

République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université Abderrahmane Mira de 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

Configuration et Simulation des VLANs
Cas d'étude : AGRANA

Réalisé par

M^{elle} SIDHOUM Rima
M^{elle} LALAM Kaïssa

Encadré par

M^{me} BOUADEM Nassima

Devant le jury

Examineur 1 : M^r ACHROUFENE Achour
Examinatrice 2 : M^{me} SABRI Salima

Promotion 2019-2020

****Dedicaces****

Je tien a dédier ce modeste travail à :

A mes très chers parents, aucun hommage ne pourrait être à la hauteur de l'amour dont ils ne cessent de me combler. Que dieu leur procure bonne santé et longue vie .

A mes très chères soeurs :

Mizi, son mari Ali et leurs fille Ayla .

Lydia, son mari Nabil , leurs fille Aya et fils Youyou .

Petite soeur Yasmine .

A mon très cher frère Smail, son épouse Hayet et leurs fille Dania .

A mon cher et meilleur soutenu Maci .

A mes chères amies Lilia, Lydia, Nabila et Naoual .

A mes amis(es) pour leur compréhension et fidélité .

Ainsi qu'à toute personne qui nous a soutenue .

Rima.

Dédicaces

Je tien à dédier ce modeste travail à :

A mes très chers parents, aucun hommage ne pourrait être à la hauteur de l'amour dont ils ne cessent de me combler. Que dieu leur procure bonne santé et longue vie.

A mes très chères sœurs :

Dalila, Malika

Yassmina, son mari Nadir et leurs enfants Rayan, Youba et Adame.

A mes très chers frères :

Boudjamaa,

Azouaou, son épouse Hakima et leurs enfants anias,yané et aylan.

Smail, son épouse Amel et leurs fils Massil.

A mon cher mari et meilleur soutenu Djahid.

A mes très chères cousines Silia, Rima.

A mes chères amies Amel, Salma, Hanane et Iman.

A mes amis(es) pour leur compréhension et fidélité.

Ainsi qu'à toute personne qui nous a soutenue.

Kaissa.

****Remerciements****

Tout d'abord, nous remercions Dieu, notre créateur de nous avoir donné la force, la volonté et le courage afin d'accomplir ce modeste travail.

Et nous adressons nos vifs remerciements et notre gratitude

Â :

Nos familles, surtout nos parents qui nous ont épaulés, soutenus et suivis tout au long de ce projet.

Nous tenons à adresser nos plus profonds et sincères remerciements à notre encadreur Pr BOUADEM Nassima, pour nous avoir encadrées et guidées tout au long de ce projet, pour tous ses conseils et ses encouragements, pour sa disponibilité et sa compréhension.

Aussi à tous les enseignants et employés du département Informatique qui ont contribué de près ou de loin à notre formation universitaire.

Nous tenons aussi à remercier également tous les membres de jury pour avoir accepté d'évaluer notre travail.

Enfin, nous remercions tous ceux qui nous ont soutenu et aidé dans la réalisation de ce mémoire de près ou de loin.

Table des matières	i
Liste des figures	vi
Liste des abréviations	ix
INTRODUCTION GENERALE	1
1 GENERALITES SUR LES RESEAUX ET LA SECURITE INFORMATIQUE	2
1.1 Introduction	3
1.2 Définition d'un réseau	3
1.3 Généralités sur les réseaux	3
1.3.1 Classifications des réseaux	3
1.3.1.1 PAN (Personnel Area Network).....	4
1.3.1.2 LAN (Local Area Network)	4
1.3.1.3 MAN (Metropolitan Area Network)	4
1.3.1.4 WAN (Wide Area Network)	4
1.3.2 Topologies des réseaux	5
1.3.2.1 Topologie physique	5
1.3.2.1.1 Topologie en bus	5
1.3.2.1.2 Topologie en anneau	6
1.3.2.1.3 Topologie en étoile	7
1.3.2.1.4 Topologie maillée	7
1.3.2.2 Topologie logique	8
1.3.2.2.1 Ethernet	8
1.3.2.2.2 Token Ring	8
1.3.2.2.3 FDDI	9
1.3.3 Supports de transmission	9

1.3.4	Modèle de référence OSI	10
1.3.5	Modèle de référence TCP/IP	11
1.4	Généralités sur la sécurité informatique	12
1.4.1	Définition	12
1.4.2	Objectifs de la sécurité informatique	12
1.4.3	Attaques informatiques	14
1.4.4	Stratégies de la sécurité informatique	18
1.4.4.1	Pare-feu (Firewall)	18
1.4.4.2	Zone démilitarisée	19
1.4.4.3	Systèmes de détection d'intrusion (IDS).....	19
1.4.4.4	Les VLANs	20
1.4.4.5	La cryptographie	20
1.4.4.6	Les VPNs.....	20
1.4.4.7	Les listes de contrôles d'accès(ACL).....	21
1.5	Conclusion.....	22
2	INTRODUCTION AUX RESEAUX LOCAUX VIRTUELS (VLANs)	23
2.1	Introduction	24
2.2	Equipement d'interconnexion d'un réseau local.....	24
2.3	Définition d'un VLAN.....	25
2.4	Caractéristiques des VLANs	26
2.5	Classification des VLANs	26
2.5.1	VLAN niveau 1	26
2.5.2	VLAN niveau 2.....	27
2.5.3	VLAN niveau 3.....	28
2.6	Communication inter VLAN.....	29
2.7	Les avantages des VLANs	30

2.8	Types des réseaux locaux virtuels	30
2.8.1	VLAN de données.....	31
2.8.2	VLAN par défaut	31
2.8.3	VLAN natif	31
2.8.4	VLAN de gestion	31
2.8.5	VLAN voix	31
2.9	Protocoles de transport des VLANs	32
2.9.1	Notion du TRUNK.....	32
2.9.2	Norme 802.1Q.....	33
2.9.3	Protocole ISL (Inter Switch Link Protocol).....	34
2.10	Protocoles de gestion des VLANs.....	34
2.10.1	Protocole VTP.....	34
2.10.2	Protocole VMPS	35
2.11	Conclusion.....	36
3	ETUDE DE L'EXISTANT ET REALISATION DE LA SOLUTION	37
3.1	Introduction	38
3.2	Présentation général	38
3.2.1	Présentation de l'organisme d'accueil	38
3.2.2	Situation géographique	38
3.2.3	Organigramme de l'unité	39
3.2.4	Présentation des équipements du réseau d'AGRANA.....	40
3.3	Contexte du projet à réaliser.....	40
3.3.1	Présentation du projet	40
3.3.2	Problématique	41
3.3.3	Objectif du projet à réaliser.....	41

3.3.4	Solution proposée.....	42
3.4	Présentation du simulateur Cisco Packet Tracer	43
3.4.1	Description générale de l'interface principale du Packet Tracer.....	43
3.4.2	Fonctionnement du Simulateur Packet Tracer	47
3.4.2.1	L'espace de travail logique (Logical work space).....	47
3.4.2.2	L'espace de travail physique (Physical Work Space)	48
3.4.2.3	Mode temps réel	49
3.4.2.4	Mode simulation.....	49
3.5	Configuration	49
3.5.1	Adressage des différents VLANs.....	49
3.5.2	Configurations des commutateurs.....	50
3.5.2.1	Configuration du Hostname	50
3.5.2.2	Configuration d'une sécurité de base	51
3.5.2.3	Configuration du protocole VTP (VLAN Trunking Protocol).....	55
3.5.2.4	Création des VLANs	57
3.5.2.5	Configuration des VLANs	58
3.5.2.6	Configuration de l'adresse du Vlan 9 dans le switch S-A1	59
3.5.2.7	Configuration de l'adresse du Vlan 9 dans le switch S-A2	60
3.5.2.8	Configuration de l'adresse du Vlan 9 dans le switch S-B1	61
3.5.2.9	Configuration des liens Trunk.....	62
3.5.2.10	Configuration des liens access.....	63
3.5.2.11	Configuration Inter-Vlan	64
3.5.2.12	Insertion des ACL.....	65
3.6	Test de fonctionnement	66
3.6.1	Architecture du réseau	66
3.6.2	Test 1.....	66
3.6.3	Test 2.....	67

3.6.4	Test 3.....	68
3.6.5	Test 4.....	69
3.7	Conclusion.....	70
CONCLUSION GENERALE		71
BIBLIOGRAPHIE		72

GENERALITES SUR LES RESEAUX ET LA SECURITE INFORMATIQUE

<i>Figure 1.1</i> Classification des réseaux informatiques.....	5
<i>Figure 1.2</i> Topologie en bus.....	6
<i>Figure 1.3</i> Topologie en anneau.....	6
<i>Figure 1.4</i> Topologie en étoile.....	7
<i>Figure 1.5</i> Topologie maillée.....	8
<i>Figure 1.6</i> Les couches du modèle OSI.....	11
<i>Figure 1.7</i> Comparaison entre le modèle TCP/IP et le modèle OSI.....	12
<i>Figure 1.8</i> Classification des attaques.....	14
<i>Figure 1.9</i> Attaque d'accès.....	14
<i>Figure 1.10</i> Attaque d'interruption.....	15
<i>Figure 1.11</i> Attaque de modification.....	16
<i>Figure 1.12</i> Attaque de déni de service.....	17
<i>Figure 1.13</i> Attaque de fabrication.....	17
<i>Figure 1.14</i> Attaque de rejeu.....	18
<i>Figure 1.15</i> Schéma d'une architecture réseau utilisant un Firewall.....	19
<i>Figure 1.16</i> DMZ (zone démilitarisée).....	19
<i>Figure 1.17</i> La cryptographie.....	20
<i>Figure 1.18</i> Principe de fonctionnement d'un VPN.....	21
<i>Figure 1.19</i> ACL.....	21

INTRODUCTION AUX RESEAUX LOCAUX VIRTUELS (VLANs)

<i>Figure 2.1</i> Construction des VLANs par port.....	27
<i>Figure 2.2</i> Construction des VLANs par MAC.....	28
<i>Figure 2.3</i> Construction des VLANs par sous-réseau.....	29
<i>Figure 2.4</i> Extension de la trame Ethernet modifiée par la norme 802.1Q.....	33
<i>Figure 2.5</i> Fonctionnement du protocole VTP.....	35

Figure 2.6 Principe de fonctionnement de VMPS.....	36
---	----

ETUDE DE L'EXISTANT ET REALISATION DE LA SOLUTION

Figure 3.1 Situation géographique d'AGRANA FRUIT ALGERIE	39
Figure 3.2 Organigramme d'AGRANA	39
Figure 3.3 Architecture du réseau AGRANA sans VLAN et Pare-feu.....	41
Figure 3.4 Architecture du réseau AGRANA avec VLAN et Pare-feu	42
Figure 3.5 Description générale de l'interface principale du Packet Tracer	44
Figure 3.6 Paramétrage physique du l'équipement	45
Figure 3.7 Fenêtre de configuration du l'équipement	46
Figure 3.8 Fenêtre Desktop du l'équipement	47
Figure 3.9 Espace de travail logique.....	48
Figure 3.10 Adressage des VLANs	50
Figure 3.11 Configuration du Hostname du Switch S-A1.....	51
Figure 3.12 Chiffrement du mot de passe.....	52
Figure 3.13 Mot de passe secret	53
Figure 3.14 Attribution du mot de passe console au Switch S-A1	54
Figure 3.15 Configuration du VTP Server	55
Figure 3.16 Configuration du VTP Client.....	56
Figure 3.17 Création des VLANs dans le Switch S-A1	57
Figure 3.18 Configuration des VLANs dans le Switch S-A1	58
Figure 3.19 Configuration de l'adresse du Vlan 99 dans le Switch S-A1	59
Figure 3.20 Configuration de l'adresse du Vlan 99 dans le Switch S-A2	60
Figure 3.21 Configuration de l'adresse du Vlan 99 dans le Switch S-B1	61
Figure 3.22 Configuration des liens Trunk du Switch S-A1	62
Figure 3.23 Configuration des liens d'Access du Switch S-A1.....	63
Figure 3.24 Configuration du Routage Inter-VLAN dans le Routeur R0.....	64

<i>Figure 3.25</i> Configuration des ACL.....	65
<i>Figure 3.26</i> Architecture du notre réseau	66
<i>Figure 3.27</i> Ping du Test 1 réussi	67
<i>Figure 3.28</i> Ping du Test 2 réussi	68
<i>Figure 3.29</i> Ping du Test 3 réussi	69
<i>Figure 3.30</i> Ping échoué entre le VLAN 3 et le VLAN 4	70

A

ACL	Access Control List
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
AUX	Auxiliaire

C

CFI	Chemin de Fer Industriel
CHAP	Challenge-Handshake Authentication Protocol

D

DES	Data Encryption Standard
DMZ	Zone Démilitarisée
DOS	Disk Operating System

E

EAP	Extensible Authentication Protocol
------------	---

F

FDDI	Fiber Distributed Data Interface
-------------	---

I

ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System (Systemes de détection d'intrusion)
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IPX	Inter Network Packet Exchange

ISL	Inter Switch Link
ISO	International Standards Organisation (Organisation Internationale de Normalisation)
<u>L</u>	
LAN	Local Area Network
LLC	Logical Link (Controle de la Liaison Logique)
<u>M</u>	
MAC	Media Access Control
MAN	Metropolitan Area Network
MAU	Multistation Access Unit
MD5	Message Digest 5
MS-CHAP	Microsoft Challenge-Handshake Authentication Protocol
<u>N</u>	
NVRAM	Non Volatile Random Access Memory
<u>O</u>	
OSI	Open Systems Interconnexion
<u>P</u>	
PAN	Personal Area Network
PAP	Password Authentication Protocol
PDU	Protocol Data Unit
PVID	Port Vlan ID
<u>R</u>	
RAM	Random Access Memory

ROM **Read-Only Memory**

RSA **Rivest Shamir Adleman**

S

SHA_1 **Secure Hash Algorithm_1**

SPAP **Software Product Assurance Plan**

T

TCI **Tag Control Information**

TCP **Transmission Control Protocol**

TPID **Tag Protocol Identifier**

U

UMTS **Universal Mobile Telecommunication System**

V

VID **VLAN Identifier**

VLAN **Virtual Area Network**

VMPS **VLAN Membership Policy Server**

VOIP **Voix sur IP**

VPN **Virtual Private Network**

VTP **VLAN Trunking Protocol**

VTY **Virtual Terminal Line**

W

WAN **Wide Area Network**

WIFI **Wireless Fidelity**

INTRODUCTION GENERALE

L'implication de l'informatique dans tous les secteurs d'activité a permis de rendre facile bon nombre de tâches. La plupart des entreprises aujourd'hui sont informatisées et il est inconcevable, à notre époque, de ne pas disposer de VLAN pour les gérer. La performance du système d'information d'une entreprise est d'une importance capitale pour son efficacité et son bon fonctionnement.

Le réseau informatique permet aux entreprises de centraliser leurs données, de travailler en équipe de manière productive et de limiter l'utilisation du papier (impression, déplacement) afin de faciliter le transfert d'informations. Chose qui est devenue de plus en plus nécessaire, voire même primordiale pour les entreprises.

Nous avons axé notre travail sur la réorganisation du réseau et la diminution de la bande passante grâce à la notion des VLANs qui nous a permis de réaliser notre intérêt, qui est l'objectif de notre travail. Pour cela notre projet est structuré en trois chapitres :

Le premier chapitre sera consacré à la présentation de quelques généralités sur les réseaux informatiques et leurs sécurités.

Le second chapitre présente une introduction sur les réseaux locaux virtuels (VLAN), les principales notions ainsi que les protocoles utilisés dans la stratégie des VLANs.

Le dernier chapitre sera divisé en deux parties, la première sera consacré pour l'étude de l'existant et la deuxième partie pour la simulation du réseau donné en exemple.

Enfin, nous résumant les différentes étapes parcourus tout au long de ce travail dans la conclusion générale.

Chapitre 1

GENERALITES

SUR LES

RESEAUX ET LA

SECURITE

INFORMATIQUE

CHAPITRE 1 GENERALITES SUR LES RESEAUX ET LA SECURITE INFORMATIQUE

1.1 Introduction

Dans nos jours l'internet est devenue assez présente dans la vie des êtres humains, où leurs informations et leurs données sont susceptibles à des altérations et des destructions par des logiciels/personnes malveillants ou par des virus...etc. Par conséquence, la sécurité de ces derniers est devenue un objectif primordial pour assurer à la fois la confidentialité de transfert des données et l'intégrité de ces derniers dans la mise en place des réseaux informatiques.

Dans ce chapitre, nous nous focaliserons sur les notions de base qu'on exploitera dans notre travail. Dans la première partie nous présentons les réseaux, nous parlerons en outre sur les différents types des réseaux, leurs topologies et les supports de transmissions. Ainsi, nous détaillerons les deux modèles de références OSI et TCP/IP. Ensuite, nous commençons par définir et exposer les objectifs de la sécurité informatique comme nous exposerons quelques stratégies de la sécurité informatique telles que les pare-feu, les IDS et les VLANs.

1.2 Définition d'un réseau

Un réseau (network en anglais) est un ensemble de moyens matériels et immatériels(logiciels) interconnectés pour assurer la communication entre les ordinateurs, les postes de travaux et les terminaux informatiques [1].

Les réseaux informatiques permettent aux utilisateurs d'échanger des informations (par exemple des messages), le partage de données (fichiers) ou encore l'accès à distance aux bases de données [1].

1.3 Généralités sur les réseaux

1.3.1 Classifications des réseaux

On distingue différents types de réseaux selon leur taille (en termes de nombre de machine), leur vitesse de transfert de données ainsi que leur étendue [2].

Les réseaux informatiques sont classifiés généralement en trois catégories de réseaux selon leur échelle géographique [2].

1.3.1.1 PAN (Personnel Area Network)

Un réseau PAN relie sur quelques mètres des équipements personnels (tels que les terminaux UMTS, portables, organiseurs, Pc portable, etc.) d'un même utilisateur [3].

1.3.1.2 LAN (Local Area Network)

Un réseau LAN est un réseau informatique étendu sur une échelle géographique relativement restreinte. Il permet la connexion d'un ensemble de postes d'une habitation particulière, d'une entreprise ou bien d'une salle informatique afin d'échanger ou de partager les données, il permet aussi le partage de ressources (disque, imprimante...), souvent à l'aide d'une même technologie(Ethernet). L'infrastructure est privée et 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, la taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs [2].

1.3.1.3 MAN (Metropolitan Area Network)

Un réseau MAN est un réseau informatique qui relie plusieurs réseaux LANs qui sont géographiquement proches (au maximum quelques dizaines de Km), son principe est identique à celui d'un réseau local mais les normes sont différentes. Ainsi un MAN permet à deux nœuds distants de communiquer comme s'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].

1.3.1.4 WAN (Wide Area Network)

Un réseau WAN est un réseau informatique qui interconnecte plusieurs LANs et MANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent un arbitrage avec le coût de liaison (qui augmente avec la distance) et peuvent être faibles.

Les WANs fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau. Ce type de réseau utilise les satellites pour certaines interconnexions. Le plus connu des WANs est Internet [2].

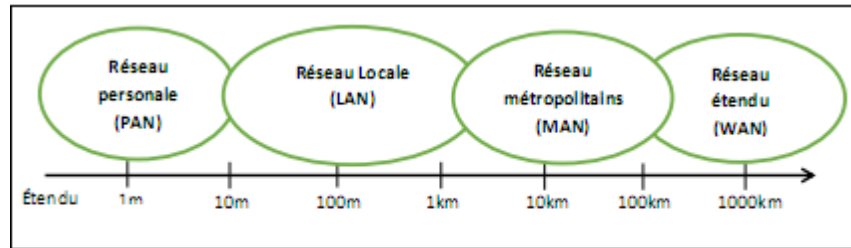


Figure 1.1 Classification des réseaux informatiques [4].

1.3.2 Topologies des réseaux

La topologie caractérise la façon dont les différents équipements sont interconnectés. On distingue deux différentes topologies : la topologie physique et la topologie logique [5].

1.3.2.1 Topologie physique

Elle décrit la manière dont les équipements du réseau sont connectés physiquement entre eux grâce à des lignes de communications (câbles réseaux) et des éléments matériels (cartes réseaux, etc.). Les topologies physiques les plus courantes sont la topologie en étoile, en anneau et en bus. Des topologies plus complexes peuvent être obtenues en combinant ou en dérivant ces topologies de base. Il existe plusieurs topologies parmi eux nous citons [5] :

1.3.2.1.1 Topologie en bus

Les stations sont reliées entre eux à l'aide d'un seul câble (généralement un câble coaxial), chaque station peut accéder à tout moment au support commun pour émettre et les données sont diffusées à toutes les stations. Les connexions des stations sur le câble sont de type passif, ce qui veut dire que le signal ne sera ni modifié ni régénéré à chaque station, ce qui limite l'étendu de ce genre de réseau. Mais par contre la défaillance de l'un d'entre eux ou l'insertion d'une nouvelle station ne perturbe pas le fonctionnement au sein du réseau. Cette topologie a comme inconvénient : la non absorption de l'énergie c'est-à-dire que lorsque le signal a été émis sur l'ensemble du bus celui-ci lorsqu'il arrive à la fin de la ligne son énergie reste la même, mais il risque de se produire un phénomène de réflexion du signal, et pour éviter ce phénomène on bouche les extrémités du réseau avec des résistances de terminaison [6].

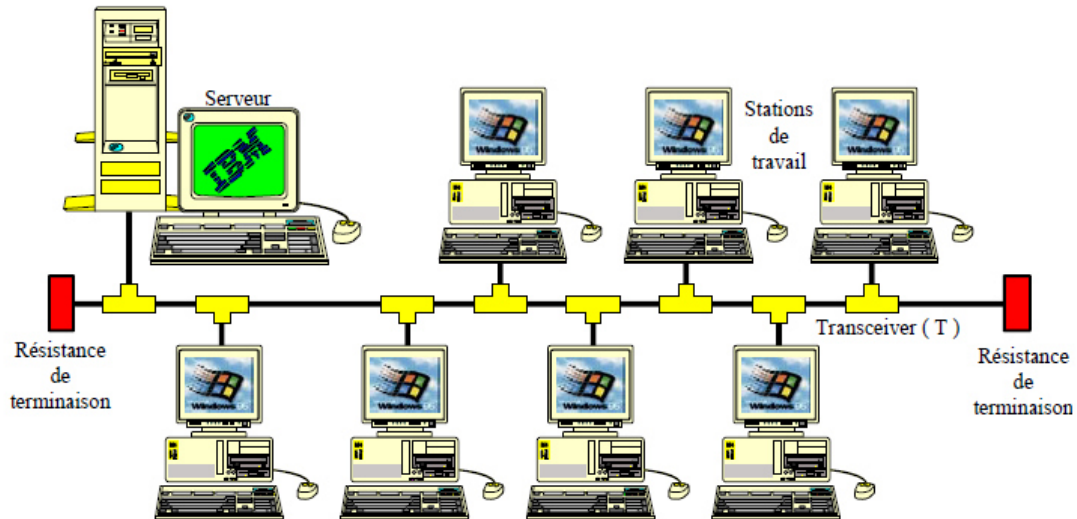


Figure 1.2 Topologie en bus [6].

1.3.2.1.2 Topologie en anneau

Les ordinateurs ou périphériques sont reliés entre eux pour former une boucle fermée. L'ordre d'accès au réseau. Les nœuds ou répartiteur (MAU : Multistation Access Unit) sont actifs, chaque nœud est connecté au support par un port d'entrée et transmet les données à la station suivante par son port de sortie, chaque station traversée prend le message, l'analyse puis le retransmet sur son port de sortie. Mais en cas de coupure de l'anneau le réseau est interrompu, ce qui est le cas lors de l'installation d'une nouvelle station de travail [6] [7].

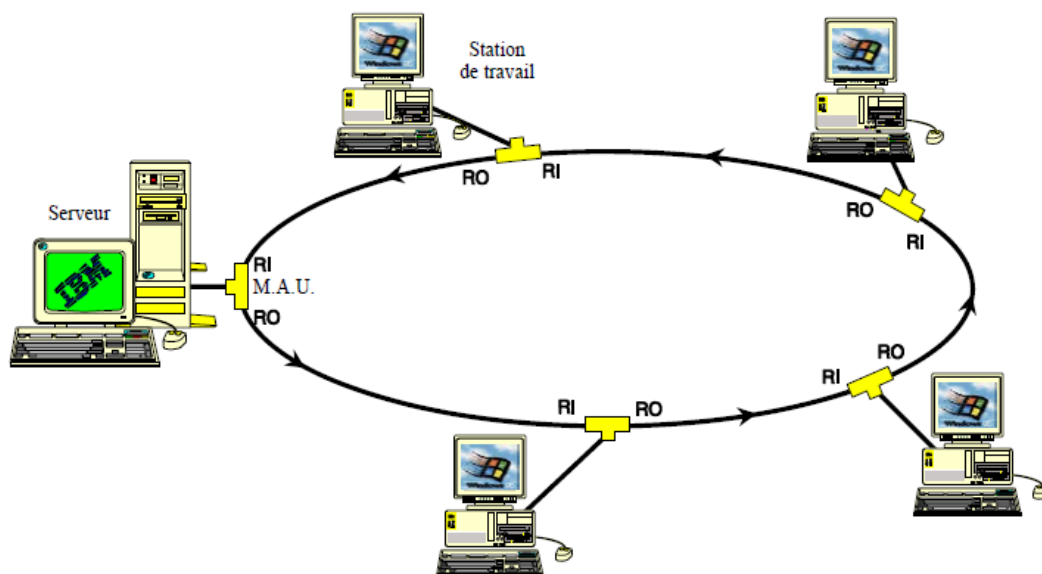


Figure 1.3 Topologie en anneau [6].

1.3.2.1.3 Topologie en étoile

Les stations sont toutes reliées à un nœud central qui est le concentrateur, ce câblage à se fait à l'aide de câble en paires torsadées, les messages envoyés entre les stations transitent par le concentrateur. Cette topologie présente un point faible, le réseau est inutilisable en cas de panne de l'équipement central [6][7].

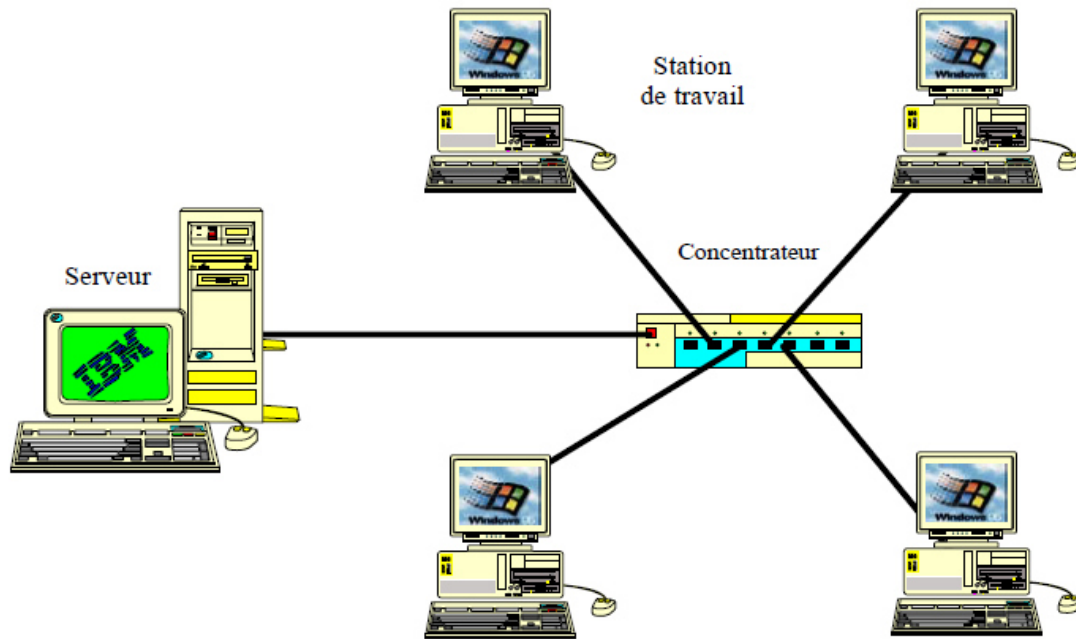


Figure 1.4 Topologie en étoile [6].

1.3.2.1.4 Topologie maillée

C'est une amélioration de la topologie en étoile, il s'agit de pouvoir relier une station à toutes les autres, de manière directe ou indirecte. L'information peut ainsi parcourir des chemins différents pour arriver au même destinataire. L'avantage principal de ce type de réseau est qu'il est très tolérant aux pannes, très évolutif, le tout simplement [8].

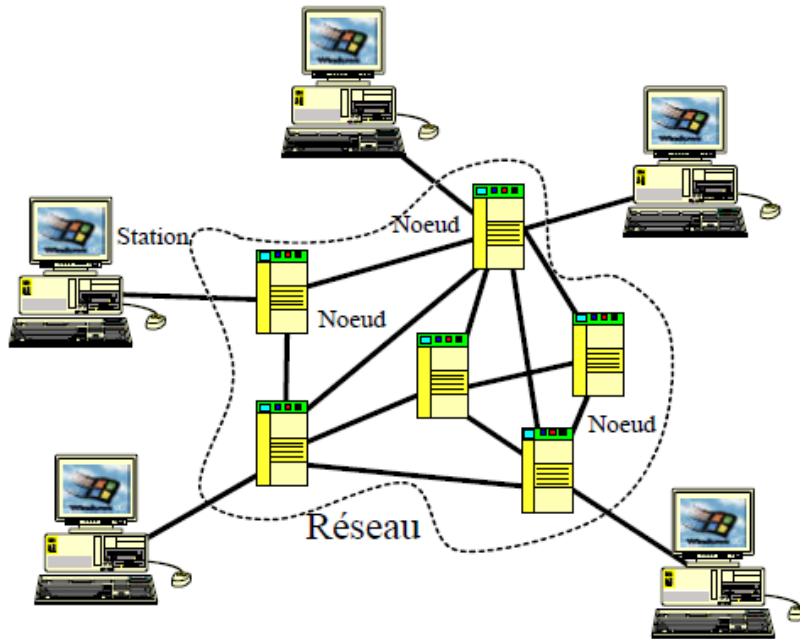


Figure 1.5 Topologie maillée [6].

1.3.2.2 Topologie logique

Elle décrit la manière dont les différentes informations (données) circulent dans les lignes de communications afin d'arriver à la/les destination(s) ou déterminer où les collisions pourraient se produire. Les topologies logiques les plus courantes sont : Ethernet, Token Ring et FDDI [5].

1.3.2.2.1 Ethernet

C'est une norme de LAN qui respectent les spécifications de la norme 802.3, elle définit les réseaux locaux utilisant la méthode CSMA/CD. Son principe repose sur un bus physique(partagé) comme support de transmission, ce qui veut dire que tous les éléments actifs sont connectés à un seule support de transmission. Dans un réseau Ethernet, la communication se fait à l'aide d'un protocole appelé CSMA/CD [9].

1.3.2.2.2 Token Ring

Token Ring repose sur une topologie en anneau (ring). Il utilise la méthode d'accès par jeton (token). Dans cette technologie, seul le poste ayant le jeton a le droit de transmettre. Si un poste veut émettre, il doit attendre jusqu'à à ce qu'il ait le jeton. Dans un réseau Token Ring, Chaque nœud du réseau comprend un MAU (Multi station Access Unit) qui peut

recevoir les connexions des postes. Le signal qui circule est régénéré par chaque MAU. Mettre en place un réseau Token Ring coûte cher, et la panne d'une station MAU provoque le disfonctionnement du réseau [7] [10].

1.3.2.2.3 FDDI

La technologie LANFDDI (Fibre Distributed Data Interface) est une technologie d'accès réseau utilisant des câbles fibres optiques. Le FDDI est constitué de deux anneaux : un anneau primaire et un anneau secondaire, L'anneau secondaire sert à rattraper les erreurs de l'anneau primaire. Le FDDI utilise un anneau à jeton qui sert à détecter et à corriger les erreurs. Ce qui fait que si une station MAU tombe en panne, le réseau continuera de fonctionner [11].

1.3.3 Supports de transmission

Pour faire transporter les informations entre les divers périphériques du réseau on a besoin de moyen de transmission. Ces moyens sont appelés supports de transmission qu'on a caractérisés dans le tableau ci-dessous [11] :

Types	Caractéristiques
Paire torsadée	<ul style="list-style-type: none"> -Un débit de 10 à100 Mb/s. -Une longueur maximale de 100 mètres. -Sa bande passante est de 4 MHz. -Affaiblissement important. -Sensibilité aux parasites d'origine électromagnétique.
Câble coaxial	<ul style="list-style-type: none"> -Un débit de 10 Mb/s. -Bande passante pouvant atteindre 300 à 400 MHz. -Résistant aux interférences et à l'atténuation du signal électrique.
Fibre optique	<ul style="list-style-type: none"> -Un débit de 100Mb/s. -Bande passante est de plusieurs

	Gigahertz. -Insensibilité aux parasites d'origine électromagnétique.
--	---

1.3.4 Modèle de référence OSI

Le modèle de référence OSI (Open System Interconnexion) définit une sorte de langage commun. Ce modèle a été mis au point par l'ISO (Organisation Internationale des Standards) et est devenu le socle de référence pour tout système de traitement de communications. Il répartit les questions relatives au domaine des communications informatiques selon sept couches classées par ordre d'abstraction croissant. Son objectif est d'assurer que les protocoles spécifiques utilisés dans chacune des couches coopèrent pour assurer une communication efficace. Décrivons succinctement le rôle de chaque couche [12].

1. Physique : Elle convertit les signaux électriques en bits de données et vice versa, selon la réception ou la transmission des informations à la couche liaison [13].

2. Liaison : Elle est divisée en deux sous-couches :

- La couche MAC qui structure les bits de données en trames et gère l'adressage des cartes réseaux [13].
- La couche LLC qui assure le transport des trames et gère l'adressage des utilisateurs [13].

3. Réseau : Elle traite la partie donnée utile contenue dans la trame. Elle connaît l'adresse de tous les destinataires et choisit le meilleur itinéraire pour l'acheminement. Elle gère donc l'adressage logique et le routage [13].

4. Transport : Elle segmente les données de la couche session, prépare et contrôle les tâches de la couche réseau. Elle peut multiplier les voies d'accès et corriger les erreurs de transport [13].

5. Session : Son unité d'information est la transaction. Elle s'occupe de la gestion et la sécurisation du dialogue entre les machines connectées, les applications et les utilisateurs (noms d'utilisateurs, mots de passe, etc.) [13].

6. Présentation : Elle convertit les données en information compréhensible par les applications et les utilisateurs, syntaxe, sémantique, conversion des caractères graphiques, format des fichiers, cryptage et la compression [13].

7. Application : C'est l'interface entre l'utilisateur ou les applications et le réseau. Elle concerne la messagerie, les transferts et partages de fichiers et l'émulation de terminaux [13].

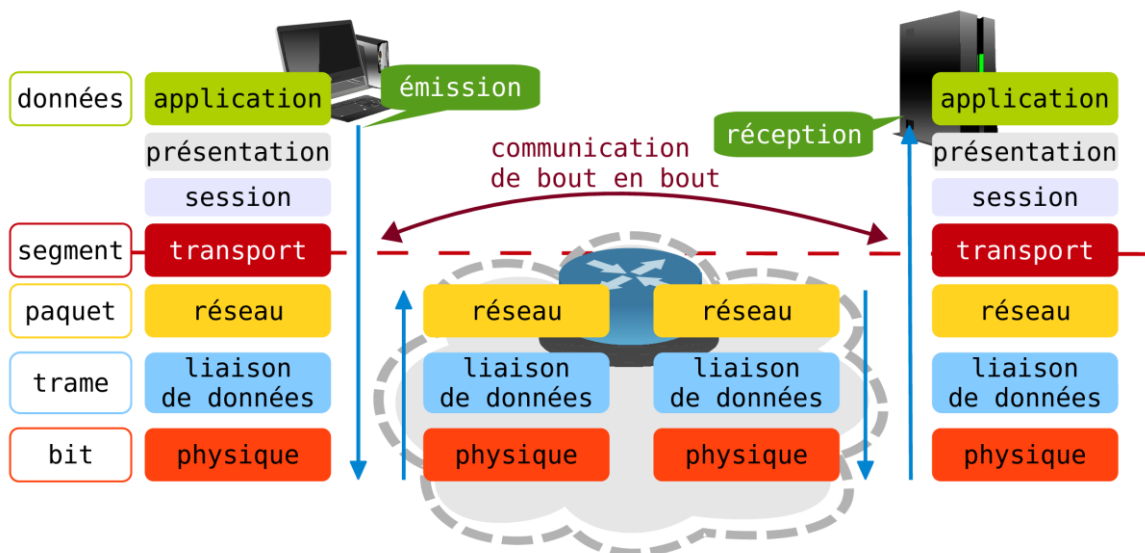


Figure 1.6 Les couches du modèle OSI [14].

1.3.5 Modèle de référence TCP/IP

Contrairement au modèle OSI, le modèle TCP/IP est né d'une implémentation mais il est inspiré du modèle OSI. Il reprend l'approche modulaire (utilisation de modules ou des couches) mais en contient uniquement quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même application [11] [15].

Le schéma ci-dessous (Figure 1.2) nous montre la différence entre ces deux modèles :

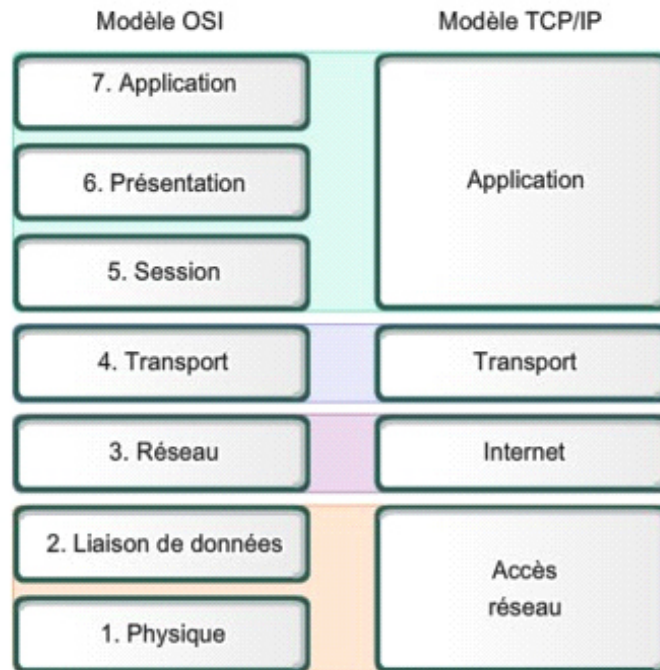


Figure 1.7 Comparaison entre le modèle TCP/IP et le modèle OSI [16].

1.4 Généralités sur la sécurité informatique

1.4.1 Définition

La sécurité informatique est l'ensemble des moyens et discipline mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces et protéger l'intégrité et la confidentialité des informations stockées dans un système informatique [17].

1.4.2 Objectifs de la sécurité informatique

La sécurité informatique vise généralement cinq objectifs :

✓ **L'intégrité** : c'est la protection des données et informations contre les changements et les altérations durant la communication. L'intégrité est assurée lorsque des données émises sont identiques à celles reçues. Des différences peuvent apparaître si quelqu'un tente de modifier ces données ou tout simplement si un problème de transmission ou réception intervient [18].

Les techniques utilisées pour faire face à cela sont, les débits de parité, les checksums (somme de contrôle) ou encore les fonctions de hachage à sens unique (SHA_1, MD5, etc.) [18].

✓ **La confidentialité** : C'est un service de sécurité qui empêche la divulgation des données à des entités (sites, organisations, personnes, ...etc.) non habilitées à les connaître, c'est-à-dire que ce service assure que seules les personnes autorisées peuvent prendre connaissances de ces données. Pour obtenir ce service, on utilise généralement le chiffrement des données concernées à l'aide d'un algorithme cryptographique [18].

Quelques algorithmes de chiffrement :

- Les algorithmes asymétriques : RSA ; Deffe-Hellman, etc.
- Les algorithmes symétriques : DES, 3DES, AES, ... etc.

✓ **La disponibilité** : C'est un service qui permet de garantir ou assurer que l'information soit toujours accessible lorsque l'utilisateur autorisé en a besoin peu importe le moment choisi. Cela veut dire que le système informatique donne l'accès à l'information pour qu'elle soit modifiée ou lues par les utilisateurs autorisés et faire en sorte qu'aucun utilisateur ne puisse empêcher les utilisateurs autorisés d'accéder à l'information [19].

✓ **La non-répudiation** : C'est un service qui permet d'empêcher qu'une entité ou un processus engagé dans une communication de nier (démenti) d'avoir reçu ou émis un message. Assuré par la signature numérique (RSA+SHA1, RSA+MD5, etc.) et la cryptographie à clé publique et privée [20].

✓ **L'authentification** : Le service d'authentification permet d'assurer qu'une communication est authentique (fournir une identification et de la prouver). Nous pouvons distinguer deux types d'authentification : L'authentification d'un tiers qui consiste pour ce dernier à prouver son identité et l'authentification de la source des données qui sert à prouver que les données reçues viennent bien d'un tel émetteur déclaré [18].

Sur la plupart des réseaux, le mécanisme d'authentification utilise une paire code d'identification /mot de passe. Cependant, en raison de la vulnérabilité constamment associée à l'utilisation des mots de passe, il est souvent recommandé de recourir à des mécanismes plus robustes tels que l'authentification par des certificats, des clés publiques ou à travers des centres de distribution des clés, les signatures numériques

peuvent aussi servir à l'authentification. Il existe plusieurs protocoles d'authentification, nous citons quelques-uns parmi eux : PAP, SPAP, CHAP, MS-CHAP, EAP, ... [18].

1.4.3 Attaques informatiques

Tout ordinateur connecté à un réseau est vulnérable à une attaque, une attaque représente les moyens d'exploiter une vulnérabilité en s'appuyant sur divers types de faiblesses telles que les faiblesses des protocoles, faiblesses d'authentification, faiblesses d'implémentation et les mauvaises configurations [21].

Les attaques peuvent être classées en deux grandes catégories : Attaques passives et Attaques actives [21].

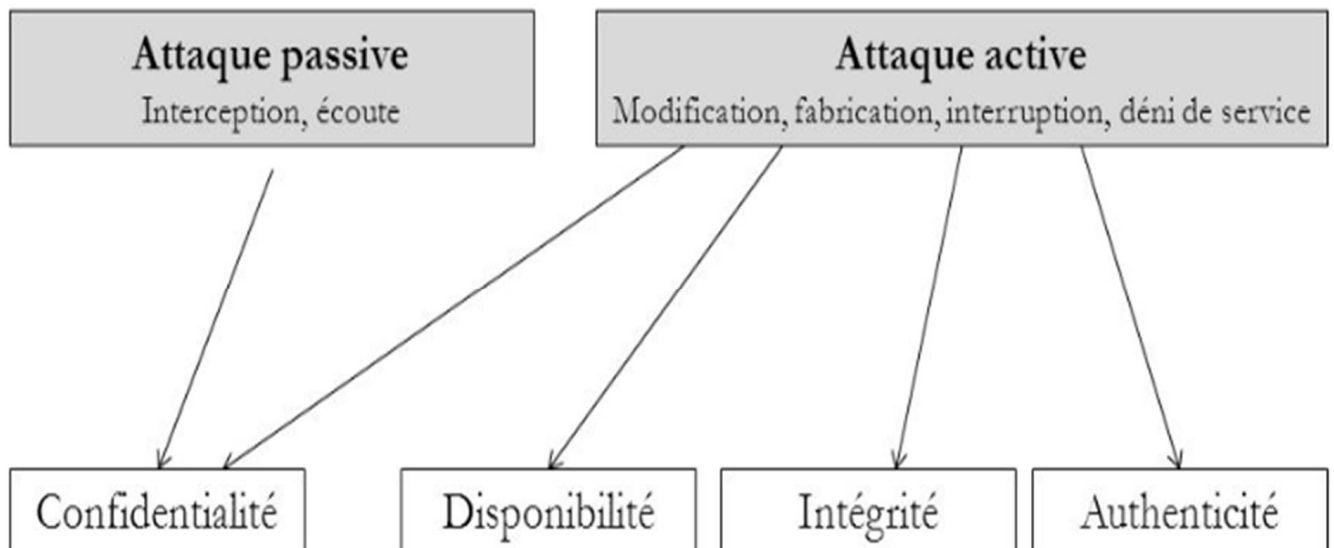


Figure 1.8 Classification des attaques [21].

On cite ci-dessous quelque types d'attaques informatique qui peuvent se produire lorsque on se connecte à un réseau :

➤ **Attaque d'accès (interception) :**

Une attaque d'accès ou une attaque d'interception est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information, et peut se produire par plusieurs techniques telles que : l'homme du milieu (Man-In-The-Middle), le sniffing, les chevaux de Troie, porte dérobée, ... [22].

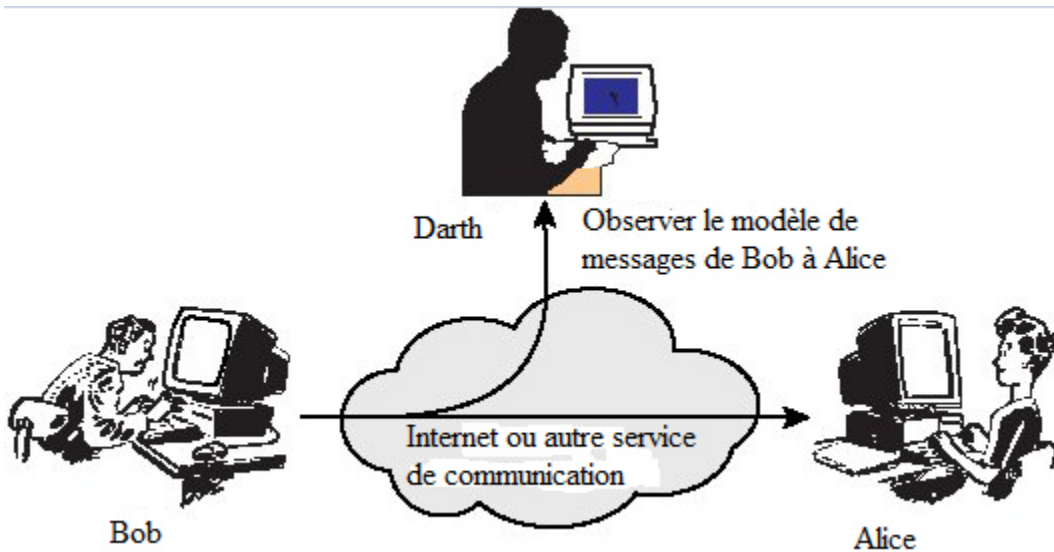


Figure 1.9 Attaque d'accès [24].

➤ **Attaque d'interruption :**

Une partie de l'application distribuée est détruite ou est devenue inaccessible. Il s'agit d'une attaque sur la disponibilité, Ce type d'attaque n'est pas géré directement par le mécanisme de sécurité mais par le mécanisme de rendez-vous. Ce dernier garantit la délivrance du message lors d'une communication. Si le rendez-vous échoue, le comportement actuel est de lever une exception afin d'en informer l'utilisateur [22].

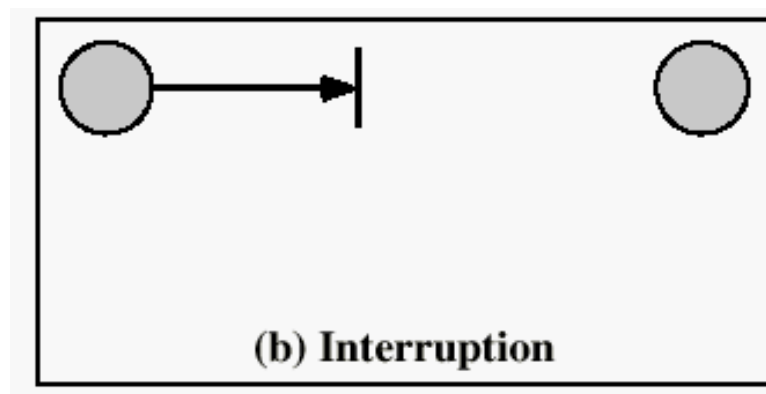


Figure 1.10 Attaque d'interruption [24].

➤ **Attaque de modification :**

Une troisième personne non autorisée intercepte des données et les altère avant de les émettre au destinataire. Il s'agit d'une attaque sur l'intégrité de l'information. Elle peut se présentée sous forme de : virus, sflooding, bombe logique, [22].

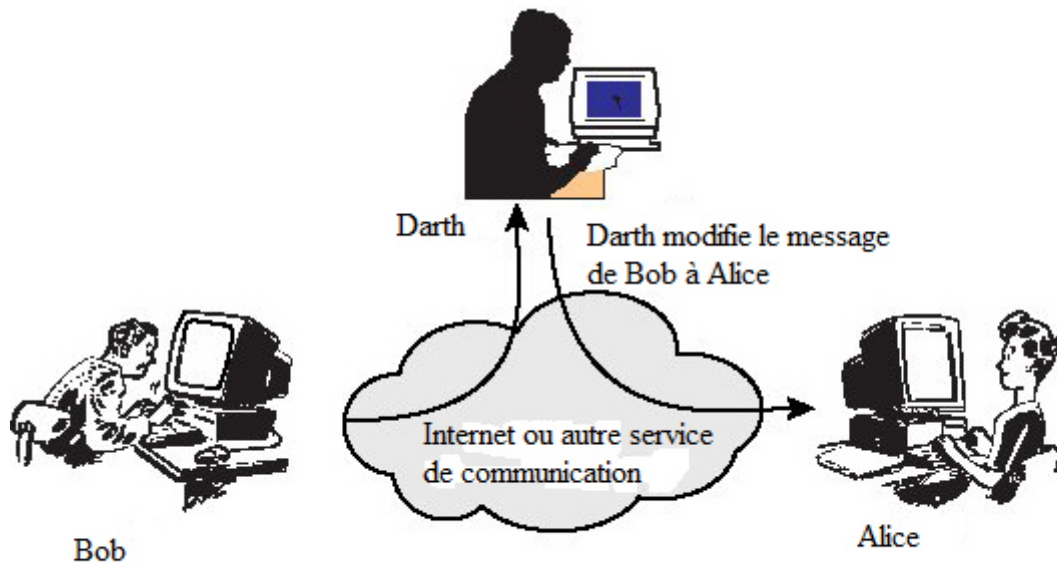


Figure 1.11 Attaque de modification [24].

➤ **Attaque de déni de service :**

Les attaques de type Denial-of-Service ont pour but de saturer un routeur ou un serveur afin de le crasher ou en préambule d'une attaque massive. Ces types d'attaque sont très faciles à mettre en place et très difficile à empêcher. Parmi les techniques utilisés pour réaliser ce type d'attaque on cite : Le flooding, le débordement de tampon, le smurf, ... [23].

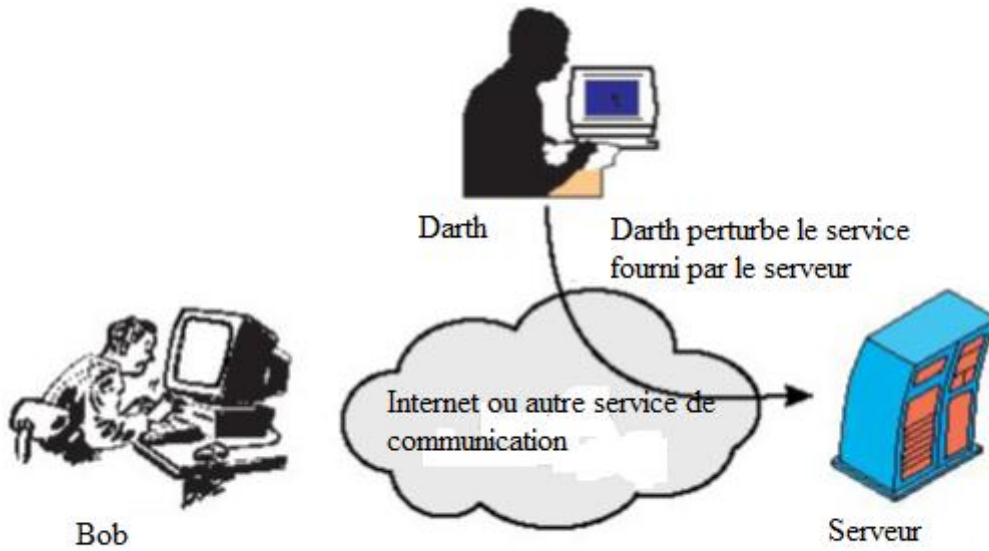


Figure 1.12 Attaque de déni de service [24].

➤ **Attaque de fabrication :**

Un tiers non autorisé insère des données contrefaites dans les communications de l'application. Il s'agit d'une attaque sur l'authentification [22].

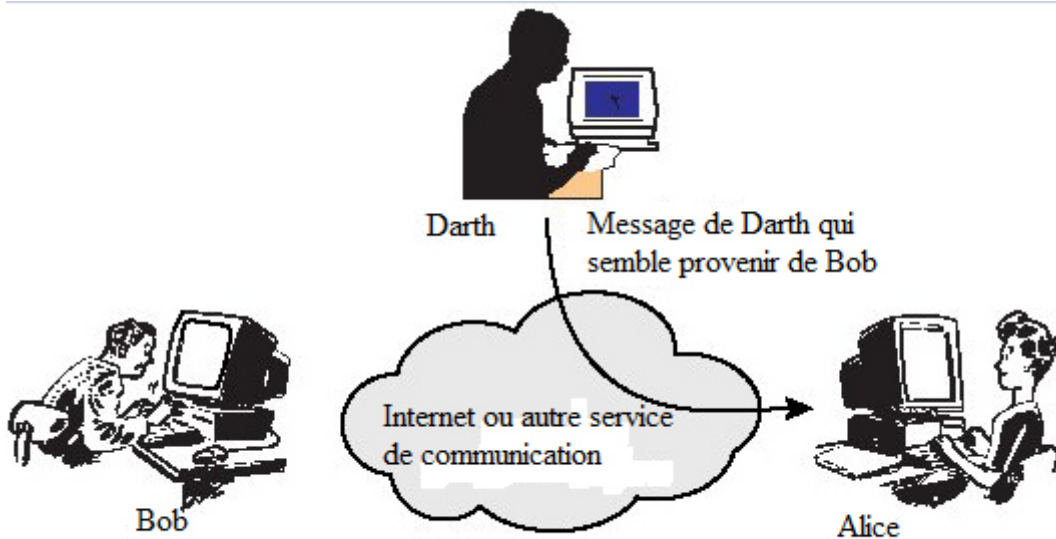


Figure 1.13 Attaque de fabrication [24].

➤ **Attaque de rejeu :**

L'attaquant qui a réussi à intercepter des messages les réémet dans le but d'obtenir des informations ou de perturber la cible de l'attaque. Nous considérons qu'il s'agit d'une attaque sur l'intégrité des messages [22].

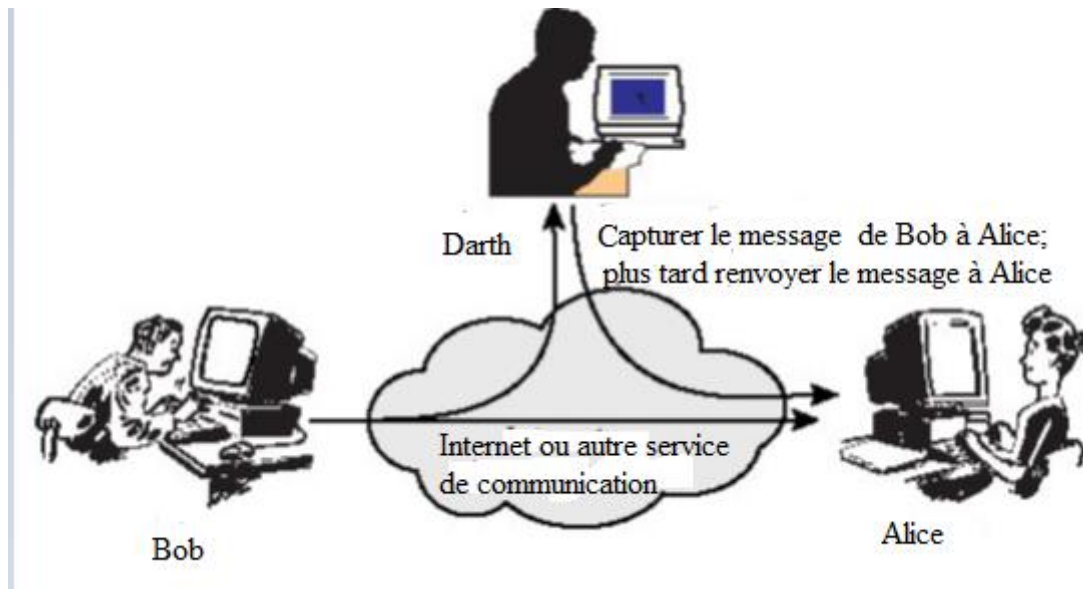


Figure 1.14 Attaque de rejeu [24].

1.4.4 Stratégies de la sécurité informatique

Les stratégies de la sécurité consistent à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans une politique de sécurité. Parmi ces mécanismes, on peut citer :

1.4.4.1 Pare-feu (Firewall)

Le pare-feu est un ensemble de différents composants matériels (physique) et logiciels (logique) qui contrôlent le trafic intérieur/extérieur selon une politique de sécurité.

Un système pare-feu fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines des réseaux, il s'agit ainsi d'une passerelle filtrante [25].

Il permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne, d'autre part, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur. Il propose un véritable contrôle sur le trafic réseau de l'entreprise, Il permet donc d'analyser, de sécuriser et de gérer le trafic réseau [25].

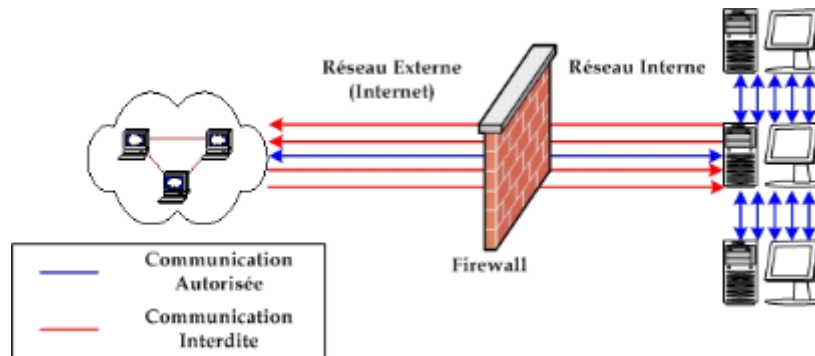


Figure 1.15 Schéma d'une architecture réseau utilisant un Firewall [26].

1.4.4.2 Zone démilitarisée

Une DMZ (Zone Démilitarisée) est une interface située entre un réseau connu (réseau interne) et un réseau externe (internet). Une série de règles de connexion configurées sur le pare-feu font de cette interface une zone physiquement isolée entre les deux réseaux. Cette séparation physique permet d'autoriser les accès internet à destination des serveurs placés dans la DMZ et non à ceux destinés au réseau privé (interne) [27].

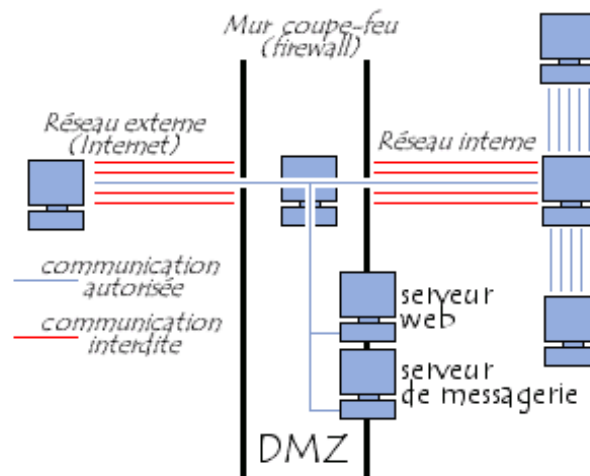


Figure 1.16 DMZ (zone démilitarisée) [28].

1.4.4.3 Systèmes de détection d'intrusion (IDS)

Un système automatisé dont le rôle est la détection des intrusions dans un système informatique tout en examinant les audits de sécurité fournis par le système d'exploitation ou

bien les outils de contrôle du réseau. Son but principal est la détection des utilisations non autorisées, les mauvaises utilisations et les abus dans un système informatique par les utilisateurs internes et externes [29].

Il faut distinguer deux aspects dans le fonctionnement d'un IDS : le mode de détection utilisé et la réponse apportée par l'IDS lors de la détection d'une intrusion [29].

1.4.4.4 Les VLANs

Un VLAN est assimilable à un domaine de diffusion (*Broadcast Domain*). Ceci signifie que toutes les stations du VLAN sont atteintes par cette diffusion. Il regroupe l'ensemble des clients de différente fonction de l'entreprise comme s'ils appartenaient au même réseau. Les communications à l'intérieur du VLAN peuvent être sécurisées et celles entre deux VLAN distincts contrôlées. Ces derniers n'ont été réalisables qu'avec l'apparition des commutateurs [30] [3].

1.4.4.5 La cryptographie

Le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement [29].

Ce principe est généralement lié au principe d'accès conditionnel. Bien que le chiffrement puisse rendre secret le sens d'un document, d'autres techniques cryptographiques sont nécessaires pour communiquer de façon sûre [29].

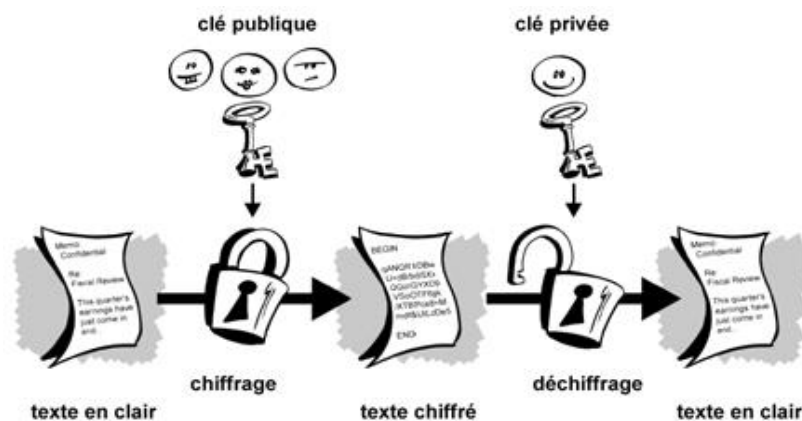


Figure 1.17 La cryptographie [31].

1.4.4.6 Les VPNs

Dans les réseaux informatiques, le réseau privé virtuel (de l'anglais *Virtual Private Network*, abrégé en VPN) permet d'établir des connexions sécurisées privées (un réseau

privé) au travers d'un réseau public comme l'internet. Ils sont sécurisés par des tunnels qui sont mis en place entre les points d'accès du VPN, ces tunnels peuvent être sécurisées en utilisant des tunnels dans lesquels les trames, paquets ou messages sont chiffrés. Les pare-feu sécurisent l'accès au réseau d'utilisateur en empêchant les flux non désirés d'entrer dans le réseau du client du VPN. Les VPN forment une class particulière de réseau partagés [3].

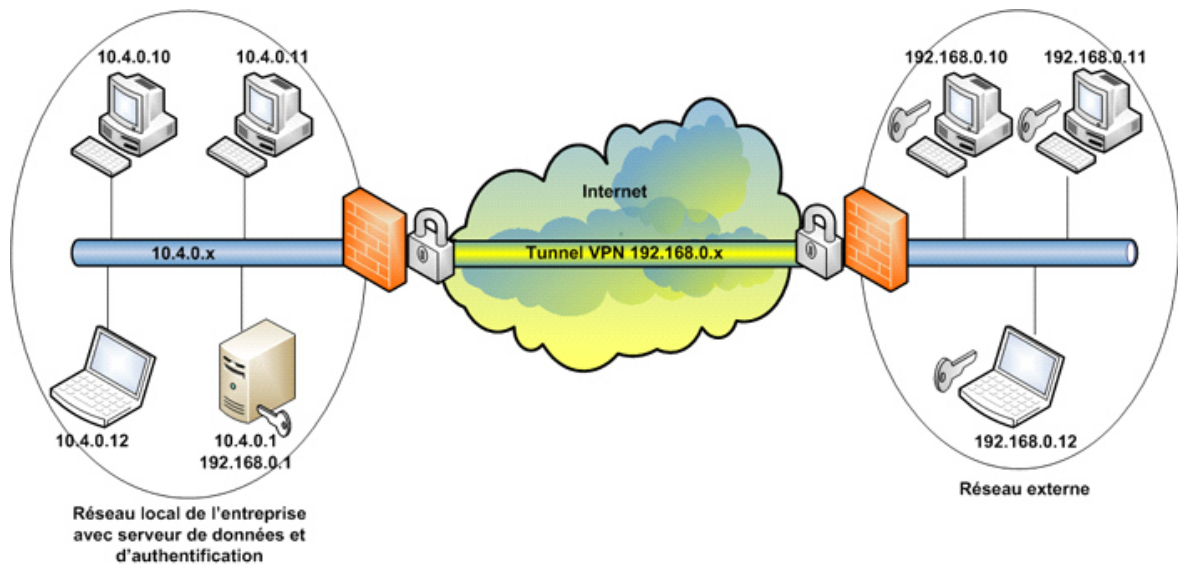


Figure 1.18 Principe de fonctionnement d'un VPN [32].

1.4.4.7 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.

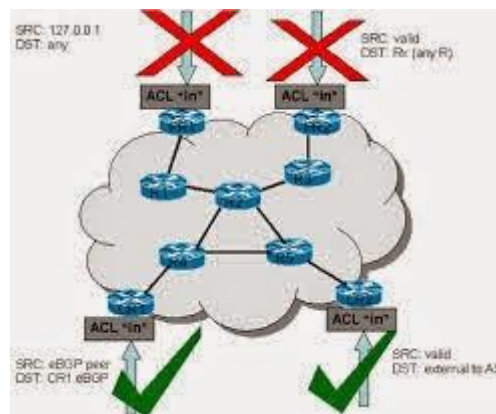


Figure 1.19 ACL [54].

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 [53].

1.5 Conclusion

Au cours de ce chapitre, nous avons présenté les réseaux informatiques, leurs types ainsi que leurs topologies et leurs supports de transmission. Ensuite, nous avons définis les deux modèles de référence OSI et TCP/IP. Par ailleurs, nous avons abordé la sécurité des réseaux informatiques qui est devenue un sérieux besoin et que la majorité des entreprises ne peuvent plus l'ignorer. Enfin, nous avons résumé quelques stratégies de sécurités telles que l'utilisation des VLANs que nous détaillerons dans le chapitre suivant.

Chapitre 2

INTRODUCTION AUX RESEAUX LOCAUX VIRTUELS (VLANs)

2.1 Introduction

Aujourd'hui, une majorité d'entreprises possède leur propre parc de réseau informatique interne sous la forme d'un LAN (Local Area Network) permettant la communication de données d'un pôle d'une entreprise à un autre et se présentant sous la forme d'un ensemble de matériels réseaux (commutateurs, routeurs, etc.) reliés entre eux. Cependant, il est parfois nécessaire de couper quelques-uns de ces liens pour des raisons sécuritaires, c'est à dire, interdire la communication d'un poste à l'autre.

Dans ce chapitre, nous explorons dans un premier temps la mise en place d'un réseau local puis une présentation des réseaux locaux virtuels : leurs caractéristiques, leurs classifications, la communication inter-vlan, ensuite, nous concentrons notre attention sur les types des réseaux locaux virtuels. Nous présenterons quelques avantages des VLANs, puis nous conclurons ce chapitre par la présentation de quelques protocoles utilisés afin de répondre aux besoins de cette technologie.

2.2 Equipement d'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 ? Comment relier des réseaux utilisant des protocoles de communication différents ? Toutes ces questions peuvent être résolues grâce à différents types de matériels qui sont :

1. Répéteur : Un répéteur (repeater) est un dispositif réseau qui travaille au niveau de la couche 1 du modèle OSI, il a comme rôle de régénérer un nouveau signal à partir du signal reçu et la propagation des collisions, il est souvent utilisé pour relier deux segments de réseaux afin d'affranchir des contraintes de distances préconisées dans le standard [30] [33].

2. Pont : Un pont (bridge) est un dispositif qui travaille au niveau de la couche 2 du modèle OSI, il assure la connexion entre les différents réseaux, convertis les formats des données réseau et filtre les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont et il filtre aussi les trafics en utilisant les adresses MAC et interconnecte deux réseaux généralement de même type [30] [33].

3. Routeur : Un routeur (router) est un dispositif de la couche 3 du modèle OSI, il a accès à toutes les informations des couches 1, 2 et 3, il est destiné à relier plusieurs réseaux de technologies différentes, c'est-à-dire qu'il assure le routage des informations à travers l'ensemble des réseaux interconnectés. Il travaille sur les adresses logiques et il utilise les multi protocoles (IP, TCP/IP, AppleTalk) ainsi que des multi interfaces (Ethernet, Token Ring) et il peut régénérer les signaux, concentrer plusieurs connexions, convertir les formats de transmission de données, gérer les transferts de données et se connecter à un réseau étendu [33] [34].

4. Passerelle : Une passerelle (Gateway) est un dispositif permettant d'interconnecter des réseaux de différentes architectures. Elle assure la traduction d'un protocole d'un haut niveau vers un autre et sert notamment à faire l'interface entre des protocoles différents [34].

5. Concentrateur : Un concentrateur (hub) est un dispositif tout comme le répéteur, opère au niveau de la couche physique du modèle OSI, permettant de connecter divers éléments de réseau, il duplique l'information et l'envoie à toutes les machines. C'est pour cela il est parfois appelé répéteur multiports, il n'utilise pas l'adresse IP et l'adresse Mac comme une multiprise quand on branche elle reçoit le signal [34].

6. Commutateur : Un commutateur (Switch) est un dispositif qui est considéré comme un port multiports, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau de la couche 2 du modèle OSI, il analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats (commutation) et permettant de relier divers éléments tout en segmentant le réseau. Le commutateur permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité [33] [34].

7. Adaptateur : un adaptateur (adapter) est un dispositif permettant de connecter un système à un autre, avec une notion de hiérarchie au passage. Eventuellement, l'Adaptateur permet de connecter deux systèmes qui n'avaient pas été conçus pour cela à l'origine [34].

2.3 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 [35].

En effet, dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs), il est possible de s'affranchir

des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.) [35].

2.4 Caractéristiques des VLANs

- Suppriment les contraintes physiques relatives aux communications d'un groupe de travail [36],
- Peuvent couvrir tout un bâtiment, relier plusieurs bâtiments ou encore s'étendre au niveau d'un réseau plus large (WAN) [36],
- Une station peut appartenir à plusieurs VLAN simultanément [36].

2.5 Classification des VLANs

Plusieurs types de VLANs sont définis, selon le critère de commutation et le niveau auquel il s'effectue [37] :

On distingue trois niveaux de VLANs qu'on va définir au-dessous :

2.5.1 VLAN niveau 1

Dans un VLAN de niveau 1, aussi appelé VLAN par port l'appartenance d'une machine (ou ensemble de machines) a un VLAN est définie par le port auquel elle est connectée. Le commutateur est équipé d'une table « port/VLAN » remplie par l'administrateur qui précise le VLAN affecté à chaque port. Dans cette situation toutes machines reliées à un même port (cas d'Ethernet partagé) doivent appartenir au même VLAN. C'est une contrainte qu'il faut gérer lorsque le réseau s'agrandit [37].

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 [39].

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 [39].

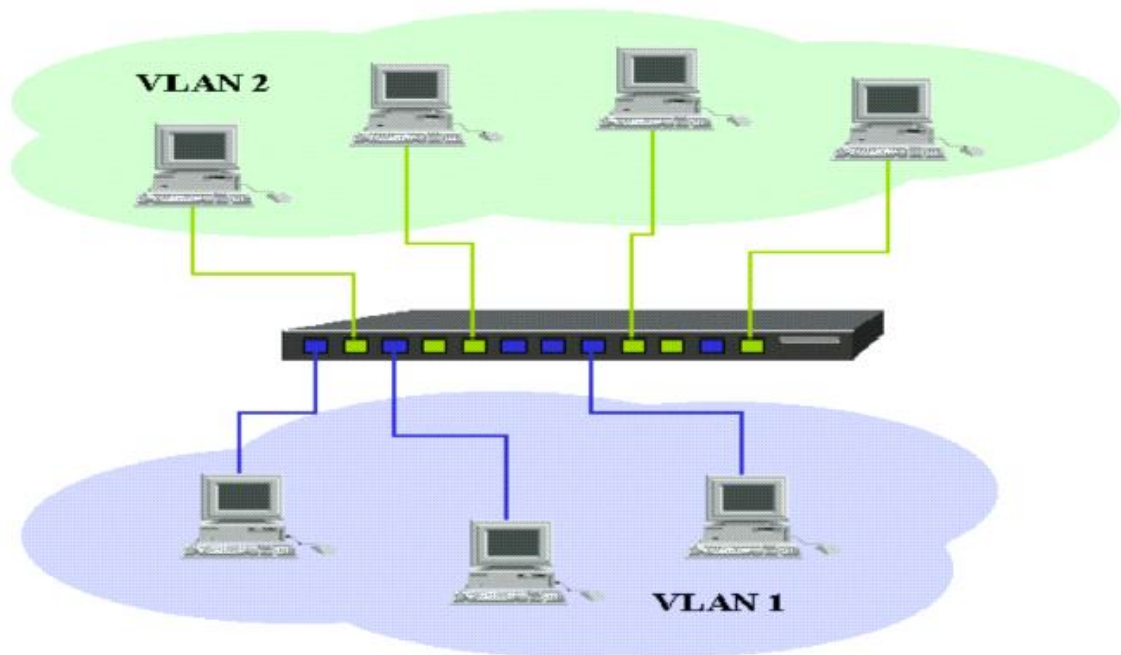


Figure 2.1 Construction des VLANs par port [40].

2.5.2 VLAN niveau 2

Un VLAN de niveau 2 est également appelé VLAN MAC, *VLAN par adresse IEEE* ou en anglais *MAC Address-Based VLAN*. Dans le VLAN niveau 2, l'adresse MAC d'une machine est affectée à un VLAN. En pratique, c'est encore le port qui est affecté à un VLAN, mais de manière dynamique. En effet, l'administrateur saisit dans la table du switch le couple adresse MAC/VLAN. Lorsque le switch découvre sur quel port est connecté la machine, il affecte dynamiquement le port au VLAN. Il gère donc une deuxième table, la table port/VLAN. Cette structure permet également de définir plusieurs VLAN par port à condition d'utiliser le marquage [37].

Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station [41].

L'un des problèmes que posent les réseaux VLAN basés sur les ports est que si le périphérique d'origine est retiré du port pour être remplacé par un autre périphérique, le nouveau périphérique appartiendra au même réseau VLAN que son prédécesseur [41].

Dans l'exemple du réseau VLAN composé d'imprimantes, imaginons qu'une imprimante soit retirée d'un port du commutateur pour être remplacée par un périphérique du service de

comptabilité. Ce dernier dépendra désormais du réseau VLAN des imprimantes. Ceci risque de limiter l'accès du périphérique de comptabilité aux ressources du réseau [41].

Les réseaux VLAN basés sur les adresses MAC permettent de résoudre ce problème. En effet, dans ce cas, l'appartenance au réseau VLAN dépend de l'adresse MAC du périphérique et non du port de commutation physique. Lorsque le périphérique est retiré pour être connecté à un autre port, son appartenance au réseau VLAN le suit. Malheureusement, la corrélation entre les adresses MAC et le numéro VLAN prend pas mal de temps et donc ce type de réseau VLAN est rarement utilisé [37].

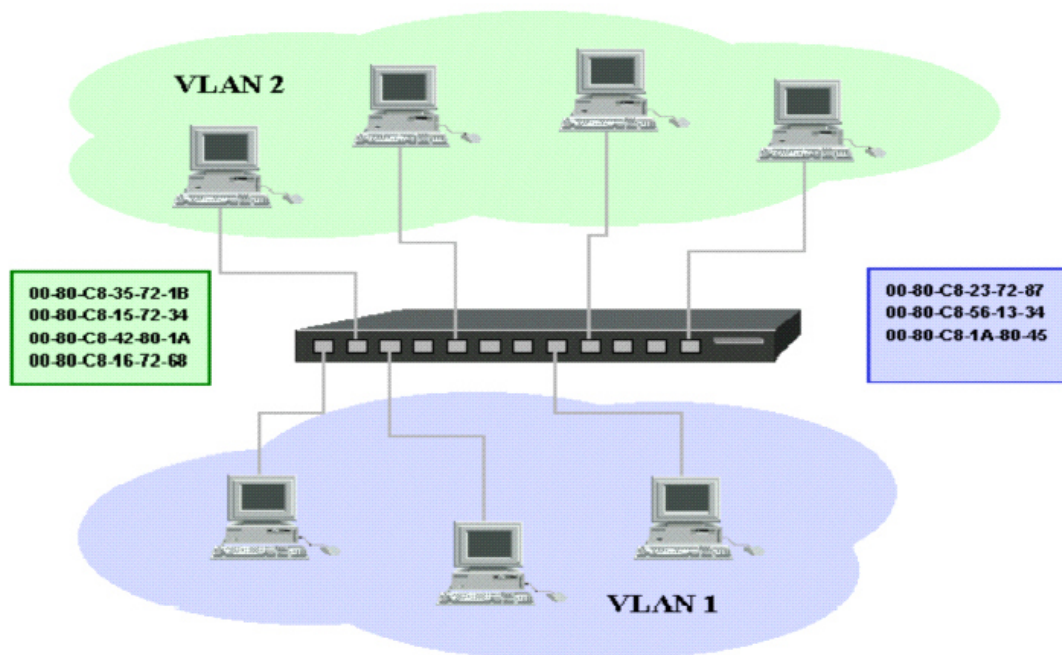


Figure 2.2 Construction des VLANs par MAC [40].

2.5.3 VLAN niveau 3

Un VLAN de niveau 3, on distingue plusieurs types de VLAN de niveau 3 :

- Le VLAN par sous-réseau (en anglais *Network Address-Based VLAN*) associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement [41].

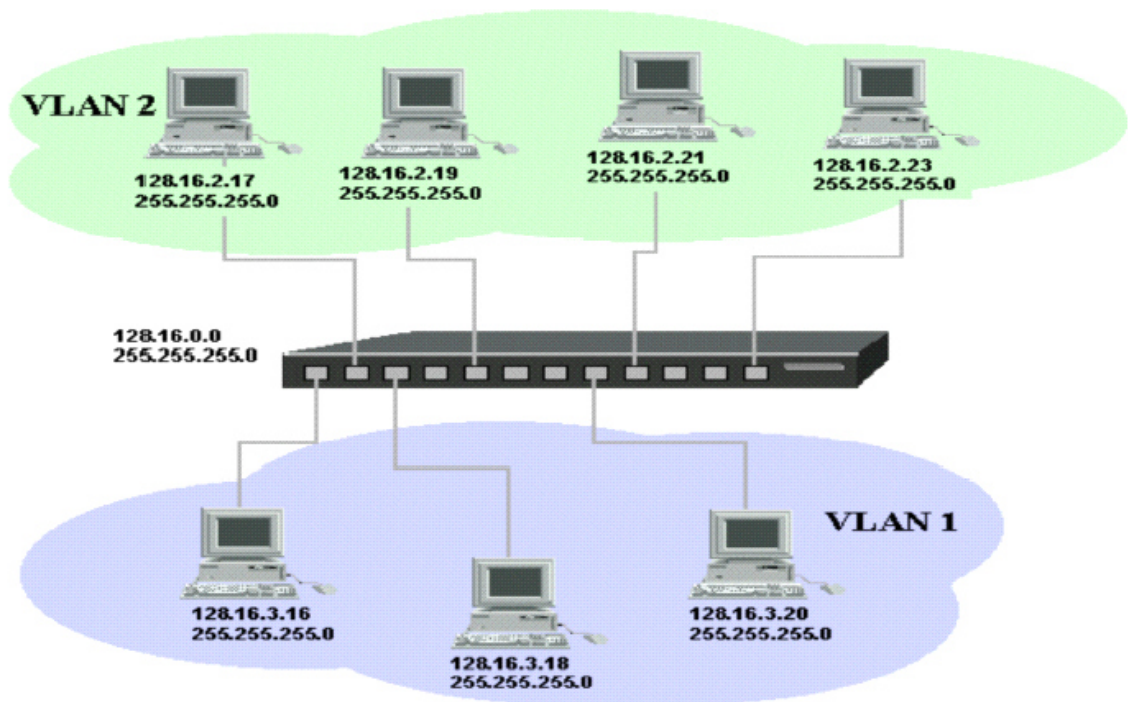


Figure 2.3 Construction des VLANs par sous-réseau [40].

- Le VLAN par protocole (en anglais *Protocol-Based VLAN*) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau [41].

Avec les réseaux VLAN basés sur les protocoles, c'est le protocole de couche 3 transporté par la trame qui permet de déterminer l'appartenance aux réseaux VLAN. Cette méthode peut fonctionner dans un environnement où figurent plusieurs protocoles, mais n'est pas très pratique sur un réseau à prédominance IP [41].

2.6 Communication inter VLAN

Le principe des réseaux locaux virtuels est de limiter la diffusion des informations entre eux. Ce qui rend imperméable la communication entre deux machines situées sur des VLAN différents. Les ports d'interconnexion entre commutateurs supportant les VLANs sont dénommés *trunk*. Cette dénomination permet de prendre en compte de façon particulière la communication inter commutateurs. Cette communication maintient l'isolement entre les VLANs. La seule solution technique permettant de partager des ressources ou d'échanger des données est soit de passer par un routeur qui assurera la communication à l'aide de ses tables de routage, soit de rendre disponibles les ressources aux deux VLANs [42].

2.7 Les avantages des VLANs

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique. Par conséquent, il offre les avantages suivants [43] :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs [43],
- Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées [43],
- Réduction de la diffusion du trafic sur le réseau [43],
- Réduction des messages de diffusion (notamment les requêtes ARP) limités à l'intérieur d'un VLAN. Ainsi les diffusions d'un serveur vont être limitées aux clients de ce serveur [43],
- Création de groupes de travail indépendants de l'infrastructure physique, possibilité de déplacer la station sans changer de réseau virtuel [43],
- Augmentation de la sécurité par le contrôle des échanges inter-VLAN utilisant des routeurs (filtrage possible du trafic échangé entre les VLANs) [43],
- 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 [43],
- Amélioration de la sécurité du réseau en isolant les utilisateurs accédant aux données et applications sensibles [43],
- Division d'un réseau en réseaux logiques plus petits. Le risque de tempête de diffusion est ainsi moins important [43].

2.8 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'autres tirent leur nom en raison de la nature ou d'une fonction spécifique du VLAN effectuée. La section suivante décrit les types de VLAN communs [36] [45].

2.8.1 VLAN de données

Un VLAN de données (peut être nommé en tant que VLAN utilisateur) est configuré pour ne transporter que le trafic généré par l'utilisateur. L'importance de la séparation des données utilisateur à partir de tout autre type de VLAN est la gestion du commutateur et un contrôle adéquat [44].

2.8.2 VLAN par défaut

Le VLAN par défaut est le VLAN auquel sont, par défaut, associées les trames et les ports s'il n'y a pas de configuration spécifique sur le matériel, lorsque la mise en œuvre des VLAN est réalisée. Généralement le VLAN par défaut est le VLAN 1. Lors de la mise en œuvre des VLAN sur un matériel au moins un VLAN doit être défini, d'où la nécessité du VLAN par défaut [44].

2.8.3 VLAN natif

La notion de VLAN natif entre en compte dans le cas d'association de VLAN par port. Cela correspond au PVID sur port trunk. Ainsi lorsqu'une trame non tagguée arrive sur un port trunk, elle sera associée à un VLAN en fonction du PVID du port. On dit alors que la trame est associée au VLAN natif du port. En résumé, le VLAN natif observe et identifie le trafic provenant de chaque extrémité de lien trunk [44].

2.8.4 VLAN de gestion

Un VLAN de gestion est tout VLAN configuré 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 défini 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 [36].

2.8.5 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 minimales (150-180 millisecondes) [36].

2.9 Protocoles de transport des VLANs

2.9.1 Notion du TRUNK

Pour communiquer entre plusieurs réseaux locaux virtuels et assurer la répartition de ces derniers sur plusieurs équipements, il est nécessaire d'élaborer une technique de partage des réseaux locaux entre équipements. Cette technique consiste à étiqueter les trames pour identifier le trafic des différents réseaux locaux sur un même canal physique. Ainsi, les réseaux locaux sont distribués sur les différents équipements via des liaisons logiques dédiées appelées *trunks*. Le *trunk* est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels. Les trames qui traversent le *trunk* sont complétées avec un identificateur de réseau local virtuel (VLAN id). Grâce à cette identification, les trames sont conservées dans un même VLAN (ou domaine de diffusion) [45].

Les *trunks* peuvent être utilisés :

- **Entre deux commutateurs**

C'est le mode de distribution des réseaux locaux le plus courant. C'est la solution du second problème énoncé ci-dessus [45].

- **Entre un commutateur et un hôte**

C'est le mode de fonctionnement à surveiller étroitement. Un hôte qui supporte le *trunking* a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels [45].

- **Entre un commutateur et un routeur**

C'est le mode de fonctionnement qui permet d'accéder aux fonctions de routage ; donc à l'interconnexion des réseaux virtuels par routage inter-VLAN. C'est la solution du premier problème énoncé ci-dessus [45].

2.9.2 Norme 802.1Q

Le protocole IEEE 802.1Q est un protocole normalisé par L'IEEE (il fonctionne sur tous les équipements.). Il est de nos jours le protocole le plus utilisé pour faire du *trunking*. Le principe consiste à ajouter dans l'entête de la trame Ethernet un marqueur qui va identifier le VLAN. Il existe quelques solutions propriétaires pour réaliser ceci, mais le système s'est avéré tellement intéressant qu'une norme a été définie, il s'agit de la norme 802.1Q [45].

La norme 802.1Q rajoute deux champs à l'entête de protocole de niveau 2 appelés tag. Voici l'exemple d'une trame Ethernet pour laquelle les champs TPID et TCI ont été ajoutés [46].

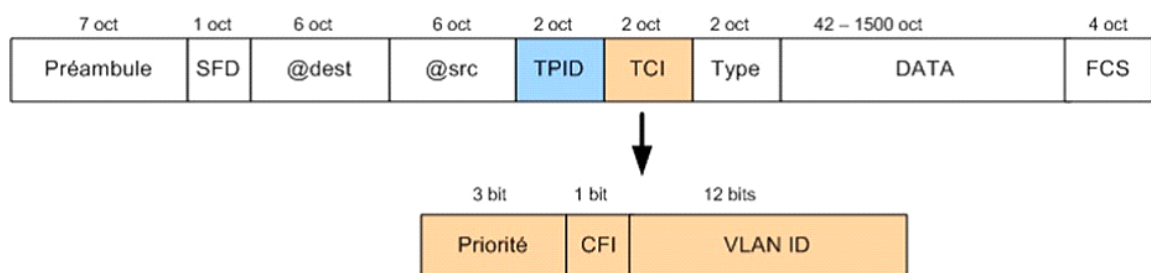


Figure 2.4 Extension de la trame Ethernet modifiée par la norme 802.1Q [47].

- **Le champ TPID (*Tag Protocol Identifier*)**

C'est la partie qui détermine le type du tag (0x8100 pour 802.1Q) ce champ est utilisé pour prévoir des évolutions futures afin de pouvoir utiliser le principe du *tagging* pour différentes fonctionnalités [46].

- **Le champ TCI (*Tag Control Information*)**

Cette partie se décline en plusieurs éléments :

- **Priorité** : niveaux de priorité définis par l'IEEE 802.1P. Ce champ permet de réaliser une priorisation des flux. Le champ étant sur trois bits il est possible de déterminer 7 niveaux de priorité [46].
- **CFI** : Ce bit permet de déterminer si le tag s'applique à une trame de type Ethernet ou Token-Ring [46].
- **VID** : VLAN identifier. C'est l'identifiant du VLAN. L'appartenance d'une trame à un VLAN se fait grâce à cet identifiant. Le champ étant sur 12 bits, il est donc possible de déclarer jusqu'à 4096 VLANs. (Les valeurs 0 et FFF sont réservés) [46].

2.9.3 Protocole ISL (Inter Switch Link Protocol)

Le protocole ISL est un protocole propriétaire Cisco (il ne peut être utilisé qu'entre équipements Cisco) qui date d'avant la création du protocole IEEE 802.1Q. ISL encapsule complètement la trame Ethernet en ajoutant un en-tête et une queue, en laissant la trame initiale intacte. L'en-tête ISL contient un champ identifiant du VLAN et l'adresse MAC de la trame, permettant d'acheminer le paquet vers le routeur et les commutateurs appropriés [42].

Lorsqu'elle atteint le réseau destination, l'en-tête est supprimé et la trame est acheminée vers l'équipement récepteur [42].

2.10 Protocoles de gestion des VLANs

2.10.1 Protocole VTP

Pour éviter de redéfinir tous les VLANs existant sur chaque commutateur, Cisco a développé un protocole permettant un héritage de VLANs entre commutateur. 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 [48].

- **Principe**

Un commutateur doit alors être déclaré en serveur, on lui attribue également un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifié ou supprimé. Ainsi chaque commutateur client présent dans le domaine héritera automatiquement des nouveaux VLANs créés 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 qu'agréable dans un environnement abondamment commuté et comprenant de multiples VLANs. Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants [48] :

- **Mode serveur** : dans lequel le commutateur est chargé de diffuser la configuration aux commutateurs du domaine VTP [48].
- **Mode client VTP** : dans lequel le commutateur applique la configuration émise par un commutateur en mode serveur [48].
- **Mode transparent** : dans lequel le commutateur ne fait que diffuser, sans prendre en compte, la configuration du domaine VTP auquel il appartient [48].

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

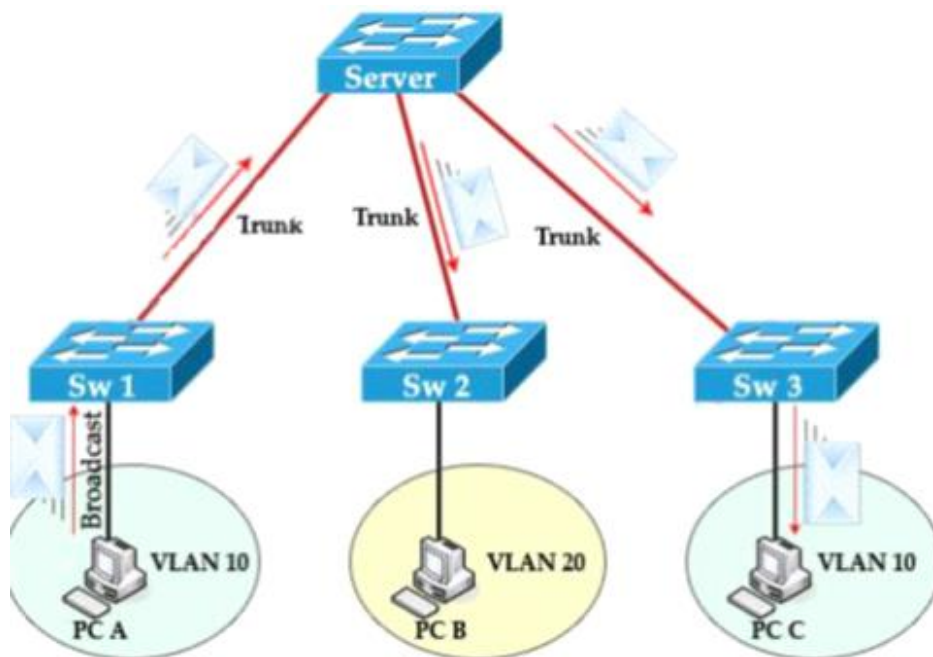


Figure 2.5 Fonctionnement du protocole VTP [48].

2.10.2 Protocole VMPS

La gestion de VLANs est devenue fastidieuse, il a alors fallu trouver une solution pour automatiser cette gestion. Le VMPS est un service, créé par Cisco, chargé de faire correspondre un VLAN à une (ou plusieurs) adresse MAC et s'impose donc comme la solution [14].

- **Principe**

Pour que le VMPS fonctionne bien comme il faut, ce dernier nécessite des commutateurs qui doivent être de la marque Cisco et un serveur VMPS. Pour ce faire, toutes les machines qui sont connectées au commutateur envoient leurs adresse MAC dans la trame IP, puis ce dernier récupère cette adresse et envoi au serveur VMPS une requête pour indiquer à quel VLAN mettre cette machine. Le serveur répond au commutateur, qui met le port concerné dans le VLAN proposé. Donc les machines auront les fonctionnalités disponibles dans ce VLAN [49]. Ce principe est schématisé dans la figure suivante :

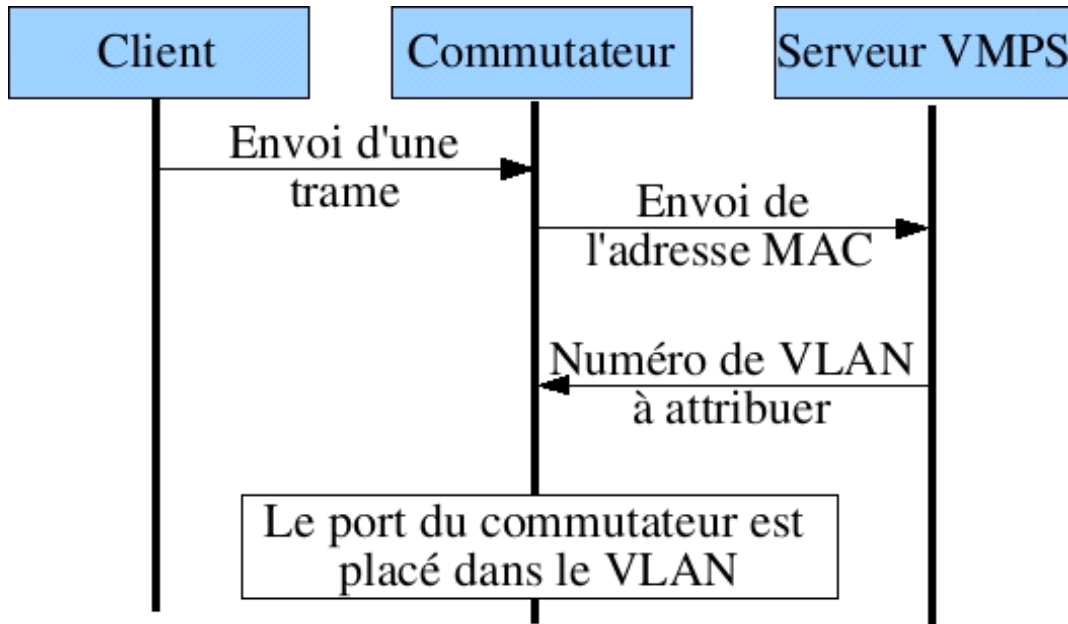


Figure 2.6 Principe de fonctionnement de VMPS [49].

2.11 Conclusion

Nous avons vu tout au long de ce chapitre que la technologie des VLANs est vaste et qu'elle ajoute beaucoup de propriétés aux réseaux locaux comme la sécurité des réseaux et la mobilité des utilisateurs ... En fait, cette technologie est une nouvelle manière de mettre à profit la technique de la commutation pour donner plus de flexibilité aux réseaux locaux tout en gardant une sécurité assez fiable et moins coûteuse au sein de l'entreprise.

Après avoir étudié l'architecture actuelle du réseau local d'AGRANA, et après avoir vu en théorie les VLANs dans les chapitres précédents, nous allons implémenter notre solution proposée qui consiste à créer de différents VLANs en exposant les différentes configurations nécessaires, tout cela sera abordé dans le chapitre suivant.

Chapitre 3

**ETUDE DE
L'EXISTANT ET
REALISATION
DE LA
SOLUTION**

3.1 Introduction

Dans ce dernier chapitre, on va présenter notre cas d'étude 'AGRANA' dans la première partie. Tout d'abord on va présenter l'organisme d'accueil, sa situation géographique, son organisme et ces différents équipements. Et puis au final on va étudier leur existant pour qu'on puisse donner une solution aux problèmes rencontrés.

Dans la deuxième partie, on va présenter le simulateur Packet Tracer, puis on va entamer la dernière étape qui est la réalisation de notre travail où on va implémenter la solution proposée.

3.2 Présentation général

3.2.1 Présentation de l'organisme d'accueil

AGRANA ou ex ELAFRUITTS est le leader mondial des préparations de fruits. Possède des usines sur les 5 continents. AGRANA Fruit est déjà implantée dans 21 pays avec 29 sites de production. En Algérie, ils ont un usine située á Akbou, en charge de livrer le marché local ainsi que d'effectuer des exports dans les pays proches. Avec l'acquisition de 49% des actions d'ELAFRUITTS.

3.2.2 Situation géographique

AGRANA Algérie est implantée dans une zone industrielle « TAHARACHET » véritable carrefour économique de Bejaia, de quelque 70 unités de productions agroalimentaire et en cours d'expansion. La figure ci-dessous nous montre la situation géographique d'AGRANA.

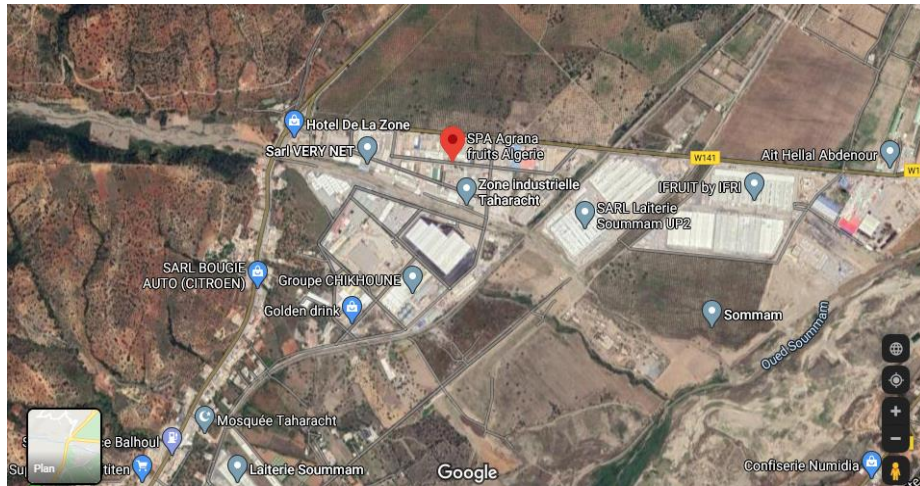


Figure 3.1 Situation géographique d'AGRANA FRUIT ALGERIE.

3.2.3 Organigramme de l'unité

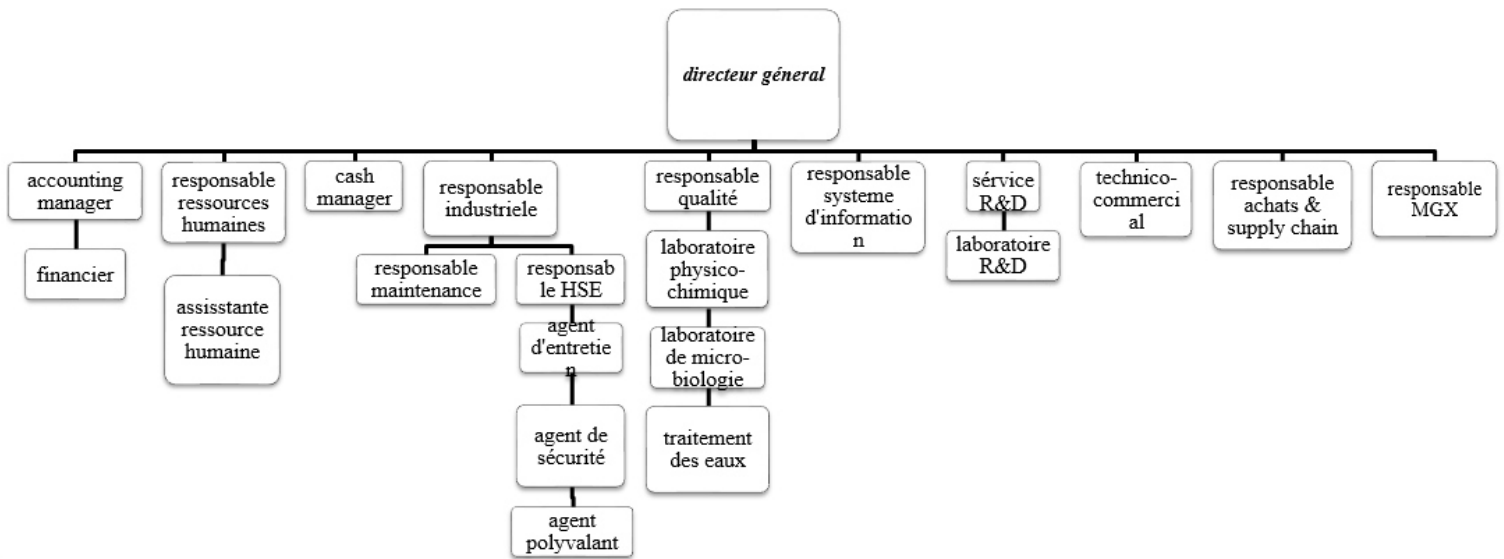


Figure 3.2 Organigramme d'AGRANA.

3.2.4 Présentation des équipements du réseau d'AGRANA

Le réseau d'AGRANA se compose de :

- ✓ 43 Ordinateurs.
- ✓ 3 Commutateurs.
- ✓ 10 Imprimantes.
- ✓ 6 Point d'Accès.
- ✓ 1 Routeur.
- ✓ 2 Pare-feu.
- ✓ 1 Modem.
- ✓ 6 Serveurs.
- ✓ 2 Capteurs d'Empreinte.

3.3 Contexte du projet à réaliser

3.3.1 Présentation du projet

Notre projet intitulé 'Configuration et simulation des VLANs, cas d'étude : AGRANA', qui ce dernier consiste à créer et configurer des VLANs afin de bien gérer, organiser et sécuriser le réseau d'AGRANA.

3.3.2 Problématique

Après avoir analysé le réseau d'AGRANA nous avons remarqué une surcharge très grande au niveau des commutateurs, une forte utilisation de la bande passante à cause de la mal organisation des équipements de l'entreprise et aussi le manque de sécurité dans le réseau.

Alors comment peut on faire pour résoudre ces problèmes ?

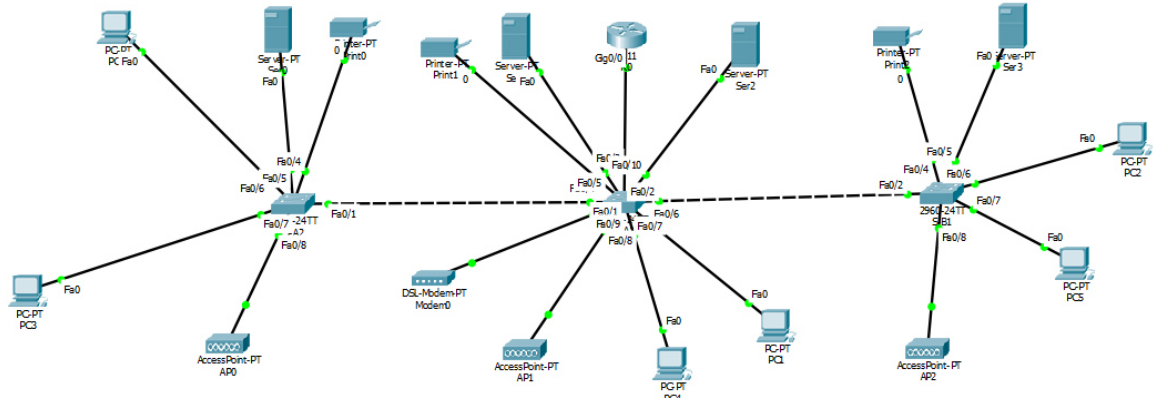


Figure 3.3 Architecture du réseau AGRANA sans VLAN et Pare-feu.

3.3.3 Objectif du projet à réaliser

Notre objectif principal est de remédier aux problèmes rencontrés dans le réseau d'AGRANA et d'essayer de trouver une solution optimale pour la gestion du réseau local du district.

3.3.4 Solution proposée

Comme nous avons vu dans la problématique, le réseau a comme problème le mal organisation, l'utilisation abusé de la bande passante et le manque de sécurité. Alors pour régler ce problème nous avons pensé à créer des VLANs qui vont regrouper les équipements qui ont les mêmes propriétés ou qui sont de la même nature et renforcer la sécurité en ajoutant des pare-feu et des listes de contrôles d'accès (ACL) au niveau du Routeur.

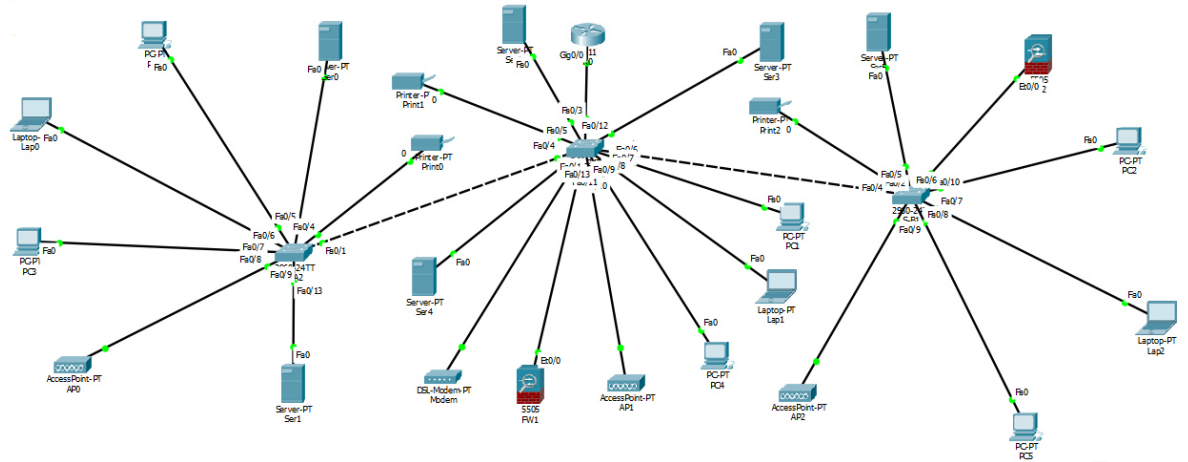


Figure 3.4 Architecture du réseau AGRANA avec VLAN et Pare-feu.

Dans ce qui suit on va entamer la deuxième partie de notre chapitre qui est la simulation de notre réseau d'étude.

3.4 Présentation du simulateur Cisco Packet Tracer

C'est un outil pédagogique (logiciel) et simulateur de réseau. Il 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 Networking Academy). Il est développé pour concevoir, configurer, dépanner et visualiser le trafic réseau dans un environnement de programmes simulé et contrôlé.

Packet Tracer permet 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 pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc. [51].

3.4.1 Description générale de l'interface principale du Packet Tracer

Cette interface est décomposée en une barre de menu classique (zone 2), une barre d'outils principale (zone 3) ainsi que d'autres éléments comme la zone de travail (zone 1), les types d'appareillages (les routeurs, les commutateurs, les câbles (câble console, câble droit, fibre optique, ...), les concentrateurs, ...) (zone 8), les différents modèles d'appareils (zone 7), l'ensembles des outils (outil de sélection, redimensionner la forme,...) (zone 4), La zone (5) permet d'ajouter des indications dans le réseau. Enfin, la zone (6) permet de passer du mode temps réel au mode simulation [50]. Cette interface est illustrée dans la figure ci-après :

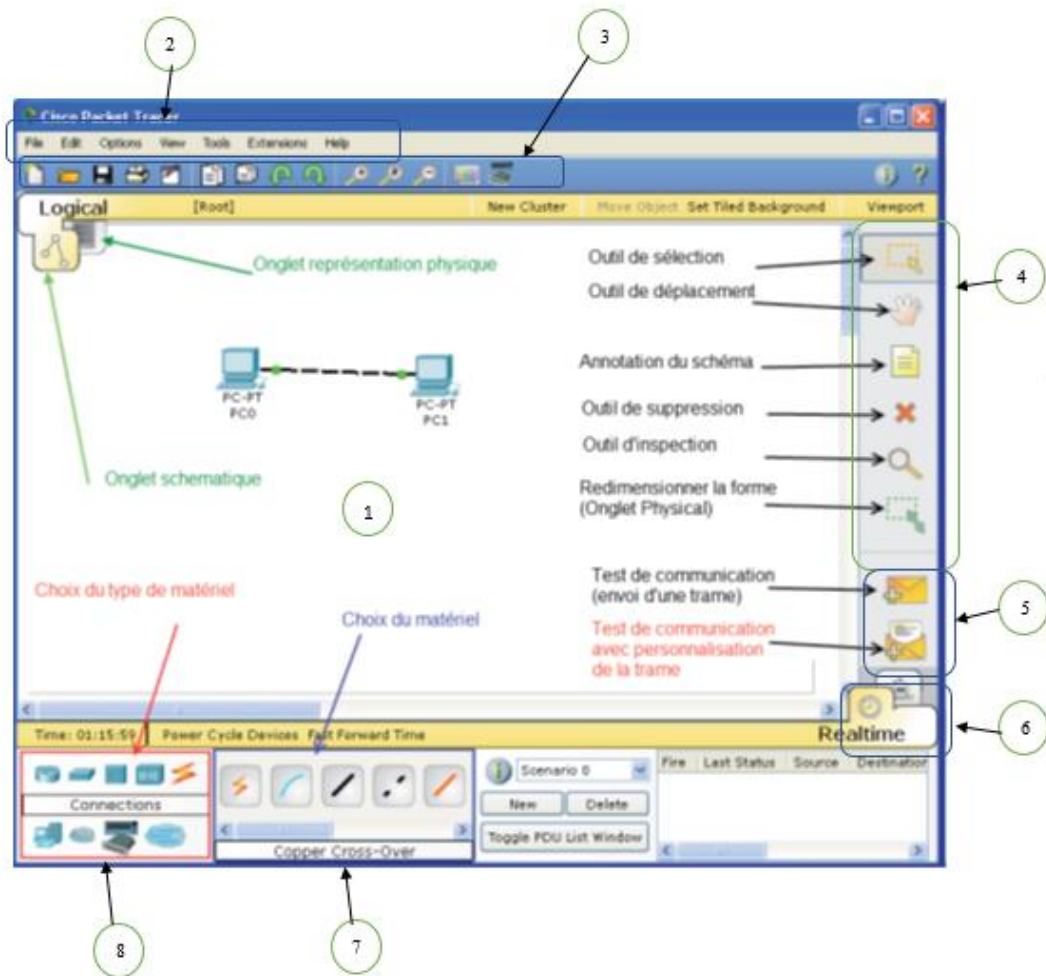


Figure 3.5 Description générale de l'interface principale du Packet Tracer [50].

➤ Paramétrage des appareils

Pour accéder au paramétrage d'un appareil, il faut cliquer sur ce dernier. Deux ou trois onglets sont accessibles avec la fenêtre qui apparait [50] :

✓ Paramétrage physique (Physical)

Le paramétrage physique consiste à placer les bonnes cartes dans l'appareil [50].

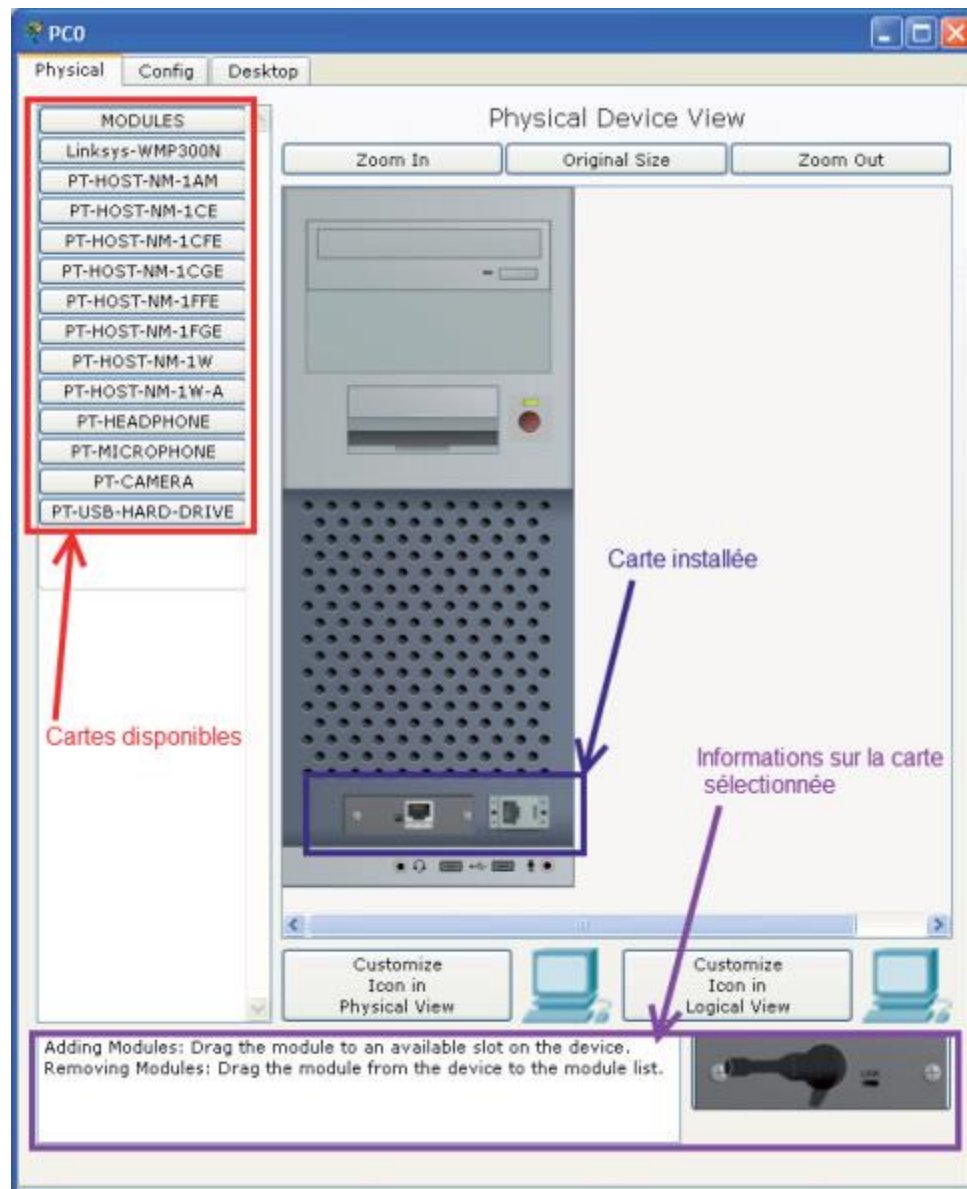


Figure 3.6 Paramétrage physique du l'équipement [50].

✓ Configuration

L'onglet 'Config' permet de configurer essentiellement les paramètres réseau de l'équipement sélectionné. Les boutons situés à gauche de la fenêtre déterminent le groupe de paramètres à configurer [50].

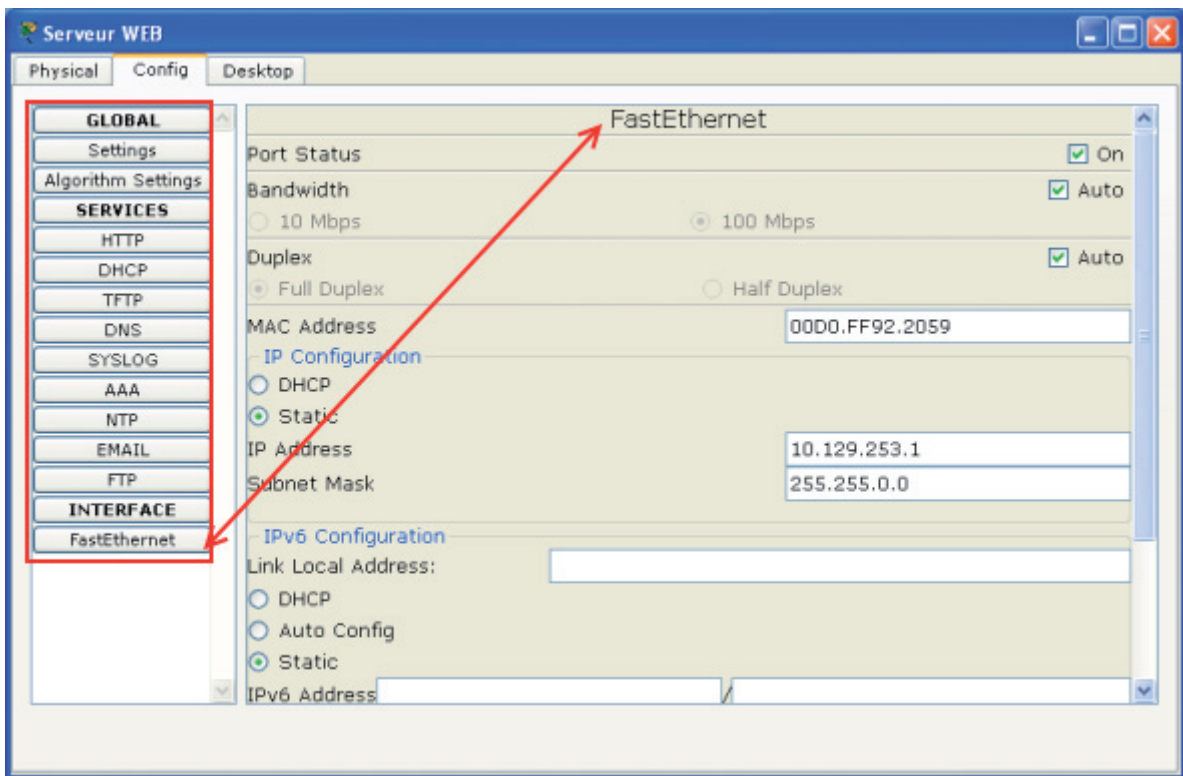


Figure 3.7 Fenêtre de configuration de l'équipement [50].

✓ Desktop

L'onglet Desktop permet de configurer tous les outils logiciels habituels des équipements [50].

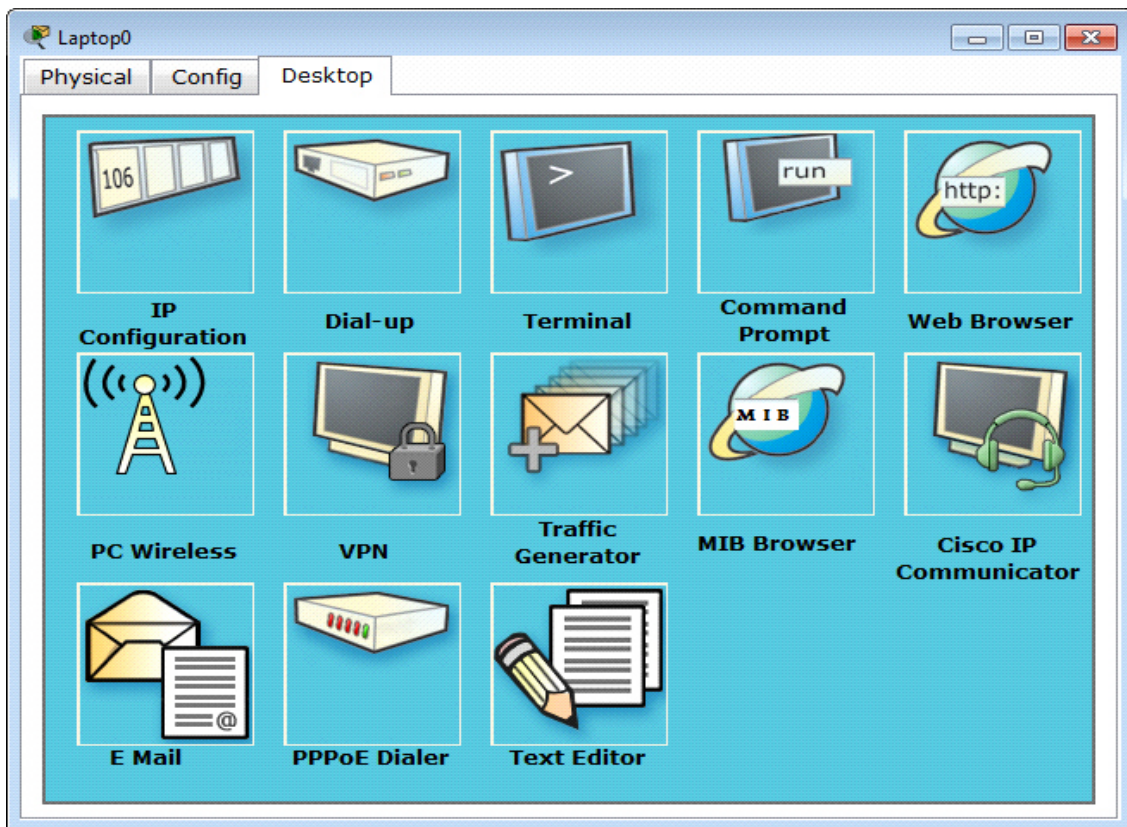


Figure 3.8 Fenêtre Desktop du l'équipement [50].

3.4.2 Fonctionnement du Simulateur Packet Tracer

Le simulateur fonctionne sous deux différents aspects. Il permet ainsi de visualiser l'état du réseau en deux points de vue distincts.

3.4.2.1 L'espace de travail logique (Logical work space)

C'est dans cette partie du logiciel qu'on passe beaucoup de temps, car il permet de créer et de configurer le réseau qu'on étudie [50] [51].

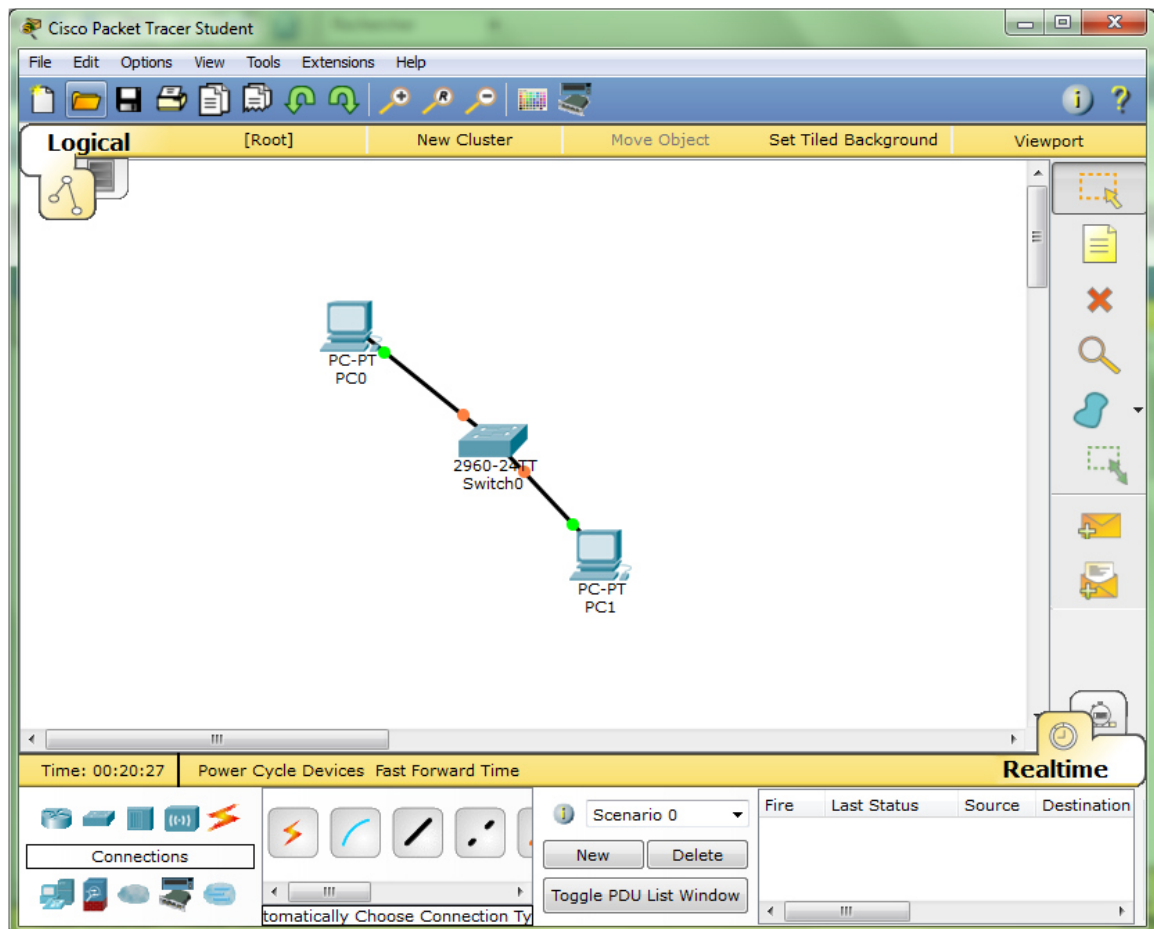


Figure 3.9 Espace de travail logique.

3.4.2.2 L'espace de travail physique (Physical Work Space)

Le but de la zone de travail physique est de donner une dimension physique de la topologie logique du réseau. Cette espace de travail est divisée en 4 couches pour illustrer 4 environnements dans le cas réel [50] [51].

- **L'interurbain** : L'espace interurbain permet de visualiser les connexions à longue distance, c'est-à-dire dans une superficie vaste [50] [51].

Une zone Interurbain peut contenir plusieurs villes [50] [51].

- **Ville** : Chaque ville peut contenir plusieurs bâtiments [50] [51].
- **Bâtiment** : Dans chaque bâtiment on trouve les étages où sont rangés les différents compartiments pour placer les cabinets [50] [51].

Les cabinets sont présentés par l'existence d'une étagère pour le rangement des équipements [50] [51].

- **Cabinet de câblage :** Le cabinet de câblage contient les dispositifs permettant de ranger les équipements et de les interconnecter [50] [51].
- Le Simulateur propose aussi deux modes de fonctionnements qui reflètent l'arrangement en temps du réseau. On peut voir ainsi le fonctionnement direct d'une simulation et les étapes de transmission des informations dans le réseau [50] [51].

3.4.2.3 Mode temps réel

Dans ce mode le réseau fonctionne dans un modèle à temps réel. Le réseau répond immédiatement aux actions qu'on lui exerce et fonctionne exactement comme dans un vrai réseau (en tenant compte les notions de temps) [50] [51].

3.4.2.4 Mode simulation

Dans ce mode on peut voir le réseau en mode opérationnel, le but est de montrer son fonctionnement qui on peut le visualiser à un rythme lent. C'est-à-dire l'administrateur peut visualiser les chemins et les paquets échangés toute au long de la simulation [50] [51].

3.5 Configuration

3.5.1 Adressage des différents VLANs

Nous avons quatre VLANs qu'on site au tableau ci-dessous:

Ce tableau présente le dimensionnement de notre réseau au niveau des VLANs.

Nom de VLAN	ID VLAN	Adresse de sous réseau	Description
Vlan-gestion	9	192.168.9.10/24	Vlan qui fait la gestion.
Vlan-serveur	3	192.168.10.0/24	Vlan qui regroupe les serveurs.
Vlan-pc-authentifier	4	192.168.11.0/24	Vlan qui regroupe les pcs authentifiés.

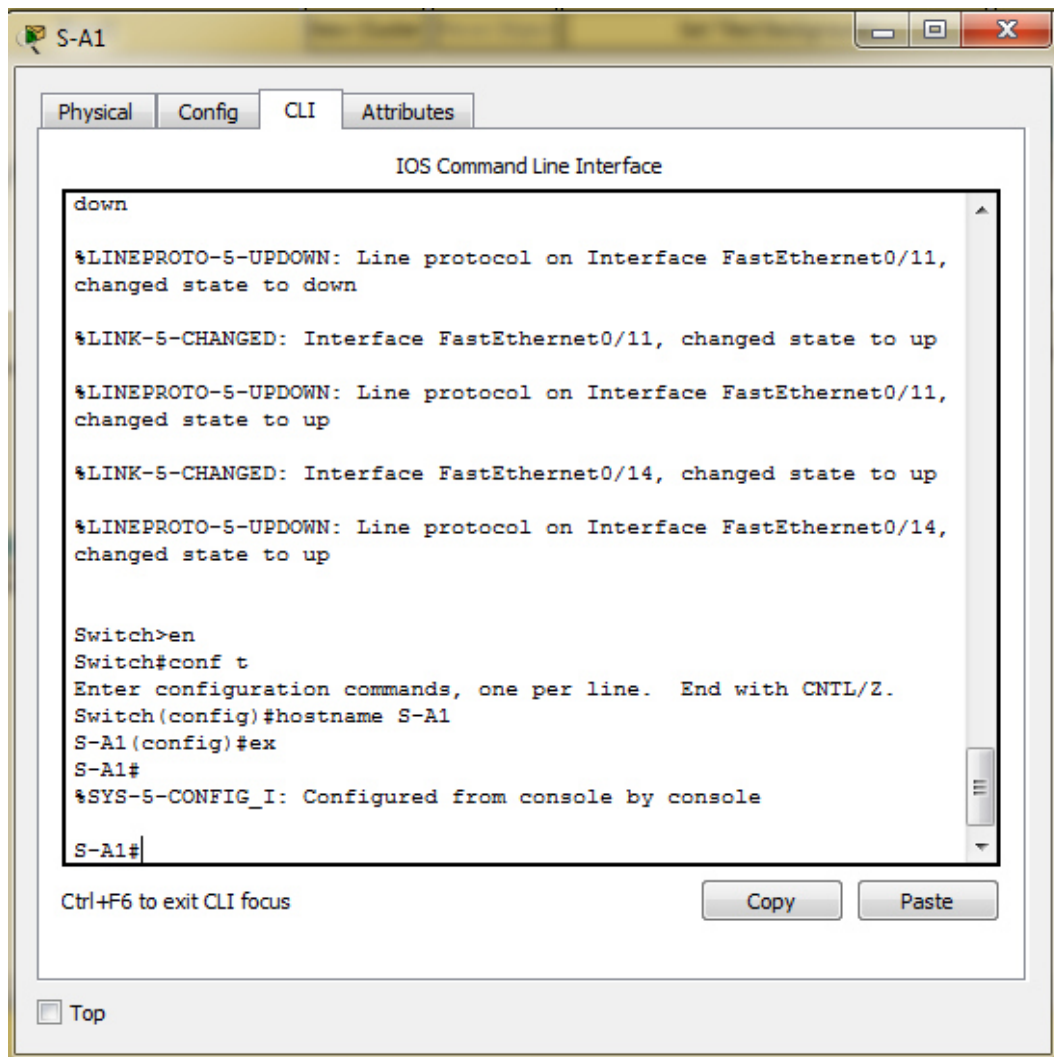
Vlan-pc-non-authentifier	5	192.168.12.0/24	Vlan qui regroupe les pcs non authentifiés.
Vlan-printer.	6	192.168.13.0/24	Vlan qui regroupe les imprimantes.
Vlan-point-acces	7	192.168.14.0/24	Vlan qui regroupe les points d'accès.
Vlan-pare-feu	8	192.168.15.0/24	Vlan qui regroupe les pare-feu.

Figure 3.10 Adressage des VLANs.

3.5.2 Configurations des commutateurs

3.5.2.1 Configuration du Hostname

Cette configuration a pour but de renommer les commutateurs par des noms significatifs. Nous prendrons comme exemple le Switch1, sachant que c'est la même procédure pour les autres commutateurs.



```
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11,
changed state to down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11,
changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/14,
changed state to up

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S-A1
S-A1(config)#ex
S-A1#
%SYS-5-CONFIG_I: Configured from console by console

S-A1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

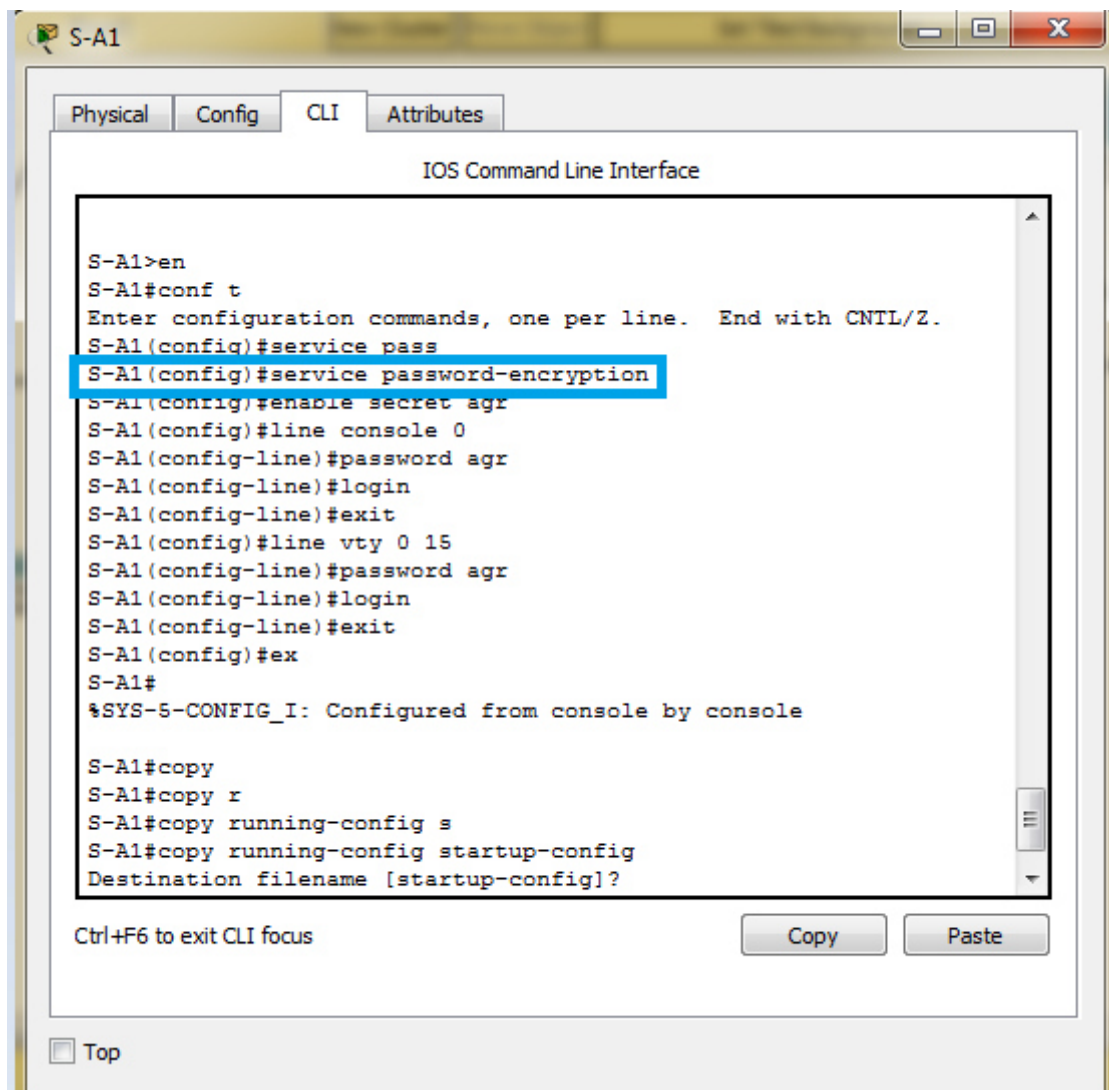
Figure 3.11 Configuration du Hostname du Switch S-A1.

3.5.2.2 Configuration d'une sécurité de base

Maintenant nous allons passer à la configuration des mots de passe.

➤ Chiffrer les mots de passe

Nous allons premièrement chiffrer les mots de passe en clair à l'aide de la commande service password-encryption.



```
S-A1>en
S-A1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S-A1(config)#service pass
S-A1(config)#service password-encryption
S-A1(config)#enable secret agr
S-A1(config)#line console 0
S-A1(config-line)#password agr
S-A1(config-line)#login
S-A1(config-line)#exit
S-A1(config)#line vty 0 15
S-A1(config-line)#password agr
S-A1(config-line)#login
S-A1(config-line)#exit
S-A1(config)#ex
S-A1#
%SYS-5-CONFIG_I: Configured from console by console

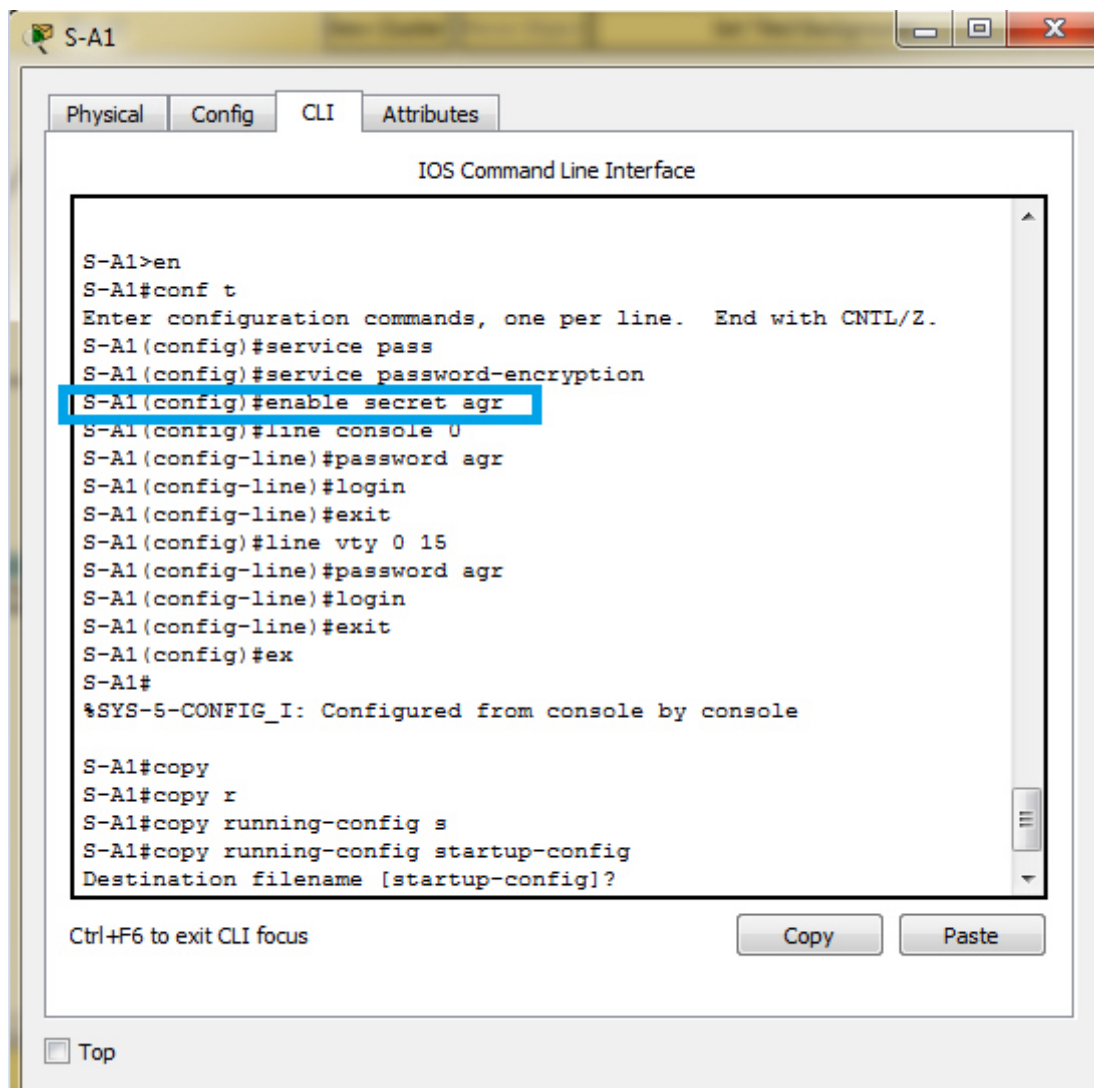
S-A1#copy
S-A1#copy r
S-A1#copy running-config s
S-A1#copy running-config startup-config
Destination filename [startup-config]?

Ctrl+F6 to exit CLI focus
```

Figure 3.12 Chiffrement du mot de passe.

➤ **Sécuriser l'accès à la ligne console**

Nous avons choisi « agr » comme mot de passe via console, l'exemple que nous prendrons est le Switch1. La figure 3.12 montre les commandes de mise en place du mot de passe. La même chose sera faite pour les autres commutateurs.



```
S-A1>en
S-A1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S-A1(config)#service pass
S-A1(config)#service password-encryption
S-A1(config)#enable secret agr
S-A1(config)#line console 0
S-A1(config-line)#password agr
S-A1(config-line)#login
S-A1(config-line)#exit
S-A1(config)#line vty 0 15
S-A1(config-line)#password agr
S-A1(config-line)#login
S-A1(config-line)#exit
S-A1(config)#ex
S-A1#
%SYS-5-CONFIG_I: Configured from console by console

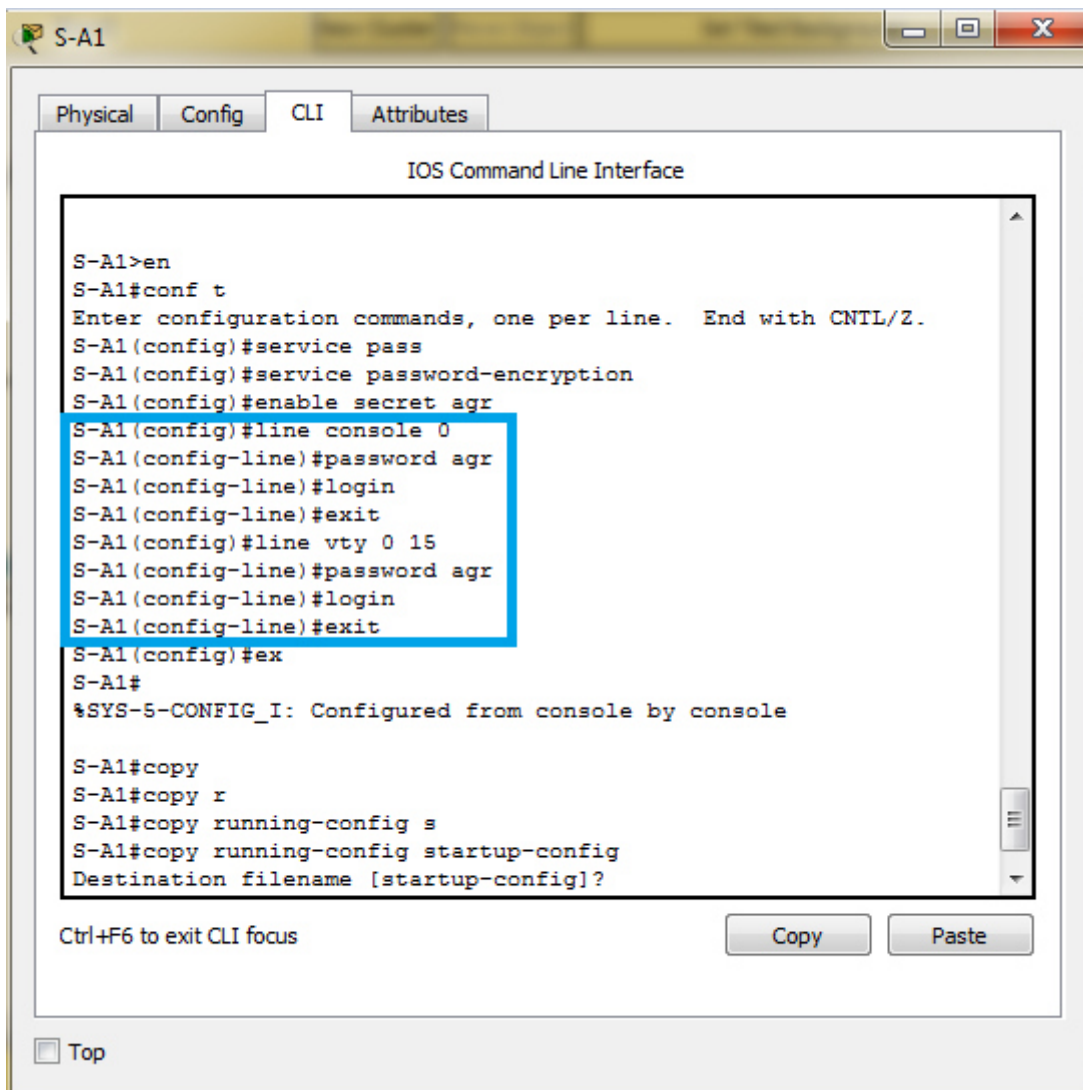
S-A1#copy
S-A1#copy r
S-A1#copy running-config s
S-A1#copy running-config startup-config
Destination filename [startup-config]?

Ctrl+F6 to exit CLI focus
```

Figure 3.13 Mot de passe secret.

➤ **Configurez un mot de passe chiffrer 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 « agr » en tant que mot de passe secret actif.



```
S-A1>en
S-A1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S-A1(config)#service pass
S-A1(config)#service password-encryption
S-A1(config)#enable secret agr
S-A1(config)#line console 0
S-A1(config-line)#password agr
S-A1(config-line)#login
S-A1(config-line)#exit
S-A1(config)#line vty 0 15
S-A1(config-line)#password agr
S-A1(config-line)#login
S-A1(config-line)#exit
S-A1(config)#ex
S-A1#
%SYS-S-CONFIG_I: Configured from console by console

S-A1#copy
S-A1#copy r
S-A1#copy running-config s
S-A1#copy running-config startup-config
Destination filename [startup-config]?
```

Ctrl+F6 to exit CLI focus

Copy Paste

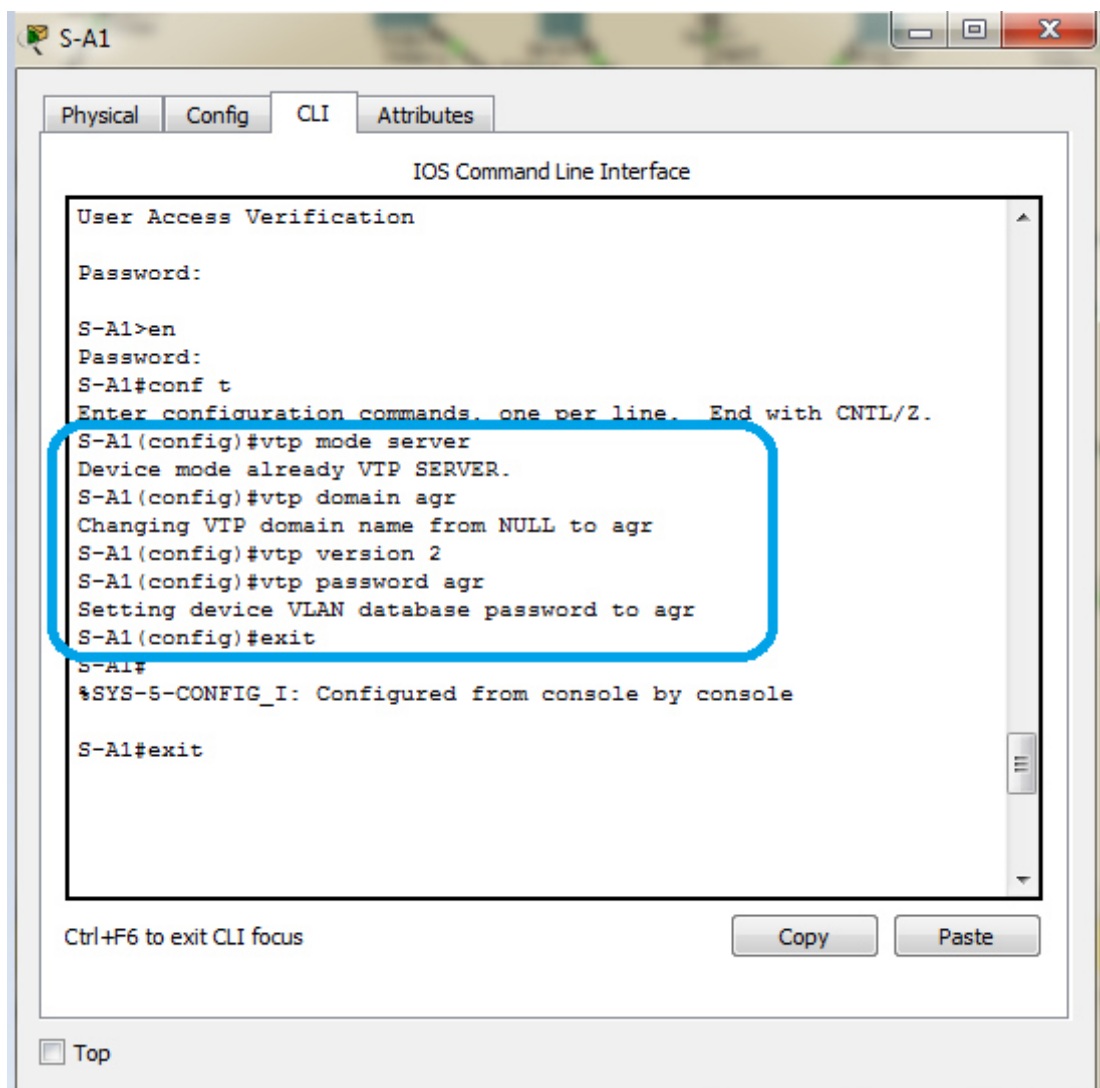
Top

Figure 3.14 Attribution du mot de passe console au Switch S-A1.

3.5.2.3 Configuration du protocole VTP (VLAN Trunking Protocol)

Maintenant nous allons configurer le protocole VTP :

- ✓ **Mode server**



The screenshot shows a terminal window titled 'S-A1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following sequence of commands and responses:

```
User Access Verification

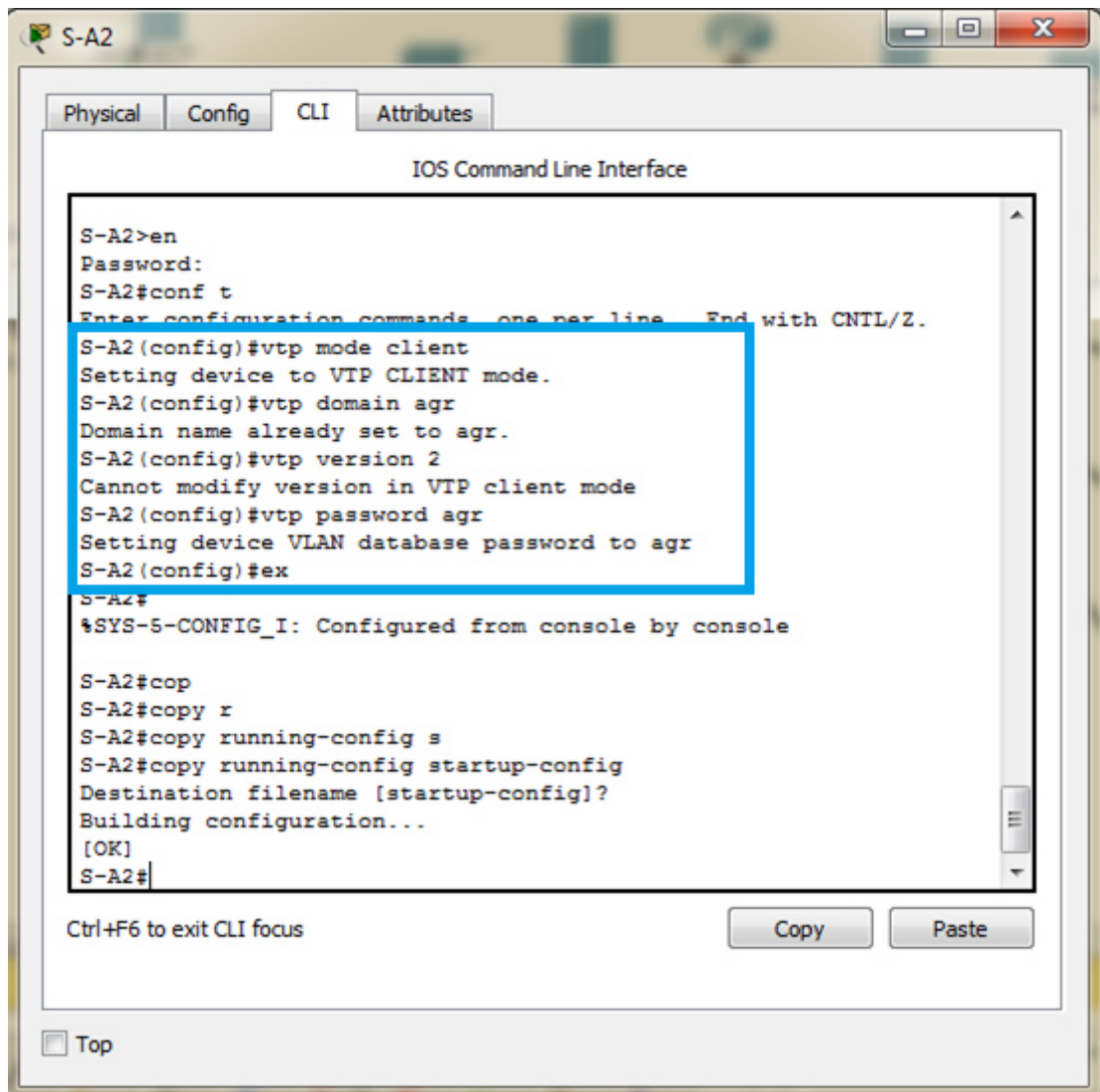
Password:

S-A1>en
Password:
S-A1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S-A1(config)#vtp mode server
Device mode already VTP SERVER.
S-A1(config)#vtp domain agr
Changing VTP domain name from NULL to agr
S-A1(config)#vtp version 2
S-A1(config)#vtp password agr
Setting device VLAN database password to agr
S-A1(config)#exit
S-A1#
%SYS-5-CONFIG_I: Configured from console by console

S-A1#exit
```

A blue rounded rectangle highlights the configuration commands: `vtp mode server`, `vtp domain agr`, `vtp version 2`, and `vtp password agr`. At the bottom of the terminal window, there is a prompt 'Ctrl+F6 to exit CLI focus' and two buttons labeled 'Copy' and 'Paste'. A 'Top' button is also visible at the bottom left of the window.

Figure 3.15 Configuration du VTP Server.

✓ **Mode client**

The screenshot shows a terminal window titled "S-A2" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and responses:

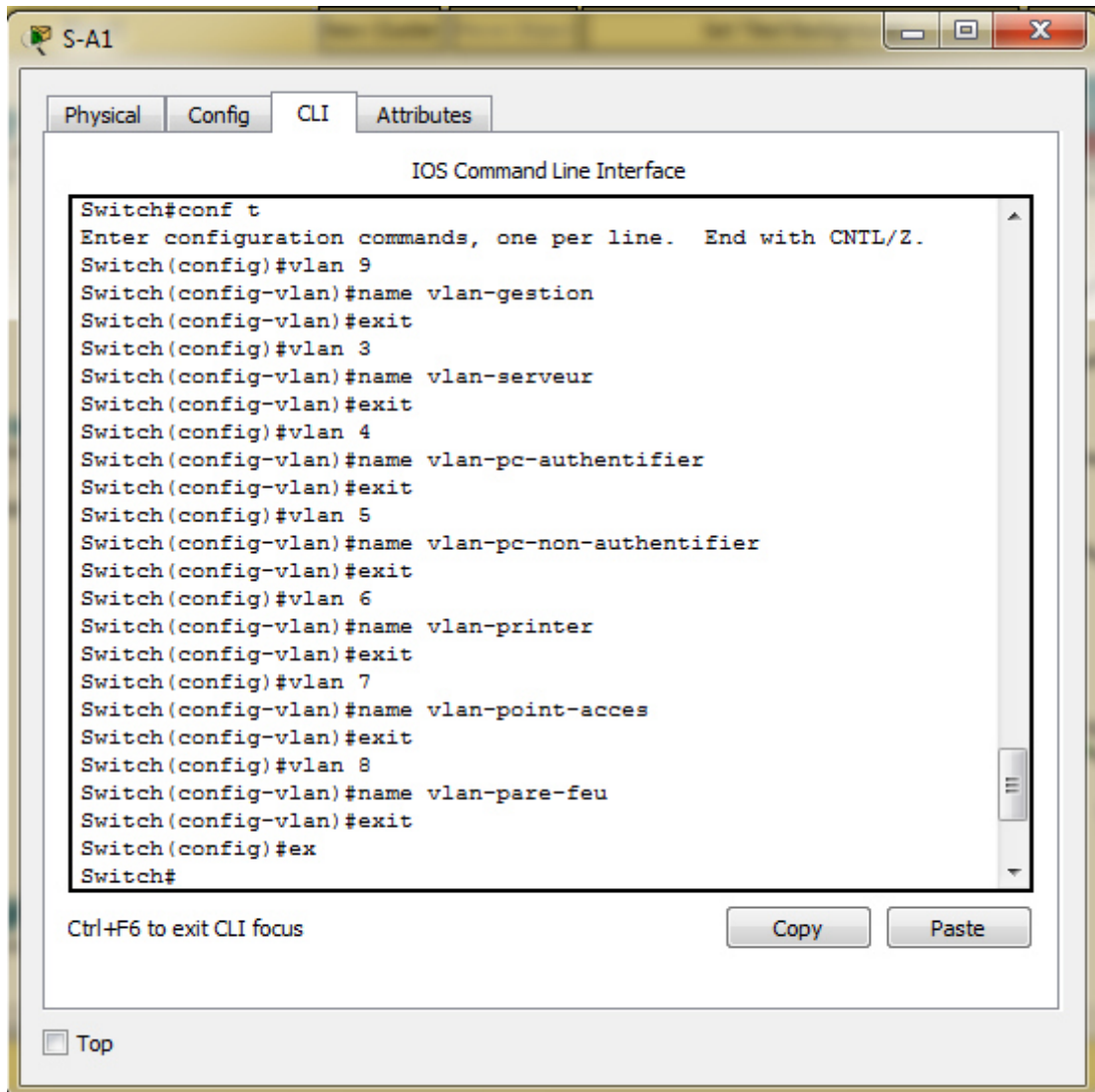
```
S-A2>en
Password:
S-A2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S-A2(config)#vtp mode client
Setting device to VTP CLIENT mode.
S-A2(config)#vtp domain agr
Domain name already set to agr.
S-A2(config)#vtp version 2
Cannot modify version in VTP client mode
S-A2(config)#vtp password agr
Setting device VLAN database password to agr
S-A2(config)#ex
S-A2#
%SYS-5-CONFIG_I: Configured from console by console

S-A2#cop
S-A2#copy r
S-A2#copy running-config s
S-A2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S-A2#
```

At the bottom of the window, there is a "Ctrl+F6 to exit CLI focus" message, "Copy" and "Paste" buttons, and a "Top" button.

Figure 3.16 Configuration du VTP Client.

3.5.2.4 Création des VLANs



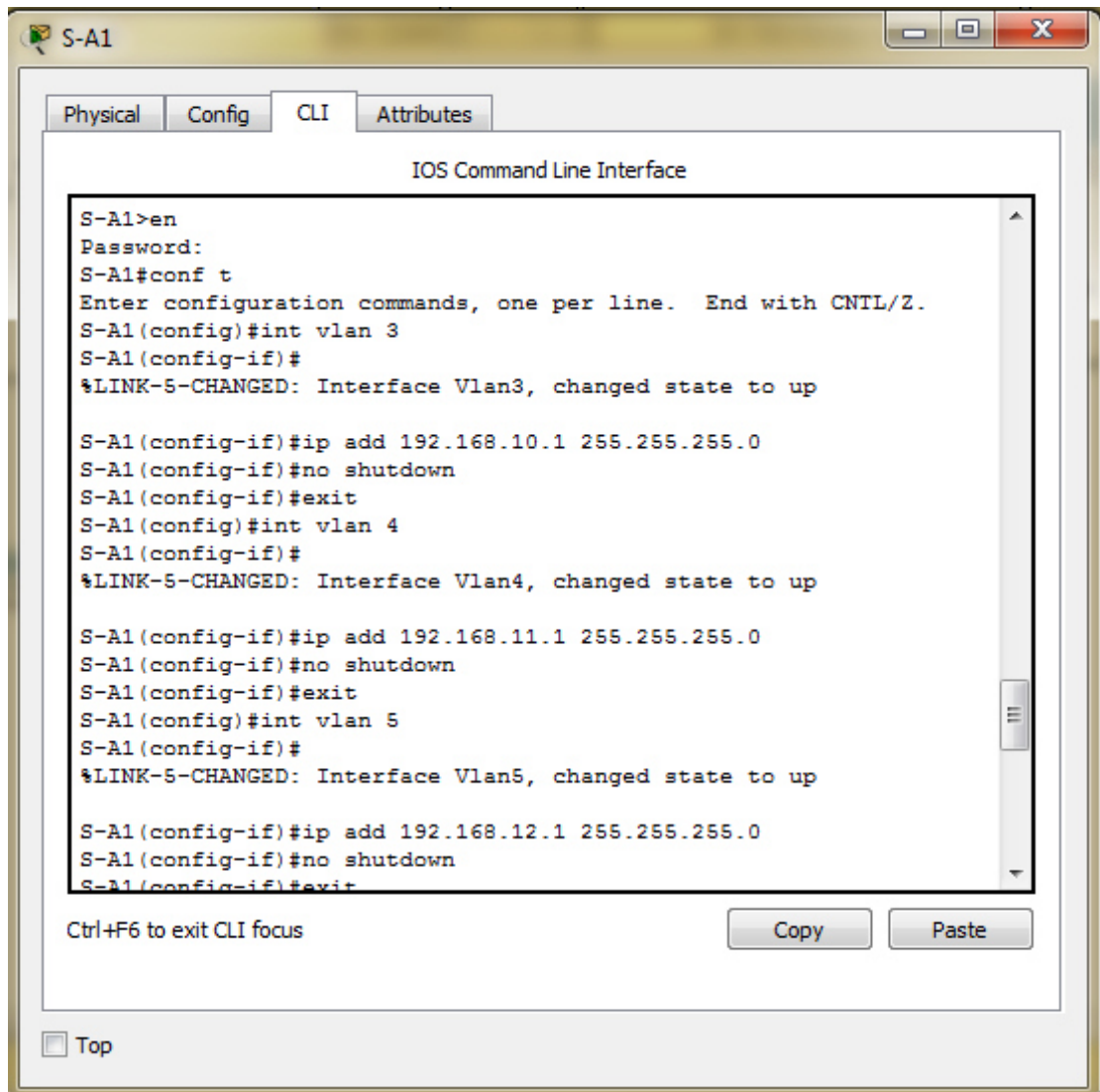
The screenshot shows a window titled 'S-A1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following commands and responses:

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 9
Switch(config-vlan)#name vlan-gestion
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name vlan-serveur
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name vlan-pc-authentifier
Switch(config-vlan)#exit
Switch(config)#vlan 5
Switch(config-vlan)#name vlan-pc-non-authentifier
Switch(config-vlan)#exit
Switch(config)#vlan 6
Switch(config-vlan)#name vlan-printer
Switch(config-vlan)#exit
Switch(config)#vlan 7
Switch(config-vlan)#name vlan-point-acces
Switch(config-vlan)#exit
Switch(config)#vlan 8
Switch(config-vlan)#name vlan-pare-feu
Switch(config-vlan)#exit
Switch(config)#ex
Switch#
```

At the bottom of the CLI window, there is a prompt 'Ctrl+F6 to exit CLI focus' and two buttons labeled 'Copy' and 'Paste'. A 'Top' button is also visible at the bottom left of the window.

Figure 3.17 Création des VLANs dans le Switch S-A1.

3.5.2.5 Configuration des VLANs



```
S-A1>en
Password:
S-A1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S-A1(config)#int vlan 3
S-A1(config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

S-A1(config-if)#ip add 192.168.10.1 255.255.255.0
S-A1(config-if)#no shutdown
S-A1(config-if)#exit
S-A1(config)#int vlan 4
S-A1(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

S-A1(config-if)#ip add 192.168.11.1 255.255.255.0
S-A1(config-if)#no shutdown
S-A1(config-if)#exit
S-A1(config)#int vlan 5
S-A1(config-if)#
%LINK-5-CHANGED: Interface Vlan5, changed state to up

S-A1(config-if)#ip add 192.168.12.1 255.255.255.0
S-A1(config-if)#no shutdown
S-A1(config-if)#exit
```

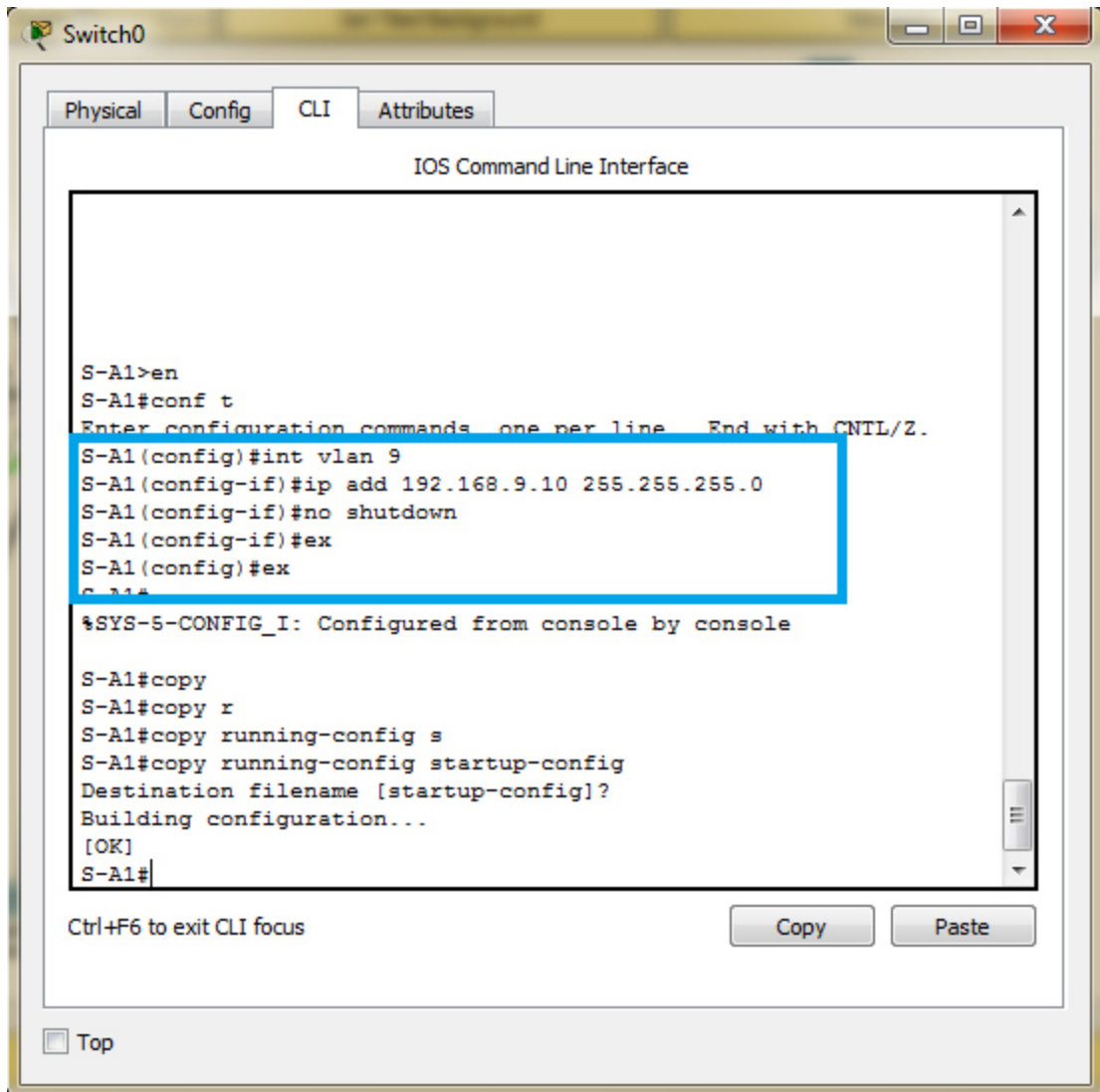
Ctrl+F6 to exit CLI focus

Copy Paste

Top

Figure 3.18 Configuration des VLANs dans le Switch S-A1.

3.5.2.6 Configuration de l'adresse du Vlan 9 dans le switch S-A1



The screenshot shows a window titled "Switch0" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following commands and responses:

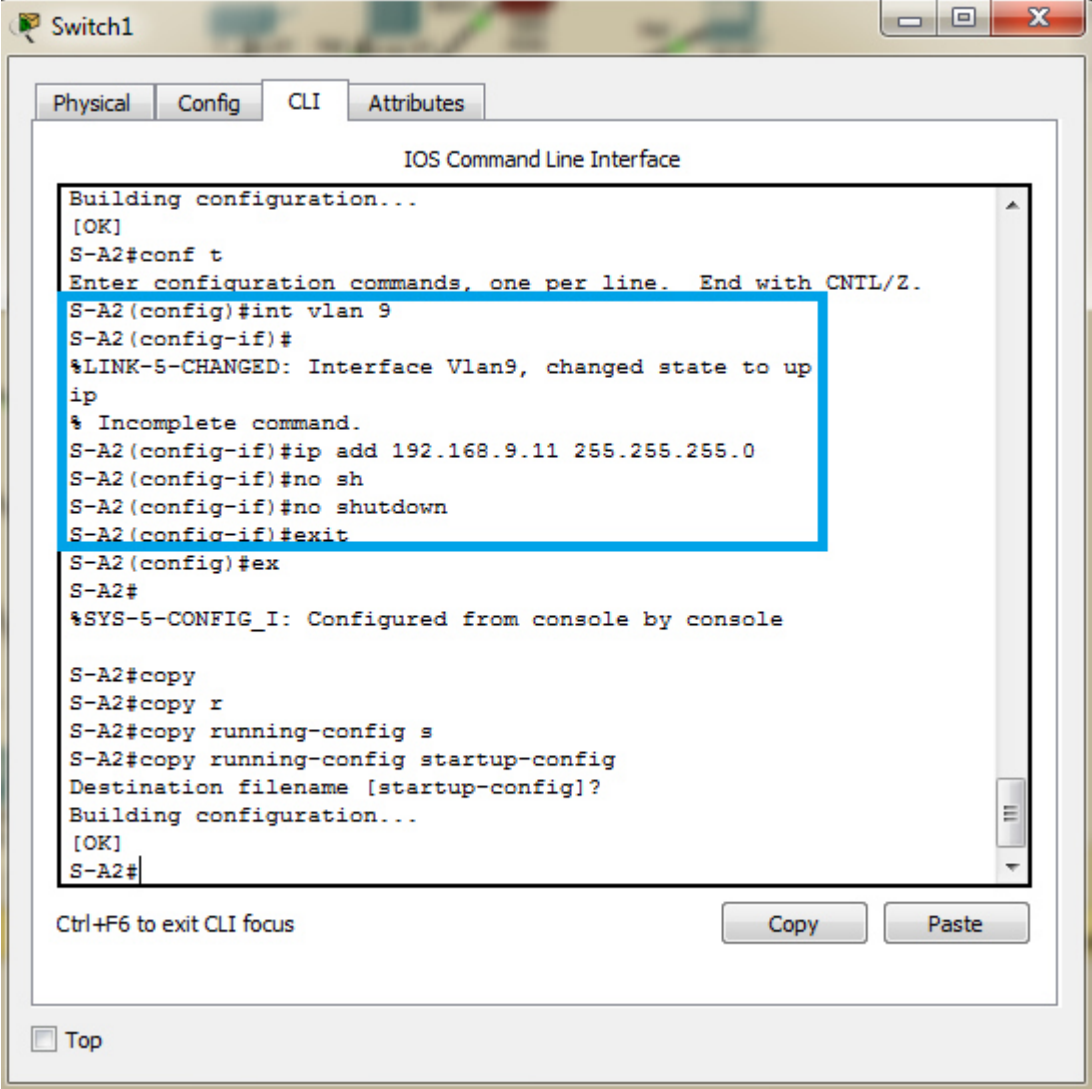
```
S-A1>en
S-A1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S-A1(config)#int vlan 9
S-A1(config-if)#ip add 192.168.9.10 255.255.255.0
S-A1(config-if)#no shutdown
S-A1(config-if)#ex
S-A1(config)#ex
S-A1#
%SYS-5-CONFIG_I: Configured from console by console

S-A1#copy
S-A1#copy r
S-A1#copy running-config s
S-A1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S-A1#
```

At the bottom of the window, there is a "Ctrl+F6 to exit CLI focus" message and "Copy" and "Paste" buttons. A "Top" button is also visible at the bottom left.

Figure 3.19 Configuration de l'adresse du Vlan 9 dans le Switch S-A1.

3.5.2.7 Configuration de l'adresse du Vlan 9 dans le switch S-A2



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

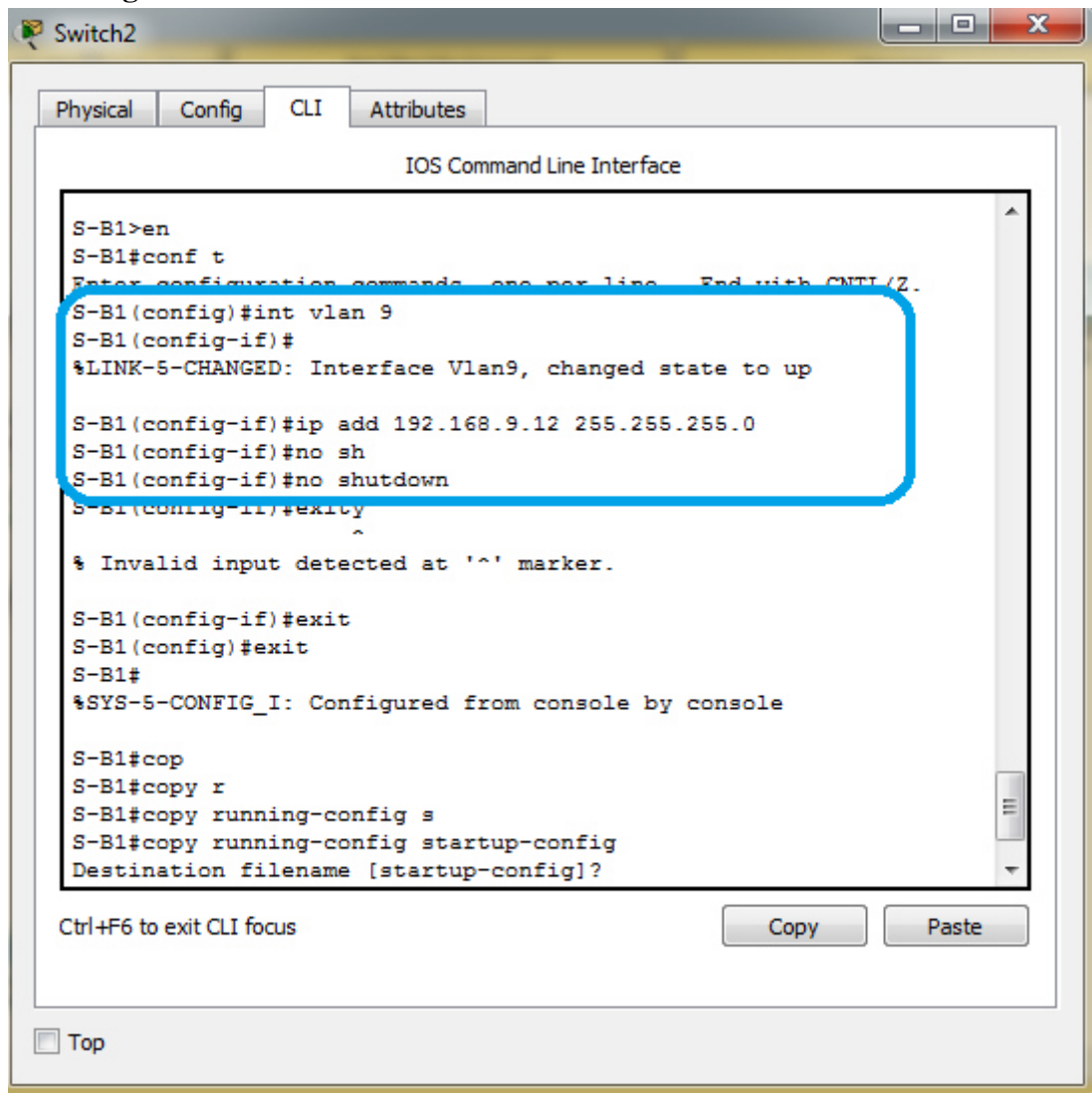
```
Building configuration...
[OK]
S-A2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S-A2(config)#int vlan 9
S-A2(config-if)#
%LINK-5-CHANGED: Interface Vlan9, changed state to up
ip
% Incomplete command.
S-A2(config-if)#ip add 192.168.9.11 255.255.255.0
S-A2(config-if)#no sh
S-A2(config-if)#no shutdown
S-A2(config-if)#exit
S-A2(config)#ex
S-A2#
%SYS-5-CONFIG_I: Configured from console by console

S-A2#copy
S-A2#copy r
S-A2#copy running-config s
S-A2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S-A2#
```

At the bottom of the window, there is a "Ctrl+F6 to exit CLI focus" message, "Copy" and "Paste" buttons, and a "Top" button.

Figure 3.20 Configuration de l'adresse du Vlan 9 dans le Switch S-A2.

3.5.2.8 Configuration de l'adresse du Vlan 9 dans le switch S-B1



```
Switch2
Physical Config CLI Attributes
IOS Command Line Interface
S-B1>en
S-B1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S-B1(config)#int vlan 9
S-B1(config-if)#
%LINK-5-CHANGED: Interface Vlan9, changed state to up
S-B1(config-if)#ip add 192.168.9.12 255.255.255.0
S-B1(config-if)#no sh
S-B1(config-if)#no shutdown
S-B1(config-if)#exit
^
% Invalid input detected at '^' marker.
S-B1(config-if)#exit
S-B1(config)#exit
S-B1#
%SYS-5-CONFIG_I: Configured from console by console
S-B1#cop
S-B1#copy r
S-B1#copy running-config s
S-B1#copy running-config startup-config
Destination filename [startup-config]?
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

Figure 3.21 Configuration de l'adresse du Vlan 9 dans le Switch S-B1.

3.5.2.9 Configuration des liens Trunk

Nous allons configurer les liaisons entre es commutateurs en mode trunk.

La figure suivante illustre les configurations faites.

```
S-A1>en
S-A1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S-A1(config)#int f0/1
S-A1(config-if)#switchport mode trunk

S-A1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

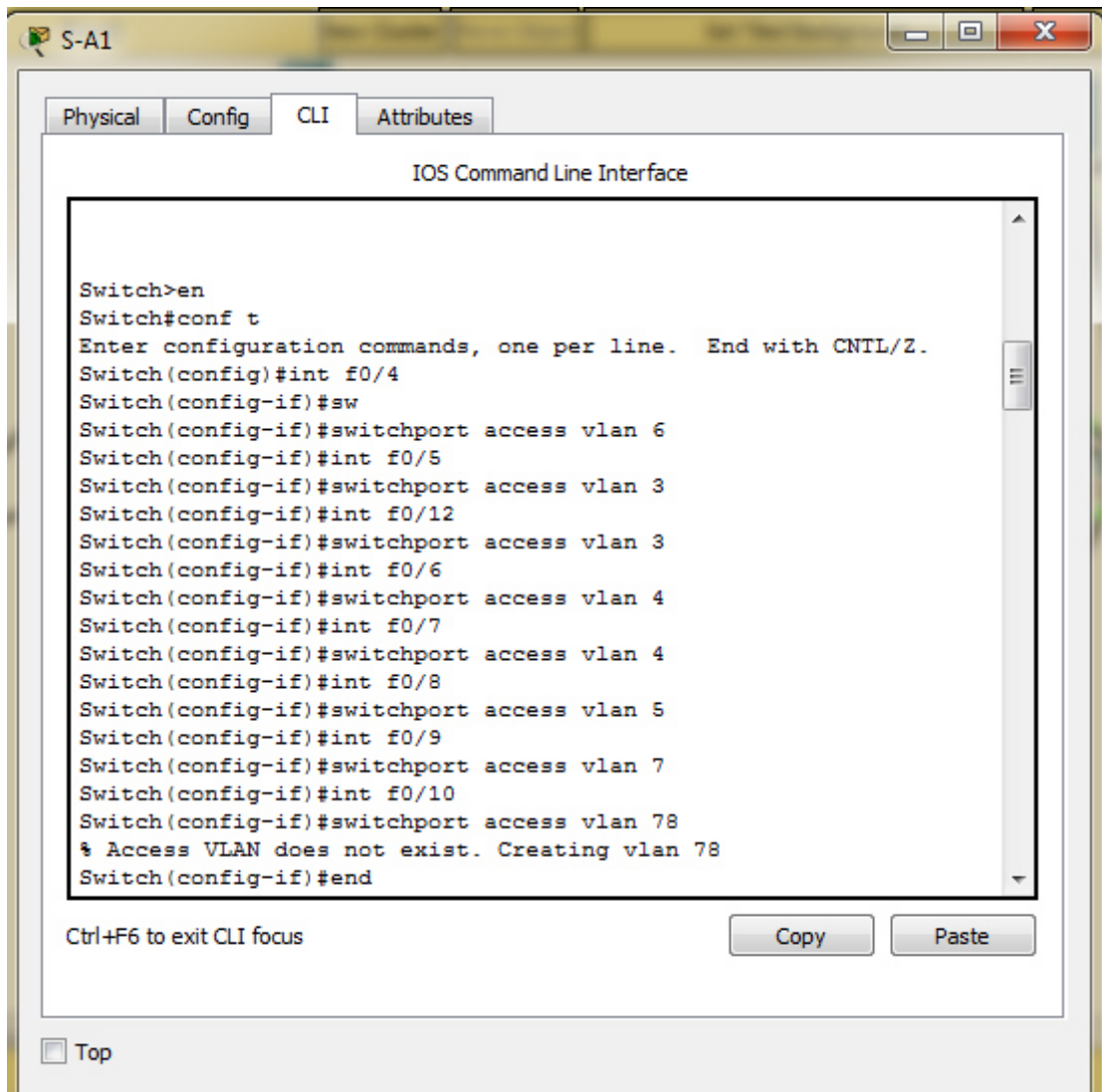
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan9, changed
state to up

S-A1(config-if)#switchport trunk native vlan 9
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (9), with S-A2 FastEthernet0/1 (1).
exi
S-A1(config)#exit
S-A1#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 3.22 Configuration des liens Trunk du Switch S-A1.

3.5.2.10 Configuration des liens access

Les interfaces en mode accès se trouvent au niveau des liens entre les commutateurs d'accès et les PC. La figure suivante illustre les configurations faites.



```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f0/4
Switch(config-if)#sw
Switch(config-if)#switchport access vlan 6
Switch(config-if)#int f0/5
Switch(config-if)#switchport access vlan 3
Switch(config-if)#int f0/12
Switch(config-if)#switchport access vlan 3
Switch(config-if)#int f0/6
Switch(config-if)#switchport access vlan 4
Switch(config-if)#int f0/7
Switch(config-if)#switchport access vlan 4
Switch(config-if)#int f0/8
Switch(config-if)#switchport access vlan 5
Switch(config-if)#int f0/9
Switch(config-if)#switchport access vlan 7
Switch(config-if)#int f0/10
Switch(config-if)#switchport access vlan 78
% Access VLAN does not exist. Creating vlan 78
Switch(config-if)#end
```

Ctrl+F6 to exit CLI focus

Copy Paste

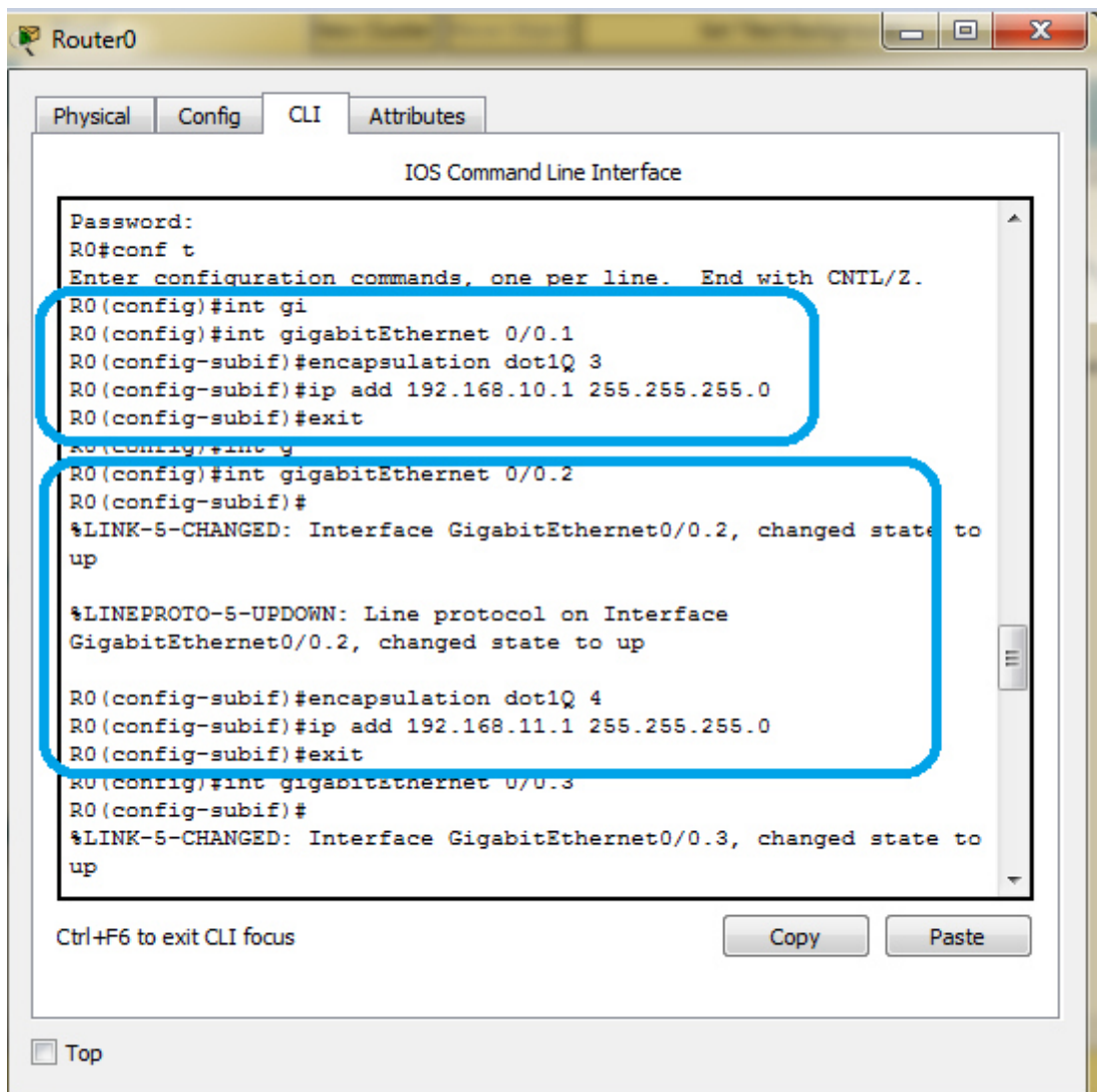
Top

Figure 3.23 Configuration des liens d'Access du Switch S-A1.

3.5.2.11 Configuration Inter-Vlan

Nous allons maintenant configurer le routage inter-VLAN en utilisant des sous-interfaces au niveau du routeur.

La figure ci-dessous nous montre les commandes à suivre :

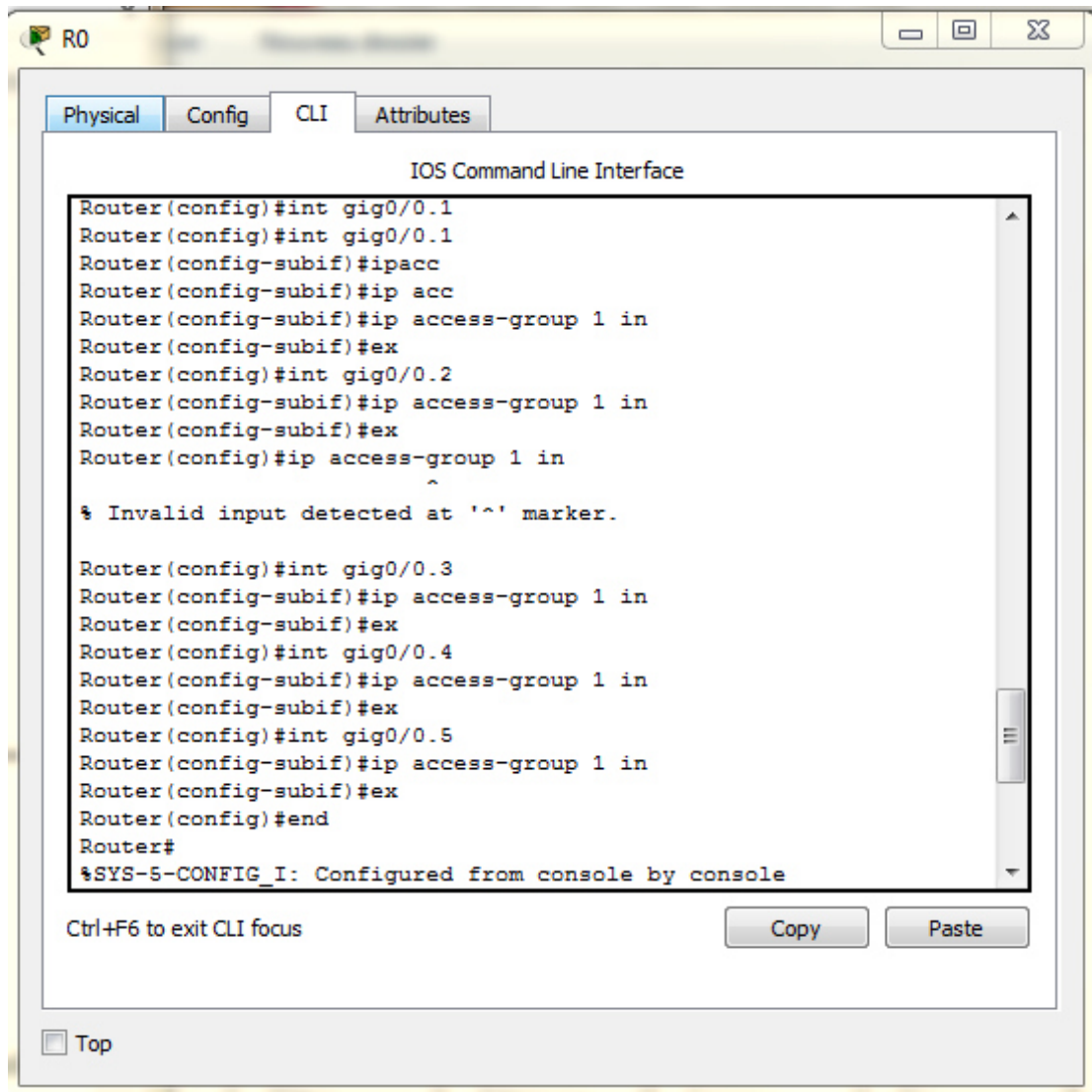


```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Password:
R0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#int gi
R0(config)#int gigabitEthernet 0/0.1
R0(config-subif)#encapsulation dot1Q 3
R0(config-subif)#ip add 192.168.10.1 255.255.255.0
R0(config-subif)#exit
R0(config)#int g
R0(config)#int gigabitEthernet 0/0.2
R0(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.2, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.2, changed state to up
R0(config-subif)#encapsulation dot1Q 4
R0(config-subif)#ip add 192.168.11.1 255.255.255.0
R0(config-subif)#exit
R0(config)#int gigabitEthernet 0/0.3
R0(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed state to
up
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

Figure 2.24 Configuration du Routage Inter-VLAN dans le Routeur R0.

3.5.2.12 Insertion des ACL

Nous allons maintenant utiliser les listes des contrôles d'accès afin de limiter la communication entre certains VLANs, nous avons configuré une ACL au niveau du VLAN 3 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 :



```
Router(config)#int gig0/0.1
Router(config)#int gig0/0.1
Router(config-subif)#ipacc
Router(config-subif)#ip acc
Router(config-subif)#ip access-group 1 in
Router(config-subif)#ex
Router(config)#int gig0/0.2
Router(config-subif)#ip access-group 1 in
Router(config-subif)#ex
Router(config)#ip access-group 1 in
^
% Invalid input detected at '^' marker.

Router(config)#int gig0/0.3
Router(config-subif)#ip access-group 1 in
Router(config-subif)#ex
Router(config)#int gig0/0.4
Router(config-subif)#ip access-group 1 in
Router(config-subif)#ex
Router(config)#int gig0/0.5
Router(config-subif)#ip access-group 1 in
Router(config-subif)#ex
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 3.25 Configuration des ACL.

3.6 Test de fonctionnement

3.6.1 Architecture du réseau

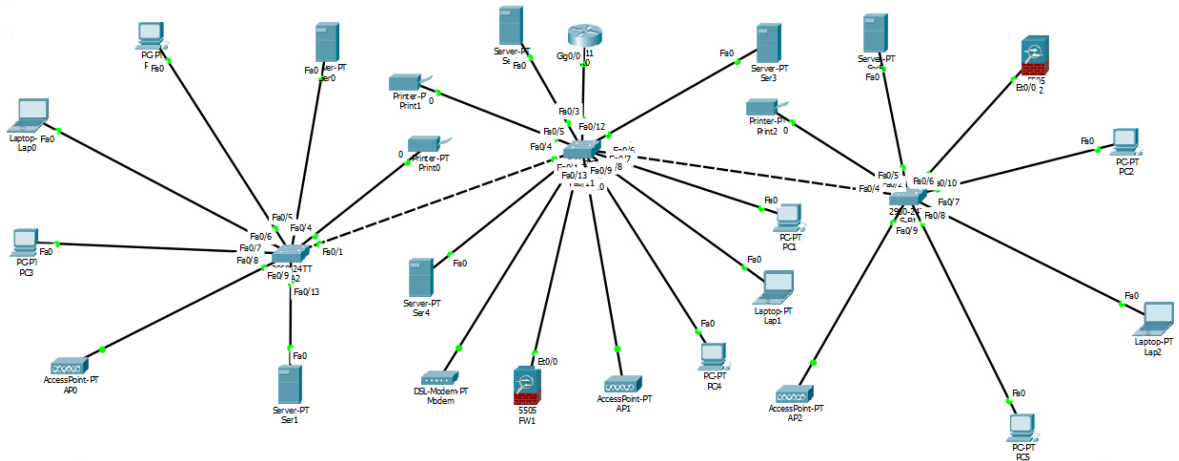


Figure 3.26 Architecture du réseau.

Dans cette architecture, nous effectuerons quatre tests :

- ✓ Deux tests qui permettent de vérifier la connectivité entre les hôtes qui se trouvent dans un même VLAN (intra-VLAN).
- ✓ Un test qui permettra de vérifier la connectivité entre les hôtes qui se trouvent dans des VLANs différents (inter-VLAN).
- ✓ Un test qui va nous servir à démontrer que le Laptop2 du VLAN 4 (192.168.11.7) ne peut pas communiquer avec le Serveur0 du VLAN 3 (192.168.10.2) car nous avons limité l'accès au VLAN 3 grâce à des ACL préalablement implémentées.

3.6.2 Test 1

Nous allons effectuer un Ping entre le PC0 et Laptop 2

PC0:192.168.11.2.

Laptop2:192.168.11.7.

Le Ping a été effectué dans l'invite de commande par la commande : ping 192.168.11.7

Test réussi.

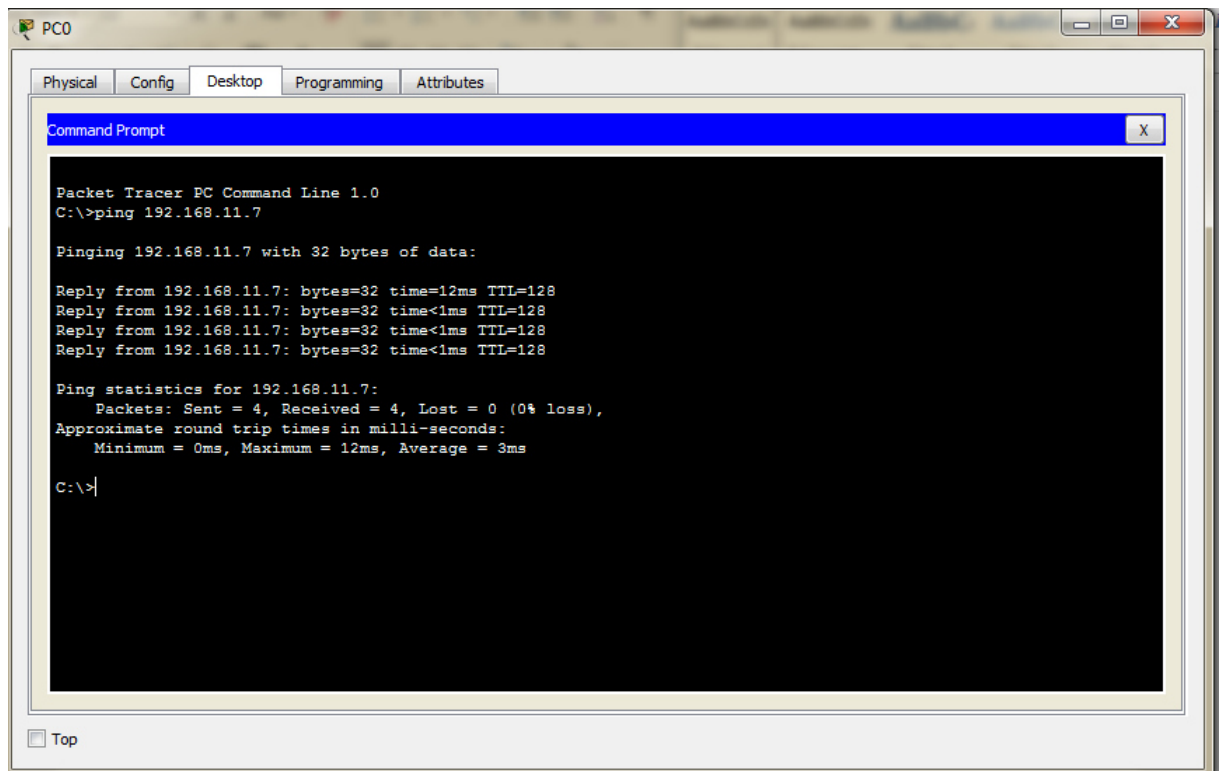


Figure 3.27 Ping du Test 1 réussi.

3.6.3 Test 2

Nous allons effectuer un Ping entre PC1 et le PC2

PC1:192.168.11.4.

PC2:192.168.11.6.

Le Ping a été effectué dans l'invite de commande par la commande : ping 192.168.11.6

Test réussit.

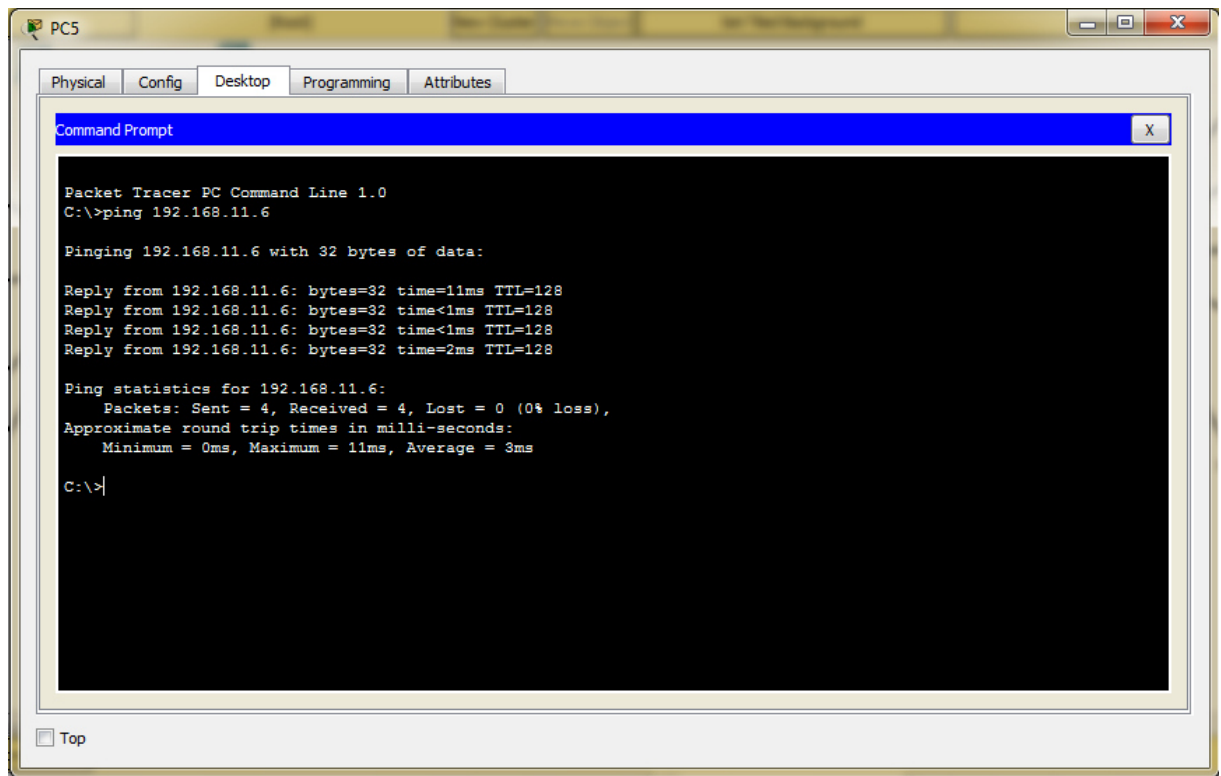


Figure 3.28 Ping du Test 2 réussi.

3.6.4 Test 3

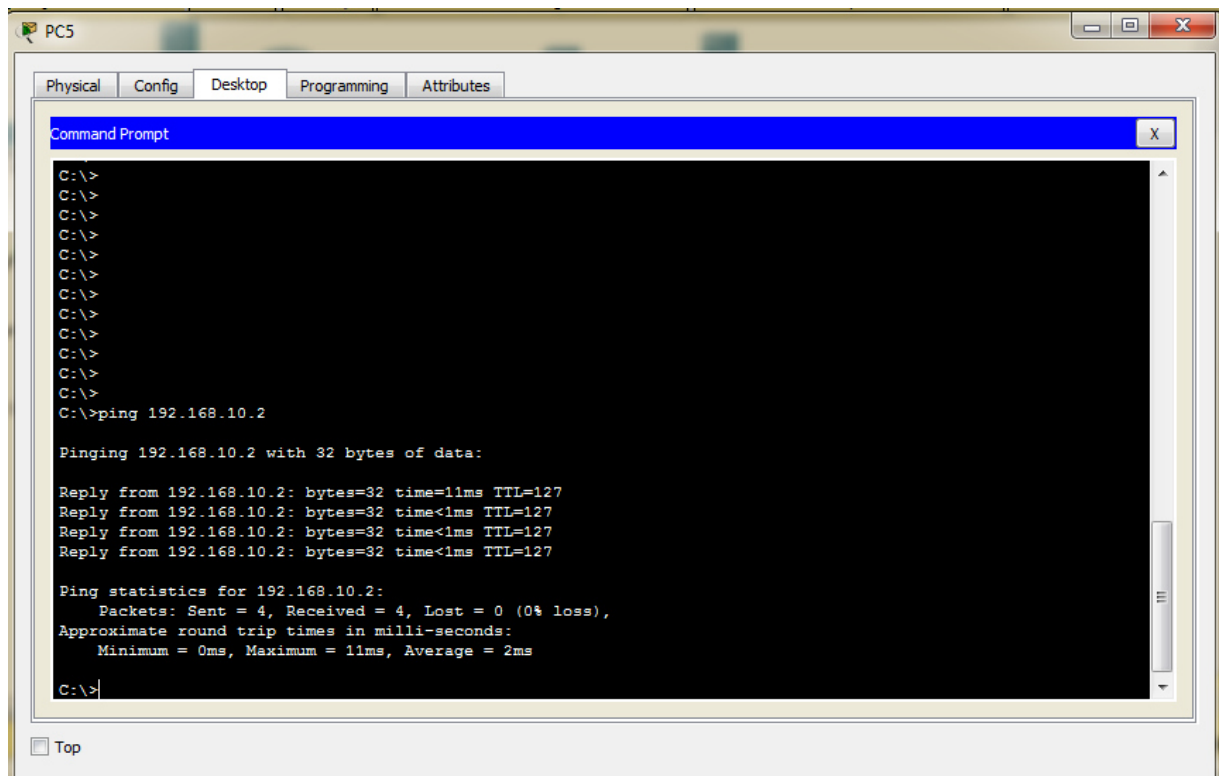
Nous allons effectuer un Ping entre le PC5 et le Server0

PC5 : 192.168.12.4

Server0 : 192.168.10.2

Le Ping a été effectué dans l'invite de commande par la commande : ping 192.168.10.2

Test réussi



The image shows a screenshot of a Windows Command Prompt window titled "Command Prompt" with a blue header bar. The window is open on a desktop environment, with tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes" visible at the top. The command prompt shows the following text:

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time=11ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 2ms

C:\>
```

At the bottom left of the window, there is a "Top" button.

Figure 3.29 Ping du Test 3 réussi.

3.6.5 Test 4

Nous allons effectuer un Ping entre le Laptop2 et le Server0

Laptop2 : 192.168.11.7

Server0 : 192.168.10.2

Le Ping a été effectué dans l'invite de commande par la commande : ping 192.168.10.2

Test réussi

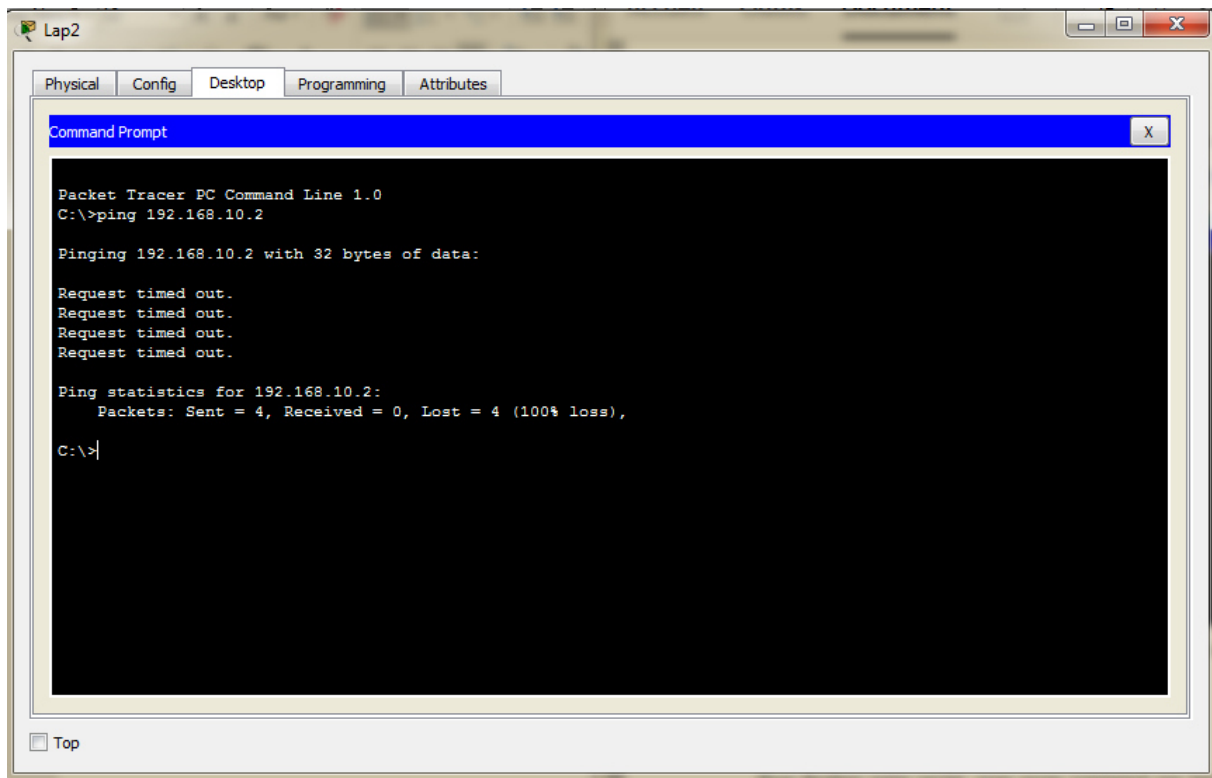


Figure 3.30 Ping échoué entre le VLAN 3 et le VLAN 4.

3.7 Conclusion

Afin de réaliser la création et la configuration de notre réseau en introduisant des VLANs. Nous avons choisi d'organiser les VLANs par équipement, puis nous avons ajouté des pare-feu pour renforcer la sécurité du réseau. 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. Puis, nous avons vérifié le bon fonctionnement de notre solution à travers des tests et vérification de connexion entre tous les composants.

CONCLUSION GENERALE

La sécurité des réseaux informatique plus précisément les réseaux locaux de l'entreprise est en évolution, ceci est à cause de l'ouverture des systèmes informatiques sur internet. Cette interconnexion Internet les a exposés à des attaques informatiques complexes. Et pour cela les entreprises doivent sécuriser et protéger leurs réseaux en constatant des solutions efficaces de protection tel que les VLANs.

Dans un premier temps, nous avons fait une étude générale sur les réseaux informatiques tels que leurs classifications et topologies ainsi que les supports de transmission existants. Puis, nous avons expliqué les deux modèles de références OSI et TCP/IP. Ensuite, nous avons présenté des généralités sur la sécurité informatique. De ce fait, nous avons cité quelques objectifs et stratégies de la sécurité. Après, nous avons présenté les réseaux locaux virtuels : leurs types, avantages et protocoles de transports et de gestion. Ensuite, nous avons présenté notre cas d'étude. Et au final, nous avons présenté le Simulateur Packet Tracer utilisé pour réaliser notre travail qui est la création des VLANs et l'ajout des pare-feu. De même, nous avons montré les étapes suivis pour la création des VLANs avec les tests nécessaires du bon fonctionnement.

Enfin, ce travail nous a permis d'assurer la sécurité du réseau, sa réorganisation et l'amélioration de la bande passante.

- [1] : Liste des termes, expressions et définitions du vocabulaire de l'informatique. Journal officiel, octobre 1998, <http://www.marche-public.fr/Marches-publics/Textes/Definition/Definition-informatique-19981010.htm>. Accéder le 28 juin 2020.
- [2] : Types de réseaux, <https://web.maths.unsw.edu.au/~lafaye/CCM/initiation/types.htm>. Accéder le 28 juin 2020.
- [3] : G. PUJOLLE, " Les réseaux ", 6ème édition, Eyrolles, 2008.
- [4] : G. PUJOLLE, " Initiation-aux-réseaux ", Eyrolles, Edition 2000.
- [5] : Topologie des réseaux, <https://www.commentcamarche.net/contents/512-topologie-des-reseaux>. Accéder le 28 juin 2020.
- [6] : LA TOPOLOGIE DES RESEAUX, <http://doc.lagout.org/programmation/La%20topologie%20des%20reseaux.pdf>. Accéder le 24 octobre 2020.
- [7] : D. DROMARD, D. SERET, "Architecture des réseaux", Edition Pearson Education France, 2009.
- [8] : Topologies des réseaux – Vulgarisation-informatique.com, <http://www.vulgarisation-informatique.com/topologie-reseau.php>. Accéder le 24 octobre 2020.
- [9] : D. DROMARD, D. SERET, " Architecture des réseaux ", Pearson France, 2009.
- [10] : Claude Duvallet, "UF9 - Architectures et protocoles de réseaux", Licence Professionnelle Informatique, Université du Havre, Année scolaire 2007-2008.
- [11] : Cours supports de transmission, <https://www.univ-chlef.dz/ft/wp-content/uploads/2020/04/supports-trans.pdf>. Accéder le 28 juin 2020.
- [12] : P. ATELIN, " Réseaux Informatiques Notions fondamentales (Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, Wi-Fi, ...) ", Editions ENI, 2009.
- [13] : P. Erny, "Les réseaux informatiques d'entreprise", Edition Ellipse, 1998.
- [14] : Le modèle OSI, <https://inetdoc.net/articles/modelisation/modelisations.osi.html>. Accéder le 8 septembre 2020.
- [15] : Sylvain le modèle TCP/IP, <http://www.frameip.com/tcpip/>, 2003.

- [16] : Formation ISN - Modélisations, http://math.univ-lyon1.fr/irem/Formation_ISN/formation_reseau/reseaux_modelisations/modelisations.html. Accéder le 8 septembre 2020.
- [17] : Définition de sécurité informatique - Concept et Sens, <https://lesdefinitions.fr/securite-informatique>. Accéder le 10 octobre 2020.
- [18] : I. HAJJEH, " Conception et validation d'un nouveau protocole pour la sécurisation des échanges. ", thèse doctorat, Ecole Nationale Supérieure des Télécommunication, Paris, décembre 2004.
- [19] : A. SAIDANE, " Conception et réalisation d'une architecture tolérant les intrusions pour des serveurs Internet ", thèse doctorat, Institut National des Sciences Appliquées de Toulouse, janvier 2005.
- [20] : J. PETIT, " Surcoût de l'authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires ", thèse doctorat, Université de Toulouse, Juillet 2011.
- [21] : S. Bouam et J. Ben-Othman, protocole de sécurisation des données à base de routage dans les réseaux AD HOC, 2004.
- [22] : A. CONTES, " Une Architecture De Sécurité Hiérarchique, Adaptable Et Dynamique Pour La Grille ", thèse doctorat, Université de Nice - Sophia Antipolis, Septembre 2005.
- [23] : Les attaques en déni de service(DDoS), <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/attaque-en-deni-de-service-ddos>. Accéder le 10 octobre 2020.
- [24] : B. Cousin, "Sécurité des réseaux", Master 2 Pro en Informatique, Université de Rennes 1, 2009.
- [25] : Pare-feux('Firewalls') Cours de sécurité – Cnam, http://deptinfo.cnam.fr/Enseignement/CycleProbatoire/SECURITE/cours_parefeux.pdf. Accéder le 28 juin 2020.
- [26] : Qu'est-ce qu'un Firewall ? Fonctionnement et types de Firewall, [https://wikimemoires.net/2012/08/08/quest-ce-quun-firewall-fonctionnement-et-types-de-firewall/#:~:text=Un%20syst%C3%A8me%20Firewall%20fonctionne%20sur,interne%20et%20une%20machine%20ext%C3%A9rieure.&text=%20Type%20de%20paquet%20\(TCP%2C%20UDP%2C%20etc.\)%3B](https://wikimemoires.net/2012/08/08/quest-ce-quun-firewall-fonctionnement-et-types-de-firewall/#:~:text=Un%20syst%C3%A8me%20Firewall%20fonctionne%20sur,interne%20et%20une%20machine%20ext%C3%A9rieure.&text=%20Type%20de%20paquet%20(TCP%2C%20UDP%2C%20etc.)%3B). Accéder le 8 septembre 2020.

- [27] : Jabou Chaouki, Schillings Michaël et Hantach Anis, " TER Détection d'anomalies sur le réseau ", Rapport de projet, Université Paris Descartes, 2009.
- [28] : DMZ (Zone démilitarisée) – Comment Ça Marche, <https://www.commentcamarche.net/contents/991-dmz-zone-demilitarisee>. Accéder le 8 septembre 2020.
- [29]: J. Kim, "Integrating Artificial Immune Algorithms for Intrusion Detection ", these doctorat, University College London, 2002.
- [30] : D. DROMARD, D. SERET, " Architecture des réseaux ", Pearson France, 2009.
- [31] : Principe de base de la cryptographie - David Carella's web site, <http://david.carella.free.fr/fr/cryptographie/principes-de-base.html>. Accéder le 8 septembre 2020.
- [32] : Installation et Configuration d'un VPN OpenVPN - Linux, <https://mathieu-androz.developpez.com/mathieu-androz/articles/linux/vpn/>. Accéder le 8 septembre 2020.
- [33] : J.F. PILLOU, " Tous sur les réseaux et Internet ", Edition Dunod, Paris, 2006.
- [34] : Cours réseaux : introduction, <http://www.netalya.com/fr/reseaux5.asp>. Accéder le 15 juin 2020.
- [35] : VLAN – Réseaux virtuels, <https://www.commentcamarche.net/contents/543-vlan-reseaux-virtuels>. Accéder le 8 septembre 2020.
- [36] : Genaël VALET. "Les LANs virtuels. Greta industriel de technologies avancées", 2007.
- [37]: Les VLAN, <http://projet.eu.org/pedago/sin/ISN/8-VLAN.pdf>. Accéder le 13 juillet 2020.
- [38] : Les VLAN. Informatique et Science du Numérique, <http://docplayer.fr/30423599-Les-vlan-informatique-et-science-du-numerique.html>. Accéder le 24 octobre 2020.
- [39] : Les réseaux locaux virtuels (vlans) – DocPlayer.fr, <https://docplayer.fr/634418-Les-reseaux-locaux-virtuels-vlan.html>. Accéder le 13 juillet 2020.
- [40] : S. ASSOUL, "Réseaux à haut/très haut débit", Edition 2014-2015.
- [41]: LES RESEAUX VIRTUELS VLAN, http://mariepascal.delamare.free.fr/IMG/pdf/VLAN_CM.pdf. Accéder le 24 octobre 2020.
- [42] : Les VLAN, <http://perso.modulonet.fr/placurie/Ressources/BTS2-AMSI/Chap-10-%20Les%20VLAN.pdf>. Accéder le 15 septembre 2020.

- [43] : Avantages des VLAN,
<http://cisco.ofppt.info/ccna2/course/module3/3.1.1.2/3.1.1.2.html>. Accéder le 15 septembre 2020.
- [44] : VLAN : 5 types et avantages, <https://www.summitir.com/2017/08/30/vlans-types-benefits/>. Accéder le 15 septembre 2020.
- [45] : inter-vlan-routing | inetdoc.net, <https://www.inetdoc.net/articles/inter-vlan-routing/inter-vlan-routing.vlan.html#intervlan-routing.vlan.definitions>. Accéder le 15 septembre 2020.
- [46] : VLANs - IGM,
<http://igm.univmlv.fr/~dr/XPOSE2007/vlanparlegrandquinapascomprislesconsignes/8021QTrame.html>. Accéder le 10 aout 2020.
- [47] : La trame 802.1Q – IGM, <http://www-igm.univ-mlv.fr/~dr/XPOSE2007/vlanparlegrandquinapascomprislesconsignes/8021QTrame.html>. Accéder le 13 juillet 2020.
- [48] : F. Nolot, "Cours5-VTP", Académie Cisco, 2007.
- [49] : Protocole VMPS – CNRS CRIC,
<https://cric.grenoble.cnes.fr/Administrateurs/Documentations/SiteWebAuthentification/ProtocoleVMPS.php#:~:text=VMPS%20est%20un%20protocole%20propri%C3%A9taire,identification%20de%20la%20machine%20connect%C3%A9e>. Accéder le 20 septembre 2020.
- [50] : CisCo PACKET TRACER Prise en main du logiciel –
http://www.siloged.fr/cours/docs/manuels/doc_packettracer.pdf. Accéder le 14 octobre 2020.
- [51] : Présentation et utilisation de Packet Tracer,
<http://www.i3s.unice.fr/~map/Cours/LPSILADMIN/UtilisationPacketTracer.pdf>. Accéder le 14 octobre 2020.
- [52] : A. Roux, " Cisco - Configurez routeurs et Commutateurs : Exercices et corrigés ", Editions ENI, 11 juillet 2018.
- [53] : Qu'est-ce que l'ACL(Access Control List) et Comment La Configurer,
<https://www.fs.com/fr/what-is-access-control-list-and-how-to-configure-it-aid-962.html>. Accéder le 01 décembre 2020.
- [54] : Réseaux Informatiques, http://1.bp.blogspot.com/aeitAu-7N_4/VWTId28hhhI/AAAAAAAAAB0W/t5h2QO2A1sk/s1600/images.jpg. Accéder le 01 décembre 2020.

****Résumé****

Les réseaux locaux virtuels ou VLANs ont transformé radicalement 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 d'AGRANA en réseaux logiques et l'ajout des pare-feu afin de faciliter la gestion et améliorer la sécurité, mais ce travail ne peut pas être réalisé sans faire une étude de l'architecture existante du réseau d'AGRANA.

Mots clés : Réseau informatique, Sécurité des réseaux, Réseaux locaux virtuels (VLANs), communication inter VLANs, ACL, Pare-feu, Cisco Packet Tracer.

****Abstract****

Virtual local networks or VLANs have radically transformed the concept of network segmentation, they allow to constitute as many logical networks as we want on a single infrastructure in order to improve its security and to use the bandwidth well.

The objective of our work is to implement a solution with VLANs in order to segment AGRANA's network into logical networks and the addition of firewalls in order to facilitate management and improve security. But, this work cannot be achieved without carrying out a study of the existing architecture of the AGRANA network.

Keywords: Computer network, Network security, Virtual local area networks (VLANs), inter VLAN communication, ACL, Firewall, Cisco Packet Tracer.