de projet ou d'application, sans tenir compte des emplacements physiques des utilisateurs.

VLAN ont les mêmes attributs que les LAN physique, mais vous pouvez finir groupe stations, même si elles ne sont pas physiquement situés sur le même segment de réseau local.

Tout port de commutateur peut appartenir à un VLAN, et unicast, broadcast et multicast paquets sont transmis et inondées pour finir station du VLAN. Chaque VLAN est considéré comme un réseau logique, et les paquets à destination des stations qui n'appartient pas au VLAN doit être transmis par le biais d'un routeur ou d'un pont.[13]

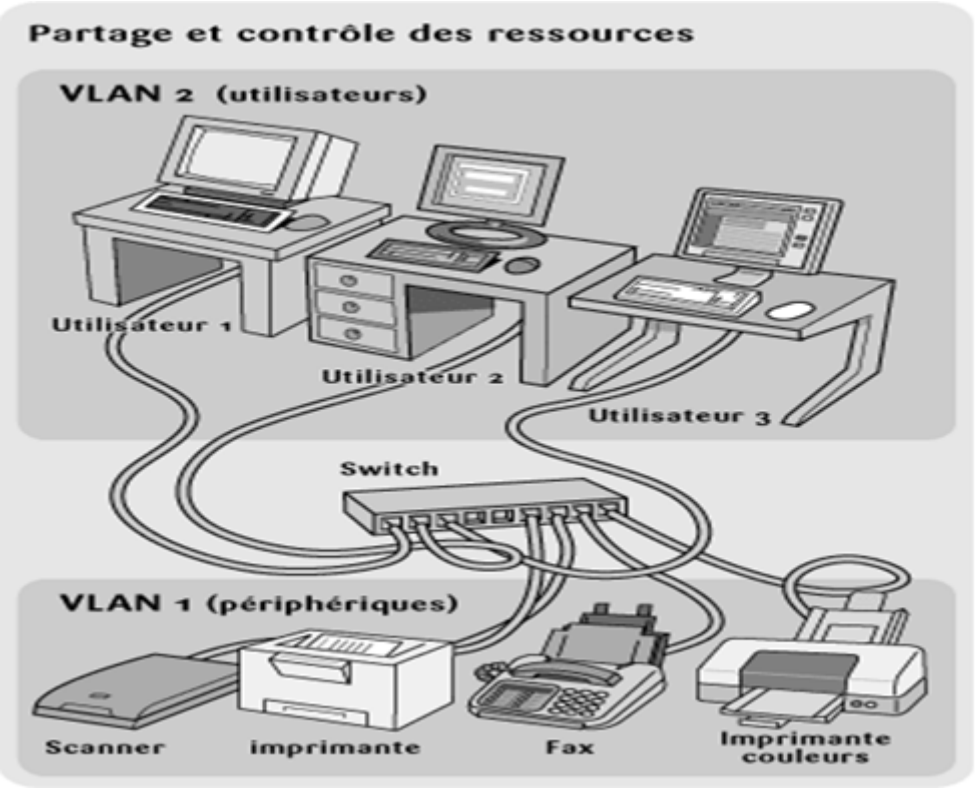

FIGURE 2.1: Subdivision du réseau en VLAN[9]

2.3 Caractéristiques d'un VLAN

- ✓ Supprime les contraintes physiques relatives aux communications d'un groupe de travail.
- ✓ Peut couvrir tout un bâtiment, relier plusieurs bâtiments ou encore s'étendre au niveau d'un réseau plus large (WAN).
- ✓ Une station peut appartenir à plusieurs VLAN simultanément.[13]

2.4 Classification des VLAN

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue[13] :

2.4.1 Les VLAN de niveau 1

Chaque port physique du commutateur est configuré par l'administrateur du réseau pour appartenir à un VLAN, et toute machine (ou ensemble de machines) qui se trouve branchée sur ce port fera partie de ce VLAN. C'est le mode de fonctionnement le plus simple et le plus déterministe, c'est à dire celui où potentiellement les défauts de logiciel sont le moins probable. Ce type de réseaux virtuels n'a rien de bien innovant. Lorsque les équipements réseau étaient simples et fiables, on faisait déjà des VLAN par port tout simplement en construisant des réseaux physiquement séparés, chacun ayant son câblage et ses propres équipements actifs. C'est bien le branchement physique sur un port d'un concentrateur plutôt qu'un port d'un autre concentrateur qui déterminait l'appartenance à un réseau.

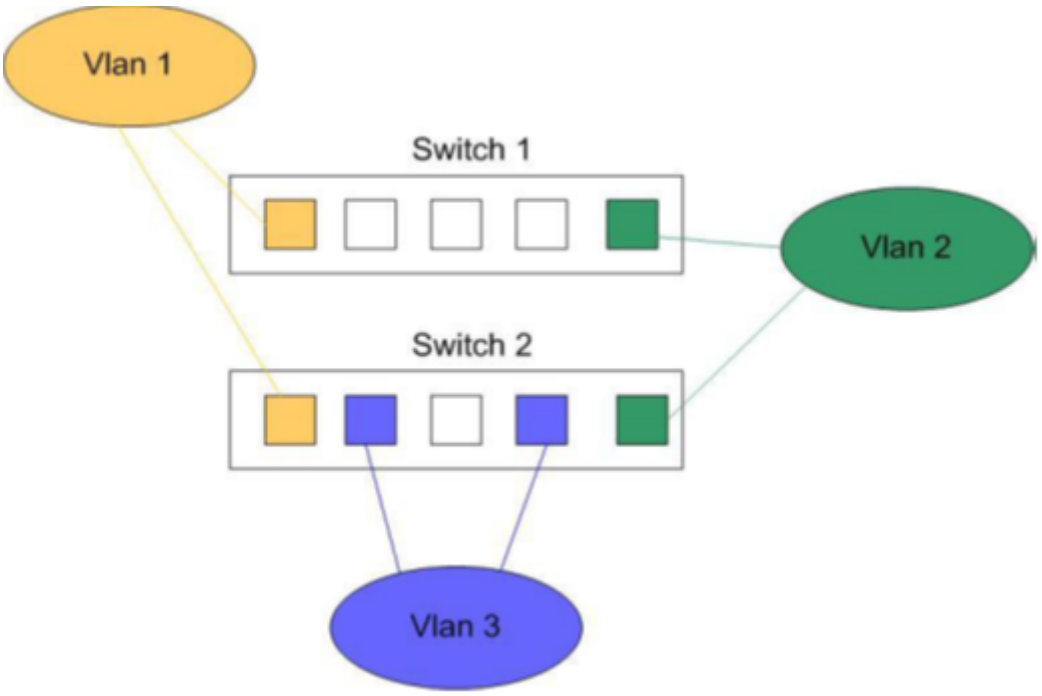

FIGURE 2.2: VLAN par port[9]

2.4.2 Les VLAN de niveau 2

Dans ce modèle, le VLAN auquel appartient une station est déterminé par son adresse MAC. Les adresses MAC étant physiquement liée aux stations, ce modèle permet de conserver la répartition des VLANs même après le déplacement d'une station. Contrairement au modèle de VLAN basé sur le port, des stations appartenant à des VLAN différents peuvent être connectées au même port d'un commutateur. Une station peut théoriquement être membre de plusieurs VLANs différents. Le principal inconvénient de ce modèle est la mise à jour des correspondances entre les VLANs et les adresses MAC, qui peut être ardue dans des réseaux de grande taille.

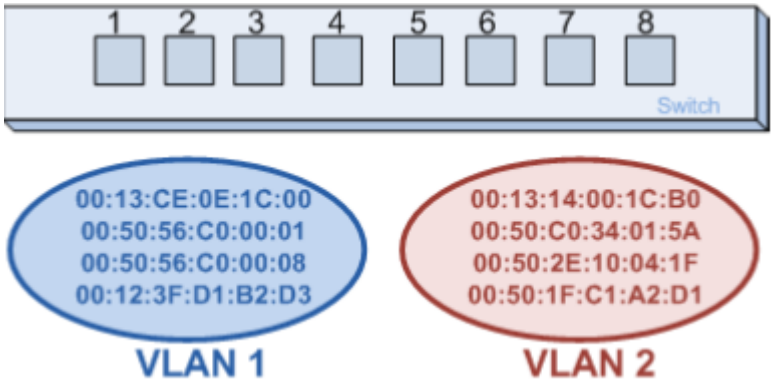

FIGURE 2.3: VLAN par adresse MAC[9]

2.4.3 Le VLAN de niveau 3

on distingue deux types :

✓ Vlan par sous réseau ou les vlan sont constitué selon les adresse IP.

✓ Vlan par protocoles ou les vlan sont constitué selon le type de protocole.

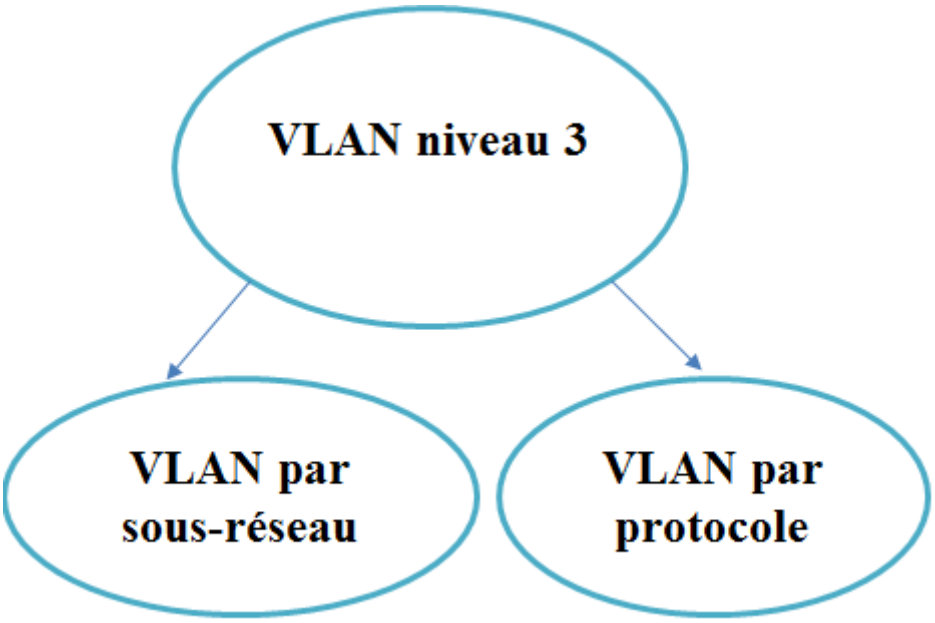

FIGURE 2.4: VLAN de niveau 3

2.5 Types des réseaux locaux virtuels

Il existe différents types de VLAN. Le type de trafic du réseau qu'ils portent définit un type particulier de réseau local virtuel et d'autre tirent leur noms en raison de la nature ou une fonction spécifique du VLAN effectue. La section suivante décrit VLAN commun[13] :

2.5.1 VLAN par défaut

Au démarrage initial du commutateur, tous les ports du devient membre du VLAN par défaut, ce qui les rend tous partie du même domaine de diffusion. Cela permet à tout dispositif de réseau connecté à un des ports de commutation pour communiquer avec d'autres dispositifs sur d'autres ports de commutateur. Sur commutateurs Cisco le VLAN par défaut est VLAN 1. Le VLAN 1 possède toutes les caractéristiques des VLAN, sauf que vous ne pouvez pas renommer ou supprimer.

2.5.2 VLAN de données

Un VLAN de données qui peut aussi être considéré comme utilisateur VLAN. Ceci est configuré pour ne transporter que le trafic généré par les utilisateurs. L'importance de séparer

les données de l'utilisateur à partir de tout autre type de VLAN est la gestion et le contrôle de l'interrupteur approprié.

2.5.3 VLAN natif

Un réseau local virtuel natif est affecté à un accès de jonction 802.1Q. Un port d'agrégation 802.1Q prend en charge le trafic provenant de plusieurs VLAN ainsi que le trafic qui ne viennent pas d'un VLAN. Le port d'agrégation 802.1Q place trafic non balisé (trafic qui ne provient pas d'un VLAN) sur le VLAN natif. En résumé, le VLAN natif observe et identifie le trafic provenant de chaque extrémité d'un lien de tronc.

2.5.4 VLAN de gestion

Un VLAN de gestion est tout VLAN configurer pour accéder aux fonctions de gestion d'un interrupteur. Votre configuration VLAN de gestion se fait en lui attribuant une adresse IP et un masque de sous-réseau. Tout port d'un commutateur VLAN peut être configurée comme la gestion de VLAN si vous n'avez pas configuré ou définit un VLAN unique de servir le VLAN de gestion dans certains cas, un administrateur de réseau définit de manière proactive VLAN 1 comme la gestion de VLAN, ce qui permet une échappatoire pour une connexion non autorisée à un commutateur.

2.5.5 VLAN voix

Un VLAN voix est configurée pour transporter le trafic voix. Les réseaux virtuels vocaux sont principalement la priorité de transmission sur d'autres types de trafic réseau. La communication sur le réseau n'est pas complète sans des appels téléphoniques. Les appels sont plus effectués sur le réseau que les autres formes de transmission de message. Envoi de courriers électroniques et des messages texte sont aussi des formes de l'interrelation, mais l'écoute d'une vraie voix donne de la légitimité et de l'assurance. Il est considéré parmi les administrateurs de réseau pour concevoir un réseau qui prenne en charge VOIP avec une bande passante assurée pour assurer la qualité de la voix, et la

Capacité d'être acheminés vers les zones congestionnées sur le réseau avec des retards minimes (150-180 millisecondes).

2.6 Le protocole VTP (VLAN Trunking Protocol)

Afin de ne pas redéfinir tous les VLANs existant sur chaque commutateur, CISCO a développé un protocole permettant un héritage de VLANs entre commutateurs. C'est le protocole VTP. Ce protocole est basé sur la norme 802.1q et exploite une architecture client-serveur avec la possibilité d'instancier plusieurs serveurs.[14]

2.6.1 Comprendre le VTP (VLAN Trunking Protocol)

Un commutateur doit alors être déclare en serveur, on lui attribue également un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifie ou supprimé. Ainsi chaque commutateur client présent dans le domaine héritera automatiquement des nouveaux VLANs créent sur le commutateur serveur. La mise en place d'un domaine VTP permet de centraliser la gestion des VLANs, ce qui peut s'avérer plus que plaisant dans un environnement abondamment commuté et comprenant de multiples VLANs. Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants :

- ✓ Mode serveur : dans lequel le commutateur est chargé de diffuser la configuration aux commutateurs du domaine VTP.
- ✓ Mode client VTP : dans lequel le commutateur applique la configuration émise par un commutateur en mode serveur.
- ✓ Mode transparent, dans lequel le commutateur ne fait que diffuser, sans prendre en compte, la configuration du domaine VTP auquel il appartient.

Pour comprendre le fonctionnement des VTP, nous allons l'illustrer dans cet exemple ci-dessous.

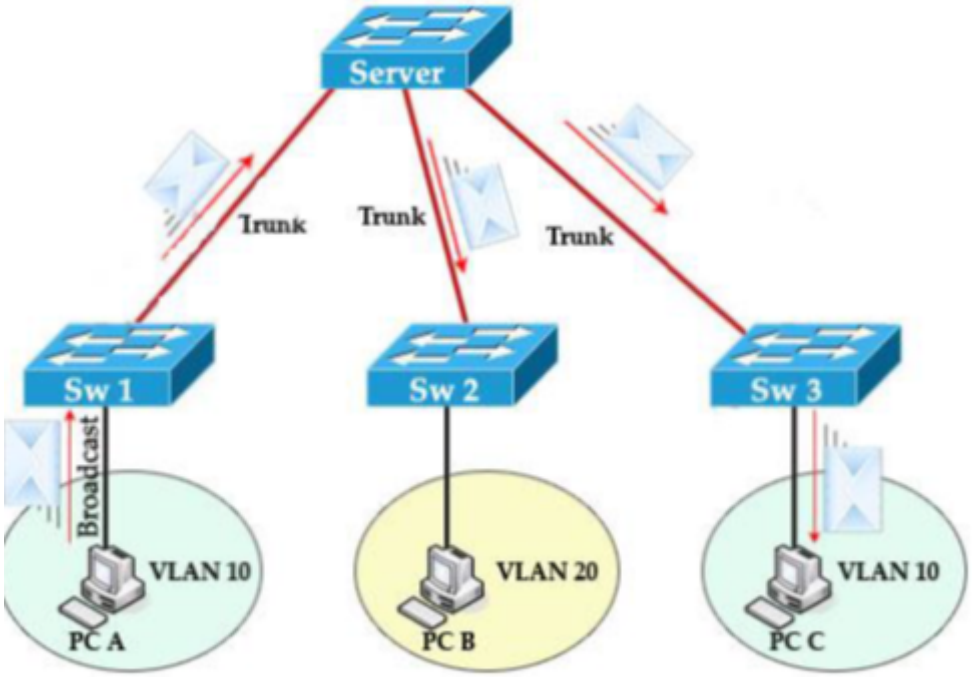

FIGURE 2.5: Fonctionnement du protocole VTP[14]

Les administrateurs peuvent changer les informations des VLAN sur les switchs fonctionnant en mode serveur uniquement. Une fois que les modifications sont appliquées, elles sont distribuées à tout le domaine VTP au travers des liens "trunk". En mode transparent, les modifications sont locales mais non distribuées. Les switchs en mode client appliquent automatiquement les changements reçus du domaine VTP. Les configurations VTP successives du réseau ont un numéro de révision. Si le numéro de révision reçu par un switch client est plus grand que celui en cours, la nouvelle configuration est appliquée. Sinon, elle est ignorée. Quand un nouveau switch est ajouté au domaine VTP, le numéro de révision de celui-ci doit être réinitialisé pour éviter les conflits.

Deuxième partie

PRESENTATION DE L'ORGANISME D'ACCUEIL

Dans cette partie, nous allons présenter l'entreprise d'accueil NAFTAL district carburant de Bejaia, avec ces déférents services en citant chaque service avec son rôle. Elle a pour mission principale, la distribution et la commercialisation des produits pétroliers et dérivés sur le marché national.

2.7 Présentation générale

2.7.1 Situation géographique

NAFTAL dis se trouve à l'entrée de la ville de Bejaia par la RN 12, au lieu-dit «Bir Slem», jouxtant la bordure de la route côté droit, soit pour sortir de la ville de Bejaia, soit pour entrer à la ville par le boulevard Krim Belkacem ou bien par Bir Slem.

FIGURE 2.6: Situation géographique

2.7.2 Historique de NAFTAL

Issue de SONATRACH, (société nationale pour la recherche, transport, production, transformation, la commercialisation des hydrocarbures), l'entreprise nationale de raffinage et de distribution de produits pétroliers (ERDP) a été créé par le décret N 80-101 du 06 avril 1980. Entrée en activité le 01 janvier1982, elle est chargée de l'industrie de raffinage et de la distribution de produits pétroliers. Le 04 mars 1985, les anciens districts (Carburants, lubrifiants, pneumatique et bitume) ont été regroupés sous le nom UND (unité NAFTAL de distribution). En 1987, l'activité raffinage est séparée de la distribution, conformément au Décret n 87- 189 du 25 Août 1987 modifiant le décret n 80-101 du 6 Avril 1980, modifié, portant création de l'Entreprise nationale de raffinage et de distribution de produits pétroliers, il est créé une Entreprise nationale dénommée : ≪ Entreprise nationale de commercialisation et de distribution de produits pétroliers ≫, sous le sigle de ≪ NAFTAL ≫. A partir de 1998, elle change de statut et devient société par action filiale à 100 pour 100 de SONATRACH, en intervenant dans les domaines suivants : - De l'enfûtage GPL - De la formulation des bitumes - De la distribution, stockage et commercialisation des carburants, GPL, lubrifiants, bitumes, Pneumatique, GPL /produits spéciaux. - Du transport des produits pétroliers. Elle est chargée, dans le cadre du plan national de développement économique et social, de la commercialisation et de la distribution des produits pétroliers et dérivé. Le 01 janvier 2000 l'activité GPL enfûtage est séparée de l'activité CLP. Par décision n S 554 du 29 mars 2000, il a été procédé à l'organisation générale de la division CLP et l'identification des zones de distribution ≪ CLP ≫ (carburants, lubrifiants et pneumatiques) Par décision n S 555 du 29 mars 2000, il a été procédé à la création des zones de distribution CLP. Par décision n S 606 du 10 Février 2001, il a été procédé à l'organisation et la classification des centres Bitumes de la Division Bitume. Pardécision n S 705 du 17 Juin 2002, il a été procédé à la dénomination des zones dedistribution CLP et GPL en District. Par décision n S 766 du 22 Décembre 2003, il a été procédé à la dissolution de la Branche CLPB. Par décision n S 770 du 03 Janvier 2004, il a été procédé à la dissolution des Districts CLP et création des Districts Commercialisation. A partir du 01.12.2006 l'activité Carburants est séparée de l'activité commercialisation.

2.7.3 Présentation de la branche carburant de NAFTAL

NAFTALest une société par actions, filial deSONATRACH, ayant pour mission lacommercialisions et la distribution des produits pétroliers. La branche carburant est l'une des trois branches de NAFTAL. Elle est chargée des activités d'approvisionnement, de stockage et de livraison des carburants.

2.7.4 Structure et organigramme

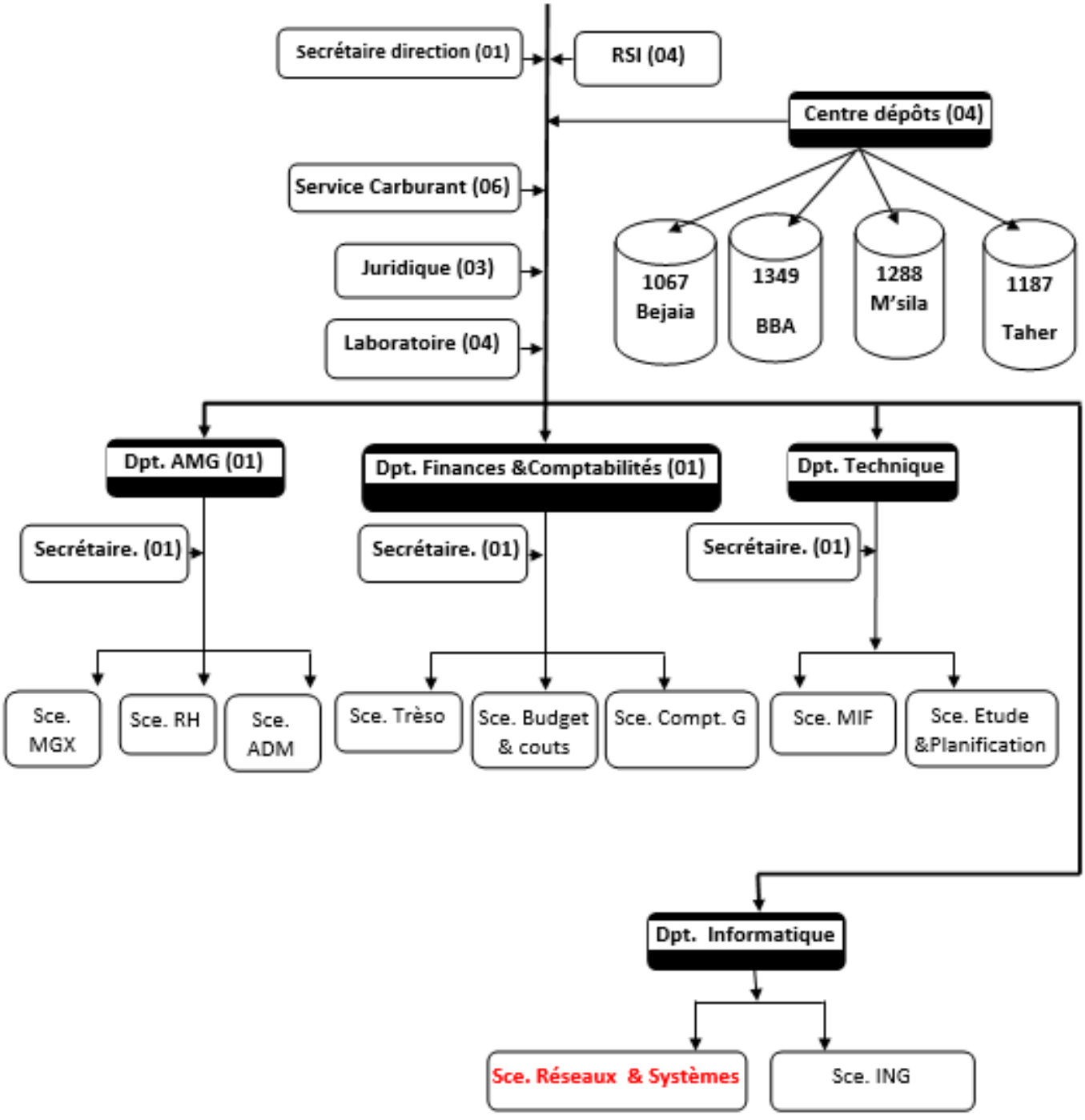

FIGURE 2.7: L'organigramme de l'organisme d'accueil

2.8 Description et rôle de chaque département au sein du district CBR Bejaia

Le District CBR Bejaia est organisé comme suit :

2.8.1 Direction

le responsable de la sécurité industrielle (RSI), la secrétaire, lelaboratoire, le service carburant, la cellule juridique, la chargée de communication, et les différents départements et dépôts carburants, sont rattachés à la direction. Ses principales tâches et responsabilités sont :

- ✓ Identifier et recenser les infrastructures, équipements et autres moyens matériels (camions, canalisations) relevant de l'activité carburants du District ainsi que les structures d'organisation (services maintenance, installations fixes, surveillance entretien canalisations, reconnaissance produits ... etc.) et les moyens humains œuvrant pour l'activité carburante.
- ✓ Suivre les plans établis par la Branche Carburants pour l'approvisionnement et ravitaillement en carburants des dépôts et communiquer régulièrement les états d'exécution aux structures concernées.
- ✓ Gérer les stocks en carburants au niveau des dépôts et communiquer régulièrement des points de situation aux structures concernées de la Branche.
- ✓ Suivre l'exploitation et la maintenance des infrastructures de stockage et autres moyens (camions, canalisations) carburants de la Branche rattachés au District.
- ✓ Exécuter les plans, budgets et autres objectifs arrêtés par la Branche et l'entreprise et proposer voire prendre des mesures correctives en cas de dérive.

2.8.2 Département Informatique

Le département informatique est assuré par un chef de département, son rôle principal est de garantir la continuité de service des systèmes informatiques déployés au niveau du Districts et centres opérationnels et veiller à la mise à disposition des informations de gestion aux structures du District, les Branches et les structures centrales. Le département est divisé en deux

services :

- ✓ Service système et réseaux que nous allons présenter en détails par la suite .
- ✓ Service Information De Gestion (ING).

2.8.2.1 Service information de gestion (ING)

Ce service est composé d'un chef de service ING et d'un Cadre d'étude comme on le voit dans la figure si dessous :

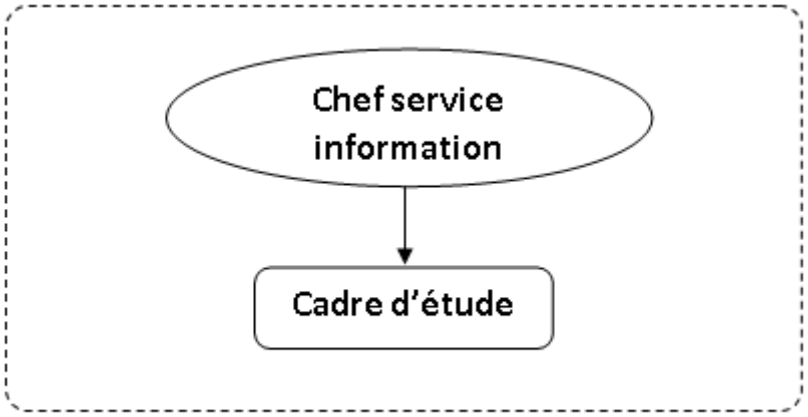

FIGURE 2.8: Organigramme du service information de gestion

Rôles du service information de gestion est :

- ✓ Gérer et mettre à jour une banque de données de toutes les activités du District.
- ✓ Procéder au calcul de la PRC (Prime de Rendement du Collectif) des différents collectifs du District.
- ✓ Consolider les différents plans et budgets des structures du District.
- ✓ Préparer les différentes présentations (COD, réunions de travail, regroupements, actions de communication.
- ✓ Collecter, contrôler et analyser les informations concernant les activités du District.
- ✓ Participer à l'élaboration des rapports d'activité périodiques et les tableaux de bord .

✓ Assurer la diffusion des PV des Conseils de Direction du District aux membres présents et aux structures centrales de la Branche Carburants

2.8.3 Département AMG (administration et moyens généraux)

Les missions du département AMG sont :

✓ Assurer la gestion des moyens généraux du district
✓ Assurer la gestion des ressources humaines
✓ Assurer la gestion de l'administration
✓ Assurer la gestion des œuvres sociales et culturelles.

Le département AMG est composé de 4 services :

1. **Service administration :**
   ✓ Section gestion du personnel.
   ✓ Section gestion paie.
   ✓ Section prestations sociales.

2. **Services ressources humaines**
3. **Services du moyen généraux :** Ses activités sont assurées par trois sections :
   ✓ Section BOG (bureau d'ordre).
   ✓ Section entretien bâtiment.
   ✓ Section économat.

4. **Cellule OSC (Ouvre sociales et culturelles)**

2.8.4 Département finances et comptabilité

Le département finance et comptabilité a pour mission de :

- ✓ Coordonner et suivre toutes les activités de comptabilité de trésorier, budget et patrimoine.
- ✓ Consolider, analyser les états comptables et veiller à la sincérité des comptes du District.
- ✓ Veiller à la concordance des écritures comptables avec les flux physiques et financiers.

Il comprend trois services à savoir :

1. **Service trésorerie :** Il est composé de deux sections, la Section recettes et la Section dépense.
2. **Service comptabilité générale :** Il est composé de deux sections, la Section SVCD et la Section comptabilité.
3. **Service budgets et coûts :**

2.8.5 Département Technique

Il a pour mission :

- ✓ Élaborer les plans de maintenance préventive et curative des équipements des dépôts.
- ✓ Élabore les plans annuels et pluriannuels de transport, en prenant en charge les besoins de distribution et ravitaillement des produits commercialisés.
- ✓ Suivi de la réalisation des travaux.
- ✓ Elaborer les plans et budgets d'investissement (rénovation, extension, remise à niveau, remplacement) des installations fixes, canalisation, et autres.
- ✓ Etablir un rapport d'activité périodique.

Ce département comporte les services suivants :

1. **Service maintenance des installations fixes (M I F)** .
2. **Service études et réalisation :** Le District dispose de deux (02) dépôts carburants a Bejaia, un (01) â TAHER /W.JIJEL, un (01) â Bordj Bou Arreridj et un (01) â M'SILA.

2.9 Présentation du service d'accueil (service Informatique : Système et Réseaux)

2.9.1 Organisation

Le service système et réseaux se présente comme suit :

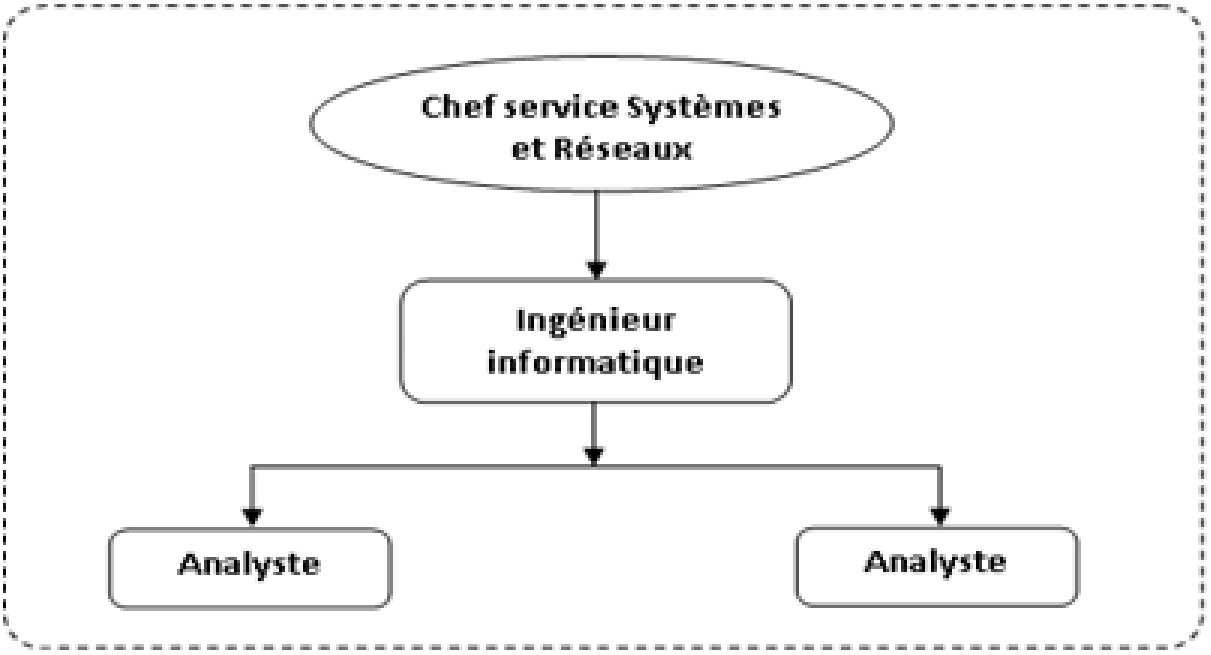

FIGURE 2.9: l'organigramme de service systèmes et réseaux

Ce service est composé d'un (1) chef de service SYSTEMES et RESEAUX, d'un (1) ingénieur informatique et de deux (2) analystes.

2.9.2 Activités du service d'accueil

Le rôle du service Systèmes et réseau est de prendre en charge les infrastructures réseauxfilaires et Wifi, et des services généralistes (sécurité, distribution logicielle, gestion despostes de travail. . .), assure aussi la maintenance des équipements informatique et assuré des formationssur le fonctionnement de certains logiciels ou applications. Ce service il assure deux tâches principales :

1. **La maintenance informatique :**
   - ✓ Assure la maintenance corrective de tous types de matériels informatiques .

- ✓ Analyse les causes pannes et y apporte la solution adéquate dans les meilleurs délais.
- ✓ Prendre en chargé aussi l'installation de matériels neufs, de modification et d'adaptation des matériels.

2. **L'infrastructure réseau :** Mis en place et configure le réseau informatique del'entreprise, il intervient à chaque étape de sa mise en place :

- ✓ La pose du câblage informatique .
- ✓ La configuration des postes utilisateurs, système d'exploitation, messagerie, internet, intranet, FTP .
- ✓ Assure aussi la gestion des domaines, groupe et ressource du réseau.
- ✓ Administrer les serveurs de réseaux (serveur FTP, messagerie, web,).

En plus de ces deux taches le service système et réseau assure des services généraux : la sécurité, distribution logicielle et gestion des postes de travail. Le District dispose de deux (01) dépôts carburants à Bejaia, un (01) à TAHER /W. JIJEL, un (01) à Bordj Bou Arreridj et un (01) à M'SILA.

2.10 Etude de l'existant

Le réseau local du District CBR de Bejaia interconnecte tous les ordinateurs du parc Informatique et leur permet d'accéder aux ressources du réseau et à internet. Pour adresser facilement les hôtes du réseau, un service DHCP est fonctionnel dans le LAN. Les machines du parc ont deux systèmes d'exploitation, Windows 7, et Windows server 2008 pour leur serveur. Des imprimantes sont mises en réseau pour étre partagées entre les employés afin que ceux-ci puissent y accéder sans avoir à transporter les documents d'un poste a un autre. Il est également à noter que, ce réseau LAN se compose d'un réseau filaire et d'un réseau wifi pour permettre l'accès à internet aux visiteurs. Des onduleurs sont également mis à contribution en cas de coupures brusques du courant électrique. On dénombre un dans chacun des deux services informatique et d'autre dans les services cités plus haut.

2.10.1 Présentation des équipements du réseau du district CBR

Le réseau du district CBR de Bejaïa se compose de :

- ✓ **173 ordinateurs.**
- ✓ **13 Switchs type C Cisco 2960 24ports.**
- ✓ **01 Switchs type B Cisco 3750G.**
- ✓ **37 Imprimantes(dont 18 en Réseau).**
- ✓ **01 Router.**
- ✓ **260 prises KJ45.**
- ✓ **04 Points d'accès Wi-Fi (un pour chaque étage).**
- ✓ **01 Serveur Windows 2012.**
- ✓ **01 Serveur N.A.S.**
- ✓ **Téléphonie IP (Full IP).**
- ✓ **Ligne RMS (Algérie Telecom).**
- ✓ **Un Modem 3G++ wifi de Mobilis (en cas de coupure de connexion sur la ligne principale).**

2.10.2 Contexte du projet à réaliser

2.10.2.1 Présentation du projet

Notre projet intitule " Organisation du réseau au sein du district CBR de Bejaïa ", qui ce dernier consiste à mettre en place d'une solution VLAN afin de bien gérer le réseau du district.

2.10.2.2 Objectif du projet à réaliser

Notre objectif principal est de remédier aux problèmes rencontrés durant notre période de stage et d'essayer de trouver une solution optimale pour la gestion du réseau local du district.

2.10.2.3 Problématique

Durant notre période de stage au sein du district CBR de Bejaïa, nous avons remarqués qu'elle dispose d'un réseau local de taille importante composé d'une plateforme de services reliant les différents départements et composants de ce district, nous avons pu mettre le point sur le manquement du réseau à savoir :

✓ Le réseau constitue une seule entité hétérogène peuplée par les différents services de chaque département ce qui provoque une charge énorme sur ce dernier.

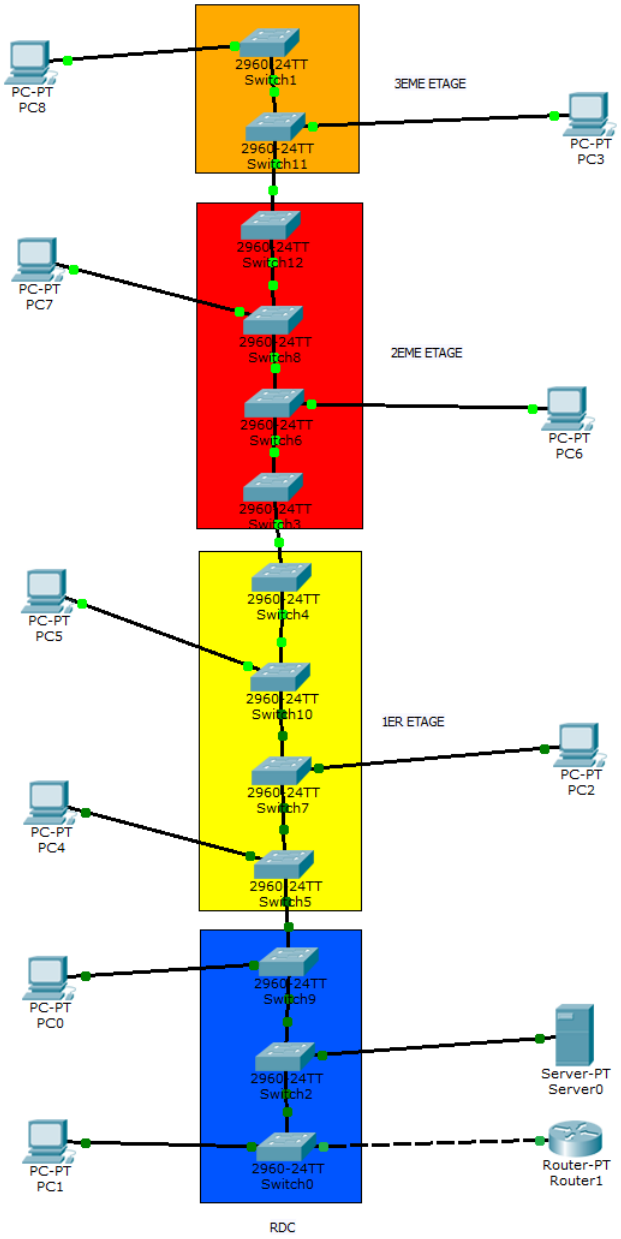

FIGURE 2.10: topologie du réseau de NAFTAL sans VLAN

2.10.2.4 Solution proposée

En analysant l'architecture de ce réseau, nous avons constaté qu'il y a une forte utilisation de la bande passante et que le réseau est sur les bornes de la saturation d'où nous sommes parties pour la segmentation du réseau du district en un ensemble de vlans, chaque département représente donc un vlan hétérogène.

VLAN 10---> Informatique @10.64.10.0
VLAN 20--->AMG @10.64.20.0
VLAN 30--->Finance @10.64.30.0
VLAN 40--->Technique @10.64.40.0
VLAN 50--->Direction @10.64.50.0

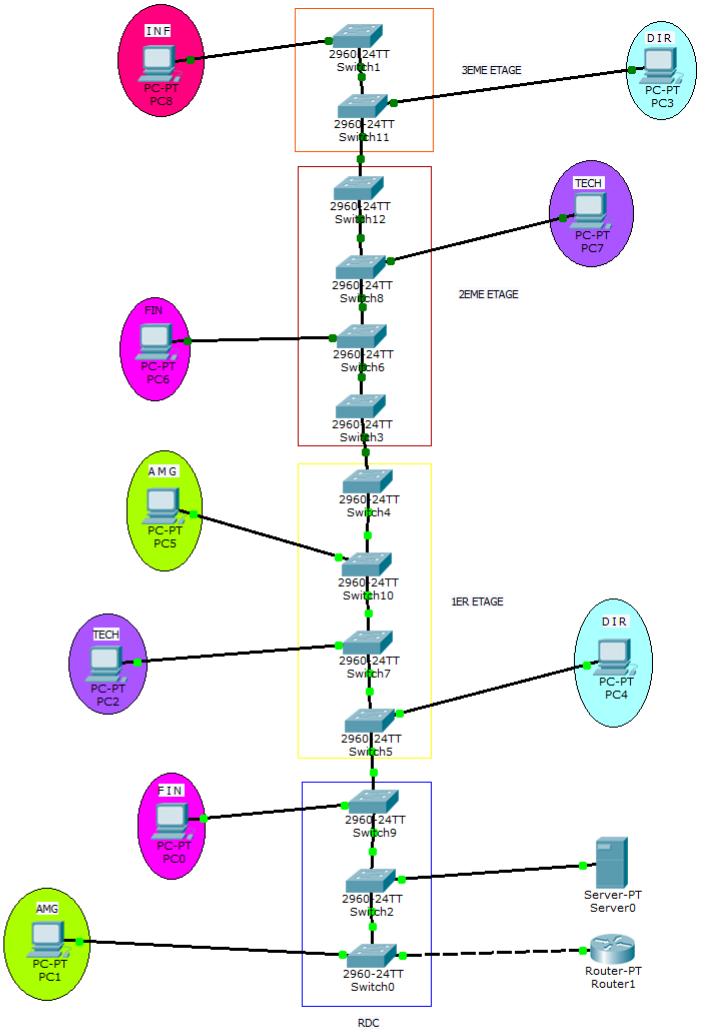

FIGURE 2.11: topologie du réseau de NAFTAL avec VLAN

Conclusion

Nous avons vu tout au long de ce chapitre que la technologie des VLANs repose sur des concepts principaux et essentiels tels que la limitation des domaines de broadcast, la mobilité des utilisateurs et sans oublier la sécurité.

D'une autre part L'étude de l'existant nous a permis de nous familiariser avec le district CBR de Bejaïa ainsi l'architecture réseau dont elle dispose Les problèmes que rencontre le district se sont imposés suite à une étude profonde de leur réseau et à sa critique, ce qui nous a permis de cerner la problématique de notre projet et de proposer des solutions.

CHAPITRE 3

REALISATION

Introduction

Dans ce chapitre, nous allons passer à la dernière étape qui est la réalisation. Cette phase est cruciale pour la mise en place de tout ce que nous avons vu et fait auparavant, nous implémenterons la solution précédemment proposée et conçu, pour ce faire nous commencerons par la présentation du simulateur utilisé, puis nous expliquerons en détail les différentes étapes suivies pour la réalisation de l'architecture LAN et la création des VLANs.

3.1 Présentation du simulateur « Cisco Packet Tracer »

Packet Tracer est un simulateur de matériel réseau Cisco .Cet outil est créé par Cisco Systems qui le fournit gratuitement aux centres de formation, étudiants et diplômés participants, ou ayant participé, aux programmes de formation Cisco (Cisco Networking Academy). Le but de Packet Tracer est d'offrir aux élèves et aux professeurs un outil permettant d'apprendre les principes du réseau, tout en acquérant des compétences aux technologies spécifiques de Cisco. Il peut être utilisé pour s'entraîner, se former, préparer les examens de certification Cisco, mais également pour de la simulation réseau. Pour notre travail nous avons utilisé la version 6.3.

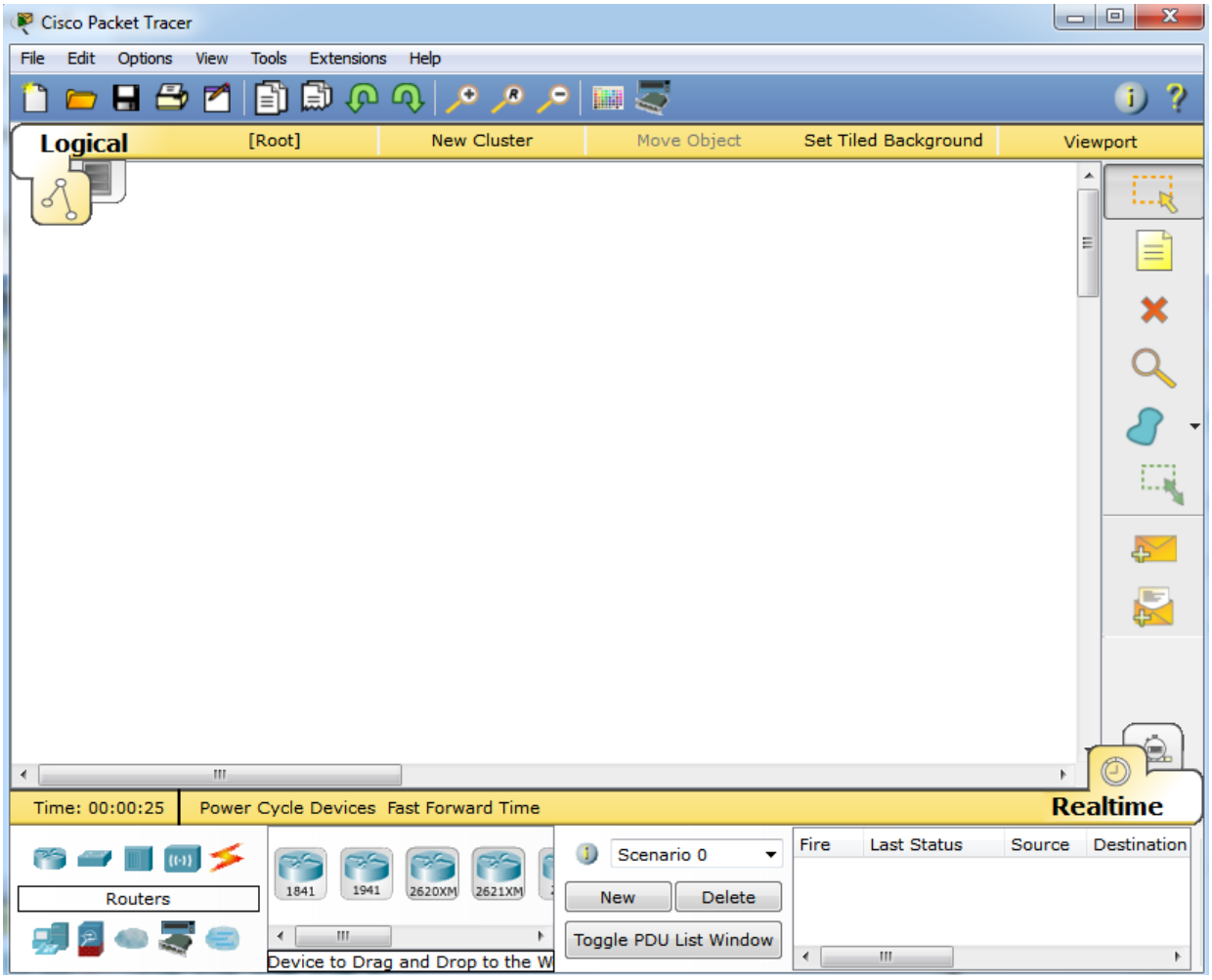

FIGURE 3.1: Interface Packet Tracer

3.2 Configuration des commutateurs

Nous allons commencer par la création des VLANs, sachant qu'il y aura en tout 6 VLANs (10,20, 30,..,60).

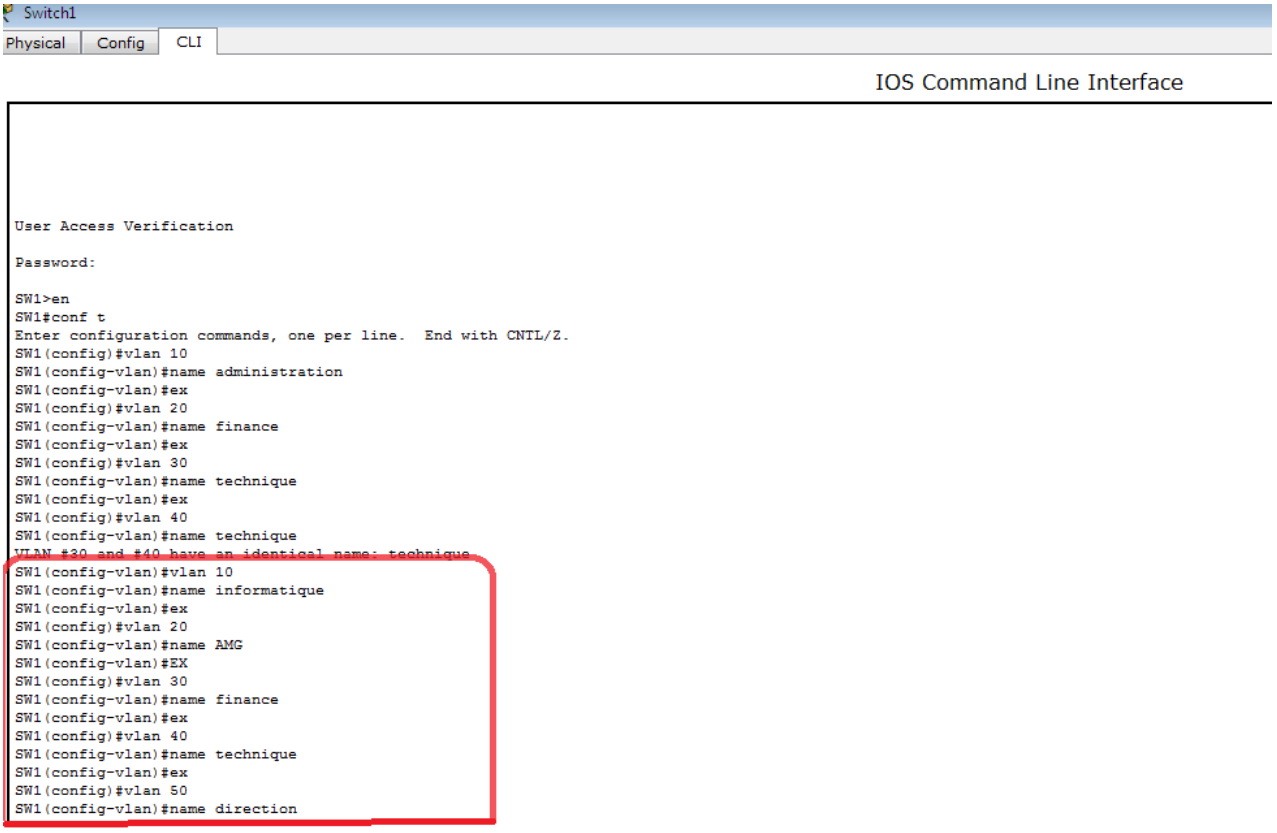

FIGURE 3.2: Création des VLANs

Ensuite nous allons suivre les étapes de configurations illustrées ci-dessous :

1. Configuration de Hostname.
2. Configuration des mots de passe.
3. Configuration de VTP.
4. Configuration des VLANs.
5. Configuration des interfaces.
6. Configuration de Spanning-Tree.
7. Configuration des inter-VLANs.
8. Insertion des ACL.

1. **Configuration de Hostname**

   Cette configuration a pour but de renommer les commutateurs par des noms significatifs Nous prendrons comme exemple le switch 1, sachant que c'est la même procédure

pour les autres commutateurs.

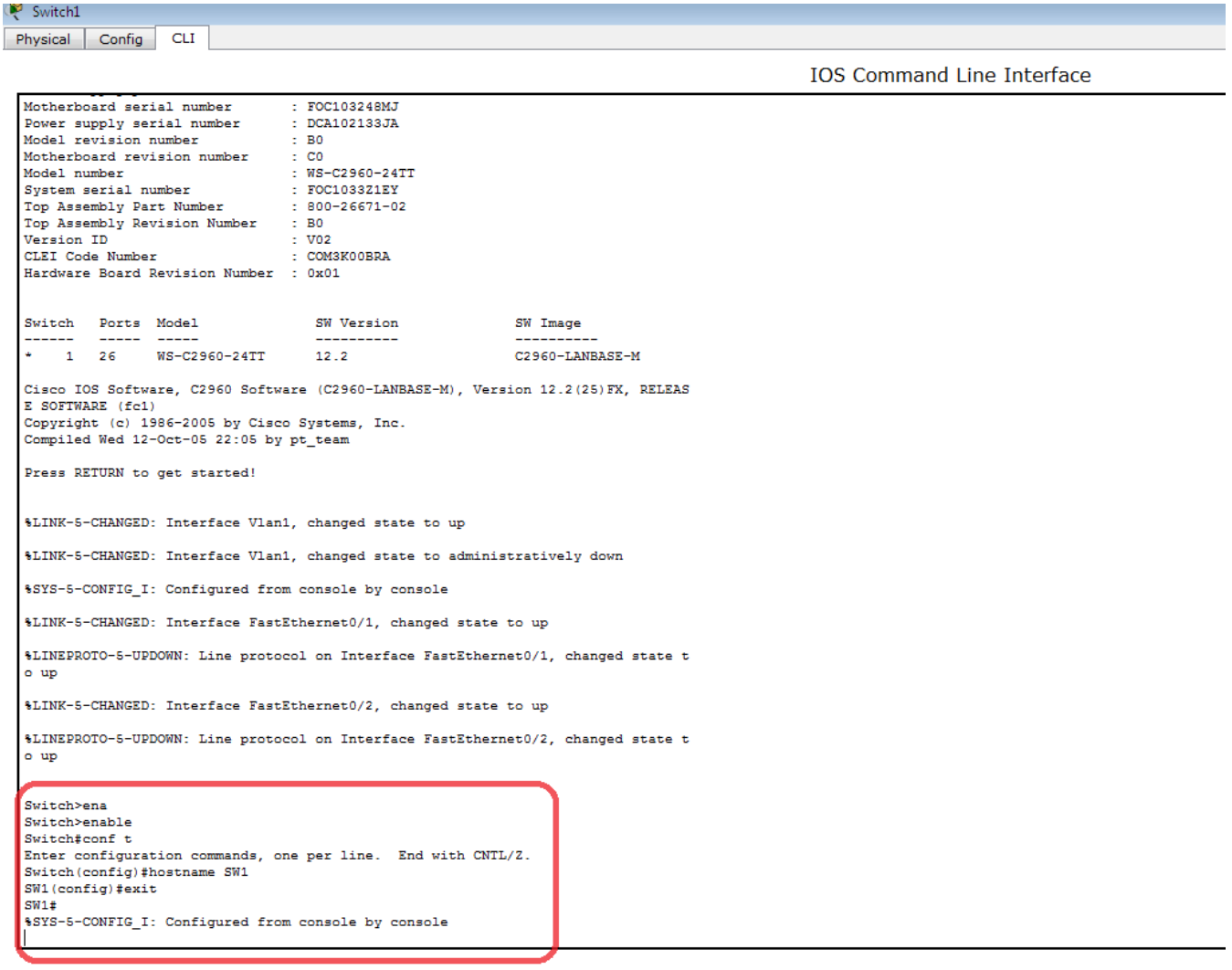

FIGURE 3.3: Nomination d'un switch

2. **Configuration des mots de passe**

Nous allons maintenant passer à la configuration des mots de passe.

✓ **Sécuriser l'accès à la ligne de console**

Notre choix c'est porté sur «naftal » comme mot de passe via console, l'exemple que nous prendrons est le SW 1. La figure 4.4 montre les commandes de mise en place du mot de passe. La même chose sera faite pour les autres commutateurs.

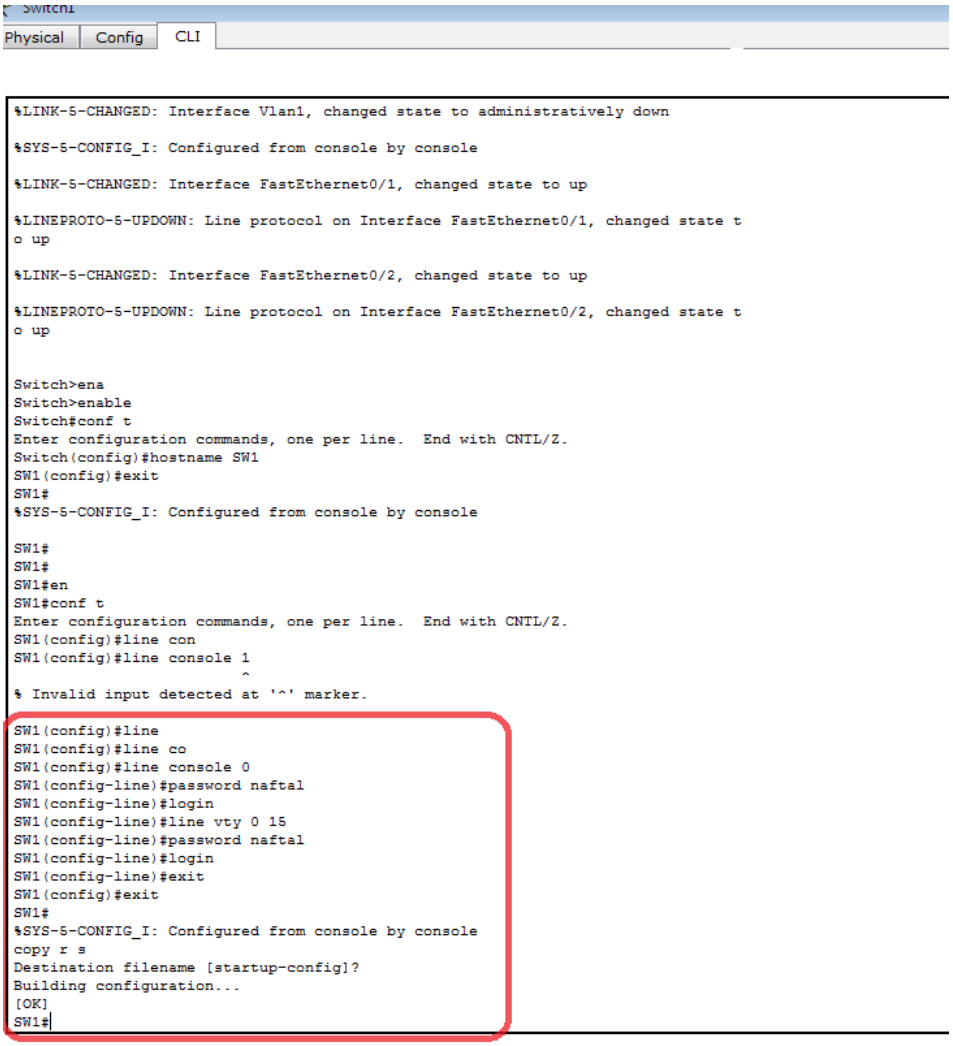

FIGURE 3.4: Attribution du mot de passe console au SW 1

✓ **Sécuriser l'accès au mode privilégié**

Pour sécuriser l'accès au mode privilégié, nous avons choisi le mot de passe naftal-sec.

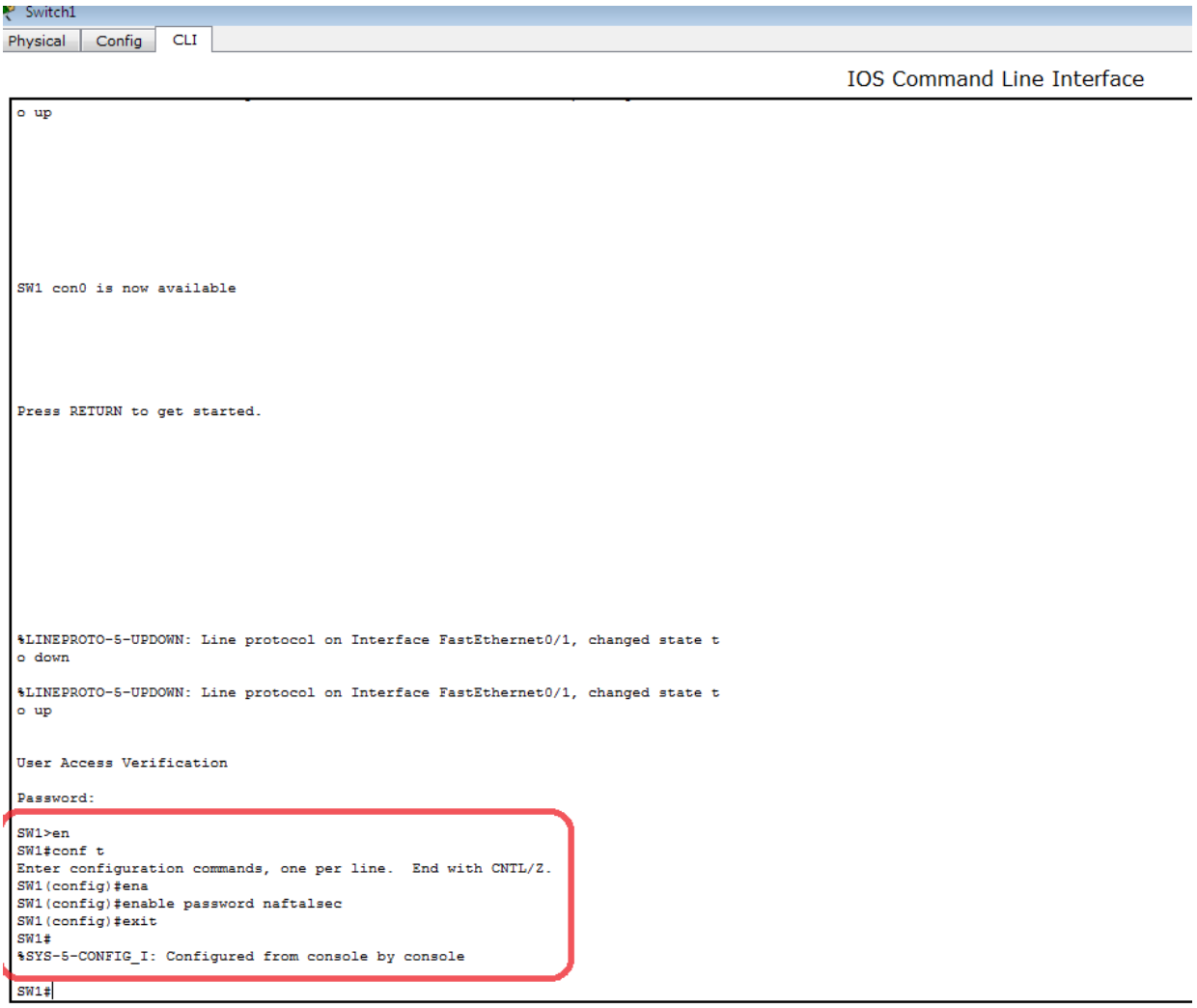

FIGURE 3.5: Attribution du mot de passe pour le mode privilégié au SW 1

✓ **Configurez un mot de passe chiffré pour sécuriser l'accès au mode privilégié**

Le mot de passe d'activation (enable) doit être remplacé par le mot de passe secret chiffré à l'aide de la commande enable secret. Nous avons choisi naftalsec en tant que mot de passe secret actif.

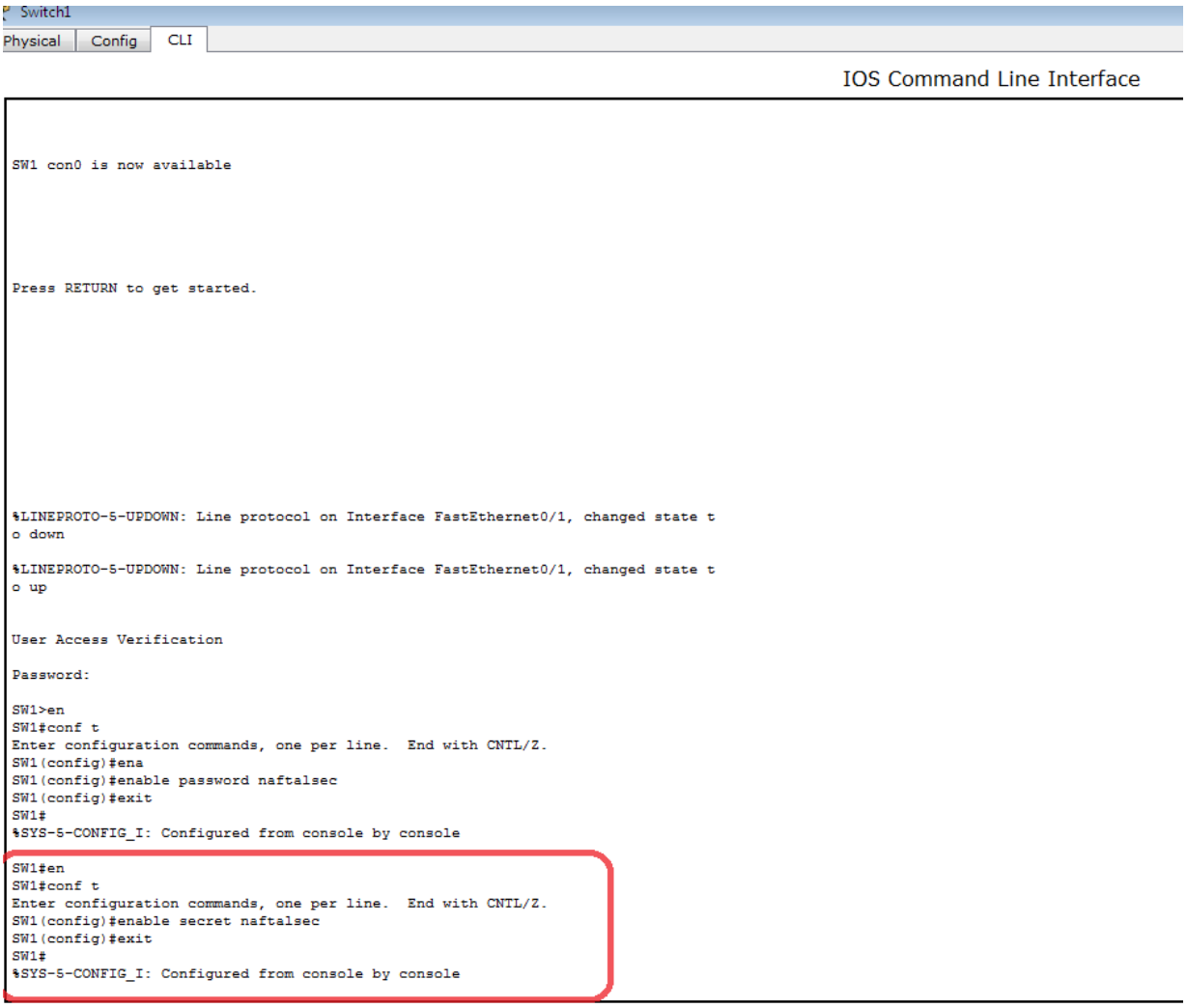

FIGURE 3.6: Mot de passe secret

✓ **Chiffrer les mots de passe**

Le mot de passe secret actif (enable secret) a été chiffré, mais les mots de passe d'activation (enable) et de console sont toujours en clair. Nous allons maintenant chiffrer ces mots de passe en clair à l'aide de la commande service password-encryption.

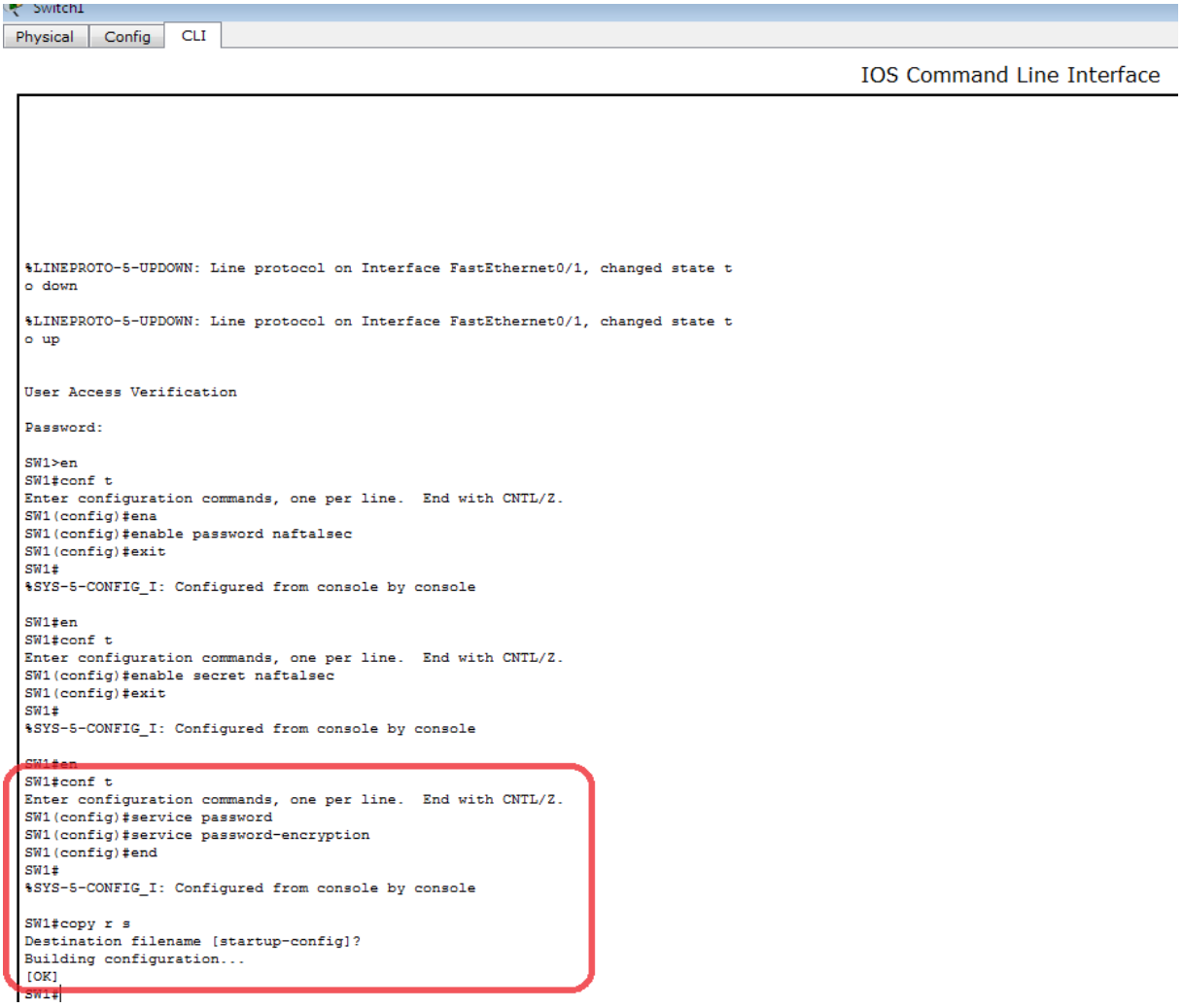

FIGURE 3.7: Chiffrement du mot de passe

✓ **Sécuriser l'accès à distance avec SSH**

L'accès à distance via Telnet sur un équipement Cisco n'est pas sécurisé. Il est préférable d'utiliser le protocole SSH qui chiffre les informations afin d'apporter une couche de sécurité à la connexion à distance.

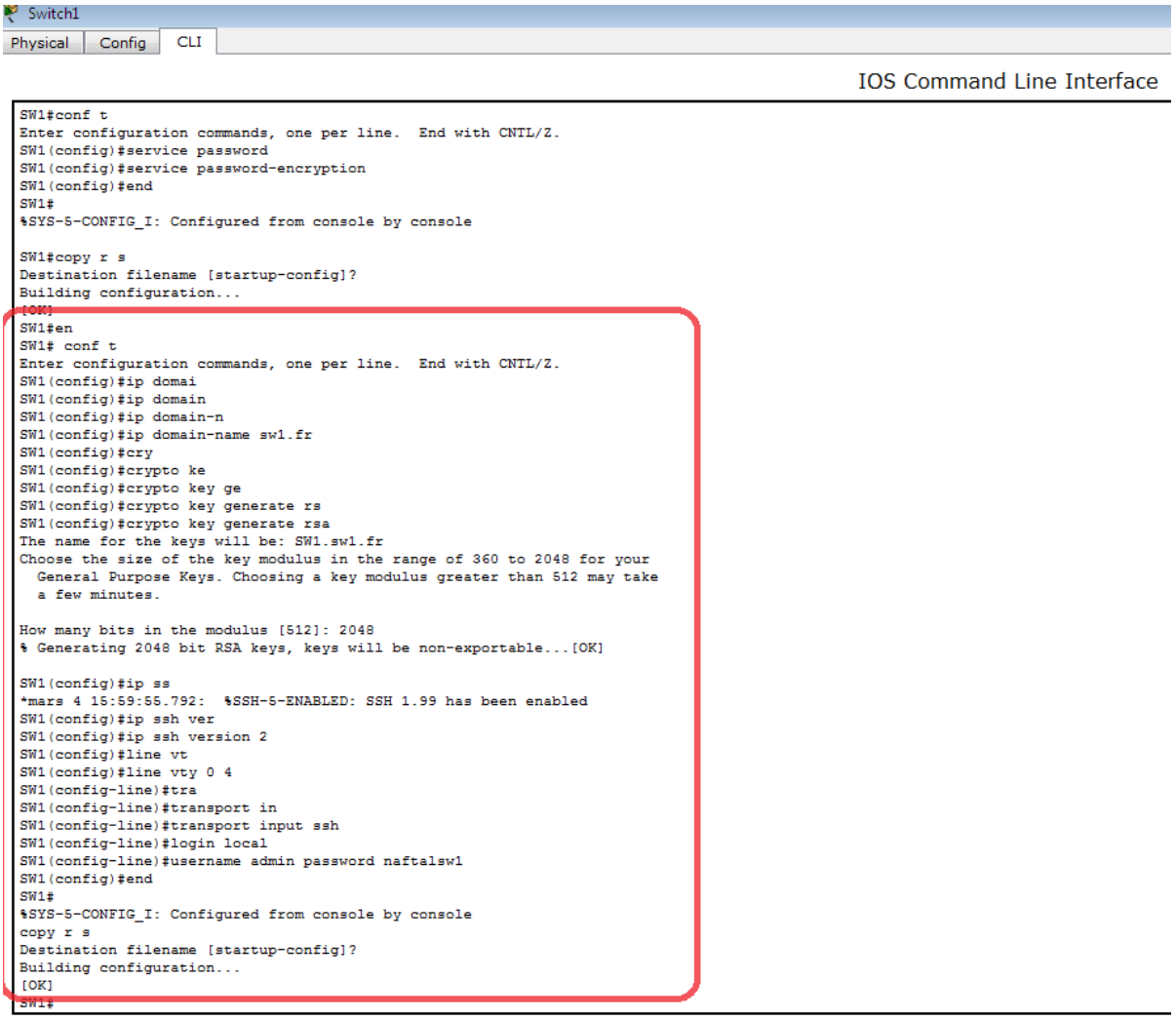

FIGURE 3.8: Sécuriser l'accès SSH sur un switch

3. **Configuration du VTP**

   Maintenant nous allons configurer le protocole VTP :

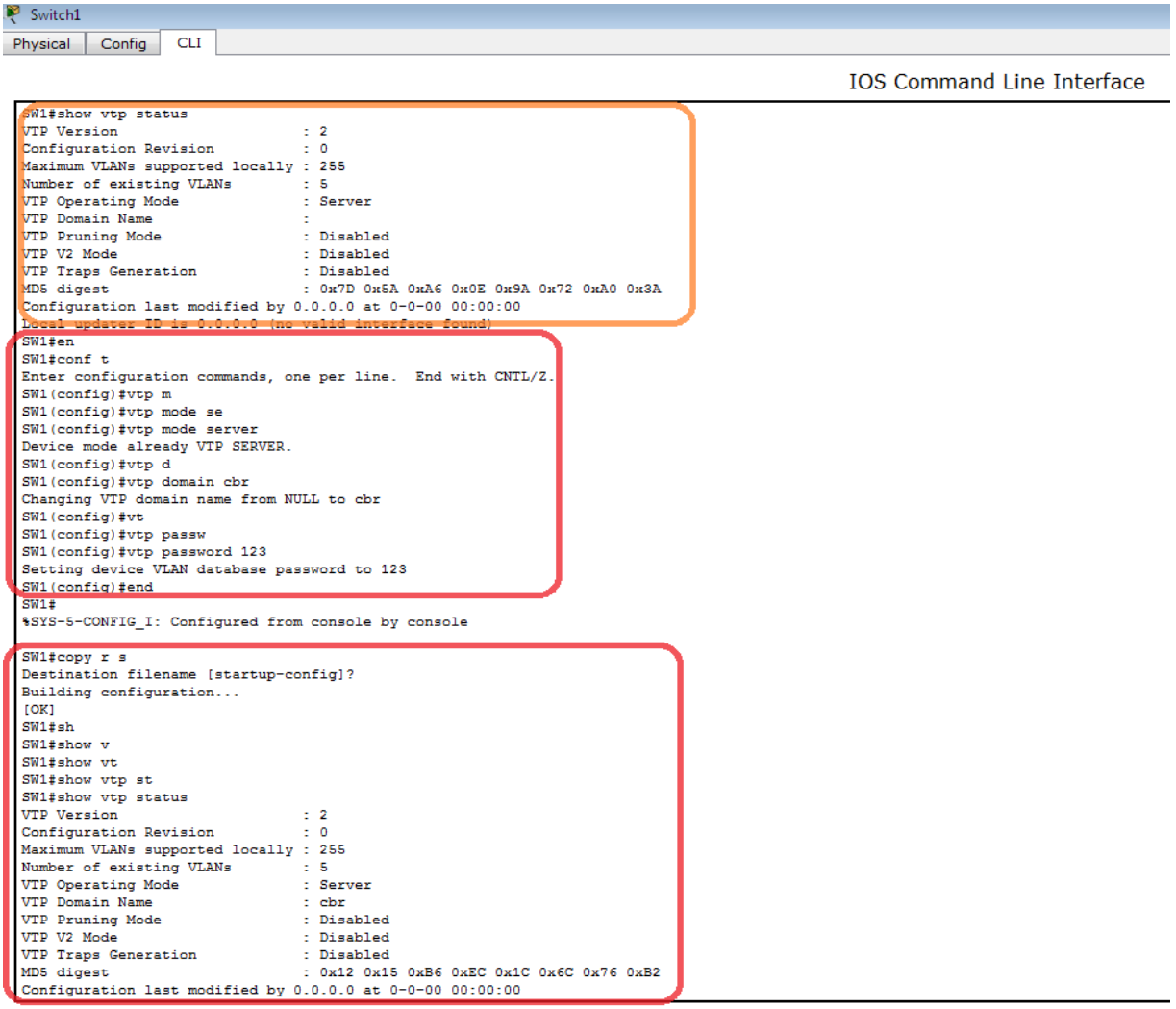

FIGURE 3.9: configuration du protocole VTP

4. **Configuration des VLANs**

   Dans cette partie de configuration nous allons attribuer les adresses IP de passerelle pour chaque VLAN au niveau du Switch.

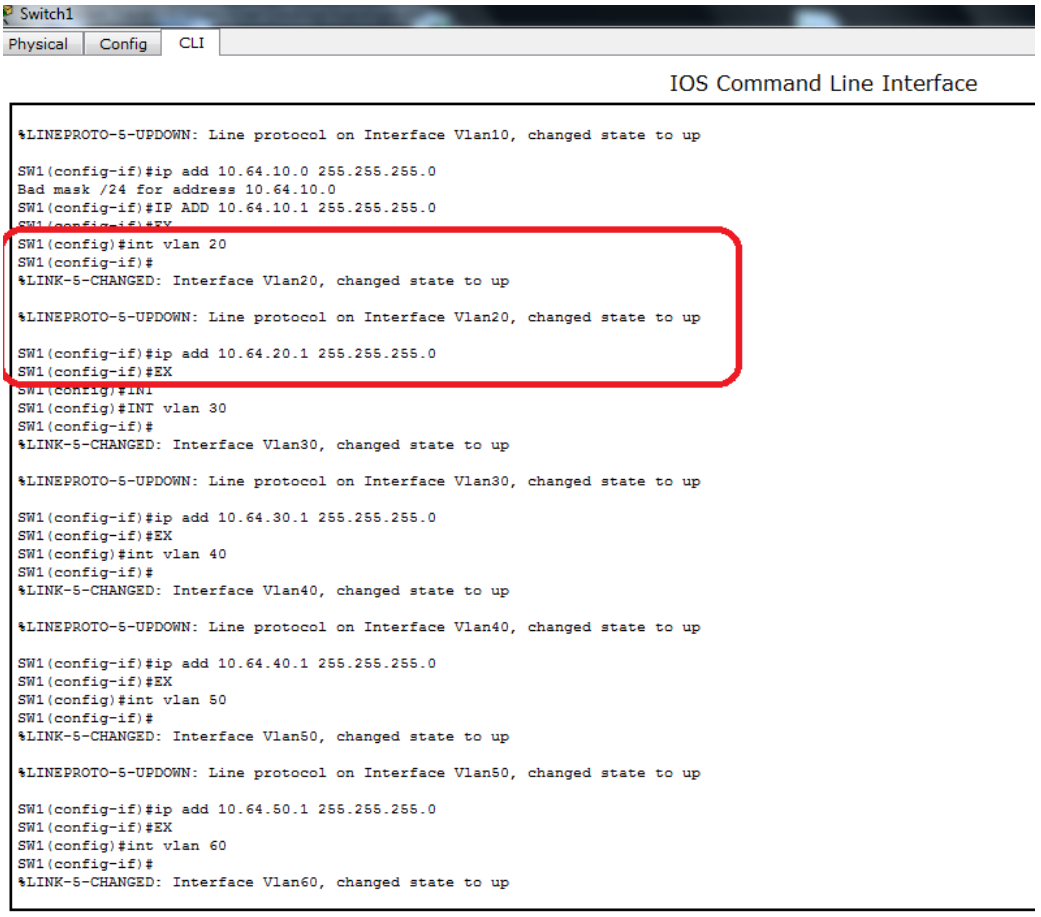

FIGURE 3.10: configuration des VLANs au niveau de switch

5. **Configuration des interfaces**

   Nous allons configurer les liaisons entre les commutateurs en mode trunk. Par contre les interfaces en mode accès se trouvent au niveau des liens entre les commutateurs d'accès et les PC.

   Les figures suivantes illustrent les configurations faites.

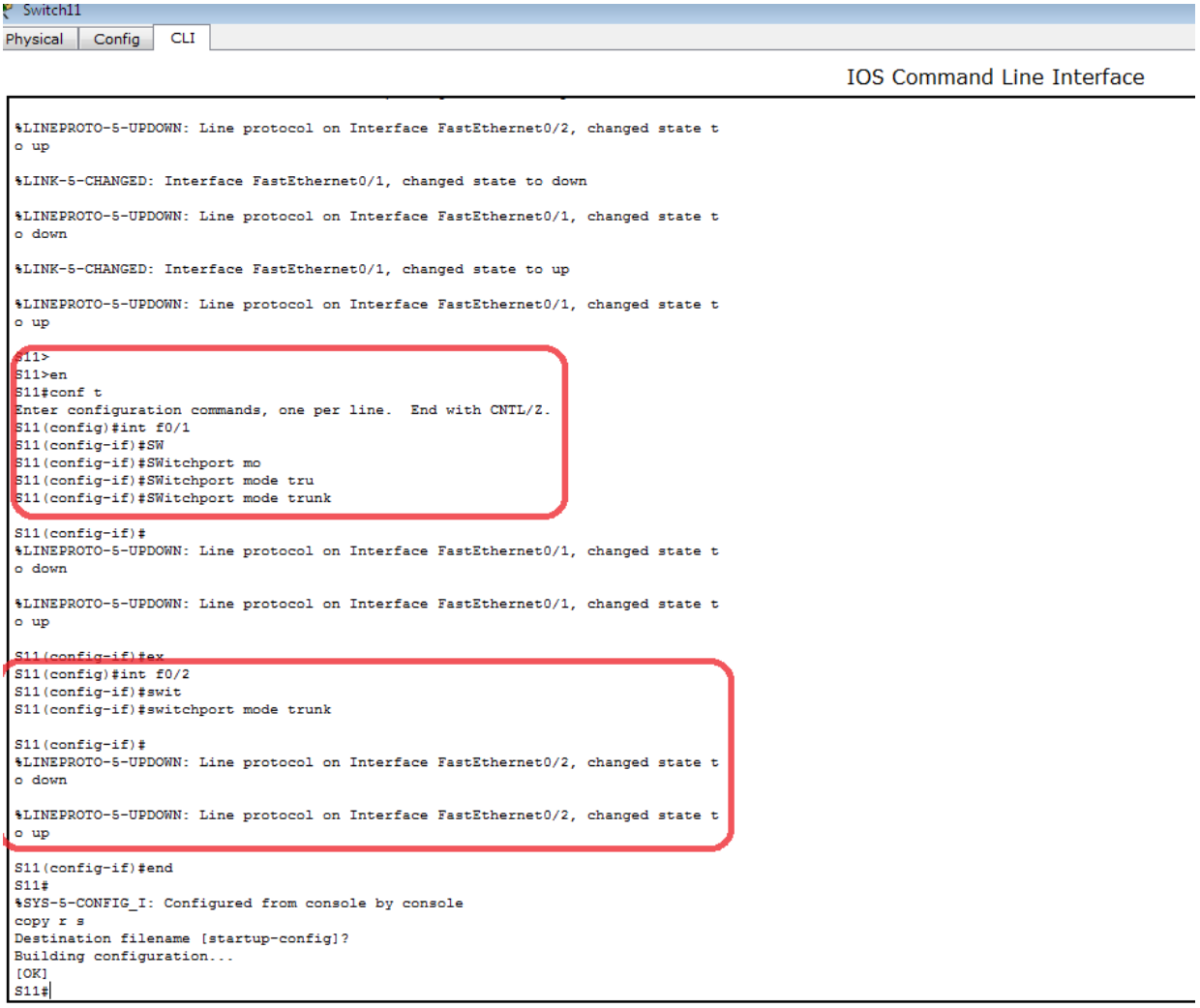

FIGURE 3.11: Activation des liens trunk au niveau du switch principal

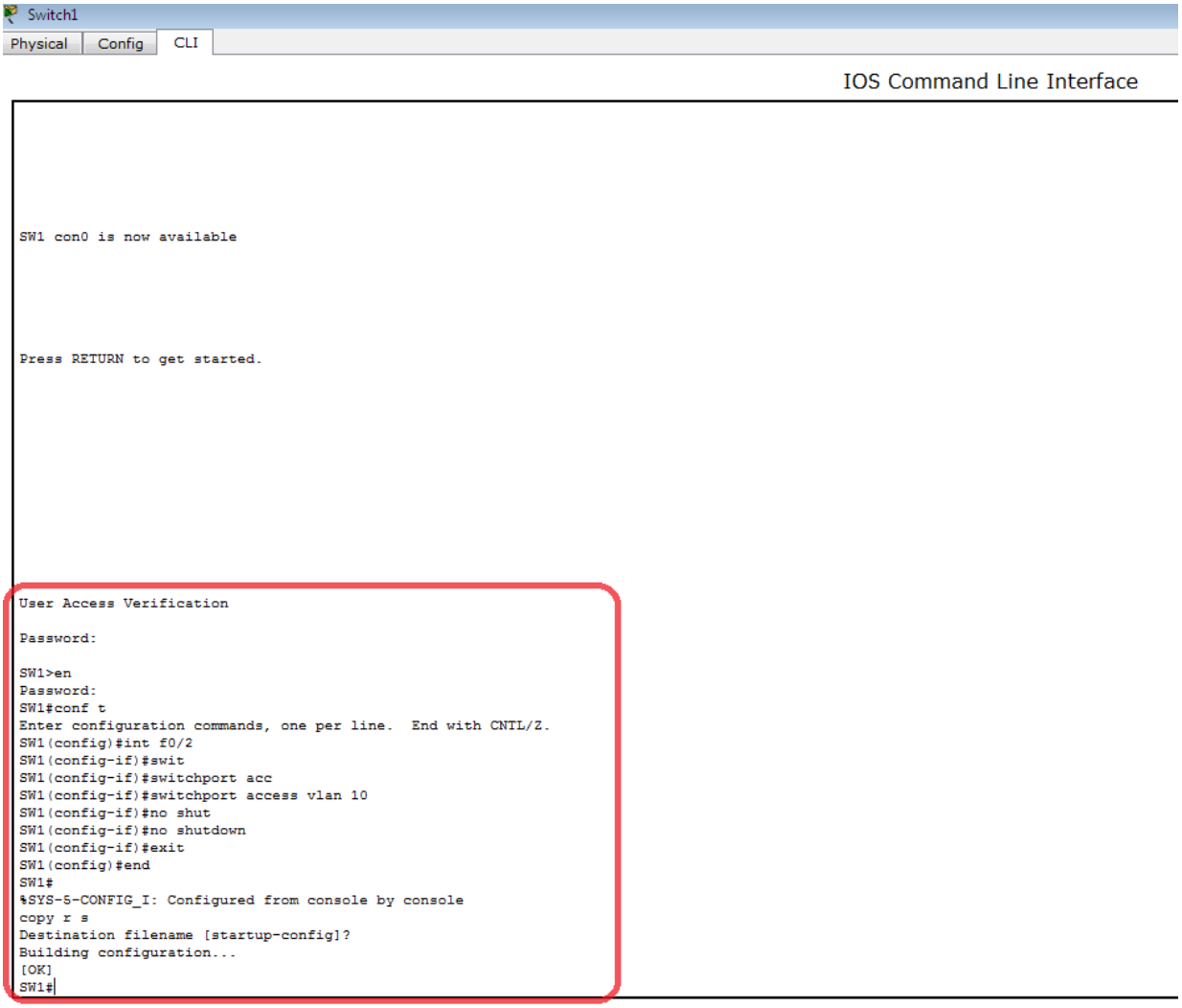

FIGURE 3.12: Activation des liens Access au niveau du switch 1

6. **Configuration de Spanning-Tree**

   Maintenant nous allons configurer le protocole Spanning-Tree pour définir le switch principal en tant que switch racine.

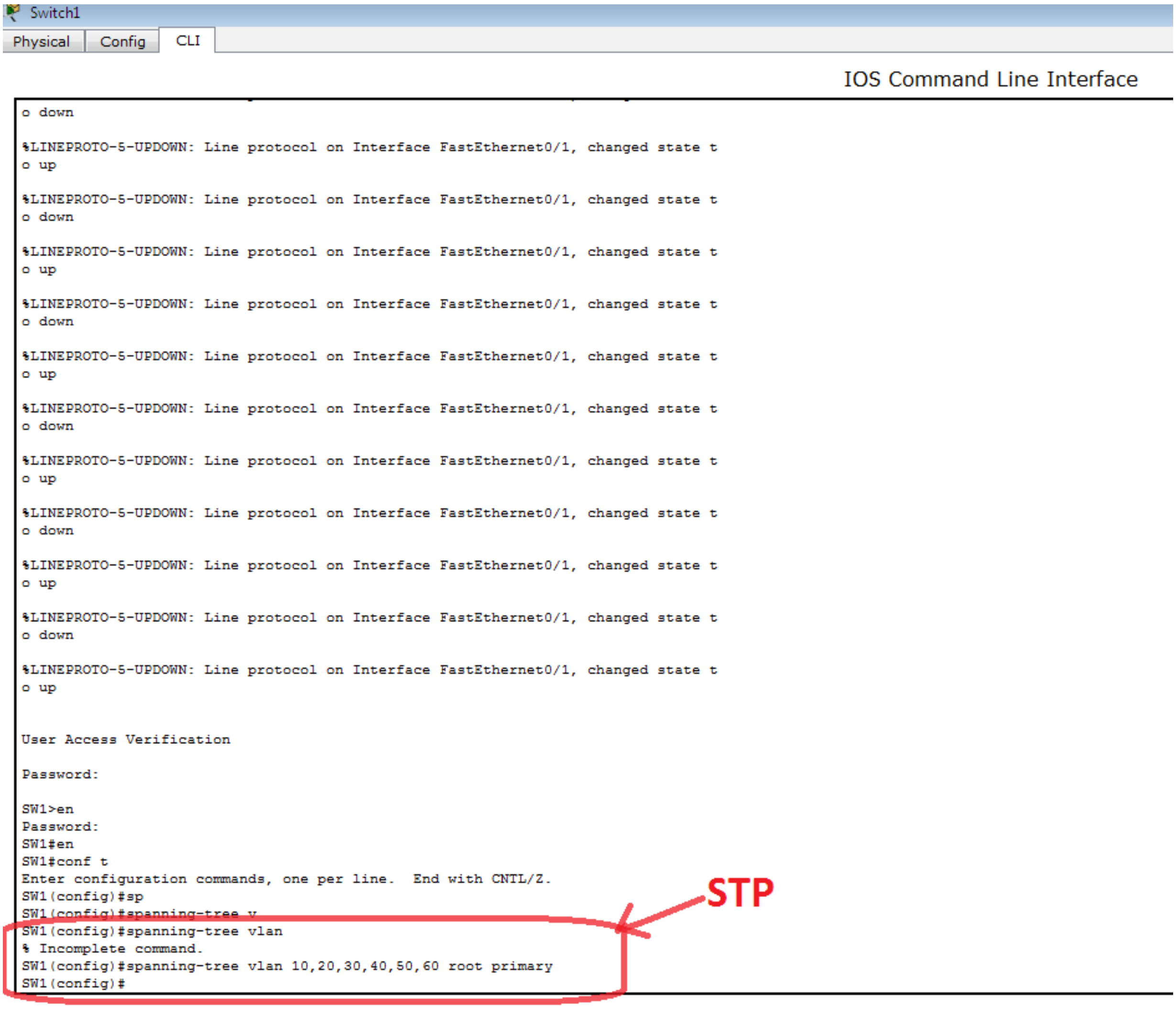

FIGURE 3.13: Configuration de Spanning-Tree

7. **Configuration des inter-VLAN**

   Nous allons maintenant configurer le routage inter-VLAN en utilisant des sous-interfacesau niveau du routeur,la figure ci-dessous nous montre les comandes à suivre :

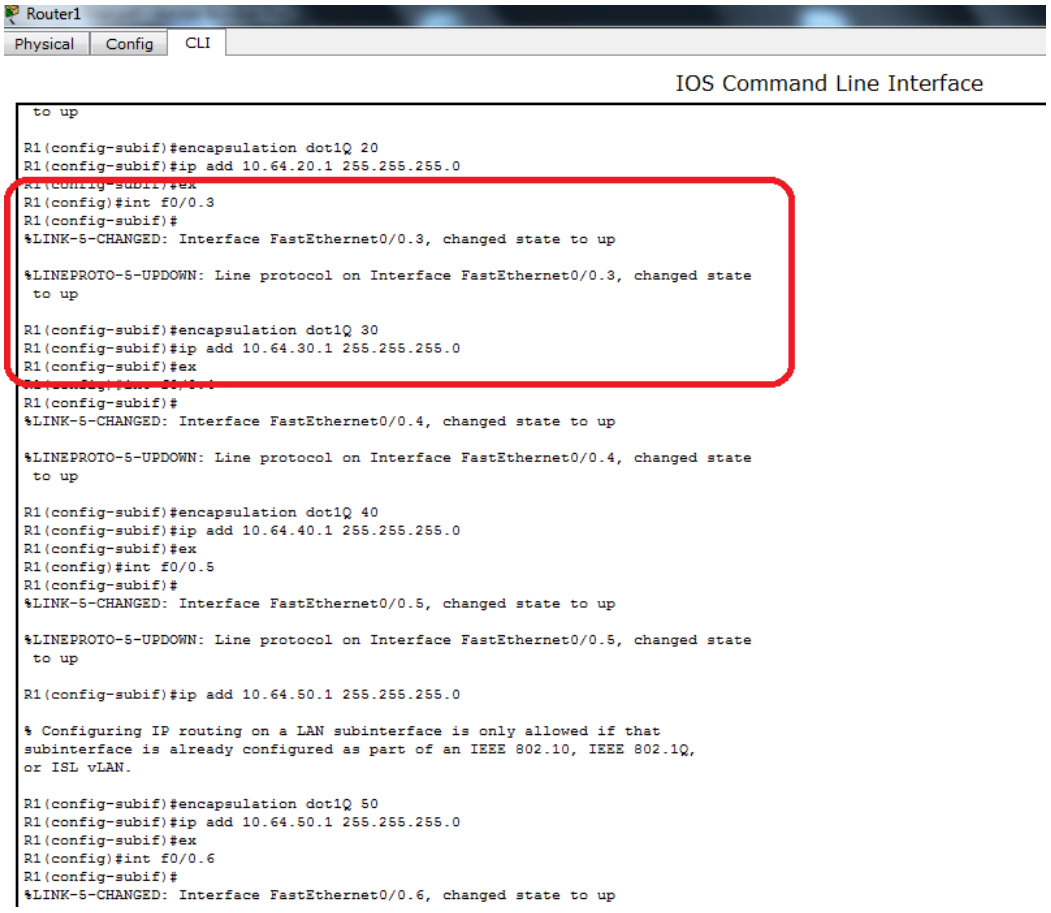

FIGURE 3.14: Le routage inter-VLAN

8. **Insertion des ACL**

Nous allons maintenant utiliser les listes des contrôles d'accès afin de limiter la communication entre certains VLANs, nous avons configurer une ACL au niveau du VLAN informatique en bloquant l'accès entrant vers eux c'est-à-dire que les autres n'auront pas accès sur leurs données, la figure ci-dessous montre sa configuration au niveau du routeur :

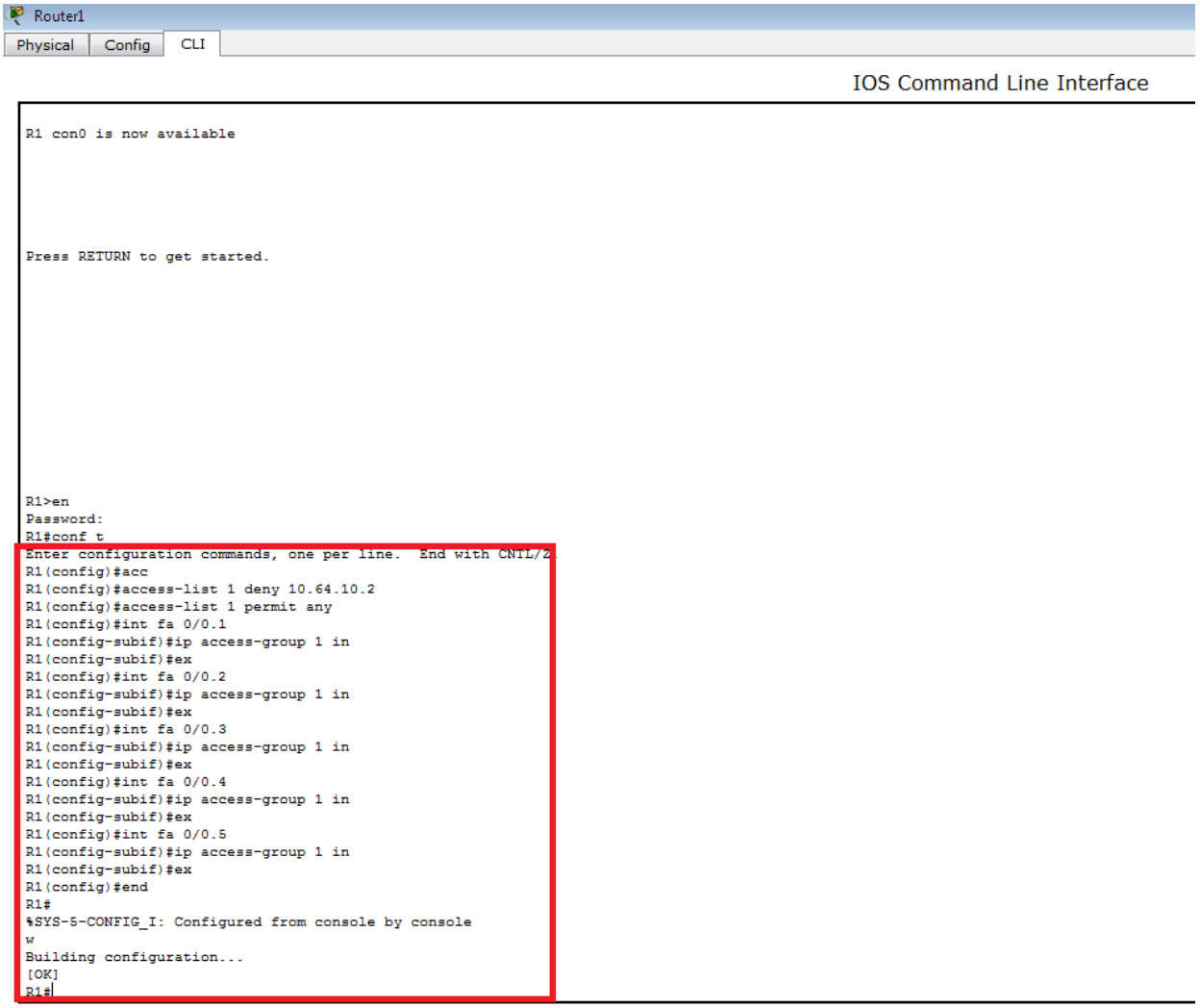

FIGURE 3.15: configuration des ACL

3.3 Test des configurations

Dans cette partie nous allons vérifier les communications entre quelques équipements en utilisant la commande « Ping ». Ces tests sont faits entre équipements (PC, Switchs et routeurs), inter-VLANs, et intra-VLANs. Il est à noter que la commande Ping aide à vérifier la connectivité au niveau IP.

1. **test intra-VLAN**

   Ping reussi entre le PC1 (10.64.20.3) et le PC5(10.64.20.2) qui appartiennent au méme VLAN (le VLAN AMG)

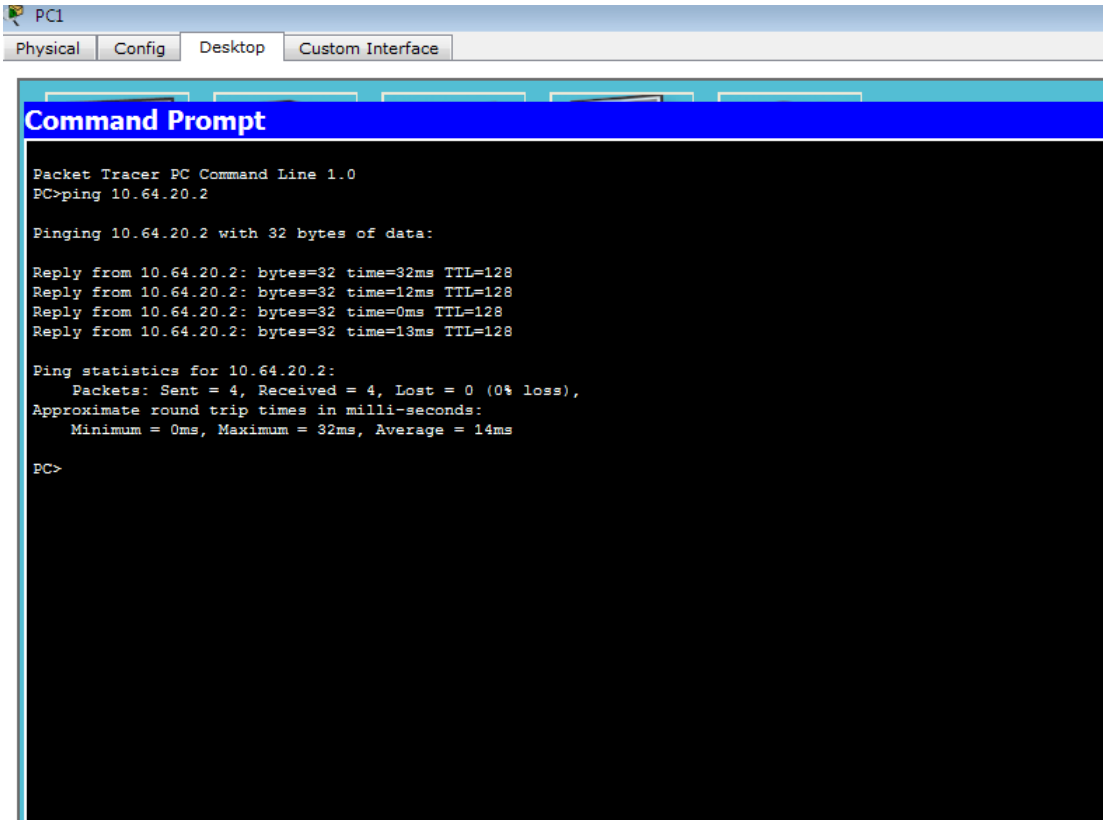

FIGURE 3.16: Ping réussi entre PC1 et PC5

2. **test inter-VLAN**

   Nous allons maintenant illustrer deux exemples, dans le premier, nous ferons un test de communication entre le pc du VLAN informatique (10.64.10.2) et le pc du VLAN AMG (10.64.20.2), sachant que le service informatique doit pouvoir accéder à tout les autres VLAN.

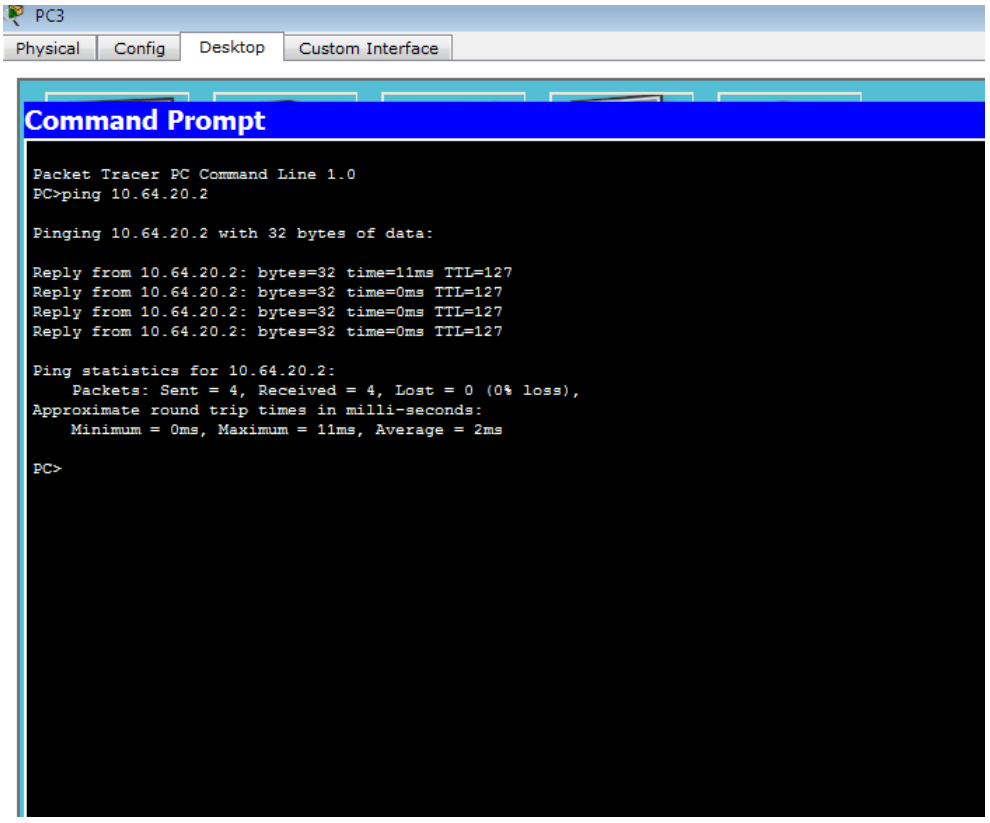

FIGURE 3.17: Ping réussi entre le VLAN informatique et le VLAN AMG

Par contre dans le deuxième exemple, nous allons démontrer que le PC du VLAN AMG (10.64.20.2) ne peut pas communiquer avec le pc du VLAN informatique (10.64.10.2) car nous avons limité l'accès au VLAN informatique grâce à des ACL préalablement implémentées.

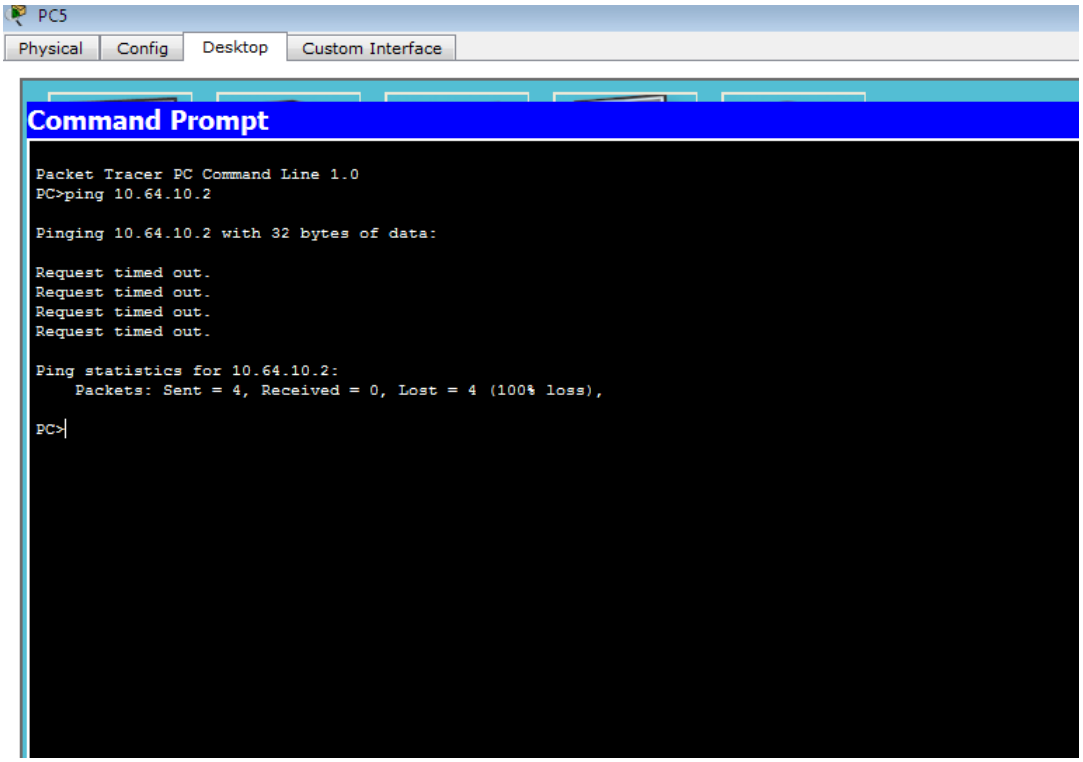

FIGURE 3.18: Ping échoué entre le VLAN AMG et le VLAN informatique

Conclusion

Pour finaliser notre projet, nous avons commencé par introduire le simulateur Packet tracer, nous l'avons par la suite utilisé pour la configuration de notre architecture réseau, puis nous avons expliqué comment configuré les commutateurs (créations des VLANs, mots de passe, insertion des ACL, etc.) et le routeur, ensuite nous sommes passé à des tests de vérification.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

Au terme de ce projet, il convient de dire d'une part sa réalisation s'est révélée très enrichissante et bénéfique, et que d'autre part ce travail n'a pas été facile à mettre en œuvre car il fallait non seulement comprendre les notions des vlan et pouvoir la simulation avec le logiciel cisco packet tracer.

Nous avons essayé à travers ce mémoire d'apporter une solution pour organiser le réseau informatique de l'entreprise NAFTAL . Comme nous l'avons constaté, NAFTAL est constituée de plusieurs services à savoir le service informatique,l'administration des moyens généraux, service technique,finance... etc. Alors nous avons opté pour une solution basée sur les réseaux virtuels en procédant à la segmentation logique du réseau local de l'entreprise afin d'améliorer sa sécurité et l'utilisation de la bande passante.

En fin ce travail nous a permis d'acquérir une expérience personnelle et professionnelle très bénéfique.ce fut une occasion pour nous de se familiariser avec l'environnement du travail et de la vie professionnelle, d'élargir et d'approfondir nos connaissances sur l'administration des réseaux informatique.

BIBLIOGRAPHIE

[1] Liste des termes, expressions et définitions du vocabulaire de l'informatique. *Journal officiel*, octobre 1998.

[2] R. CIREDDU. *cours sur la topologie des réseaux*. lycée La Martinière Monplaisir.

[3] G. PUJOLLE. *Initiation aux réseaux*. Édition eyrolles, 2014.

[4] Spanning-tree, . URL http://cisco.goffinet.org.

[5] P.ATELEN. *Réseaux informatique notion fondamental*. 3eme édition ENI, 2009.

[6] JF.PILLOU. *Tout sur les systèmes d'information*. Paris Dunod, 2006.

[7] G.DESGEORGE. *La sécurité des réseaux*. 3eme édition Dunod, 2012.

[8] S. GHERNAOUTI-HELIE. *Sécurité informatique et réseaux*. DUNOD, Paris, 2011.

[9] type de vlan, . URL http://www-igm.univ-mlv.fr.

[10] Acl, . URL http://www.linux-france.org.

[11] T.LAMMEL. *CCNA CISCO certified network associate study guide*. 6éme edition, 2007.

[12] réseaux, . URL http://www.netalya.com.

[13] Génael VALET. *Les LANs virtuels*. Greta industriel de technologies avancées, 2007.

[14] F.Nolot. *cours5-VTP*. Académie Cisco, 2007.

Résumé

Les réseaux locaux virtuels ou VLANs ont révolutionné le concept de segmentation des réseaux, ils permettent de constituer autant de réseaux logiques que nous désirons sur une seule infrastructure afin d'améliorer sa sécurité et de bien utiliser la bande passante.

L'objectif de notre travail consiste à implémenter une solution avec les réseaux locaux virtuels dans le but de segmenter le réseau de NAFTAL-District Bejaïa en réseaux logiques afin de facilité la gérance et améliorer la sécurité, mais ce travail ne peut pas être réalisé sans faire une étude de l'architecture existante du District.

Sur le plan applicatif, nous avons choisi d'organiser les VLANs par service, par la suite nous sommes passés à la configuration des listes de contrôle d'accès (ACL) afin de filtrer le trafic réseau.

Pour la simulation de notre architecture réseau avant et après l'implémentation des VLANs nous avons eu recours au simulateur de matériel réseau Cisco Packet Tracer, qui nous a permis de configurer les différents composants.

Mots clés: VLAN, LAN, ACL, Cisco Packet Tracer.

Abstract

Virtual LANs or VLANs have revolutionized the concept of network segmentation, making it possible to build as many logical networks as we want on a single infrastructure to improve its security and use the bandwidth.

The objective of our work is to implement a solution with the virtual local area networks in order to segment the network of NAFTAL-District Bejaia into logical networks in order to facilitate management and improve security, but this work can not be done without Do a study of the existing architecture of the District.

On the application side, we chose to organize the VLANs by service, and then we moved on to the configuration of the access control lists (ACLs) in order to filter the network traffic.

To simulate our network architecture before and after VLAN implementation, we used the Cisco Packet Tracer network hardware simulator, which enabled us to configure the various components

Keywords : VLAN, LAN, ACL, Cisco Packet Tracer.