République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mouloud Mammeri de Tizi-Ouzou

Faculté De Génie Electrique et d'Informatique
Département de Télécommunications

Mémoire de Fin d'Etudes de

MASTER ACADEMIQUE

Spécialité :

Réseaux & Télécommunications

Filière :

Télécommunications

Par
HASSANI Massicelia
REKHIS Liza

Thème

Mise en place du routage inter-VLAN pour optimiser le trafic de données

Soutenu le : 25/06/2024

Devant le jury :

Président :	T .BECHA	Maître de conférences B
Promoteur :	M.Lazri	Professeur
Examinatrice :	S .Bouallegue	Maître de conférences B

Remerciements

Nous remercions tout d'abord le bon Dieu, le tout puissant de nous avoir donné la chance, la patience et le courage pour achever ce travail.

Nous exprimons notre profonde gratitude envers nos encadreurs, le Professeur LAZRI et Monsieur ISTANBOULI, qui nous ont pleinement accompagnés sans retenir aucune information, et qui ont été présents à chaque étape de la réalisation de ce projet.

Nos remerciements vont aussi à l'endroit des membres du jury, pour l'évaluation et la révision de ce mémoire, afin d'améliorer sa qualité.

Un immense merci à toutes les personnes ayant contribué de près ou de loin à la réussite de ce travail.

Nous adressons également nos sincères remerciements à nos familles et amis, qui ont toujours cru en nos capacités tout au long de notre parcours d'études.

Dédicace

Je dédie ce modeste Travail :

À mes chers parents, Yahia et Fatma, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études.

À mes chères sœurs, Wardia et Wissam, pour leurs encouragements permanents et leur soutien moral.

À mon cher frère, Ahcene, pour son appui et son encouragement.

À toute ma famille pour leur soutien tout au long de mon parcours universitaire.

Que ce travail soit l'accomplissement de vos vœux tant souhaités, et le fruit de votre soutien infaillible.

Merci d'être toujours là pour moi.

REKHIS Liza

Dédicace

Je dédie ce modeste travail :

À mes chers parents, Mustapha et Ouiza, pour leur soutien et leurs encouragements constants à chaque étape de ma vie, ainsi que pour tous leurs sacrifices, leur amour et leur tendresse. Que Dieu les garde et les protège.

À ma sœur Fettouma et à mon cousin Kamel, qui m'ont aidé et soutenu.

A ma grand-mère, mes tantes, mes oncles, mes chers cousins, et toute ma famille qui était toujours à mes côtés.

A mes chères cousines Farida, Nadia, Amina, Tinhinnane, Inia, Thaninna, Rania, Lena, Romaissa, Maya et Sarah.

HASSANI Massicelia

Sommaire

Chapitre II : Généralités sur la sécurité.

Chapitre III : VLAN et routage inter-VLAN

Chapitre IV : Test et Simulation du réseau avec un Routage inter-VLAN

Liste des tableaux

Liste des figures

Chapitre I: Généralités sur les réseaux informatiques

Chapitre II : Généralités sur la sécurité

Chapitre III : VLAN et routage inter-VLAN

Chapitre IV : Test et Simulation du réseau avec un Routage inter-VLAN

Liste des abréviations

ACL	*Access Control Liste*
CISCO	*Computer Information System Company*
CLI	*Command Language Interface*
CPU	*Central Processing Unit*
DHCP	*Dynamic Host Configuration Protocol*
DMZ	*Demilitarized Zone*
DNS	*Domain Name System*
DOS	*Denial of Service*
EIGRP	*Enhanced Interior Gateway Routing Protocol*
FCS	*Frame Check Sequence*
FTP	*File Transfer Protocol*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IP	*Internet Protocol*
ICMPv4	*Internet Control Message Protocol version 4*
ICMPv6	*Internet Control Message Protocol version 6*
IEEE	*Institute of Electrical and Electronics Engineers*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
IoT	*Internet of Things*
IPSEC	*Internet Protocol Security*
ISL	*Inter-Switch Link*

ISO	*International Organization for Standardization*
LAN	*Local Area Network*
LLC	*Logical Link Control*
MAC	*Media Access Control*
MAN	*Metropolitan Area Network*
OSI	*Open Systems Interconnection*
OSPF	*Open Shortest Path First*
PAN	*Personal Area Network*
POP	*Post Office Protocol*
PPP	*Point-to-Point Protocol*
QoS	*Quality of Service*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
SVI	*Switch Virtual Interface*
TCP	*Transmission Control Protocol*
TCP/IP	*Transmission Control Protocol/ Internet Protocol*
UDP	*User Datagram Protocol*
VLAN	*Virtual Local Area Network*
VoIP	*Voice over Internet Protocol*
VTP	*Virtual Trunking Protocol*
WAN	*Wide Area Network*

Introduction générale

Le rôle des réseaux informatiques a considérablement évolué ces dernières années et ne se limite plus au simple transfert d'informations de base en toute sécurité. Aujourd'hui, ils contribuent à la rationalisation des ressources utilisateurs et à l'optimisation des performances applicatives. Par conséquent, il est nécessaire de disposer de moyens et de techniques permettant la diffusion efficace d'un message à un groupe d'utilisateurs, qu'il soit vaste et hétérogène.

Actuellement, les réseaux locaux (LANs) font souvent usage des VLAN (Virtual Local Area Networks). Les VLANs permettent de réduire le trafic en segmentant le réseau en sous-réseaux plus restreints. Cette segmentation facilite les échanges de données et le trafic entre les utilisateurs au sein d'un même segment, sans être perturbés par le trafic provenant d'autres parties du réseau. Les administrateurs peuvent organiser les VLANs selon différents critères tels que la zone géographique, le profil des utilisateurs, le type d'appareils, ou d'autres paramètres pertinents. Les VLANs offrent de nombreux avantages et peuvent être exploités de diverses manières intéressantes. Dans les réseaux modernes, l'utilisation des VLANs en combinaison avec le routage entre eux est courante. Cette approche présente de nombreux bénéfices tant pour la conception que pour le fonctionnement des réseaux.

Dans ce contexte, nous avons sécurisé un réseau informatique de type LAN en utilisant principalement le routage Inter-VLAN. Le LAN que nous avons sécurisé est un réseau informatique de l'entreprise sonatrach à Boumerdes où nous avons effectué un stage pratique au niveau de département technologie d'information. Le réseau informatique de ce département est doté de deux switchs auxquels sont connectées 15 machines. Après une étude préalable du réseau, nous avons constaté certaines anomalies en termes de sécurité et de gestion. Comme indiqué ci-dessus, nous avons implémenté le mécanisme inter-VLAN pour remédier aux problèmes de sécurité et de gestion. Pour optimiser encore le fonctionnement, nous aussi configuré le SSH et les ACLs.

Pour bien structurer notre travail, ce mémoire est organisé en 4 chapitres :

Dans le premier chapitre, nous commençons par une vue d'ensemble des réseaux informatiques. Nous définissons ce qu'est un réseau et expliquons ses différentes caractéristiques. Nous introduisons également les divers types de réseaux, les architectures de réseaux, les modèles OSI et TCP/IP, ainsi que les concepts de routage et de trafic de données.

Dans le deuxième chapitre, nous avons abordé la sécurité informatique de manière générale. Nous avons commencé par définir ce qu'est la sécurité informatique, puis nous avons détaillé les critères, les risques, les contre-mesures et les protocoles de sécurité.

Le troisième chapitre, nous le divisons en deux parties. Dans la première partie, nous explorons le concept de réseau local virtuel (VLAN). Nous détaillons les différents types de VLAN, leur classification et les avantages associés. Nous examinons également leur mode de fonctionnement, en mettant en évidence des aspects tels que l'agrégation de VLAN, le protocole VTP et le mode trunk. Dans la deuxième partie, nous abordons le routage inter-VLAN en détaillant son fonctionnement ainsi que les diverses méthodes employées. Nous examinons également les défis liés à sa configuration et proposons des solutions appropriées.

Dans le quatrième chapitre, nous nous penchons sur l'environnement de simulation Packet Tracer en mettant en œuvre la simulation et la configuration d'un réseau VLAN ainsi que du routage entre ces VLAN.

Pour conclure, nous finalisons ce mémoire par une synthèse globale des éléments traités.

Chapitre I : Généralités sur les réseaux informatiques

1 Introduction

Les réseaux informatiques constituent le fondement essentiel de la connectivité moderne, jouant un rôle crucial dans la transmission, le partage et la gestion des informations à l'échelle mondiale. Ces systèmes complexes facilitent la communication entre des ordinateurs et d'autres dispositifs, permettant ainsi le partage efficace des ressources et la collaboration entre utilisateurs distants.

Dans ce chapitre, nous abordons les notions fondamentales des réseaux informatiques ainsi que les différents types de topologies réseau. Nous montrons aussi les techniques de commutation, le Modèle OSI et le modèle TCP/IP, ainsi que le routage, l'adressage et le trafic de données.

2 Définition de réseau informatique

Un réseau informatique est un ensemble des équipements reliés entre eux, tels que des Ordinateurs, des serveurs, des routeurs, des commutateurs, etc., en utilisant des moyens de Communication tels que des câbles ou des technologies sans fil. Son objectif principal est de faciliter le partage de ressources, telles que des fichiers, des imprimantes et des applications, ainsi que de favoriser la communication entre les utilisateurs et les appareils connecté. (Figure I.1)

Figure I.1 :Réseau informatique**[1]**

3 Différents types de réseaux informatiques

La diversité des réseaux informatiques permet de les différencier et de les classer en fonction de leur taille et de leur portée. Voici un aperçu des principales catégories de réseaux : (figure I.2)

3.1 PAN (Personal Area Network)

Un réseau personnel (PAN) est un petit réseau informatique limité à une courte distance, connectant des dispositifs électroniques tels que smartphones et ordinateurs pour faciliter le partage d'informations.

3.2 LAN (Local Area network)

Un réseau local (LAN) est un ensemble d'ordinateurs et de périphériques interconnectés au sein d'une zone géographique limitée, comme un bureau, une maison ou un campus. Il facilite le partage de ressources telles que fichiers, imprimantes et accès à Internet entre les appareils connectés.

3.3 MAN (Metropolitan area network)

Un Réseau Métropolitain Area Network (MAN) est une infrastructure de télécommunication qui interconnecte plusieurs Réseaux Locaux (LAN) géographiquement proches, couvrant généralement une zone métropolitaine ou une région urbaine étendue, avec des débits de transmission élevés. Un Réseau Métropolitain Area Network est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

3.4 WAN (Wide area network) :

Network (WAN) est un réseau informatique ou de télécommunications qui s’étendent sur une vaste zone géographique, souvent à l'échelle d'un pays, d'un continent, voire de la planète entière. Le réseau Internet représente le plus grand exemple de WAN.

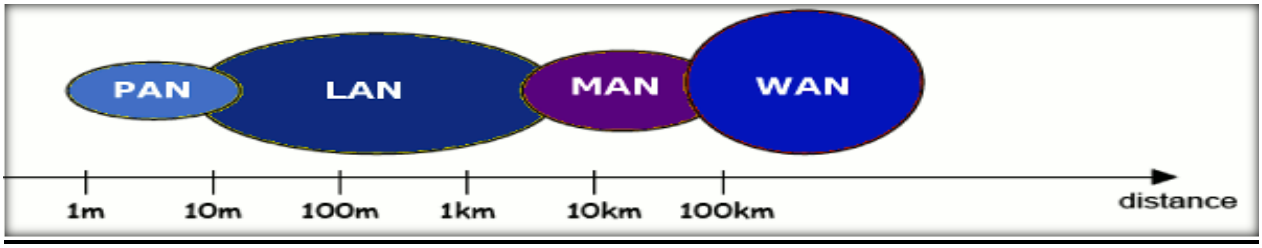

Figure I.2 : Types de réseaux **[2]**

4 Périphériques réseaux

Les périphériques réseau sont des équipements qui facilitent la communication, la gestion et le partage des ressources au sein d'un réseau informatique.

4.1 Périphériques terminaux

Le périphérique terminal est l'hôte qui est situé à l'extrémité d'une communication : par exemple un poste client et un serveur sont des hôtes terminaux**.**

Les périphériques terminaux accèdent au réseau via une technologie d'accès (L1/L2). Les périphériques clients peuvent être des ordinateurs de bureau, des mobiles ou des tablettes, mais de plus en plus des "objets" (IoT). Les serveurs sont ceux qui offrent et rendent des services à des clients. **[3]**

4.2 Périphériques intermédiaires

Les périphériques intermédiaires sont des composants clés dans un réseau informatique qui facilitent la transmission et la gestion du trafic de données entre les périphériques terminaux.

- **Routeur :** Les routeurs sont des périphériques réseau qui connectent différents réseaux et dirigent le trafic entre eux. Ils utilisent des tables de routage pour déterminer le meilleur chemin pour acheminer les données.
- **Commutateur (Switch)** : un switch est un boîtier doté de quatre à plusieurs centaines de ports Ethernet, et qui sert à relier en réseau différents éléments du système informatique. Il permet notamment de créer différents circuits au sein d'un même réseau, de recevoir des informations et d'envoyer des données vers un destinataire précis en les transportant via le port adéquat. **[4]**

- **Pont (Bridge) :** les ponts connectent deux segments de réseau pour limiter le trafic diffusé, améliorant ainsi la performance et la sécurité du réseau. Ils opèrent également au niveau de la couche de liaison de données.
- **Répéteur :** les répéteurs amplifient et régénèrent les signaux afin d'étendre la portée des réseaux. Ils sont principalement utilisés dans les réseaux filaires pour surmonter les pertes de signal.
- **Concentrateur (Hubs) :** les concentrateurs diffusent les données à tous les dispositifs connectés sur le réseau. Cependant, ils sont moins couramment utilisés aujourd'hui en raison de leurs limitations en termes de performances et de sécurité.
- **Passerelle (Gateway) :** les passerelles connectent des réseaux avec des protocoles différents, permettant ainsi la communication entre eux. Elles traduisent les données d'un format à un autre pour assurer une compatibilité.
- **Firewall :** Les pare-feu sont des dispositifs de sécurité qui filtrent le trafic réseau en fonction de règles prédéfinies. Ils protègent le réseau en empêchant l'accès non autorisé et en détectant les menaces potentielles.
- **Modem :** les modems convertissent les signaux numériques des dispositifs en signaux analogiques pour la transmission sur des lignes téléphoniques ou autres types de médias de communication.
- **Répartiteur (Splitter) :** les répartiteurs divisent un signal réseau en plusieurs canaux pour optimiser l'utilisation de la bande passante, généralement utilisés dans les réseaux de communication.
- **Proxy :** les serveurs proxy agissent en tant qu'intermédiaires entre les périphériques clients et les serveurs de destination. Ils peuvent améliorer la sécurité, la performance et la gestion des caches.
- **Switches multicouches (Layer 3 Switches) :** ces commutateurs prennent en charge des fonctionnalités de routage au niveau de la couche 3 du modèle OSI, ce qui leur permet de diriger le trafic entre différents sous-réseaux.

5 Topologies de réseaux

La topologie fait référence à la manière dont les équipements d'un réseau sont interconnectés les uns avec les autres par des supports physiques. On distingue généralement deux types de topologies :

5.1 Topologie logique

La topologie logique décrit la manière dont les équipements communiquent entre eux dans un réseau. Elle se concentre sur la configuration logique des connexions, des chemins de données et des protocoles utilisés pour faciliter la communication entre les différents dispositifs d'un réseau. **[5]**

5.2 Topologie physique

La topologie physique indique comment les différentes stations sont raccordées physiquement.

5.3 Topologie en bus

Une topologie en bus est la configuration la plus élémentaire d'un réseau, où tous les ordinateurs sont connectés à une même ligne de transmission via des câbles, généralement de type coaxial. Cette topologie est facile à mettre en place, cependant, en cas de rupture du câble ou de défaillance d'une carte réseau, toutes les communications seront interrompues**.** (Figure I.3)

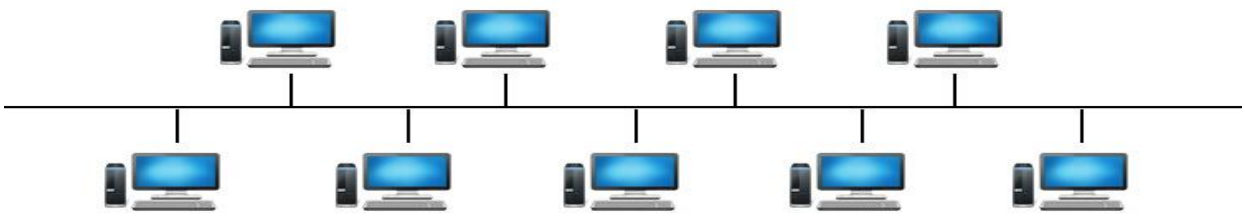

Figure I.3 : Topologie en bus**[6]**

5.3.1 Topologie en étoile

Dans une topologie de réseau en étoile, les équipements du réseau sont connectés à un dispositif central tel qu'un concentrateur (Hub), un commutateur (Switch) ou un routeur. Ce type de réseau présente l'avantage de ne pas subir une interruption totale en cas de défaillance d'une station. De plus, il permet d'ajouter ou de retirer facilement une station sans perturber le fonctionnement global du réseau. (Figure I.4)

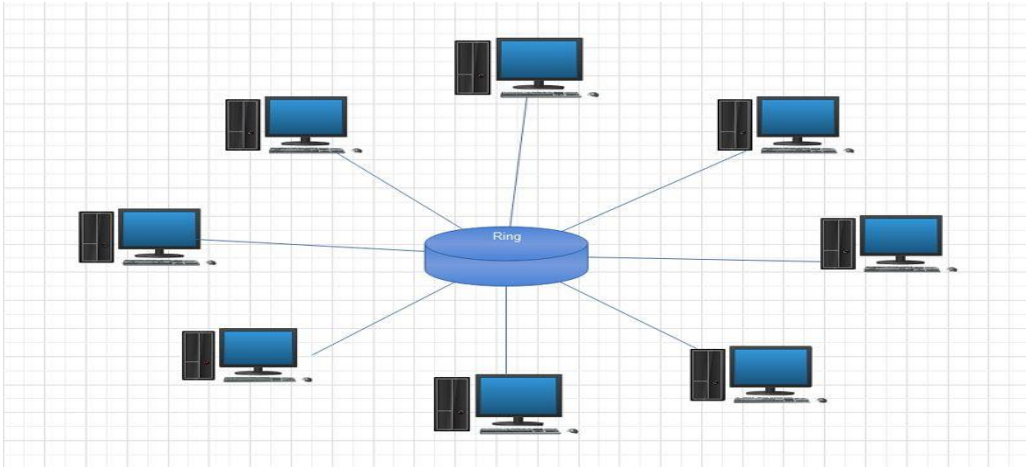

Figure I.4: Topologie en étoile**[7]**

5.3.2 Topologie en anneau

La topologie en anneau est un type de configuration de réseau informatique dans lequel les périphériques connectés sont disposés en forme d'anneau ou de boucle fermée. Chaque périphérique est connecté à exactement deux autres périphériques, formant ainsi un chemin circulaire. Les données circulent dans une direction unique à travers l'anneau, passant successivement par chaque périphérique jusqu'à atteindre la destination désirée. (Figure I.5)

Figure 1.5 : Topologie en anneau**[8]**

5.3.3 Topologie en maillée

La topologie maillée est un agencement de réseau dans lequel chaque hôte est connecté individuellement à tous les autres, sans présence d'une hiérarchie centrale. Cela crée une structure semblable à un filet, nécessitant ainsi que chaque nœud soit capable de recevoir, d'envoyer et de relayer les données. (Figure I.6)

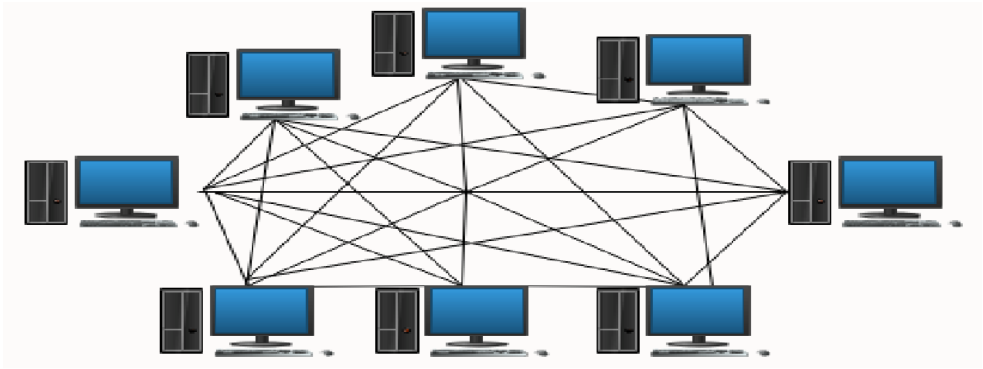

Figure I.6: Topologie maillée**[9]**

6 Technique de commutation

Les réseaux informatiques utilisent différentes techniques de commutation pour acheminer les données de manière efficace d'un point à un autre. Les deux principales techniques de commutation sont la commutation de circuits et la commutation de paquets. **[10]**

6.1 Commutation de circuit

- **Principe :** Dans la commutation de circuits, un chemin de communication dédié est établi entre l'émetteur et le récepteur pour la durée de la conversation ou de la transmission de données. Ce chemin dédié garantit une bande passante constante et prévisible pendant la communication.
- **Exemple :** Les réseaux téléphoniques traditionnels utilisent la commutation de circuits pour établir une connexion entre les appelants pendant toute la durée de l'appel.

6.2 Commutation de paquet

- **Principe :** La commutation de paquets divise les données en petits paquets, qui sont ensuite envoyés individuellement à travers le réseau. Ces paquets peuvent suivre des chemins différents pour atteindre la même destination, et ils sont réassemblés à l'arrivée.
- **Exemple :** Internet utilise la commutation de paquets, avec des protocoles tels que TCP/IP, où les données sont découpées en paquets, chacun étant routé indépendamment à travers le réseau.

7 Modèle OSI (Open Systems Interconnection)

Pour faciliter l'interconnexion des systèmes, un modèle dit d'interconnexion des systèmes ouverts, appelé encore OSI a été défini par ISO (International Standards Organization). Le modèle OSI décrit un ensemble de spécifications pour une architecture de réseau destinée à connecter des équipements hétérogènes. Le modèle OSI normalise la manière dont les matériels et les logiciels coopèrent pour assurer la communication réseau. Ce modèle est organisé en sept couches successives. **[11]** (figure I .7)

7.1 Couches de modèle OSI

Les sept couches d'abstraction du modèle OSI peuvent être définies comme suit, de haut en bas : **[12]**

7.1.1 Couche physique

La couche physique est responsable du câble physique ou de la connexion sans fil entre les nœuds réseau. Il définit le connecteur, le câble électrique ou la technologie sans fil reliant les appareils et est responsable de la transmission des données brutes (bits), qui est simplement une série de 0 et 1, tout en prenant en charge le contrôle du débit binaire.

Dans cette couche, on trouve donc des techniques de communication numérique bien connues des utilisateurs comme le Wi-Fi, l'USB, Bluetooth, Ethernet ou ADSL.

7.1.2 Couche liaison de données

La couche de liaison de données établit et met fin à une connexion entre deux nœuds connectés physiquement sur un réseau. Il divise les paquets en cadres et les envoie de la source a la destination.

Cette couche est composée de deux parties :

- Le contrôle des liens logiques (Logical Link Control – LLC), qui identifie les protocoles réseau, effectue une vérification des erreurs et synchronise les cadres
- Le contrôle d'accès aux médias (Media Access Control – MAC) qui utilise des adresses MAC pour connecter les périphériques et définir les autorisations pour transmettre et recevoir des données.

7.1.3 Couche réseau

La couche réseau rempli deux fonctions principales :

- L'une consiste à briser les segments en paquets de réseau et à réassembler les paquets à l'extrémité de réception
- L'autre est de routage des paquets en découvrant le meilleur chemin à travers un réseau physique

La couche réseau utilise des adresses réseau (généralement des adresses de protocole Internet) pour acheminer les paquets vers un nœud de destination.

7.1.4 Couche transport

Prend les données transférées dans la couche de session et la divise en « segments » à l'extrémité de transmission. Il est chargé de réassembler les segments à l'extrémité de réception, en les transformant en données qui peuvent être utilisées par la couche de session.

La couche de transport effectue un contrôle de débit, en envoyant des données à une vitesse qui correspond à la vitesse de connexion du dispositif de réception et au contrôle d'erreur, en vérifiant si les données ont été reçus de manière incorrecte et sinon, la demandant à nouveau.

7.1.5 Couche de session

La couche de session crée des canaux de communication, appelés sessions, entre les appareils. Il est responsable de l'ouverture des sessions, de s'assurer qu'ils restent ouverts et fonctionnels pendant le transfert des données et de les fermer à la fin de la communication. La couche de session peut également définir des points de contrôle lors d'un transfert de

données si la session est interrompue, les appareils peuvent reprendre le transfert de données du dernier point de contrôle.

7.1.6 Couche présentation

La couche de présentation prépare des données pour la couche d'application. Il définit comment deux périphériques doivent coder, chiffrer et comprimer les données afin qu'ils soient reçus correctement à l'autre extrémité. La couche de présentation prend toutes les données transmises par la couche d'application et la prépare à la transmission sur la couche de session.

Dans cette couche, les opérations suivantes sur les données peuvent être effectuées :

- Coder et décode les données
- Chiffrer et déchiffrer les données
- Compresser et décompresser les données

7.1.7 Couche application

La couche d'application est utilisée par les logiciels d'utilisation finale tels que les navigateurs Web et les clients de messagerie. Il fournit des protocoles qui permettent aux logiciels d'envoyer et de recevoir des informations et de présenter des données significatives aux utilisateurs.

Quelques exemples de protocoles de couche d'application sont le protocole de transfert hypertexte (HTTP), le protocole de transfert de fichiers (FTP), le protocole de poste (POP), le protocole de transfert de courrier simple (SMTP), le protocole SSH (Secure Shell) et le système de noms de domaine (DNS).

8 Modèle TCP/IP

- **TCP pour transmission Control Protocol** : c'est le protocole qui assure la transmission de données entre une source et une destination
- **IP pour Internet Protocol** : c'est un protocole sans connexion. Ce qui signifie que chaque unité de données est adressée et acheminée individuellement du périphérique source au périphérique cible, et la cible n'envoie pas d'accusé de réception à la source.

TCP/IP est donc un protocole qui permet la communication entre les équipements au sein d'un réseau. Il a pour but d'acheminer les données entre l'émetteur et le destinataire au travers de différents réseaux en mettant en place un système d'adressage hiérarchique. (Figure I.7) **[13]**

8.1 Couches du modèle TCP/IP

Le modèle TCP /IP est composé de quatre couches qui sont (figure I.8) :

- **Couche application :** Elle est la couche de communication qui s'interface avec les utilisateurs. Elle s'exécute sur les machines hôtes.
  - Exemples de protocoles applicatifs : HTTP, DNS, DHCP, FTP, …

- **Couche transport :** Elle est responsable du dialogue entre les hôtes terminaux d'une communication.
- **Couche Internet :** Elle permet de déterminer les meilleurs chemins à travers les réseaux en fonction des adresses IPv4 ou IPv6 à portée globale.
- **Couche accès réseau :** TCP/IP ne s'occupe pas de la couche accès réseau. Elle organise le flux binaire et identifie physiquement les hôtes. Elle place le flux binaire sur les supports physiques. Les commutateurs, cartes réseau, connecteurs, câbles, etc. font partie de cette couche.

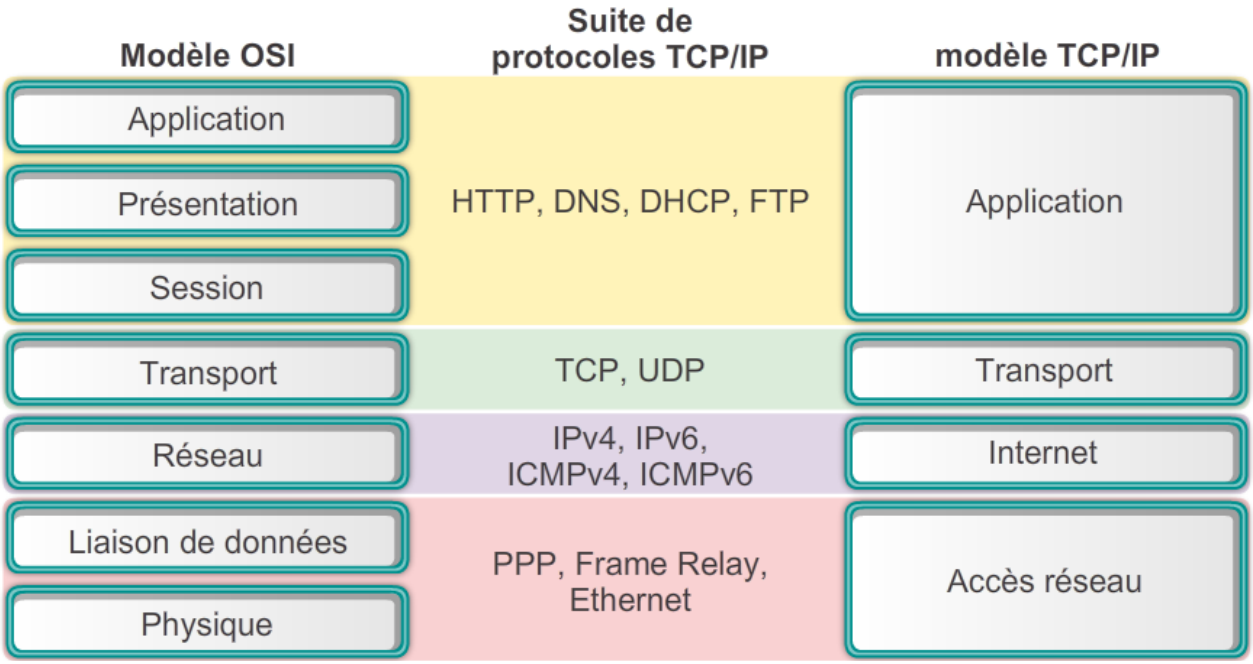

Figure I.7 : Le modèle OSI et le modèle TCP/IP **[14]**

9 Adressage IP

Une adresse IP est une représentation numérique de l'endroit où un appareil est connecté à Internet. Comprendre les bases des adresses IP est essentiel pour se déplacer sur Internet. Le terme « Adresse IP » désigne une « adresse de protocole Internet ». Le protocole Internet est un ensemble de règles qui régissent la communication sur Internet, qu'il s'agisse d'envoyer des messages, de diffuser des vidéos ou de se connecter à un site Web. Une adresse IP identifie un réseau ou un appareil sur Internet. **[15]**

9.1 Format des adresses IP

Il existe deux formats d'adresse IP : Le format IPV4 et le format IPV6.

- **Le format IPv4** : Une adresse IPv4 est une adresse hiérarchique de 32 bits qui se compose d'une partie réseau et d'une partie hôte. Les bits de la partie réseau de l'adresse doivent être identiques pour tous les périphériques installés sur le même réseau. Les bits de la partie hôte de l'adresse doivent être uniques, pour identifier un hôte spécifique dans un réseau. Pour identifier ces deux parties chaque adresse est liée à un masque de sous-réseau ce qui permet de définir sur quel réseau elle se trouve. Le format binaire d'une adresse IP est comme suit : xxxxxxxx. xxxxxxxx. xxxxxxxx. xxxxxxxx (tel que x=0 ou x=1). **[16] (**Figure I .8)

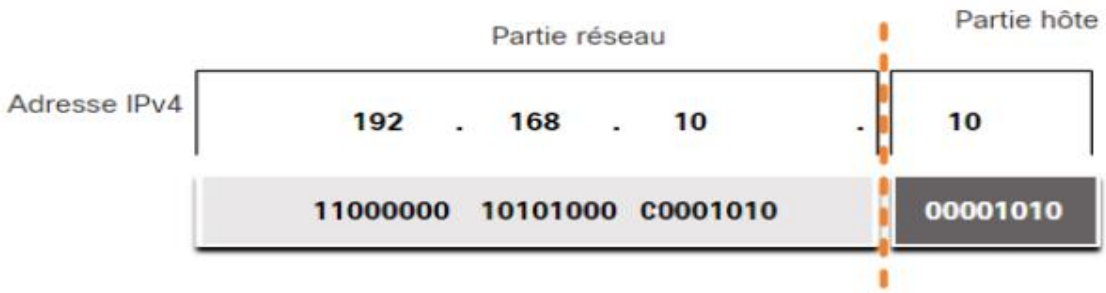

Figure I.8 : Adresse IPv4**[17]**

- ✓ **Masque réseau** : Le masque de réseau sert à séparer les parties réseau et hôtes d'une adresse. On retrouve l'adresse du réseau en effectuant un ET logique bit à bit entre une adresse complète et le masque du réseau.**[18]**
- ✓ **Classes des adresses IP** : Le but de la division des adresses IP en classes, est de facilité la recherche d'un ordinateur sur le réseau. Ainsi, l'attribution des adresses IP se fait

selon la taille du réseau. Globalement, le système d'adressage IPv4 est divisé en cinq classes d'adresses IP. Toutes les cinq classes sont identifiées par le premier octet d'adresse IP

Les classes des adresses IP sont :

- **Classe A :** Entre 0 et 127 inclus.
- **Classe B :** Entre 128 et 191 inclus.
- **Classe C :** Entre 192 et 223 inclus.
- **Classe D :** Entre 224 et 239 inclus.
- **Classe E :** Entre 240 et 255 inclus.

➢ **Format IPv6**

Grâce à l'augmentation de l'espace d'adressage de 32 à 128 bits, ce nouveau protocole permet non seulement de prévenir le risque croissant de ruptures d'adresses, mais aussi de communiquer de manière claire et sans ambiguïté.

Contrairement à IPv4, la version 6 applique formellement l'idée de base des IP, le principe de bout en bout. Les 128 bits des adresses IPv6 sont répartis sur 8 blocs de 16 bits. Un bloc de 16 bits s'écrit avec 4 caractères sous forme hexadécimale (c'est à dire les 10 nombres entiers et 6 lettres de l'alphabet).

Pour séparer ces blocs, on utilise les deux points comme signe de ponctuation. Voici un exemple : 2001 :0620 :0000 :0000 :0211 :24FF : FE80 :C12C. **[19]**

10 Routage

10.1 Définition

Le routage est une technique permettant de transférer des données d'un réseau à un autre. Il s'agit de déterminer le chemin optimal que les paquets de données doivent emprunter pour atteindre leur destination. Le routage prend en compte divers paramètres tels que les protocoles de routage, la topologie du réseau, les coûts associés aux différentes routes possibles, etc. Son objectif principal est de garantir l'acheminement efficace des données tout en évitant les congestions et les pertes de paquets. **[20]**

10.2 Table de routage

Une table de routage est un fichier qui sert à stocker des informations concernant les réseaux connectés directement et les réseaux distants :

- **Les routes connectées directement** : ces routes proviennent des interfaces actives du routeur.
- **Les routes distantes** : ces routes correspondent aux réseaux distants connectés à d'autres routeurs.

La source des entrées de la table de routage est identifiée par un code. Ce code définit comment la route a été découverte. Voici quelques exemples de codes courants :

- ✓ **C** : signale un réseau connecté directement. Les réseaux connectés directement sont automatiquement créés lorsqu'une interface est configurée avec une adresse IP activée.
- ✓ **L** : indique qu'il s'agit d'une route link-local. Les routes link-local sont automatiquement créées lorsqu'une interface est configurée avec une adresse IP et activée.
- ✓ **S** : indique que la route a été créée manuellement par un administrateur pour atteindre un réseau spécifique. Il s'agit d'une route statique.
- ✓ **D** : indique que la route a été découverte dynamiquement à partir d'un autre routeur à l'aide du protocole EIGRP (Enhanced Interior Gateway Routing Protocol).
- ✓ **O** : indique que la route a été découverte dynamiquement à partir d'un autre routeur à l'aide du protocole OSPF (Open Shortest Path First).

10.3 Types de routage

Un routeur peut apprendre des réseaux distants de deux manières :

- ➢ **Routage statique** : les réseaux distants sont saisis manuellement à l'aide de routes statiques. Les routes statiques doivent être reconfigurées manuellement à chaque modification de la topologie réseau.
- ➢ **Routage dynamique** : les routes distantes sont automatiquement acquises via un protocole de routage dynamique.

11 Trafic de données

Le trafic de données se réfère à l'échange de données numériques entre différents appareils ou réseaux. Il peut inclure des informations telles que les fichiers multimédias, les messages, les appels vocaux, les requêtes Internet, etc. Ces données sont transférées via des protocoles de communication tels que TCP/IP. Le trafic de données peut être mesuré en termes de volume de données échangées, de débit (quantité de données transférées par unité de temps) ou de nombre de connexions actives. Comprendre le trafic de données est essentiel pour les opérateurs de télécommunications afin de planifier leurs capacités réseau et de garantir des performances optimales.

11.1 Problématique du trafic de données

La problématique du trafic de données réside dans la capacité limitée des réseaux à traiter simultanément tous les types de trafic. Avec l'expansion constante des données et des applications utilisant le réseau, la congestion devient un problème courant. Le trafic de données non géré peut entraîner des retards, une dégradation de la qualité de service et une utilisation inefficace de la bande passante. Il est donc impératif de trouver des solutions pour gérer le trafic de données de manière efficace afin de garantir une utilisation optimale des ressources réseau.

11.2 Solutions pour gérer le trafic de données

Pour gérer le trafic de données de manière efficace, voici quelques solutions que l'on peut envisager :

- **Utilisation de la bande passante :**
  - ✓ Prioriser les applications et services critiques pour les opérations commerciales.
  - ✓ Limiter la bande passante des applications non essentielles ou récréatives.
- **Mise en cache et compression :**
  - ✓ Mettre en cache les données fréquemment utilisées localement pour réduire la demande de bande passante.
  - ✓ Utiliser des outils de compression pour réduire la taille des données transférées.

- **Optimisation des protocoles :**

✓ Utiliser des protocoles de transfert de données efficaces comme HTTP/2, qui permettent de réduire la latence et d'améliorer les performances.

- **QoS (Qualité de Service) :**

✓ Mettre en place des politiques de QoS pour prioriser certains types de trafic sur d'autres, en fonction de leur importance pour l'entreprise.

12 Conclusion

Dans ce chapitre, les bases essentielles des réseaux informatiques, couvrant leurs types, modèles tels qu'OSI et TCP/IP, l'adressage IP, et les équipements d'interconnexion ont été explorés. Cette base solide prépare le terrain pour notre exploration des réseaux virtuels Vlan dans les prochains chapitres.

Chapitre II : Généralités sur la sécurité

1 Introduction

L'échange de données au sein d'un réseau comporte des risques significatifs en matière de sécurité informatique. Les ordinateurs connectés à un réseau externe, tel qu'Internet, présentent des vulnérabilités pouvant être exploitées par des pirates pour mener leurs attaques. Les conséquences de ces attaques peuvent être graves, incluant le vol d'informations et l'accès à des données confidentielles. Il est donc essentiel de mettre en place des mesures de sécurité pour se protéger contre ces menaces. Dans ce chapitre, nous aborderons les différentes formes d'attaques et les moyens disponibles pour sécuriser les données informatiques.

2 Définition

La sécurité informatique englobe toutes les mesures prises afin de diminuer la vulnérabilité d'un système face aux menaces accidentelles ou intentionnelles. Il est important de repérer les exigences essentielles en matière de sécurité informatique. Elles déterminent ce que les utilisateurs de systèmes informatiques attendent en ce qui concerne la sécurité.

3 Les critères de la sécurité informatique

Pour assurer la sécurité d'un système, il est essentiel de garantir les propriétés suivantes :

- **Confidentialité :** La confidentialité concerne la protection des informations contre tout accès non autorisé. Cela signifie que seules les personnes ou les entités autorisées ont le droit d'accéder, de visualiser ou de manipuler des données sensibles ou confidentielles.
- **Disponibilité *:*** La disponibilité assure que les informations et les systèmes sont accessibles et fonctionnels pour les utilisateurs autorisés au moment où ils en ont besoin.
- **Intégrité :** L'intégrité vise à garantir que les données et les systèmes informatiques restent exacts, complets et non altérés. Il s'agit de prévenir les modifications ou les altérations non autorisées des données ou des configurations système.
- **Authenticité :** L'authenticité concerne la vérification de l'identité des utilisateurs, des appareils et des entités qui tentent d'accéder aux informations ou aux systèmes.

4 Politique de sécurité

Une politique de sécurité, ou stratégie de sécurité, représente une série de directives officielles qui définissent les normes à suivre par les individus ayant accès aux ressources et données de l'entreprise. Son but principal est de protéger le réseau de l'entreprise contre les menaces internes et externes. En d'autres termes, une politique de sécurité établit un ensemble de règles, de procédures et de bonnes pratiques visant à garantir un niveau de sécurité adapté aux besoins de l'organisation. Ses objectifs incluent l'identification des risques informatiques et de leurs éventuelles conséquences, l'élaboration de règles et de procédures adaptées aux risques identifiés dans les différents services de l'organisation, ainsi que la surveillance et la détection des failles du système informatique. [21]

4.1 Principes génériques d'une politique de sécurité réseau

Pour assurer une politique de sécurité réseau efficace et éviter les erreurs courantes, il est crucial de respecter plusieurs principes fondamentaux. Ces principes aident à clarifier les défis associés à la rédaction d'un document de politique de sécurité réseau, qui revêt une importance particulière par rapport à d'autres types de documents.

La rédaction d'une politique de sécurité réseau peut varier, allant d'un document unique à un ensemble de politiques distinctes. Ce choix dépend souvent de la taille de l'entreprise : plus elle est grande, plus il est nécessaire de segmenter les documents, chaque niveau se référant au niveau supérieur pour assurer une cohérence et une efficacité globale.

Quelle que soit la nature des biens produits par l'entreprise, sa politique de sécurité réseau vise à satisfaire les critères suivants : [22]

- **Identification** : Processus permettant de déclarer qui vous prétendez être dans un système informatique, allant d'un nom d'utilisateur à des méthodes avancées comme les empreintes digitales ou les analyses faciales.
- **Authentification** : Validation de l'identité déclarée pour vérifier que vous êtes bien la personne que vous prétendez être. Cela peut inclure des méthodes simples comme les mots de passe ou des méthodes plus sécurisées combinant quelque chose que vous possédez avec quelque chose que vous connaissez.

- **Autorisation** : Détermination des ressources de l'entreprise auxquelles un utilisateur identifié a accès et des actions qu'il est autorisé à effectuer sur ces ressources.
- **Confidentialité** : Protection des données afin qu'elles restent privées entre l'émetteur et le destinataire, assurée par des techniques comme le chiffrement des données.
- **Intégrité** : Garantie que les informations n'ont pas été altérées ou corrompues de manière non autorisée.
- **Disponibilité** : Assurance que les ressources de l'entreprise, incluant l'architecture réseau et les plans de sauvegarde, sont accessibles selon les besoins.
- **Non-répudiation** : Mécanisme assurant qu'un émetteur ne peut nier avoir envoyé un message et que le destinataire ne peut nier l'avoir reçu
- **Traçabilité** : Capacité à retrouver et à examiner les opérations effectuées sur les ressources de l'entreprise en archivant tous les événements applicatifs pour des investigations ultérieures.

5 Menaces

Une menace informatique se réfère à toute action susceptible de porter atteinte à un système informatique. En termes de sécurité informatique, ces menaces peuvent découler de diverses activités malveillantes. Elles émanent d'adversaires déterminés qui sont capables d'exploiter des vulnérabilités pour mener leurs attaques.

5.1 Type de menaces

En matière de réseaux, les menaces peuvent également être classées en deux catégories : les menaces accidentelles et les menaces intentionnelles.

5.1.1 Menaces accidentelles

Ces menaces sont dues à des erreurs involontaires des utilisateurs, telles que la perte accidentelle de données, la dégradation ou la destruction involontaire de matériel, ou encore les copies illicites de logiciels.

5.1.2 Menaces intentionnelles

Ces menaces résultent d'actions délibérées menées par des entités visant à violer la sécurité de l'information et à utiliser les ressources de manière non autorisée. Elles se divisent en deux catégories : passives et actives.

- **Menaces passives :** une menace passive consiste à écouter le trafic réseau ou les communications d'une machine cible. L'interface de la machine attaquante est en mode écoute. L'objectif est de capturer des trames du réseau cible pour rechercher des informations sensibles comme des clés de cryptage, des mots de passe ou d'autres données. Cette attaque est réalisée à l'aide d'outils tels que les sniffers et les scanners.
- **Menaces actives :** contrairement aux menaces passives, ici, l'attaquant n'est pas en mode écoute, mais agit pour modifier des données ou des messages, s'introduire dans des équipements réseau, perturber le bon fonctionnement du réseau, ou interroger le réseau cible. L'attaquant peut aussi contourner les dispositifs de sécurité existants en utilisant diverses méthodes, telles que les attaques par déni de service (DoS) et les virus.

6 Attaques informatiques

Tous les ordinateurs connectés à un réseau informatique peuvent être vulnérables à des attaques. Une attaque se produit lorsqu'une faille dans un système informatique (comme un système d'exploitation, un logiciel ou même une erreur commise par l'utilisateur) est exploitée à des fins nuisibles et souvent inconnues de l'utilisateur du système. [23]

6.1 Types d'attaques

Les attaquants informatiques utilisent plusieurs techniques d'attaques, lesquelles peuvent être classées en deux grandes familles :

6.1.1 Attaques directes

C'est l'une des attaques les plus simples où un hacker attaque directement sa victime à partir de son propre ordinateur. La plupart des "script kiddies" utilisent cette technique car les programmes de piratage qu'ils utilisent sont généralement peu configurables. Beaucoup de ces outils envoient les paquets directement à la victime sans beaucoup de personnalisation. **(Voir figure II.1)**

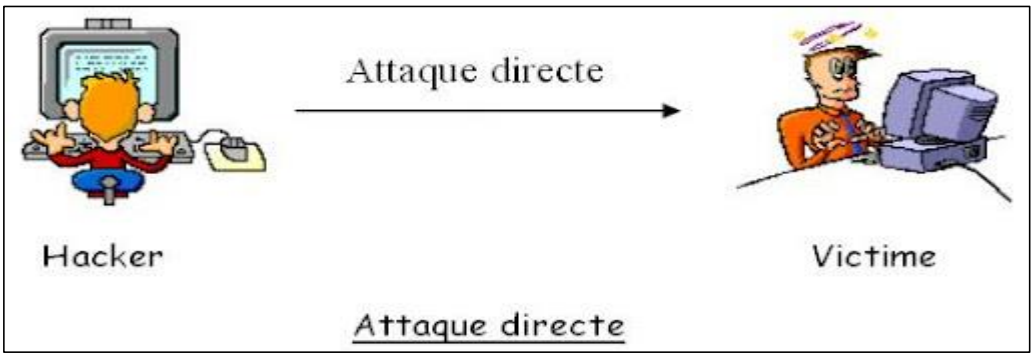

Figure II.1 : Attaque directe [24]

6.1.2 Attaques indirectes

- **Attaques indirectes par rebond :** Les attaques indirectes par rebond sont très appréciées des hackers pour deux raisons principales : (Voir figure II.2)

1. Elles permettent de masquer l'identité (c'est-à-dire l'adresse IP) du hacker en utilisant un ordinateur intermédiaire comme relais.
2. Elles permettent éventuellement d'utiliser les ressources plus puissantes (comme le CPU et la bande passante) de l'ordinateur intermédiaire pour intensifier l'attaque.

Le principe est relativement simple : les paquets d'attaque sont initialement envoyés à l'ordinateur intermédiaire, qui les répercute ensuite vers la véritable cible, d'où le terme "rebond" .

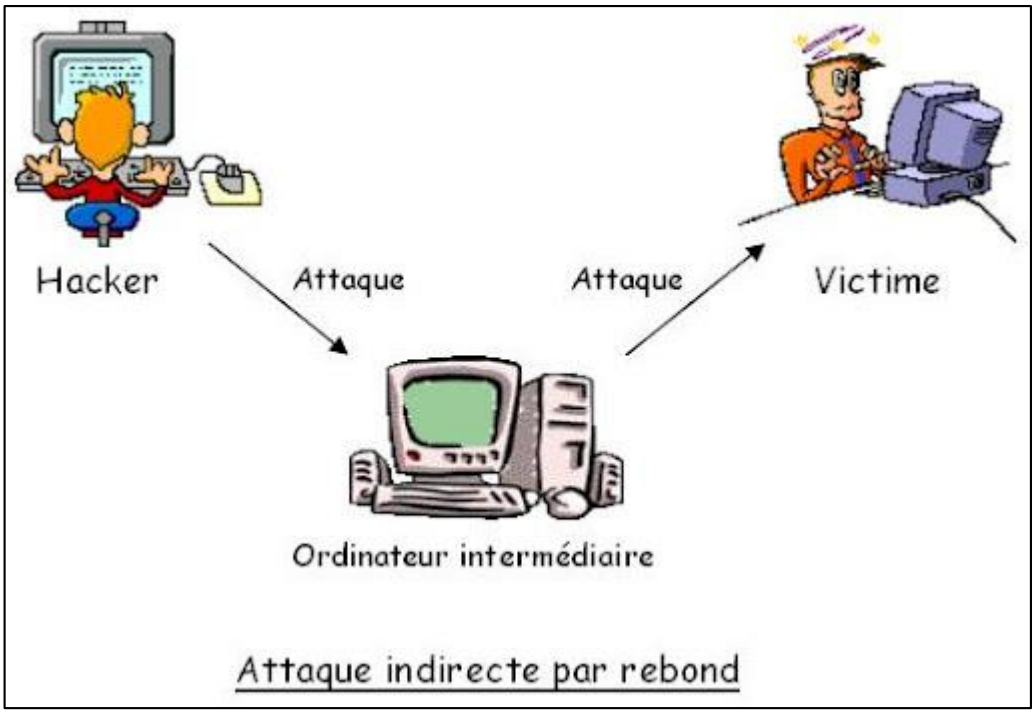

Figure II.2 : Attaque indirecte par rebond [25]

6.1.3 **Attaques indirectes par réponse :** cette attaque est une variante de L'attaque par rebond et partage les mêmes avantages du point de vue de l'hacker. Cependant, au lieu d'envoyer directement une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant envoie une requête à cet ordinateur. C'est la réponse à cette requête qui est ensuite dirigée vers l'ordinateur victime. **(Voir figure II.3)**

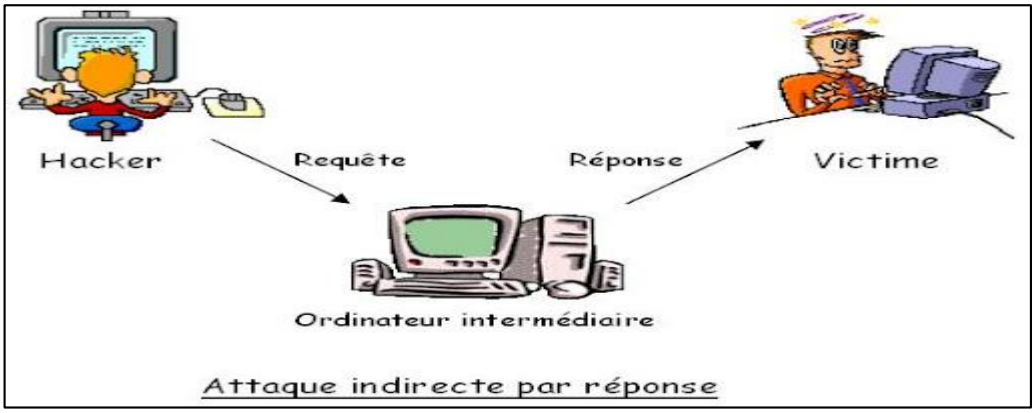

Figure II.3 : Attaque indirecte par réponse **[26]**

7 Contre-mesures de différentes attaques

Pour se défendre contre différentes attaques informatiques, voici quelques contre-mesures efficaces :

7.1 Antivirus

Les logiciels antivirus sont des logiciels capables de détecter des virus sur un ordinateur, capables de placer en quarantaine les fichiers infectés et parfois même de les réparer sans causer de dommages. Ils utilisent différentes méthodes pour cela, comme :

- ✓ Le contrôle général du système de l'ordinateur
- ✓ La surveillance des lecteurs de supports amovibles

7.2 Pare feu (firewall en anglais)

Un pare-feu est un dispositif de sécurité qui supervise et gère le trafic réseau entrant et sortant pour garantir la sécurité et la confidentialité des données des systèmes protégés**,** il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseaux suivantes :

- ✓ Une interface pour le réseau à protéger (réseau interne)
- ✓ Une interface pour le réseau externe [27]. (Voir figure II.4).

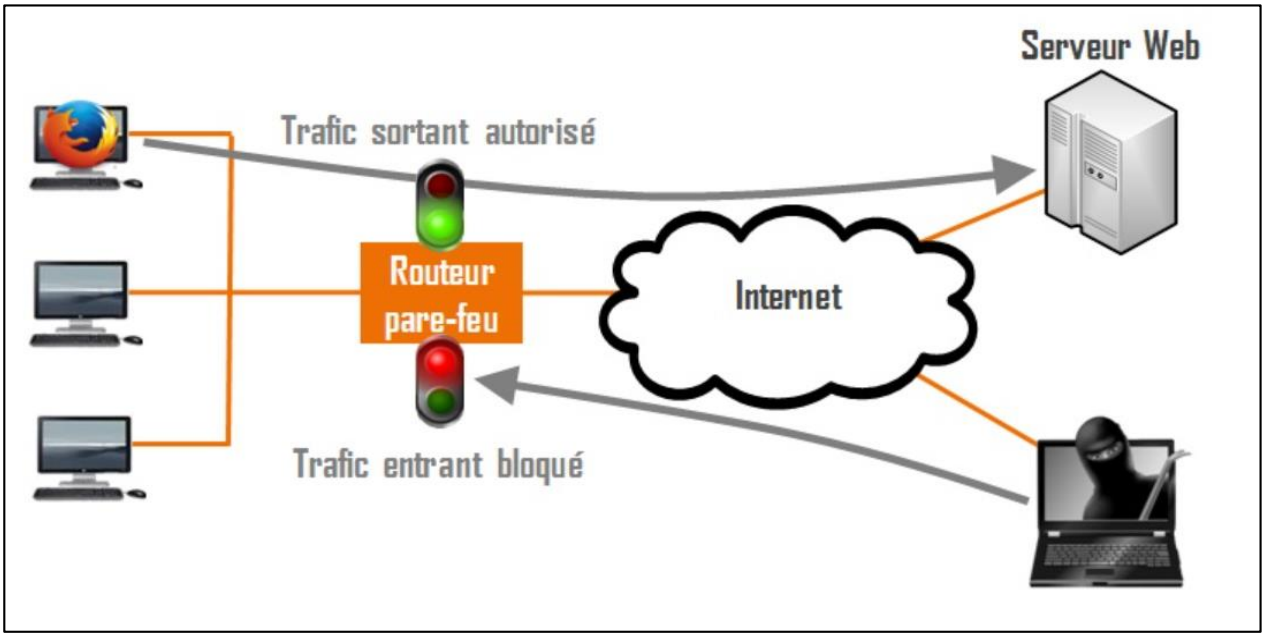

Figure II.4 : Fonctionnement d'un Pare feu[28]

7.3 Le proxy

Le principe de fonctionnement fondamental d'un serveur proxy est simple : lorsqu'un utilisateur utilise une application configurée pour accéder à Internet via un serveur proxy, l'application établit d'abord une connexion avec le serveur proxy et lui envoie sa requête. Le serveur proxy à son tour se connecte au serveur distant que l'application souhaite atteindre, transmet la requête à ce serveur, reçoit la réponse, puis la renvoie à l'application cliente. (Voir figure II.5)

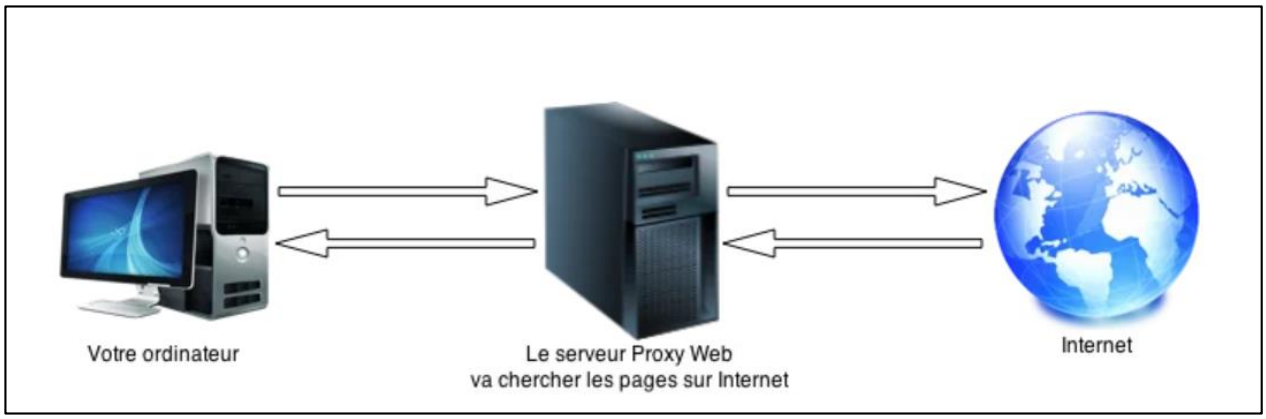

Figure II.5 : Fonctionnement d'un proxy[29]

Votre ordinateur demande les pages au Proxy. Celui-ci va chercher les pages et les retourne à votre ordinateur.

7.4 VLAN

Les VLANs permettent de regrouper des serveurs et des postes de travail en ensembles distincts et indépendants au sein d'un réseau local. Ils offrent une solution flexible pour segmenter le réseau et améliorer la gestion de la communication au sein de l'entreprise.

Un VLAN peut être défini de plusieurs manières, en fonction de critères tels que :

- **Numéro de port** : pour identifier les équipements connectés à des ports spécifiques.
- **Adresse IP** : pour regrouper des appareils ayant des adresses IP similaires ou appartenant à un même sous-réseau.
- **Adresse MAC** : en utilisant les adresses MAC des périphériques pour déterminer leur appartenance à un VLAN.

- **Adresse IP multicast** : pour regrouper les périphériques qui reçoivent le même flux multicast.
- **Protocole utilisé** : pour isoler des types de trafic spécifiques, comme le trafic VoIP ou vidéo.
- **Application utilisée** : pour regrouper des appareils utilisant une même application critique ou spécifique.

Il est également possible de définir un VLAN en fonction de critères de gestion, tels que l'utilisation d'un logiciel ou d'un matériel commun pour assurer une communication efficace.

En pratique, il est recommandé de créer des VLAN de taille réduite plutôt que de regrouper un grand nombre de stations. Cela permet une gestion plus précise et efficace du trafic réseau. Il est également crucial de ne pas regrouper des stations qui ne sont pas dans la même zone de diffusion, car cela nécessiterait une gestion complexe des tables de routage pour assurer une communication adéquate entre les VLANs.

7.5 DMZ

DMZ (zone démilitarisée) est un réseau périmétrique situé entre le réseau interne sécurisé d'une organisation (LAN) et Internet ou d'autres réseaux non fiables.

L'objectif principal d'une DMZ est de permettre à une organisation de fournir des services accessibles depuis Internet tout en minimisant les risques pour son réseau privé. Typiquement, les services et les serveurs hébergés dans une DMZ incluent des serveurs DNS, des serveurs FTP, des serveurs de messagerie, des serveurs proxy, des serveurs VoIP (Voice over IP) et des serveurs Web.

En isolant ces services dans la DMZ, l'organisation réduit la surface d'attaque potentielle sur son réseau interne, car les services exposés au public sont séparés des données et des systèmes sensibles hébergés à l'intérieur du LAN sécurisé. [30]

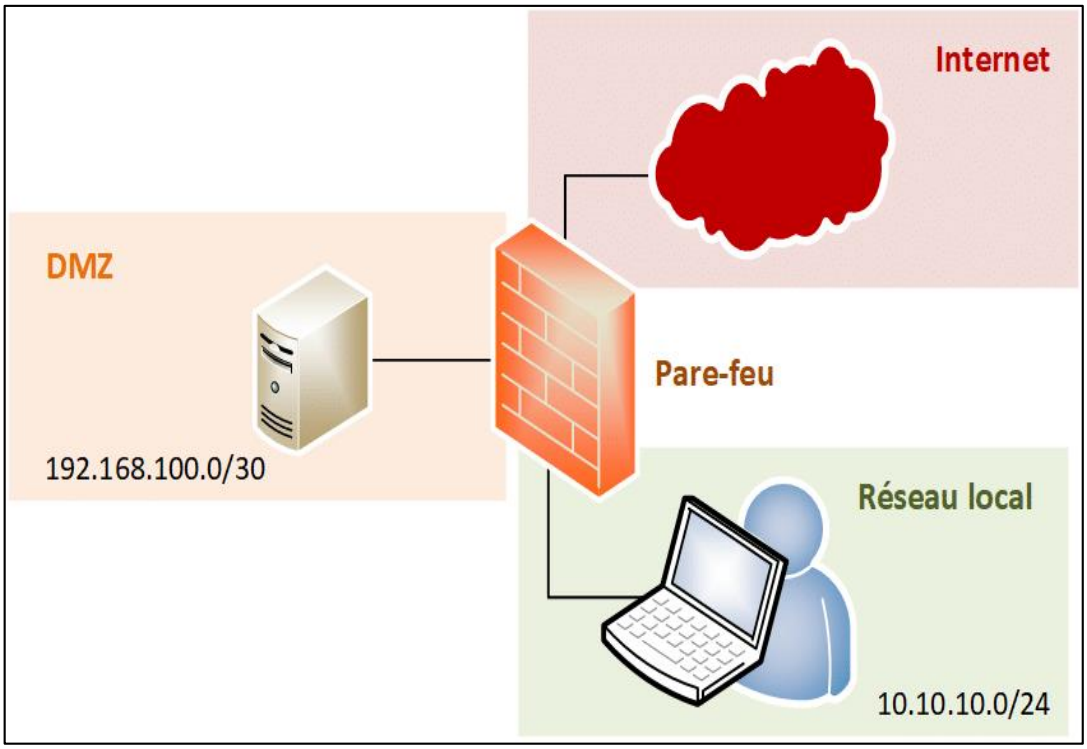

Figure II.6 : DMZ[31]

8 Protocoles de sécurité

Les protocoles de sécurité du réseau sont conçus pour remédier à ce manque de sécurité.

8.1 Protocole SSH

SSH, ou Secure Socket Shell, est un protocole réseau qui permet aux administrateurs de se connecter à distance à un ordinateur de manière sécurisée. SSH désigne également l'ensemble des outils qui mettent en œuvre ce protocole. Il garantit une authentification forte et des communications chiffrées, sécurisant ainsi les échanges de données entre deux ordinateurs connectés sur un réseau non sécurisé, comme Internet. SSH est largement utilisé par les administrateurs réseau pour gérer à distance des systèmes et des applications. Il leur permet de se connecter à d'autres ordinateurs, d'exécuter des commandes à distance et de transférer des fichiers entre machines. [32]

8.2 Protocole IPsec

IPsec est un ensemble de protocoles de communication permettant d'établir des connexions sécurisées sur un réseau. Le protocole Internet (IP) est la norme qui détermine comment les données circulent sur Internet. IPSec ajoute des mécanismes de chiffrement et d'authentification pour rendre les communications IP plus sûres. Par exemple, il chiffre les données à leur source et les déchiffre à leur destination, garantissant ainsi la confidentialité des informations. De plus, IPSec authentifie la source des données, assurant que les informations proviennent bien de l'expéditeur attendu. [33]

Les protocoles IPSec reposent sur trois modules clés pour sécuriser les communications réseau :

- **Authentication Header (AH)** : assure l'intégrité, l'authentification et la protection contre le rejeu des paquets à encapsuler.
- **Encapsulating Security Payload (ESP**) **:** définit le chiffrement des paquets assurant la sécurité, l'intégrité, l'authentification et la protection contre le rejeu.
- **Security Associations (SA) :** définissent les paramètres de sécurité et les clés pour sécuriser les communications IPSec.

8.3 Protocole SSL

SSL, ou Secure Sockets Layer, est un protocole de sécurité Internet basé sur le chiffrement. Il a été développé pour la première fois par Netscape afin de garantir la confidentialité, l'authentification et l'intégrité des données dans les communications Internet. SSL est le prédécesseur du chiffrement moderne TLS, qui est utilisé aujourd'hui.

Un site web qui met en œuvre le protocole SSL/TLS comporte « HTTPS » dans son URL au lieu de « HTTP ».

8.4 Protocole HTTPs

Le protocole HTTPS (Hyper Text Transfer Protocol Secure) est une extension sécurisée du protocole HTTP. Le « S » signifie « Secure » (sécurisé), utilisé principalement pour l'envoi de données entre un navigateur web et un site web. HTTPS chiffre les données échangées afin de renforcer la sécurité du transfert. Ceci est particulièrement important lorsque les utilisateurs

transmettent des informations sensibles, par exemple lors de la connexion à un compte bancaire, à un service de messagerie électronique, ou à un prestataire d'assurance maladie. [34]

9 Conclusion

De nos jours, garantir la sécurité des systèmes dans les réseaux devient de plus en plus difficile. Pour répondre à cette complexité, de nouvelles méthodes sont régulièrement développées pour détecter, contrôler et contrer les attaques et les menaces qui visent ces systèmes. Cette évolution constante est essentielle pour maintenir la fiabilité des infrastructures face à une variété croissante de cybermenaces.

Dans ce chapitre, nous avons abordé de manière générale les concepts fondamentaux de la sécurité informatique, notamment les critères de sécurité, les menaces, les risques et les vulnérabilités. Ensuite, nous avons présenté les différentes contre-mesures et protocoles de sécurité réseau disponibles.

Chapitre III : VLAN et routage inter-VLAN

1 Introduction

Un VLAN est une solution permettant de segmenter un réseau local physique en sous-réseaux logiques distincts. Chaque VLAN est traité comme un réseau indépendant avec ses propres règles de communication et ses propres adresses IP.

Les VLANs sont largement utilisés dans les environnements professionnels pour regrouper des utilisateurs ou des systèmes en fonction de leurs besoins spécifiques. Pour faciliter la communication entre différentes VLANs dans un réseau, le routage inter VLAN est utilisé. Pour ce faire, il est possible de créer des chemins de communication entre les VLANs, permettant aux utilisateurs d'accéder à des ressources situées sur des VLANs différents. Cette fonctionnalité est essentielle pour optimiser les performances, renforcer la sécurité et permettre une gestion flexible des adresses IP au sein d'un réseau VLAN.

Ce chapitre est divisé en deux parties. Dans la première partie, nous allons explorer les bases en définissant les VLAN, leurs avantages, leur classification, les différents types et leur fonctionnement, ainsi que les concepts de VLAN statiques et dynamiques. De plus, nous aborderons les protocoles et normes associés aux VLAN qui jouent un rôle crucial dans la configuration et la gestion des VLAN.

Dans la deuxième partie, nous abordons le routage inter-VLAN en détaillant son fonctionnement ainsi que les diverses méthodes employées. Nous examinons également les défis liés à sa configuration et proposons des solutions appropriées.

2 Réseau Locaux virtuelles

Un VLAN, ou Réseau Local Virtuel (Virtual Local Area Network), constitue une méthode de découpage logique d'un réseau informatique, permettant de le subdiviser en plusieurs sous-réseaux virtuels qui opèrent de manière indépendante en termes de communication. Chaque VLAN se comporte comme s'il était un réseau local distinct, même s'il partage l'infrastructure physique commune avec les autres VLAN. **[35]**

2.1 Avantages d'un VLAN

Le VLAN offre la possibilité de créer un réseau logique au sein du réseau physique existant, ce qui présente plusieurs avantages :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs
- Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées
- Réduction de la diffusion du trafic sur le réseau
- Réduction des coûts : des économies sont réalisées grâce à l'utilisation plus efficace de la bande passante.**[36]**

3 Classification des VLAN

Pour attribuer un équipement à un réseau VLAN, Trois méthodes sont généralement utilisées : **[37]**

- ✓ VLAN par port.
- ✓ VLAN d'adresses MAC**.**
- ✓ VLAN d'adresses IP.

3.1 VLAN de niveau 1 (VLAN par port)

Un Vlan par port est une technologie qui permet aux administrateurs réseau d'attribuer manuellement des VLAN à chaque port de commutateur. Elle convient à un réseau de petite taille sans qu'il soit nécessaire de modifier fréquemment l'infrastructure du réseau. (Figure III.1)

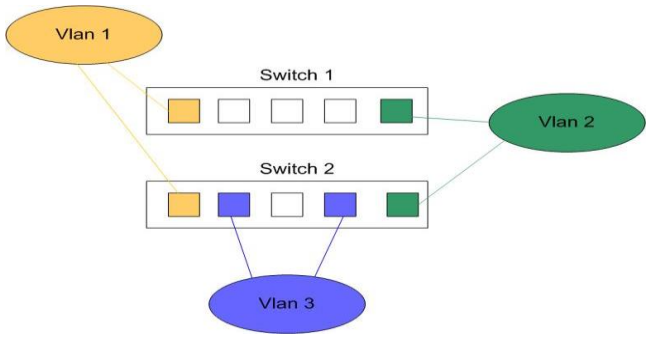

Figure III.1 : VLAN par port **[38]**

3.2 VLAN de niveau 2 (VLAN d'adresses MAC)

VLAN d'adresse MAC consiste à attribuer des VLAN en fonction de l'adresse MAC source des trames. L'application de cette technologie peut améliorer considérablement la sécurité et la flexibilité du réseau. Même si les utilisateurs changent fréquemment d'emplacement physique, l'administrateur réseau n'aura pas besoin de reconfigurer les VLAN. (Figure III .2)

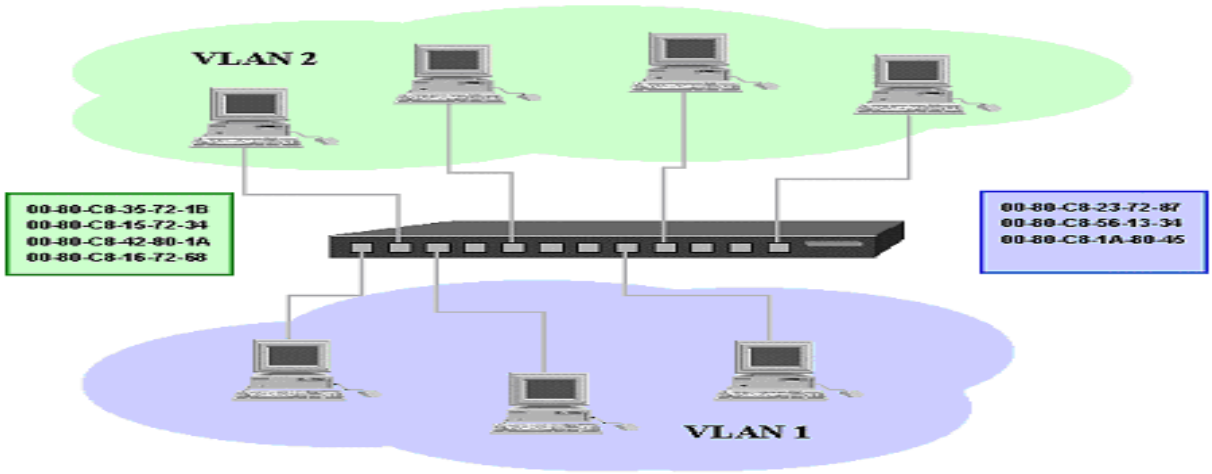

Figure III.2 : VLAN par adresse MAC **[39]**

3.3 VLAN de niveau 3 (VLAN d'adresses IP)

Vlan d'adresses IP est une méthode de segmentation du réseau dans laquelle les VLAN sont configurés en fonction des adresses IP des périphériques. Cette approche permet de créer des VLAN distincts pour différents sous-réseaux IP, ce qui peut faciliter la gestion du trafic et renforcer la sécurité du réseau. (Figure III.3)

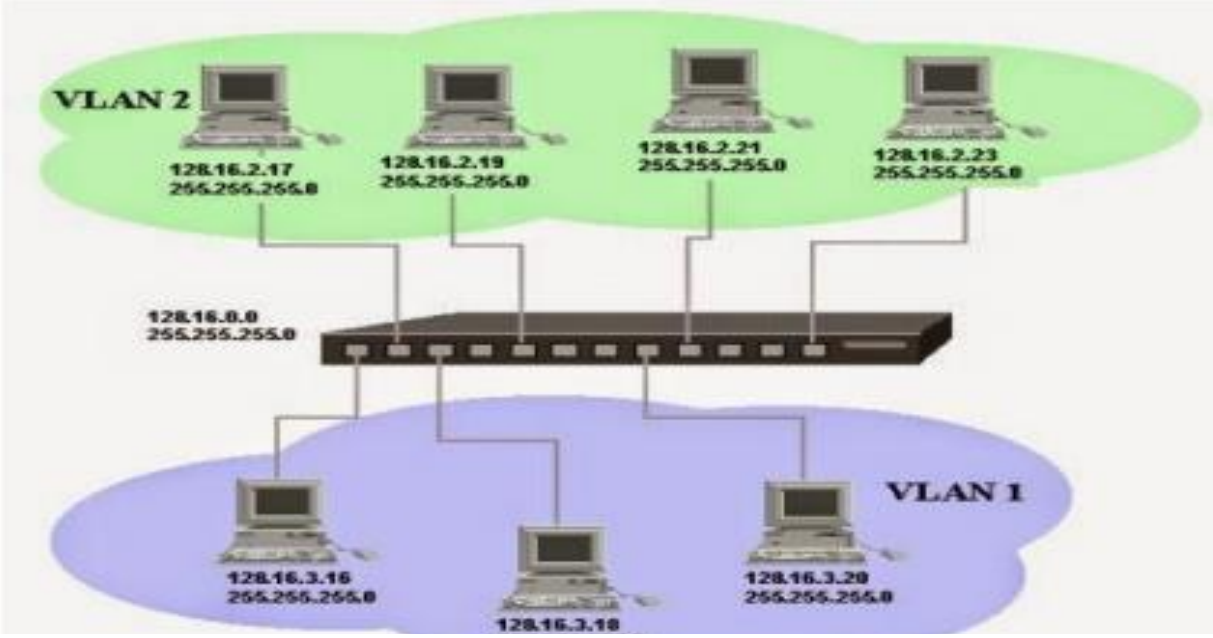

Figure III.3 : VLAN par adresse IP **[40]**

4 Types de VLAN

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

4.1 VLAN de données

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

en les isolant du trafic d'autres VLAN. Les vlan de données sont également appelés VLAN utilisateur.

4.2 VLAN par défaut :

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

4.3 VLAN natif :

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

4.4 VLAN de gestion :

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

4.5 Vlan de voix :

Le VLAN de voix est configuré pour acheminer le trafic vocal. Les VLAN vocaux bénéficient pour la plupart d'une priorité de transmission élevée par rapport aux autres types de trafic réseau. Pour garantir la qualité de la voix sur IP (VoIP) (délai inférieur à 150 millisecondes (ms) sur le réseau), nous devons disposer d'un VLAN voix séparé car cela préservera la bande passante pour les autres applications.

Les VLAN dynamiques prennent en charge la mobilité instantanée des périphériques finaux. Lorsque nous déplaçons un périphérique d'un port à un autre d'un commutateur, les VLAN dynamiques configurent automatiquement l'appartenance au VLAN.

5 Agrégation de VLAN :

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

Le trunking est couramment utilisé pour connecter des commutateurs de niveau d'accès à des commutateurs de niveau de distribution ou à des routeurs. Il permet de transporter efficacement le trafic de plusieurs VLAN sur une seule connexion. Les protocoles courants pour le trunking sont IEEE 802.1Q et ISL (Inter-Switch Link).

- **IEEE 802.1Q :**

Le standard IEEE 802.1Q définit le contenu de la balise de VLAN (VLAN tag) il n'est pas une encapsulation de plus mais un ajout d'une étiquette ou un TAG dans l'en-tête de la trame (un ensemble de champs juste après le champ d'adresse MAC d'origine). Cette étiquette a une taille de 4 octets ou 32 bits. Vu que la trame sera modifiée, le commutateur recalculera la valeur du champ FCS**. [41]** (Figure III.4)

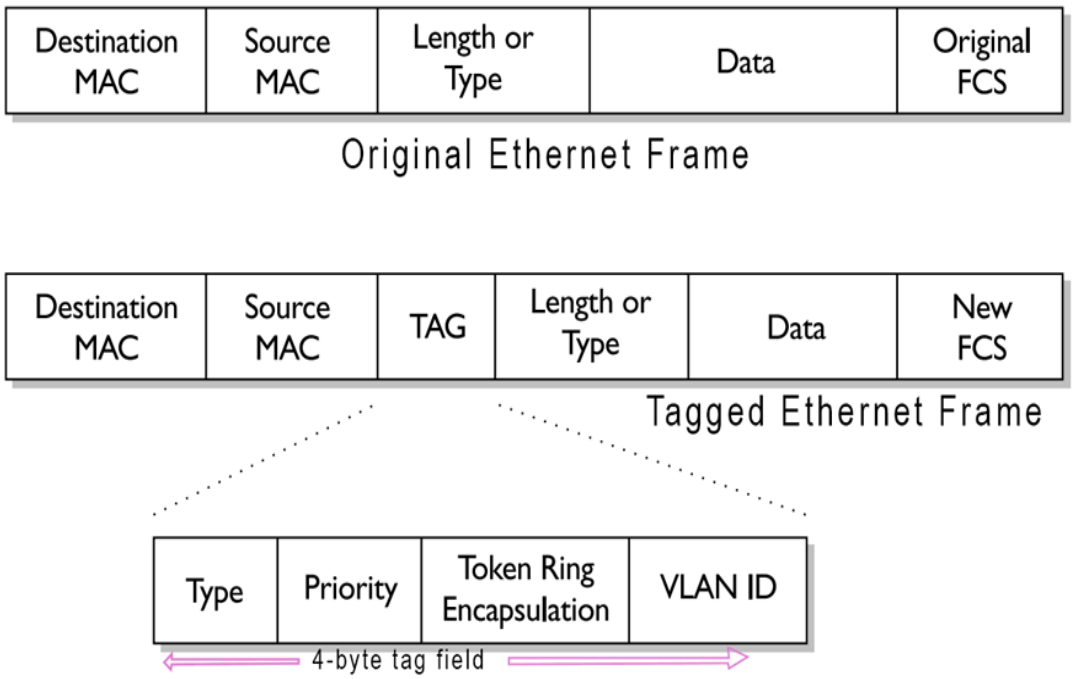

Figure III.4 : IEEE 802.1Q**[42]**

- **ISL (Inter-Switch Link)**

Le protocole ISL (Inter-Switch Link) est une technique de trunking utilisée pour transporter les VLAN à travers le réseau. Ce protocole a été développé par Cisco pour permettre aux commutateurs de reconnaître les différents VLAN transportés sur la liaison trunk.**[43]** (Figure II .5)

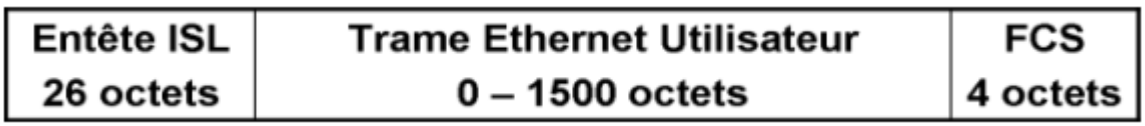

Figure III.5: ISL (Inter-Switch Link) **[44]**

6 VTP (Virtual Trunking Protocol)

Le protocole VTP (VLAN Trunking Protocol) est utilisé pour configurer et administrer les VLANs sur les périphériques CISCO. Il permet d'ajouter, de renommer ou de supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur, et cette nouvelle configuration

est propagée à l'ensemble des autres commutateurs du réseau. Le VTP permet ainsi d'éviter toute incohérence de configuration de VLANs sur l'ensemble d'un réseau local.

6.1 Fonctionnement

Un domaine VTP est composé d'un ou de plusieurs équipements interconnectés qui partagent le même nom de domaine VTP. Un commutateur ne peut appartenir qu'à un seul domaine VTP. Lorsqu'un message VTP est transmis aux autres commutateurs du réseau, il est encapsulé dans une trame de protocole d'agrégation comme ISL ou IEEE 802.1Q.**[45]**

Les commutateurs VTP exécutent l'un des trois modes suivants :

- **VTP Server :** peuvent créer, modifier et supprimer un VLAN et des paramètres de configuration VLAN pour l'ensemble du domaine. Les serveurs VTP enregistrent les informations de configuration VLAN dans la mémoire NVRAM du commutateur. Les serveurs VTP envoient des messages VTP par tous les ports multi-VLAN. (Figure III .6)

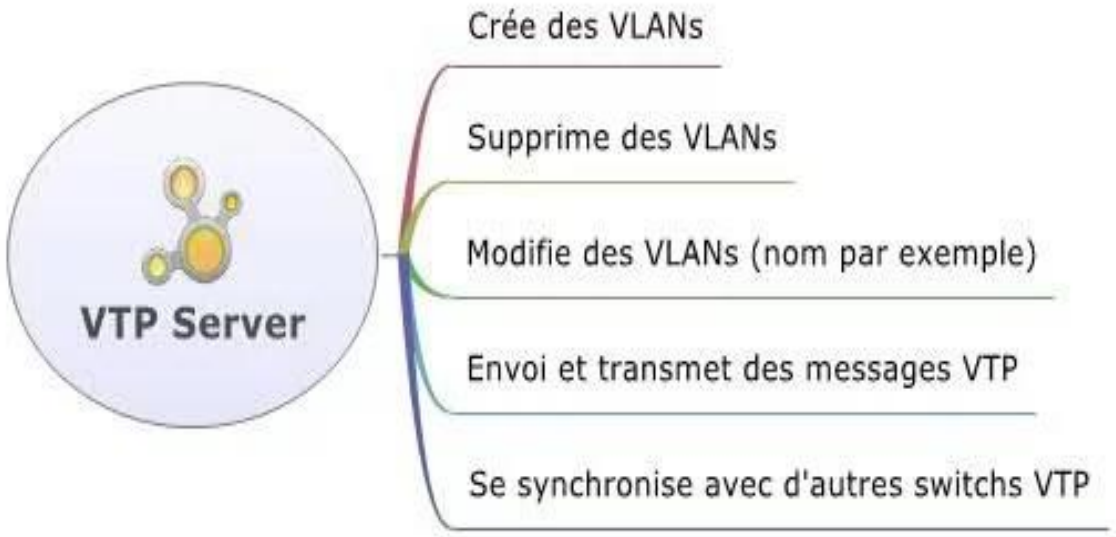

Figure III.6: VTP Server.**[46]**

- **VTP client :** ne peuvent pas créer, modifier ou supprimer des informations VLAN. Ce mode est utile pour les commutateurs qui manquent de mémoire pour stocker de grandes tables d'informations VLAN. Le seul rôle des clients VTP est de traiter les modifications VLAN et d'envoyer des messages VTP par tous les ports multi-VLAN. (Figure III.7)

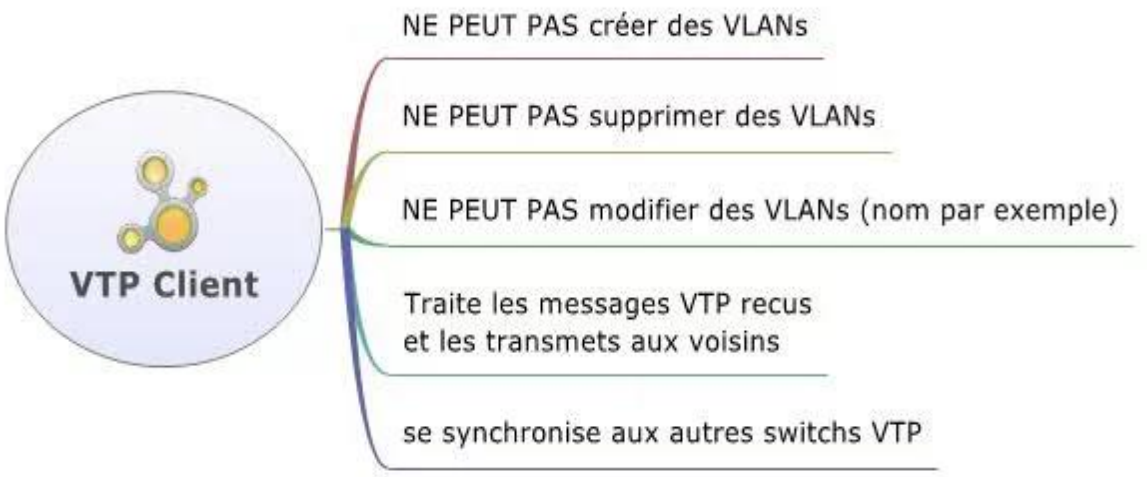

Figure III.7: VTP Client.**[47]**

➢ **VTP Transparent :** transmettent des annonces VTP mais ignorent les informations contenues dans le message. Un commutateur transparent ne modifie pas sa base de données lors de la réception de mises à jour et il n'envoie pas de mises à jour indiquant une modification apportée à son état VLAN. Excepté pour la transmission d'annonces VTP, le protocole VTP est désactivé sur un commutateur transparent.

Chaque fois qu'un commutateur reçoit une mise à jour avec un numéro de révision de configuration supérieur, il remplace les informations stockées par les nouvelles informations envoyées dans la mise à jour VTP. (Figure III.8)

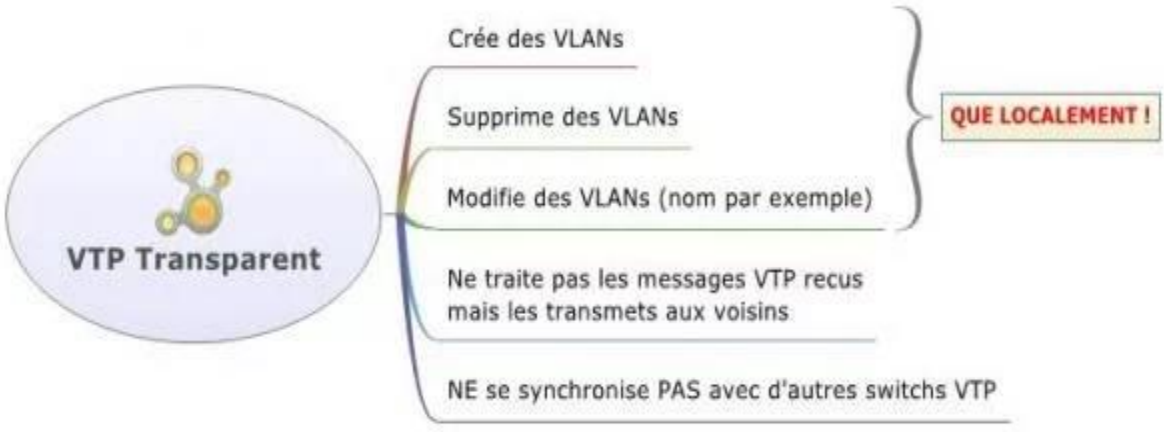

Figure III.8: VTP Transparent.**[48]**

7 Mode 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).**[49]** (Figure III.9)

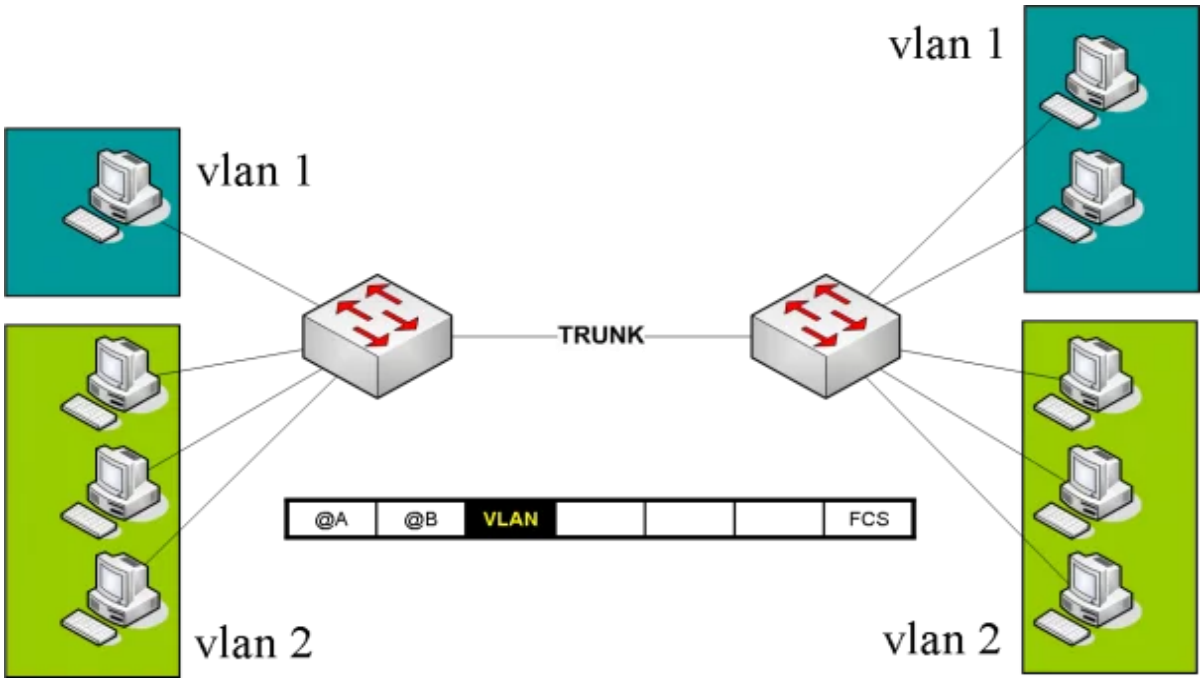

Figure III.9 : Configuration de liens inter-switch en trunk .**[50]**

Les trunks peuvent être utilisés :

- **Entre deux commutateurs** : C'est le mode de distribution des réseaux locaux le plus courant. En utilisant des trunks entre deux commutateurs, on permet le passage du trafic de plusieurs VLANs sur une seule connexion physique, ce qui facilite la gestion et la distribution du trafic entre les différents segments du réseau local.
- **Entre un commutateur et un hôte** : C'est un mode de fonctionnement à surveiller étroitement. Lorsqu'un hôte supporte le trunking, il a la capacité d'analyser le trafic

de tous les réseaux locaux virtuels auxquels il est connecté. Cela peut poser des problèmes de sécurité ou de confidentialité si le trafic n'est pas correctement isolé ou filtré.

- **Entre un commutateur et un routeur** : C'est le mode de fonctionnement qui permet d'accéder aux fonctions de routage, notamment à l'interconnexion des réseaux virtuels par routage inter-VLAN. En connectant un commutateur à un routeur via un trunk, on peut permettre au routeur de router le trafic entre les différents VLANs, offrant ainsi une connectivité entre eux. Cela résout le premier problème énoncé, qui est celui de l'interconnexion des VLANs.

8 Routage inter-VLAN

Le routage inter-VLAN est un processus qui permet de transférer du trafic réseau d'un VLAN à un autre à l'aide d'un périphérique de couche 3 comme un routeur ou un commutateur multicouche. Chaque VLAN est un domaine de diffusion unique, et chaque VLAN dispose une adresse IP réseaux. Si un ordinateur veut échanger avec une adresse IP qui ne fait pas partie de son réseau il devra passer par sa passerelle par défaut qui va nous permettre de faire communiquer plusieurs réseaux différents. .**[51]**

9 Importance du routage inter vlan

Le routage inter vlan revêt une importance majeure dans les réseaux informatiques. Il permet de segmenter le trafic réseau en fonction des besoins spécifiques de chaque VLAN, améliorant ainsi les performances et la sécurité du réseau. Grâce au routage inter vlan, les utilisateurs peuvent accéder aux ressources partagées et interagir les uns avec les autres, même s'ils se trouvent dans des VLANs différents. Cette méthode offre une plus grande flexibilité dans l'organisation et la gestion du réseau, permettant de mieux contrôler les flux de données et d'optimiser les ressources disponibles.

10 Les méthodes de routage inter-VLAN

Il existe 3 options de routage inter-VLAN :

- **Routage inter-VLAN hérité :** Il s'agit d'une solution ancienne.

- ✓ **Router-on-a-Stick** : C'est une solution acceptable pour un réseau de petit à moyen taille.
- ✓ **Commutateur de couche 3 utilisant des interfaces virtuelles commutées (SVI) :** C'est une solution acceptable pour un réseau de petit à moyen taille.

10.1 Routage inter-VLAN Hérité

La première solution de routage inter-VLAN reposait sur des routeurs dotés de plusieurs interfaces Ethernet. Chaque interface devait être connectée à un port de commutateur dans différents VLAN. Les interfaces de routeur ont servi de passerelles par défaut vers les hôtes locaux du sous-réseau VLAN.

Par exemple, reportez-vous à la topologie où R1 a deux interfaces connectées au commutateur S1.**[52]**

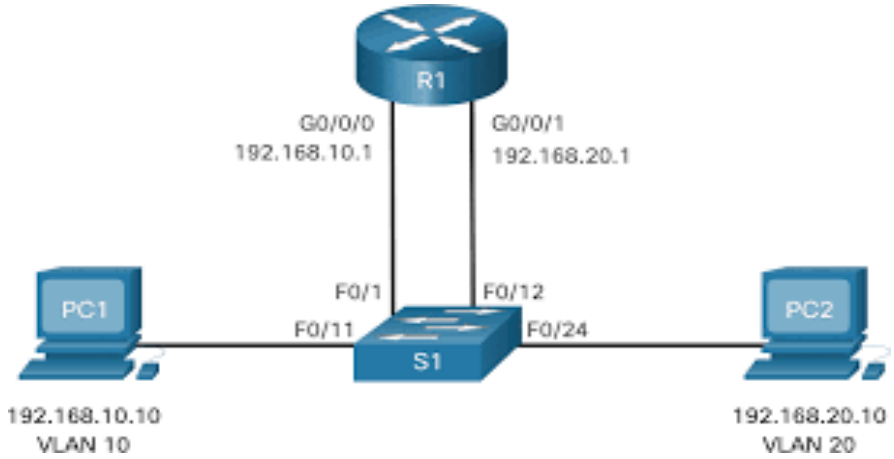

Figure III.10 : Exemple de routage inter-VLAN **[53]**

Notez dans l'exemple de table d'adresses MAC de S1 est rempli comme suit :

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

Port	Adresse MAC	VLAN
F0/1	R1 G0/0/0 MAC	10
F0/11	PC1 MAC	10
F0/12	R1 G0/0/1 MAC	20
F0/24	PC 2 MAC	20

Table III.1 : Table d'adresses MAC pour S1

Lorsque PC1 envoie un paquet à PC2 sur un autre réseau, il le transfert à sa passerelle par défaut 192.168.10.1. R1 reçoit le paquet sur son interface G0/0/0 et examine l'adresse de destination du paquet. R1 achemine ensuite le paquet sur son interface G0/0/1 vers le port F0/12 dans VLAN 20 sur S1. Enfin, S1 transmet la trame à PC2.

L'ancien routage inter-VLAN utilisant des interfaces physiques fonctionne, mais il présente une limitation importante. Il n'est pas raisonnablement évolutif car les routeurs ont un nombre limité d'interfaces physiques. La nécessité de posséder une interface de routeur physique par VLAN épuise rapidement la capacité du routeur.

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

La méthode « router-on-a-stick » est un type de configuration de routeur dans laquelle une seule interface physique achemine le trafic entre plusieurs VLAN d'un réseau. Comme vous pouvez le voir dans la figure, le routeur est connecté au commutateur S1 à l'aide d'une seule connexion réseau physique (un trunk). L'interface de routeur est configurée pour fonctionner comme une liaison trunk et elle est connectée à un port de commutateur configuré en mode trunk. Le routeur effectue le routage inter-VLAN en acceptant le trafic étiqueté VLAN sur l'interface trunk provenant du commutateur adjacent. Il procède ensuite au routage en interne entre les VLANs à l'aide de sous-interfaces. Le routeur transfère alors le trafic acheminé, étiqueté VLAN vers le VLAN de destination, depuis la même interface physique utilisée pour recevoir le trafic. Les sous-interfaces sont des interfaces virtuelles basées sur un logiciel, associées à une interface physique unique. Les sous-interfaces sont configurées dans le logiciel sur un routeur et chaque sous-interface est configurée indépendamment avec une adresse IP et une affectation VLAN. Les sous-interfaces sont configurées pour différents sous-réseaux correspondant à leur affectation VLAN afin de faciliter le routage logique. Une fois qu'une

décision de routage a été prise en fonction de la destination VLAN, les trames de données sont étiquetées VLAN et renvoyées depuis l'interface physique. (Figure II.11)

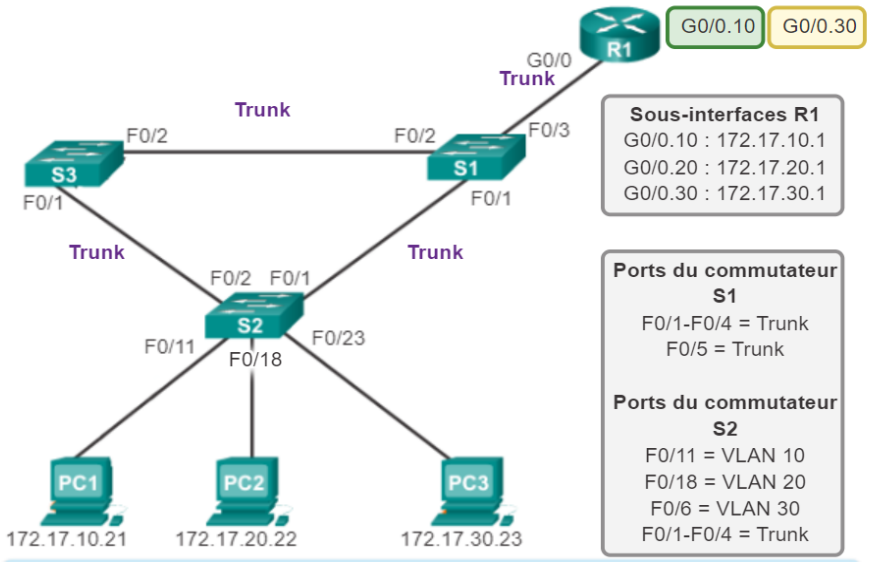

Figure III.11 : routage inter vlan de type router-on-a-stick**[54]**

- Le PC1 sur le VLAN 10 communique avec le PC3 sur le VLAN 30 via le routeur R1 en utilisant une seule interface de routeur physique.
- Le PC1 envoie son trafic de monodiffusion au commutateur S2.
- Le commutateur S2 marque alors le trafic de monodiffusion comme provenant du VLAN 10 et le transmet par sa liaison trunk au commutateur S1.
- Le commutateur S1 transfère le trafic étiqueté depuis l'autre interface trunk sur le port F0/5 vers l'interface du routeur R1.
- Le routeur R1 accepte le trafic de monodiffusion étiqueté sur le VLAN 10 et l'achemine vers le VLAN 30 en utilisant ses sous-interfaces configurées.
- Le trafic de monodiffusion est étiqueté avec le VLAN 30 lors de son transfert depuis l'interface de routeur vers le commutateur S1.
- Le commutateur S1 transmet le trafic de monodiffusion étiqueté via l'autre liaison trunk au commutateur S2.
- Le commutateur S2 supprime l'étiquette VLAN de la trame de monodiffusion et transfère la trame au PC3 sur le port F0/6.

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

La méthode moderne d'exécution du routage inter-VLAN consiste à utiliser des commutateurs de couche 3 et des interfaces virtuelles commutées (SVI). Une interface SVI est une interface virtuelle configurée dans un commutateur de couche 3, comme illustré dans la [figure III.12]. **[55]**

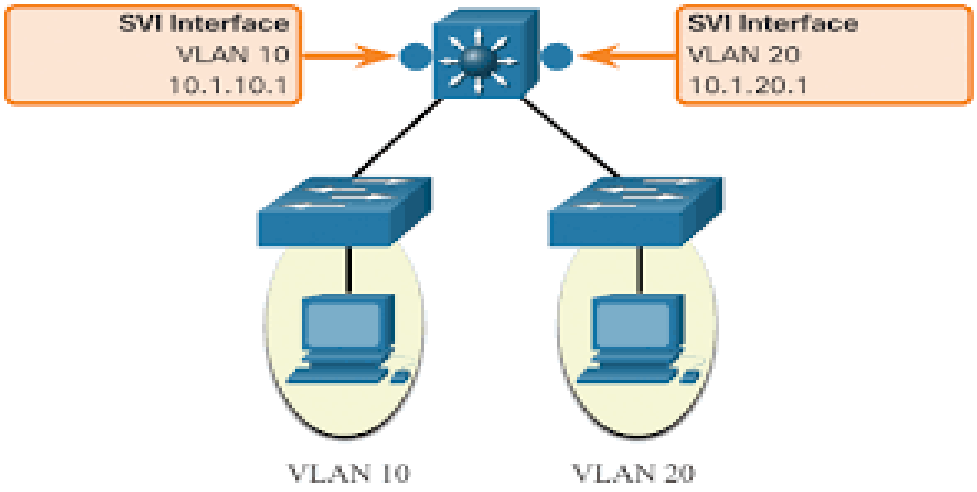

Figure III.12 : Exemple de routage inter-VLAN de commutateur de couche 3**[56]**

Les SVI inter-VLAN sont créés de la même manière que l'interface VLAN de gestion est configurée. Une interface SVI est créée pour chaque VLAN existant sur le commutateur. Bien que virtuel, le SVI exécute les mêmes fonctions pour le VLAN qu'une interface de routeur. Plus, précisément, il assure le traitement de couche 3 des paquets vers ou depuis tous les ports de commutateur associés à ce VLAN.

- Voici les avantages de l'utilisation de commutateurs de couche 3 pour le routage inter-VLAN :

✓ Cette méthode est beaucoup plus rapide que le modèle Router-on-a-stick, car l'ensemble de la commutation et du routage est assuré de manière matérielle.

✓ Il n'est pas nécessaire d'utiliser des liaisons externes entre le commutateur et le routeur pour le routage.

- ✓ Ils ne sont pas limités à une liaison, car les canaux EtherChannels de couche 2 peuvent être utilisés comme liaisons de trunk entre les commutateurs pour augmenter la bande passante.
- ✓ La latence est bien plus faible, car les données n'ont pas besoin de quitter le commutateur pour être acheminées vers un autre réseau.
- ✓ Ils sont plus souvent déployés dans un réseau local de campus que les routeurs.

  - ➢ Le seul inconvénient est que les commutateurs de couche 3 sont plus chers.

11 Dépannage du routage inter-VLAN

Le dépannage du routage inter-VLAN est une étape importante pour assurer le bon fonctionnement et la connectivité entre les différents réseaux locaux virtuels (VLANs) dans un réseau.

11.1 Problèmes de configuration inter-VLAN

Lors de la configuration du routage entre plusieurs VLAN, il est fréquent de rencontrer certaines erreurs de configuration sur le commutateur. Voici quelques problèmes courants :

11.1.1 Problème de configuration des interfaces du routeur

Lors de l'activation du routage inter-VLAN sur un routeur, l'une des erreurs de configuration les plus courantes consiste à connecter l'interface de routeur physique au mauvais port de commutateur. L'interface du routeur se trouve alors dans le mauvais VLAN, ce qui l'empêche d'atteindre les autres périphériques du même sous-réseau.

Comme l'illustre la figure, l'interface G0/0 du routeur R1 est connectée au port F0/9 du commutateur S1. Le port de commutateur F0/9 est configuré pour le VLAN par défaut, et non le VLAN 10. Le PC1 est donc incapable de communiquer avec l'interface du routeur. Par conséquent, il ne peut pas assurer le routage vers le VLAN 30. **[57]** (Figure III.13)

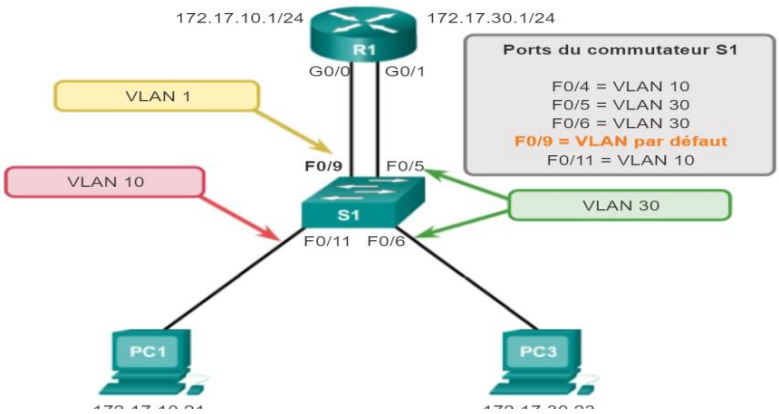

Figure III.13 : Problème de configuration de routeur **[58]**

Pour corriger ce problème, connectez physiquement l'interface G0/0 du routeur R1 au port F0/4 du commutateur S1. L'interface de routeur se trouve alors dans le bon VLAN et autorise le routage inter-VLAN. Vous pouvez également modifier l'affectation VLAN du port de commutateur F0/9 au VLAN 10. Ceci permet également à PC1 de communiquer avec l'interface G0/0 du routeur R1.

11.1.2 Problème lié aux ports de commutateur

Lors de l'utilisation du modèle de routage existant pour le routage inter-VLAN, il faut assure que les ports de commutateur se connectant aux interfaces un mécanisme de routage sont configurés sur les VLAN corrects. Si un port de commutateur n'est pas configuré pour le bon VLAN, les périphériques configurés sur ce VLAN ne peuvent pas se connecte l'interface du routeur et sont donc incapables d'envoyer des données à d'autres VLAN. **[59]**

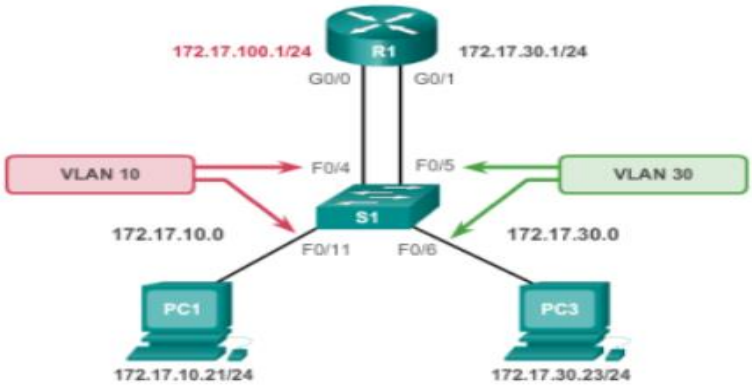

Figure III.14 : Topologie avec problème de configuration dans le switch **[**60**]**

Pour corriger ce problème, exécutez la commande de mode de configuration d'interface switchport access vlan 10 sur le port de commutateur F0/4 du commutateur S1. Lorsque le port de commutateur est configuré pour le VLAN correct, PC1 peut communiquer avec l'interface G0/0 du routeur R1, qui lui permet d'accéder aux autres VLAN connectés au routeur R1.

11.1.3 Problèmes d'adressage IP

Les VLANs correspondent à des sous-réseaux uniques sur le réseau. Pour que le routage inter-VLAN fonctionne, un routeur doit être connecté à tous les VLAN, par des interfaces physiques distinctes ou des sous-interfaces. Une adresse IP correspondant au sous réseau pour lequel elle est connectée doit être affectée à chaque interface ou sous interface.

Ceci permet aux périphériques du VLAN de communiquer avec l'interface de routeur et d'activer le routage de trafic vers d'autres VLAN connectés au routeur.

Comme l'illustre **(Figure III.15)** le routeur R1 a été configuré avec une adresse IP incorrecte sur l'interface G0/0, ce qui empêche le PC1 de communiquer avec le routeur R1 sur le VLAN 10. Pour corriger ce problème, affectez l'adresse IP correcte à l'interface G0/0 du routeur R1 à l'aide de la commande IP adress 172.17.10.1 255.255.255.0. Une fois l'adresse IP correcte affectée à l'interface du routeur, le PC1 peut utiliser cette dernière comme passerelle par défaut pour accéder à d'autres VLAN.

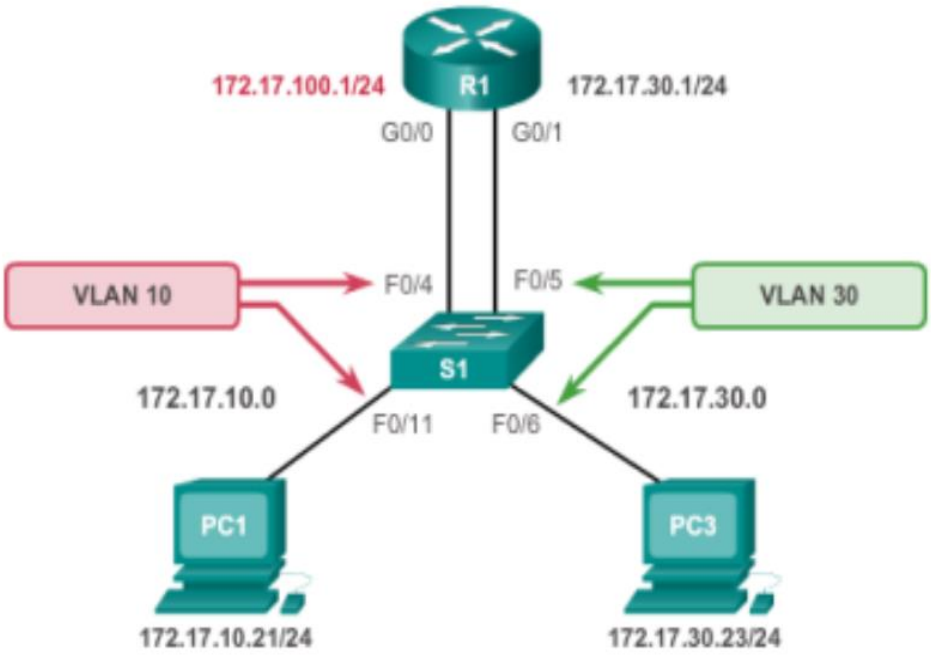

Figure III.15 : Topologie avec Adresse IP de routeur 1 mal configuré**[61]**

- Dans la **(Figure III.16)** le PC1 a été configuré avec une adresse IP incorrecte pour le sous réseau associé au VLAN 10. Ceci empêche PC1 de communiquer avec le routeur R1 sur le VLAN 10. Pour corriger ce problème, affectez l'adresse IP correcte à PC1. Selon le type de PC utilisé, les détails de configuration peuvent être différents.

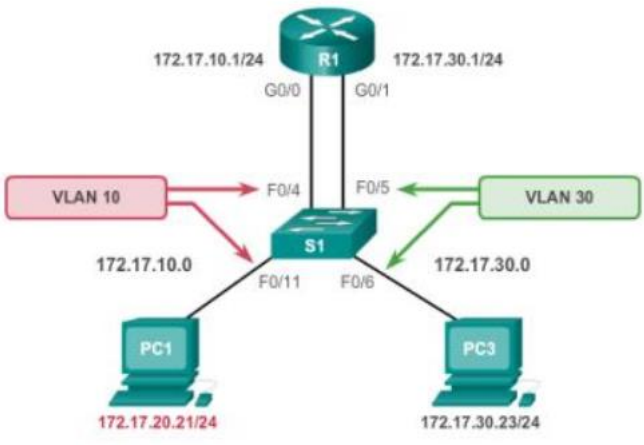

Figure III.16 : Topologie avec Adresse de PC1 mal configuré **[**62**]**

12 Conclusion

D'un point de vue technique, la technologie VLAN permet de déployer des architectures plus souples, fournissant plus de services qu'un LAN classique en combinaison à d'autres protocoles et technologies.

En effet, cette technologie a le potentiel pour répondre au besoin de mouvement en interne des entreprises. Ainsi, une entreprise peut réorganiser l'ensemble de ces services ou de ces groupes de travail sans que l'administrateur réseau ne soit à passer de longues heures à reconfigurer l'ensemble des machines du parc. Les VLANs apportent donc une très grande flexibilité dans la gestion du réseau.

Chapitre IV : Test et Simulation du réseau avec un Routage inter-VLAN

1 Introduction

Dans ce chapitre, nous allons donner la solution que nous avons proposée pour améliorer le fonctionnement du réseau local que nous avons étudié. Il s'agit de mettre au point une stratégie permettant de rendre la bande passe plus accessible et une topologie plus sécurisée. Pour ce faire, nous avons implémenté des VLANs dont le rôle est de segmenter le réseau local en plusieurs entêtés virtuelles. Les mêmes VLANs peuvent se communiquer et échanger des informations. Pour créer une communication inter-VLANs, nous avons configuré un switch multicouche. Le réseau informatique mis en place peut fonctionner avec ou sans routage inter VLAN.

Dans un premier temps, nous montrons les différentes configurations que nous avons réalisées, à savoir les configurations des switchs, des PCs et un switch multicouche. Dans un second temps, des tests de connectivités sont réalisés pour vérifier le fonctionnement du réseau.

2 Architecture initiale

À l'origine, notre réseau se composait de deux switchs et de 15 postes de travail, et cette architecture initiale présente quelques limitations et n'a aucune politique de sécurité (Figure IV.1). Rappelons que l'architecture du réseau informatique étudiée correspond à un LAN de l'entreprise Sonatrach à Boumerdes.

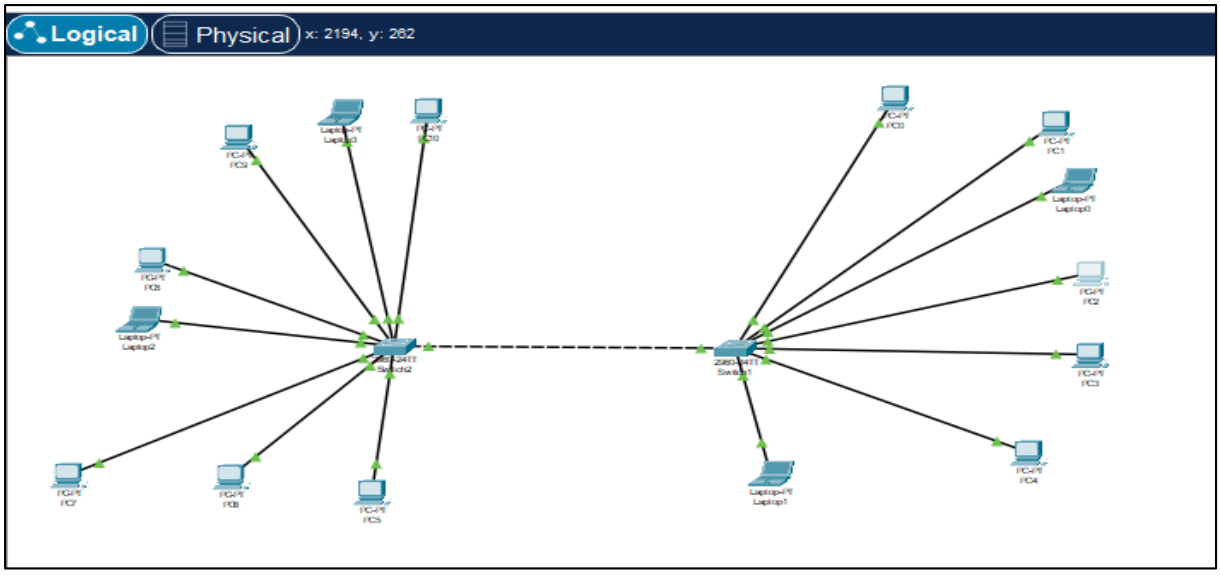

Figure IV.1 : Architecture initiale

3 Inconvénients de l'architecture

Cette architecture présente plusieurs limitations :

- **Capacité de commutation insuffisante** : avec seulement 2 switchs pour 15 postes de Travail, il est possible que la capacité de commutation (bande passante disponible) ait été limitée, ce qui est pourrait entraîner des ralentissements lorsque plusieurs périphériques sont actifs simultanément.
- **Manque de segmentation réseau** : sans VLAN, tous les périphériques et services partagent potentiellement le même espace de diffusion (broadcast domain), ce qui peut augmenter le trafic inutile et ralentir le réseau.
- **Gestion de trafic inter-VLAN** : le routage entre VLANs n'était pas possible, ce qui compliquait la communication entre différentes sections du réseau.
- **Sécurité insuffisante** : un réseau non segmenté pourrait poser des problèmes de sécurité en permettant à tout périphérique de communiquer avec n'importe quel autre, augmentant ainsi le risque d'attaques internes ou de propagation de logiciels malveillants.
- **Manque de redondance :** Avec seulement deux switches, il peut y avoir un seul point de défaillance.

4 Modifications apportées pour l'optimisation

Pour remédier aux insuffisances de l'architecture initiale, nous avons procédé ainsi :

4.1 Ajout de switchs supplémentaires

Nous avons intégré 2 switchs supplémentaires pour augmenter la capacité de notre réseau et améliorer sa résilience. (Figure IV.2)

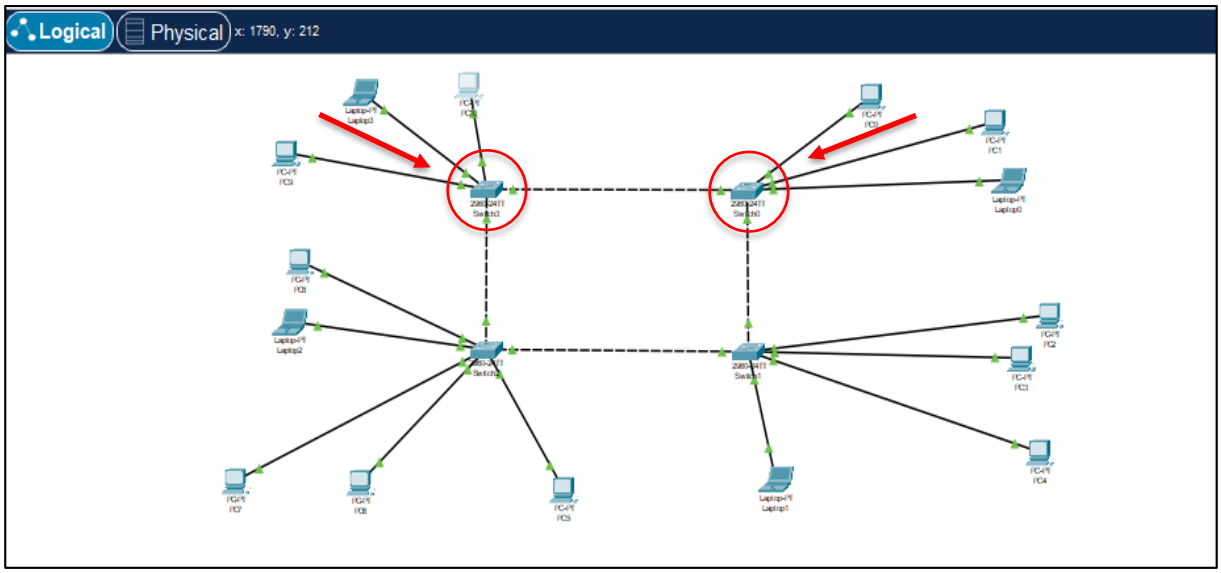

Figure IV.2 : Ajout de switchs supplémentaires

4.1.1 Configuration des switchs d'accès

Une fois tous les câbles connectés, la première étape consiste à attribuer un nom à chaque switch afin de les identifier clairement dans le réseau. Ensuite, nous procédons à la création de VLANs, des groupes virtuels qui segmentent le réseau pour une gestion plus efficace et une sécurité renforcée.

Pour permettre aux switches de communiquer entre eux et de transférer les données entre les différents VLANs, nous configurons des trunks. Ces trunks peuvent transporter le trafic de plusieurs VLANs sur une seule connexion physique, simplifiant ainsi la configuration du réseau et optimisant l'utilisation de la bande passante.

Enfin, chaque interface des switches est assignée à un VLAN spécifique, ce qui détermine quel groupe d'appareils est connecté à chaque port et quelles règles de communication s'appliquent à ce groupe.

Il est important de noter que cette configuration est d'abord réalisée sur le premier switch, puis reproduite sur les autres pour assurer une uniformité et une stabilité dans tout le système.

- Pour commencer, nous allons donner des noms aux switchs : switch A, switch B switch C et switch D. (Figure IV.3)

```
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname switchA
switchA(config)#
```

Figure IV.3: Nomination des Switch

- Exécutez la commande « show vlan brief » pour afficher les VLAN configurés sur le switch. (Figure IV.4)

```
SwitchA#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                   Gig0/1, Gig0/2
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
SwitchA#
```

Figure IV.4: Exécution de la commande show vlan brief

La fenêtre indique qu'il existe un VLAN par défaut regroupant toutes les interfaces du switch.

- Nous allons créer et nommer les VLANs. (Figure IV.5)

```
1005 trnet-default                active
SWITCHA#
SWITCHA#en
SWITCHA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCHA(config)#vlan 40
SWITCHA(config-vlan)#name ADM
SWITCHA(config-vlan)#VLAN 30
SWITCHA(config-vlan)#name TELECOM
SWITCHA(config-vlan)#EXIT
SWITCHA(config)#
```

Figure IV.5: Nomination des VLANs

- Sur nos quatre switchs, nous allons configurer les ports Fa0/1 pour le VLAN 40 et Fa0/2 et Fa0/3 pour le VLAN 30. (Figure IV.6)

```
SWITCHA(config)#interface Fa0/1
SWITCHA(config-if)#switchport access vlan 40
SWITCHA(config-if)#no shutdown
SWITCHA(config-if)#exit
SWITCHA(config)#interface Fa0/2
SWITCHA(config-if)#switchport access vlan 30
SWITCHA(config-if)#no shutdown
SWITCHA(config-if)#exit
SWITCHA(config)#interface Fa0/3
SWITCHA(config-if)#switchport access vlan 30
SWITCHA(config-if)#no shutdown
SWITCHA(config-if)#exit
SWITCHA(config)#
```

Figure IV.6: Affectation des interfaces au VLAN

Afin de mettre en œuvre les configurations VLAN souhaitées sur nos quatre switchs, nous allons exécuter les commandes suivantes sur chacun d'entre eux :

Switch B :

- Affecter les ports Fa0/1 et Fa0/2 au VLAN 40.
- Affecter le port Fa0/3 au VLAN 10.
- Affecter le port Fa0/4 au VLAN 20.

Switch C :

- Affecter le port Fa0/1 au VLAN 40.
- Affecter le port Fa0/2 au VLAN 20.
- Affecter le port Fa0/3 au VLAN 10.
- Affecter les ports Fa0/4 et Fa0/5 au VLAN 30.

Switch D :

- Affecter le port Fa0/1 au VLAN 20.
- Affecter les ports Fa0/2 et Fa0/3 au VLAN 10

- Après avoir créé les VLAN, on exécute de nouveau la commande « show vlan brief ». (Figure IV.7)

```
SWITCHA>
SWITCHA>show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
30   TELECOM                          active    Fa0/2, Fa0/3
40   ADM                              active    Fa0/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SWITCHA>
```

Figure IV.7 : Exécution à nouveau de la commande ‘show vlan brief’

La fenêtre indique que les ports Fa0/2 et Fa0/3 sont affectés au VLAN 30 et le port Fa0/1 est affecté au VLAN 40.

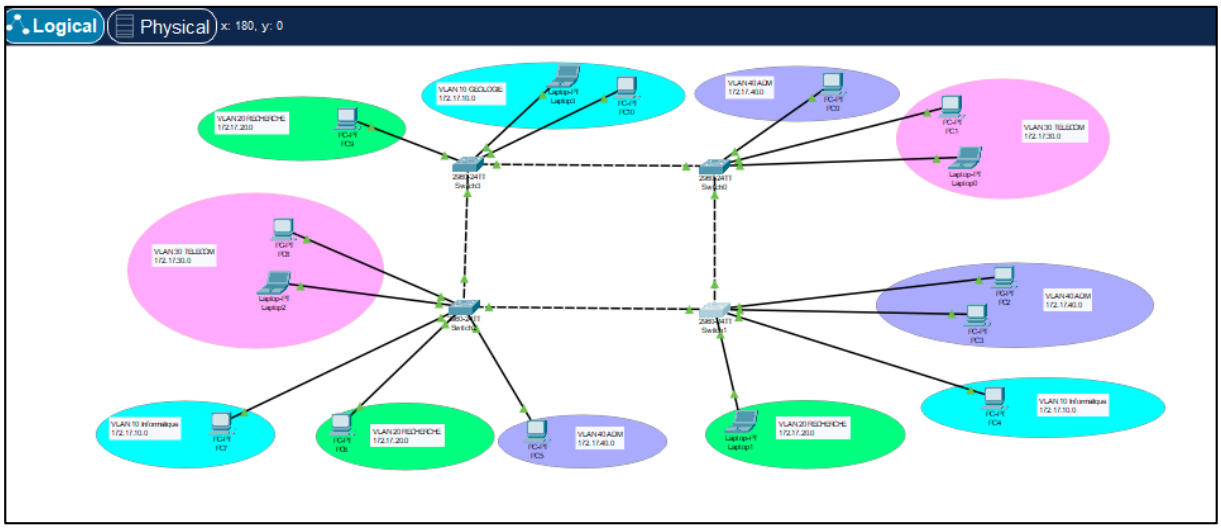

Figure IV.8 : l’architecture apres avoir configuré les switchs et créer des VLANs

4.2 Intégration d’un switch multicouche

Un switch multicouche a été ajouté pour centraliser le routage et supporter des fonctionnalités avancées telles que le routage inter-VLAN.

4.2.1 Configuration de commutateur multicouche

- Nommer le commutateur multicouche 1 (Figure IV.9).

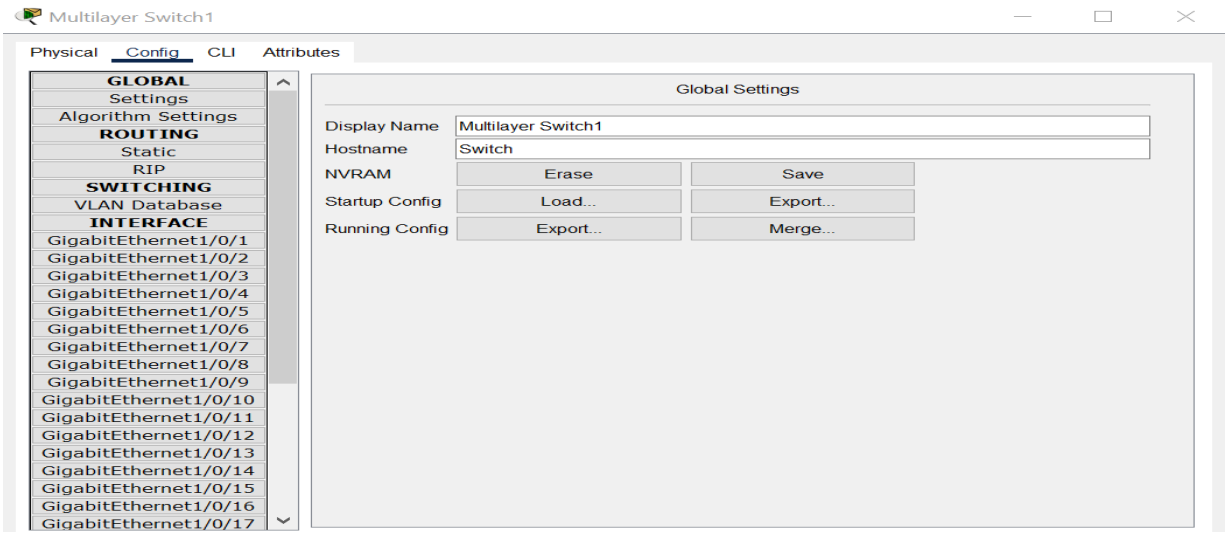

Figure IV.9 : Nomination du commutateur multicouche

- Créer les VLANs 10, 20, 30 et 40 et les nommer (Figure IV.10).

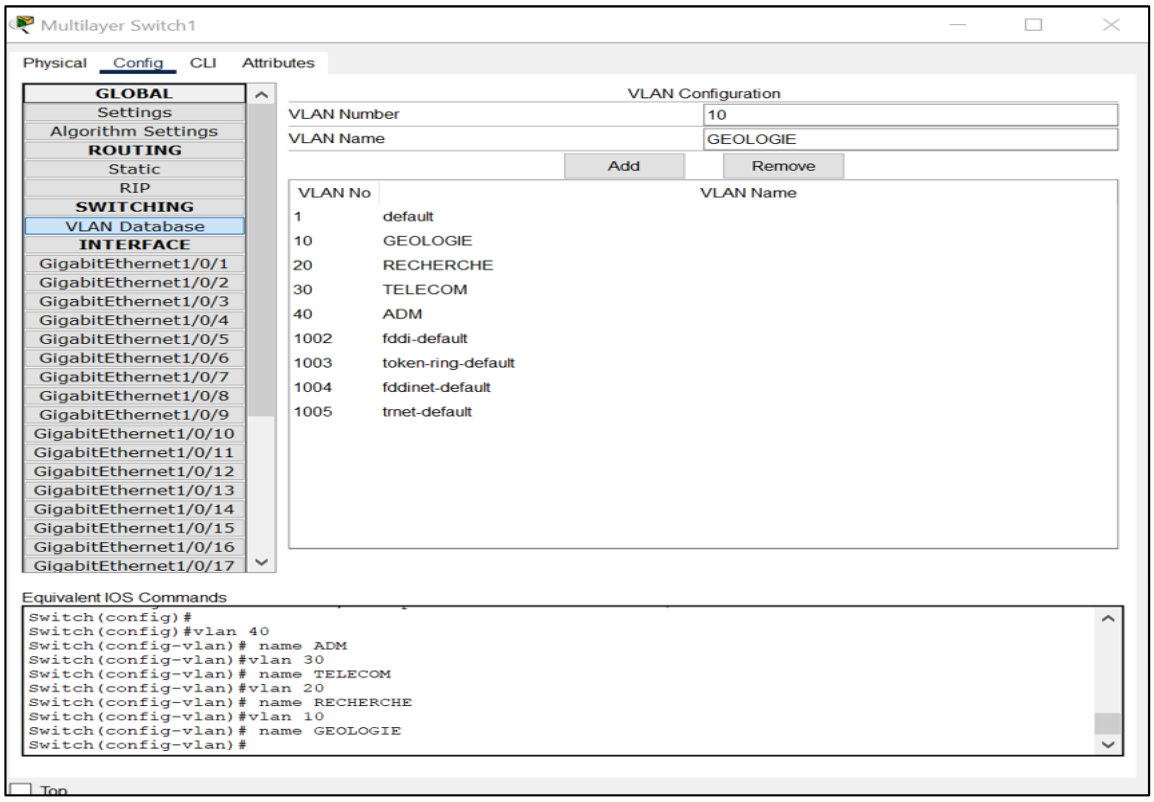

Figure IV.10: Création des VLANs

Nous allons maintenant créer nos ports trunk sur les interfaces Gigabit Ethernet 1/0/1, Gigabit Ethernet 1/0/2, Gigabit Ethernet 1/0/3 et Gigabit Ethernet 1/0/4 de commutateur multicouche (Figure IV.11).

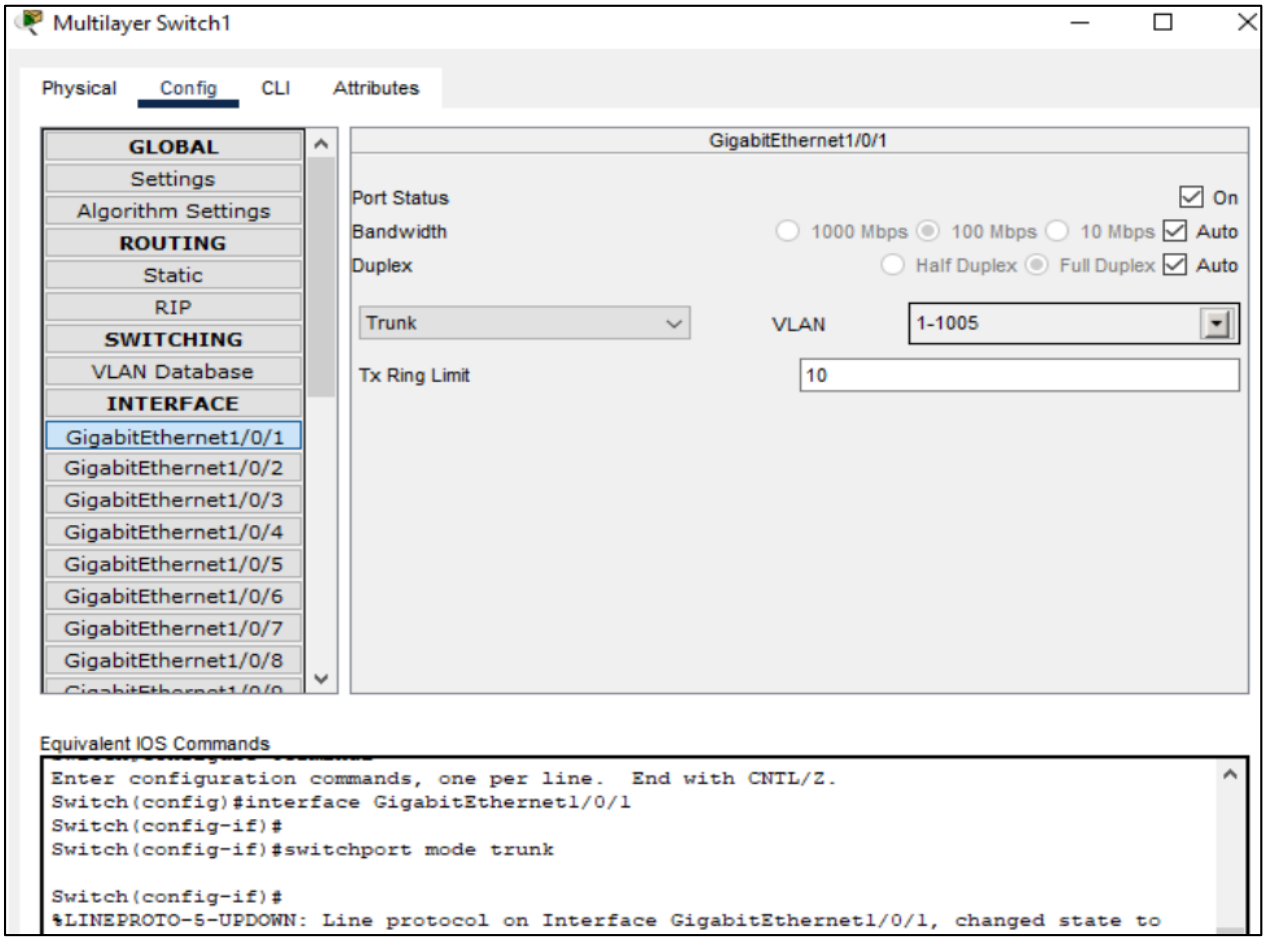

Figure IV.11: Création de port Trunk

4.3 Mise en place du routage inter-VLAN

Nous avons configuré le routage inter-VLAN sur le switch multicouche pour permettre une meilleure segmentation et une gestion optimisée du trafic entre les VLANs. Cela été réalisé en configurant les interfaces VLAN sur le switch multicouche et, si nécessaire, en utilisant des ACLs (Access Control Lists) pour contrôler le trafic entre les VLANs. Cela permet d'activer et de réactiver manuellement le routage inter-VLAN (Figure IV.12).

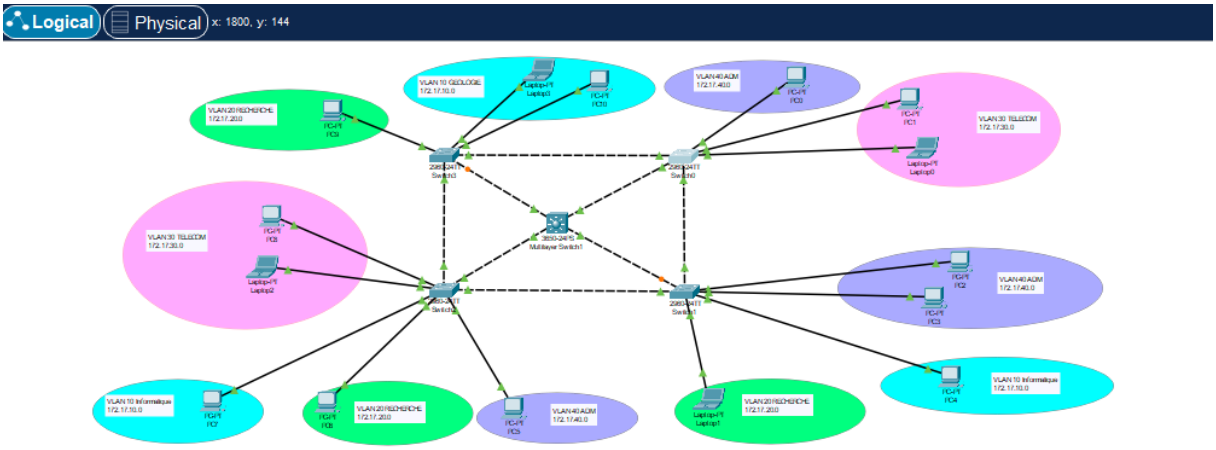

Figure IV.12 : l'architecture finale

Pour permettre au switch multicouche de router le trafic entre les VLANs, qu'ils soient sur le même switch ou sur différents switchs, plusieurs étapes doivent être suivies :

✓ **Attribution d'adresses IP et activation du routage**

Configuration des sous-interfaces VLAN avec une adresse IP (la passerelle par défaut) et activation du routage pour permettre le transfert de données entre les VLANs.

✓ **Consultation de la table de routage pour le transfert de paquets**

Lorsqu'un switch reçoit un paquet destiné à un autre sous-réseau ou VLAN, il consulte sa table de routage pour déterminer la meilleure interface de sortie.

✓ **Transfert du paquet vers l'interface VLAN de destination**

En fonction de la table de routage, le paquet est transféré vers l'interface VLAN appropriée correspondant à la destination du paquet.

✓ **Envoi du paquet au port du périphérique cible**

Enfin, le paquet est transmis physiquement via le port connecté au périphérique cible.

Ces étapes assurent que le switch multicouche peut efficacement router le trafic entre les VLANs, facilitant ainsi la communication sécurisée et optimisée dans le réseau.

➢ Pour les sous interfaces **:**

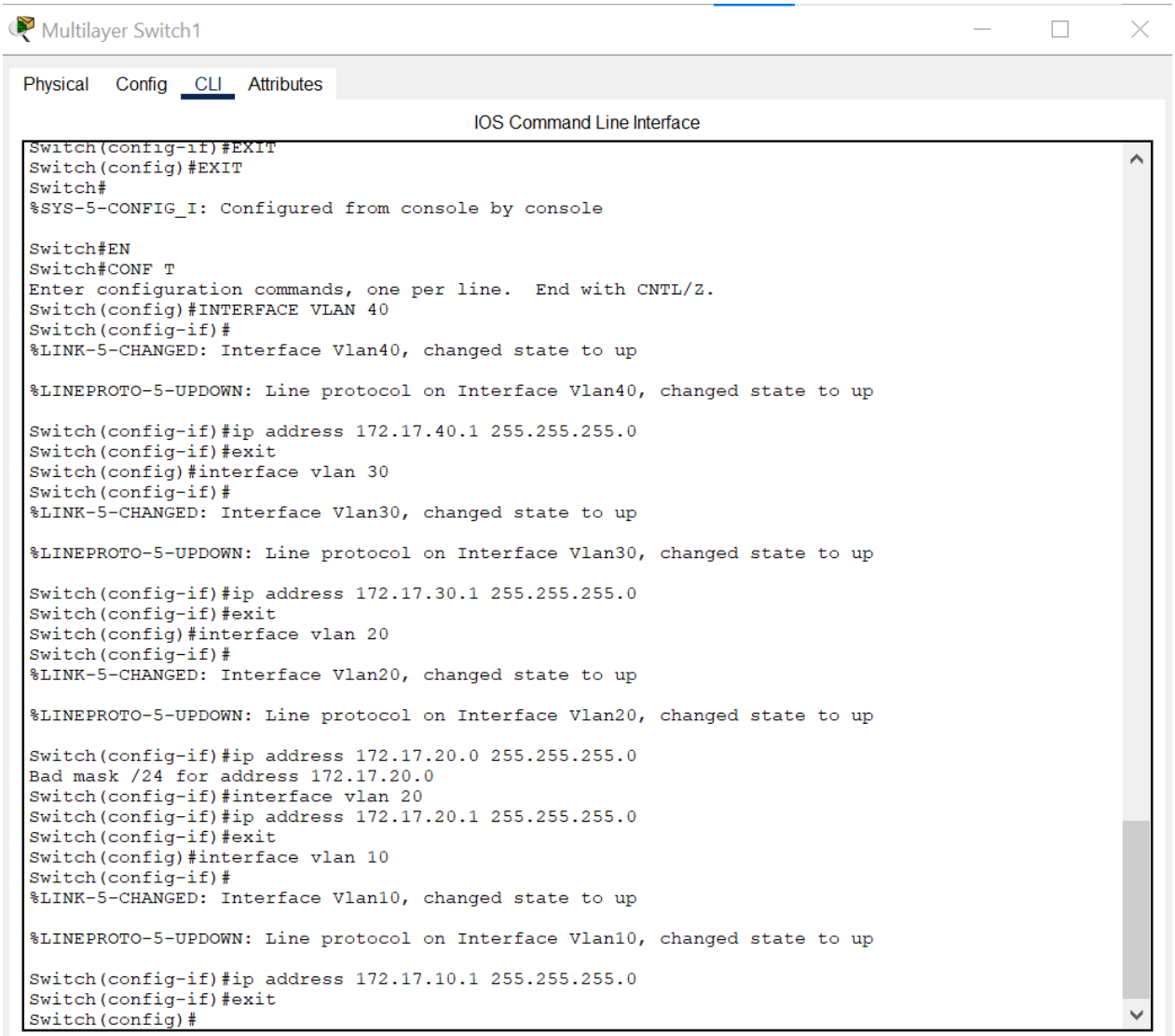

Figure IV.13 : Configuration des sous interfaces VLAN avec une adresse IP

➢ Pour le routage :

```
Switch#en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip routing
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure IV.14 : Activation du routage

4.4 Configurations des ACLs

L'utilisation des ACLs permet de contrôler précisément le trafic entre VLANs, augmentant ainsi la sécurité du réseau.

Pour ajouter des ACLs afin de désactiver et réactiver le routage inter-VLAN, voici les Etape suivantes :

1. **Créer une ACL pour bloquer le trafic inter-VLAN** : créer une liste de contrôle d'acces pour bloquer tout le trafic entre les VLANs (figure IV.15)

```
multilayerswitch>en
multilayerswitch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
multilayerswitch(config)#ip access-list extended Block_intervlan
multilayerswitch(config-ext-nacl)#deny ip any any
multilayerswitch(config-ext-nacl)#exit
```

Figure IV.15 : creation d'ACL pour bloquer le trafic inter-VLAN

2. **Appliquer l'ACL aux interface VLAN :** Appliquer l'ACL configurée aux interfaces VLAN correspondantes pour bloquer le trafic inter-VLAN (figure IV.16)

```
Switch(config)#interface VLAN 10
Switch(config-if)#ip access-group BLOCK-INTERVLAN in
Switch(config-if)#interface VLAN 20
Switch(config-if)#ip access-group BLOCK-INTERVLAN in
Switch(config-if)#interface VLAN 30
Switch(config-if)#ip access-group BLOCK-INTERVLAN in
Switch(config-if)#interface VLAN 40
Switch(config-if)#ip access-group BLOCK-INTERVLAN in
Switch(config-if)#Exit
```

Figure IV.16 : configuration d'ACL sur chaque interface VLAN

3. **Supprimer l'ACL pour réactiver le routage inter VLAN :** Retirer les ACLs des interfaces VLAN pour permettre à nouveau le routage inter-VLAN (figure IV.17).

```
multilayerswitch>en
multilayerswitch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
multilayerswitch(config)#inter vlan 10
multilayerswitch(config-if)#no ip access-group Block_intervlan in
multilayerswitch(config-if)#exit
multilayerswitch(config)#inter vlan 20
multilayerswitch(config-if)#no ip access-group Block_intervlan in
multilayerswitch(config-if)#exit
multilayerswitch(config)#inter vlan 30
multilayerswitch(config-if)#no ip access-group Block_intervlan in
multilayerswitch(config-if)#exit
multilayerswitch(config)#inter vlan 40
multilayerswitch(config-if)#no ip access-group Block_intervlan in
multilayerswitch(config-if)#exit
```

figure IV.17 : Retirer les ACLs des interfaces VLAN

4.5 Configuration de protocole SSH

Le but de ssh (secure Shell) sur un switch multicouche en ce qui concerne le routage inter VLAN est de permettre une administration sécurisée du switch lors de la configuration, de la surveillance et de la gestion des fonctionnalités liées au routage inter-VLAN. Ssh offre les avantages suivants :

- ✓ Sécurités des communications
- ✓ Accès à distance sécurisée
- ✓ Administration centralisée
- ✓ Audit et surveillance

IOS Command Line Interface

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Myswitch
Myswitch(config)#ip domain-name Master2.com
Myswitch(config)#crypto key generate rsa
The name for the keys will be: Myswitch.Master2.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2024
% Generating 2024 bit RSA keys, keys will be non-exportable...[OK]

Myswitch(config)#username admin secret Master123
*Mar 1 0:7:9.449: %SSH-5-ENABLED: SSH 1.99 has been enabled
Myswitch(config)#line vty 0 15
Myswitch(config-line)#login local
Myswitch(config-line)#transport input ssh
Myswitch(config-line)#exit
```

Figure IV.18 :Configuration de protocole SSH

Après avoir configuré SSH comme décrit précédemment, on a ajouté les commandes suivantes (figure IV.19) pour définir le délai d'attente et les tentatives d'authentification.

```
Myswitch(config)#ip ssh time-out 60
Myswitch(config)#ip ssh authentication-retries 2
Myswitch(config)#end
Myswitch#
%SYS-5-CONFIG_I: Configured from console by console
write memory
```

Figure IV.19: configuration de l'expiration de la session SSH et des tentatives d'authentification

5 Tests de connectivité

Nous allons tester la connectivité des postes situés dans le même VLAN et le même switch : On prend le poste "PC8" sur le VLAN 30 avec l'adresse IP 172.17.30.4 pour pinger le poste "Laptop 2" avec l'adresse IP 172.17.30.5 (figure IV.20).

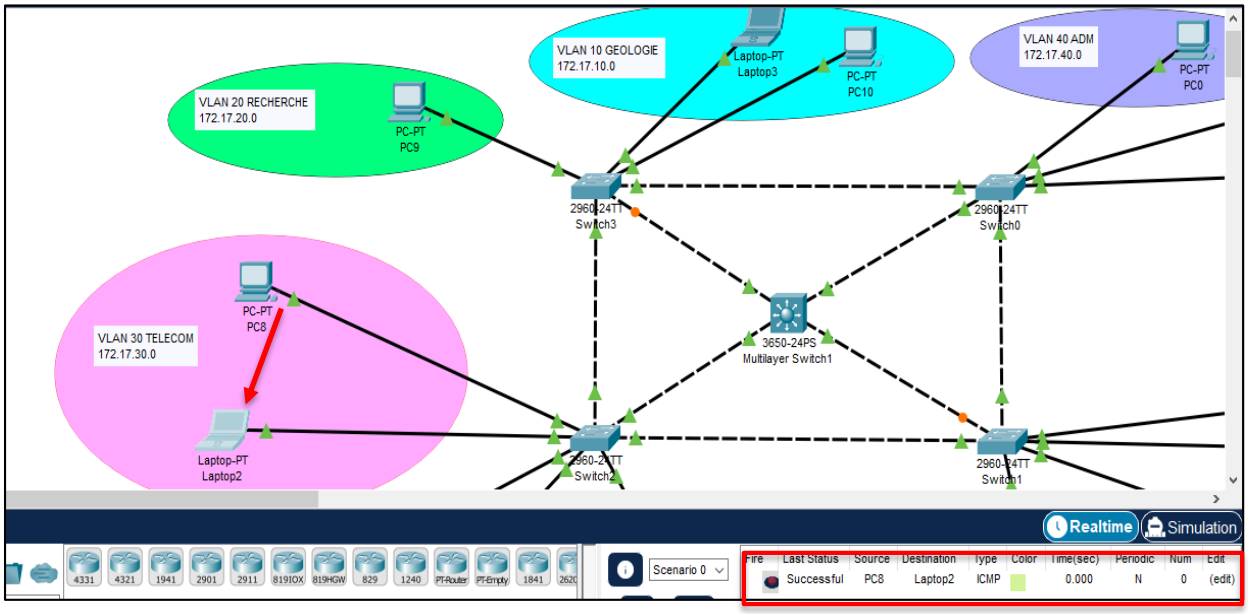

Figure IV.20 :Ping PC 8 vers laptop 2

Le ping a été exécuté avec succès.

Nous allons tester la connectivité des postes situés sur le même VLAN et différent switchs : On prend le poste "PC 4" sur le VLAN 10 avec l'IP 172.17.10.5 pour pinger le poste "PC4" avec l'IP 172.17.10.5 (figure IV.21).

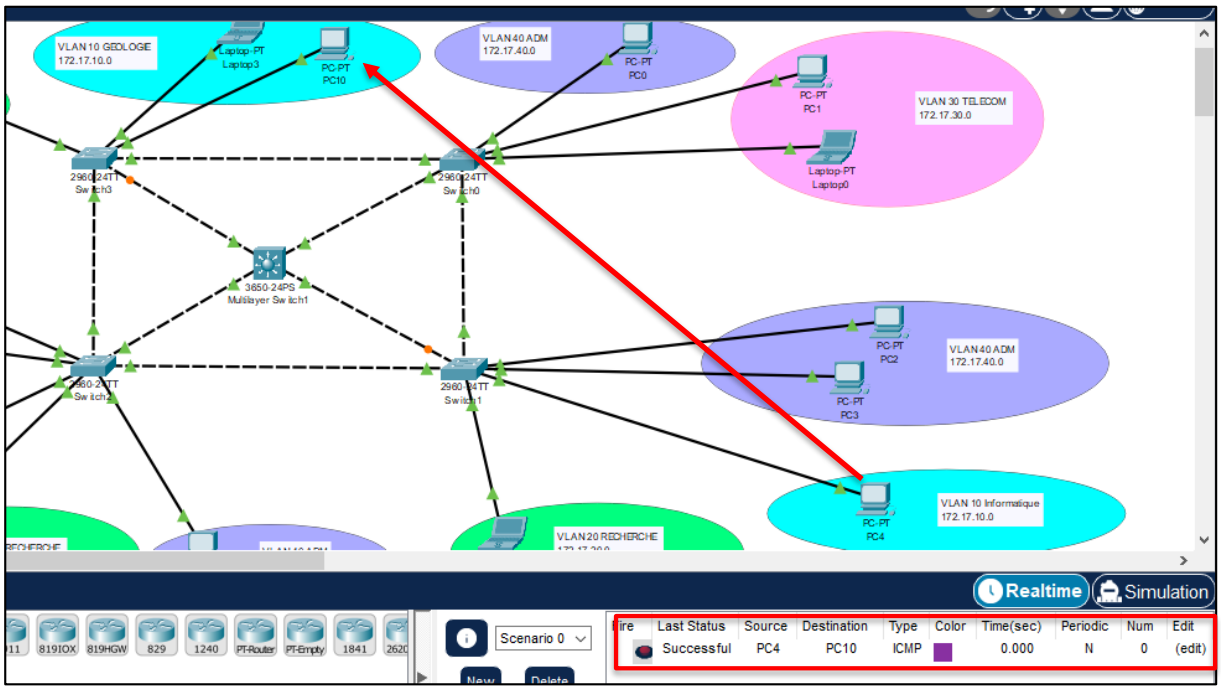

Figure IV.21 :Ping PC4 vers PC10

Le ping a été exécuté avec succès.

Nous allons tester maintenant la connectivité des postes situés dans des différents VLAN :

- **Avant la mise en place de Routage inter-VLAN**

Tester la communication entre différents VLANs sur le même switch, nous utilisons le poste 'PC4' sur le VLAN 10 avec l'adresse IP 172.17.10.2 pour envoyer un ping au poste 'PC2' sur le VLAN 40 avec l'adresse IP 172.17.40.3 (figure IV.22).

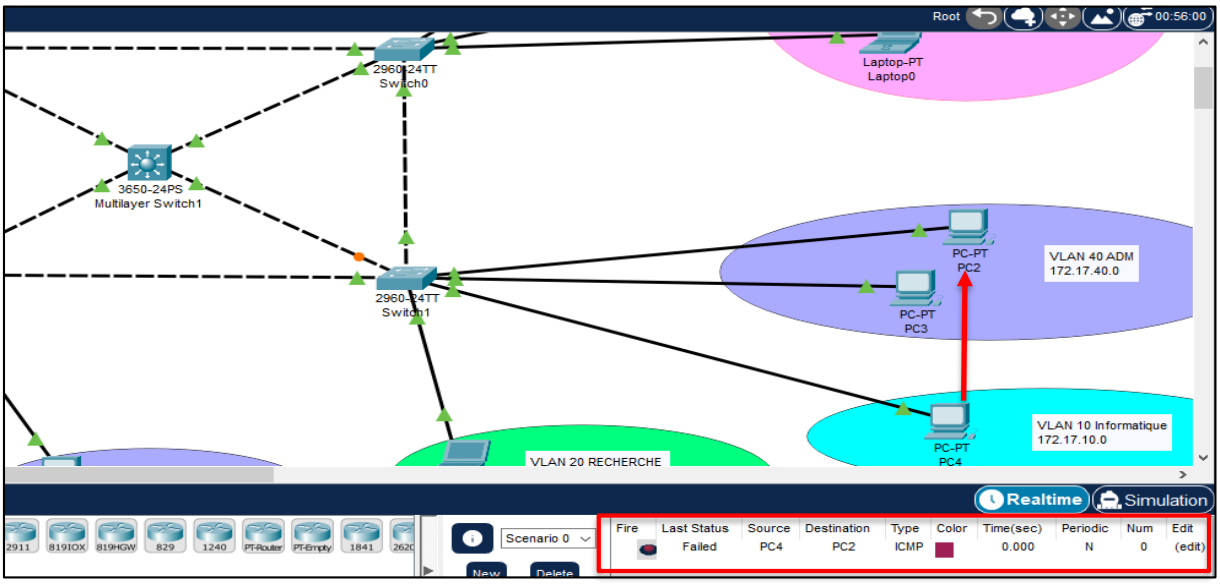

Figure IV.22 :Ping PC4 vers PC2

Le message n'a pas été envoyé.

Pour tester la communication entre différents VLANs sur différents switchs, nous utilisons le poste 'PC4' sur le VLAN 10 avec l'adresse IP 172.17.10.2 pour envoyer un ping au poste 'PC1' sur le VLAN 30 avec l'adresse IP 172.17.30.2 (figure IV.23).

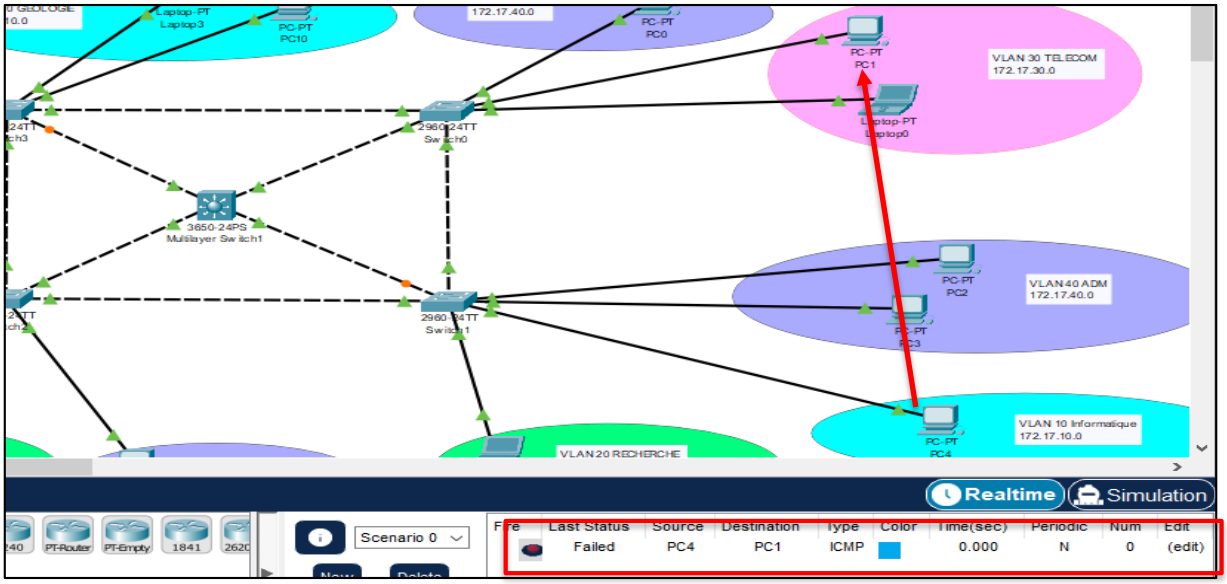

Figure IV.23 : Ping PC4 vers PC1

Le message n'a pas été envoyé

➢ **Après la mise en place de Routage inter-VLAN**

Nous allons maintenant refaire le ping entre les postes 'PC4' et 'PC2' (figure IV.24):

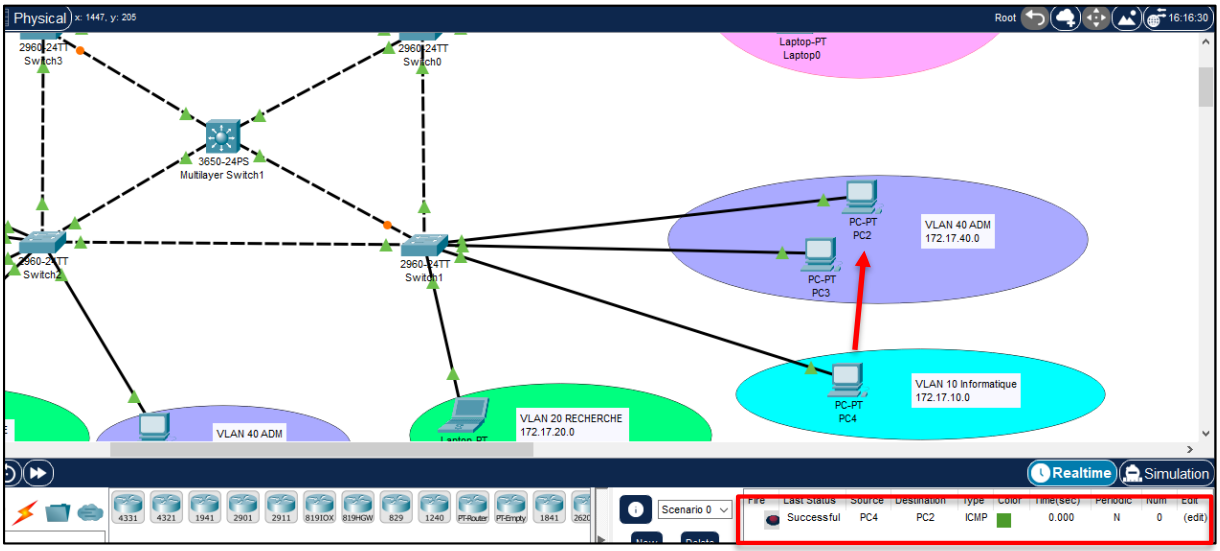

Figure IV.24 : Ping PC4 vers PC2

On constate que la transmission du message entre les deux postes via le routage inter-VLAN est effective.

Nous allons ensuite refaire le ping entre les postes 'PC4' et 'PC1' (figure IV.25) :

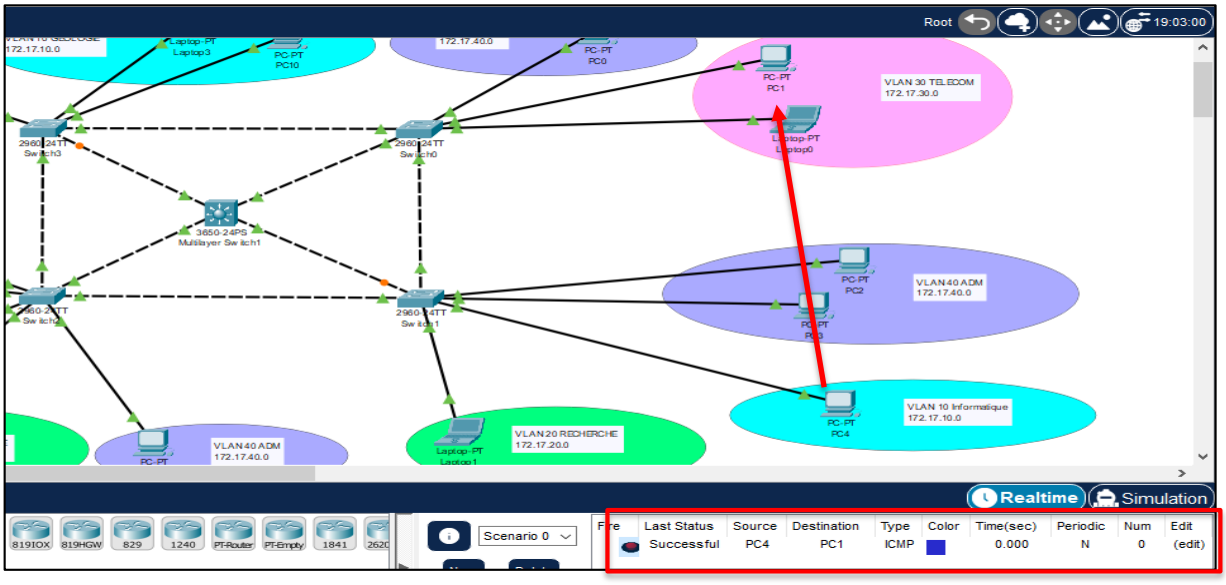

Figure IV.25 : ping entre les postes PC4 et PC1

Le message a été bien envoyé.

En ajoutant des ACL, nous avons bloqué le routage inter-VLAN. Pour vérifier cela, nous avons testé la connectivité entre des postes situés sur des VLANs et des switchs différents. Nous avons utilisé le poste 'PC4' sur le VLAN 10 avec l'adresse IP 172.17.10.2 pour envoyer un ping au poste 'PC1' sur le VLAN 30 avec l'adresse IP 172.17.30.2 (figure IV.26).

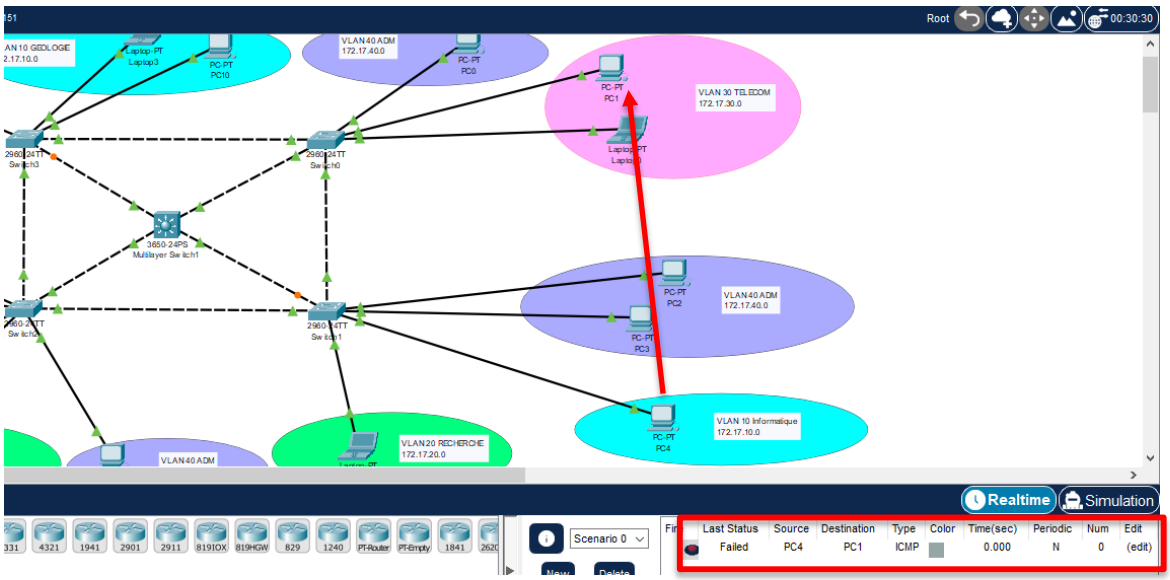

Figure IV.26 : Ping entre PC4 et PC1

Le ping n'a pas réussi.

Ensuite on teste la connectivité entre des postes situés sur les mêmes VLANs et des switchs différents, nous utilisons le poste "PC 5" qui est sur le VLAN 40 avec l'adresse IP 172.17.40.5 pour envoyer un ping au poste "PC3" sur le VLAN 40 avec l'adresse IP 172.17.40.4 (figure IV.27).

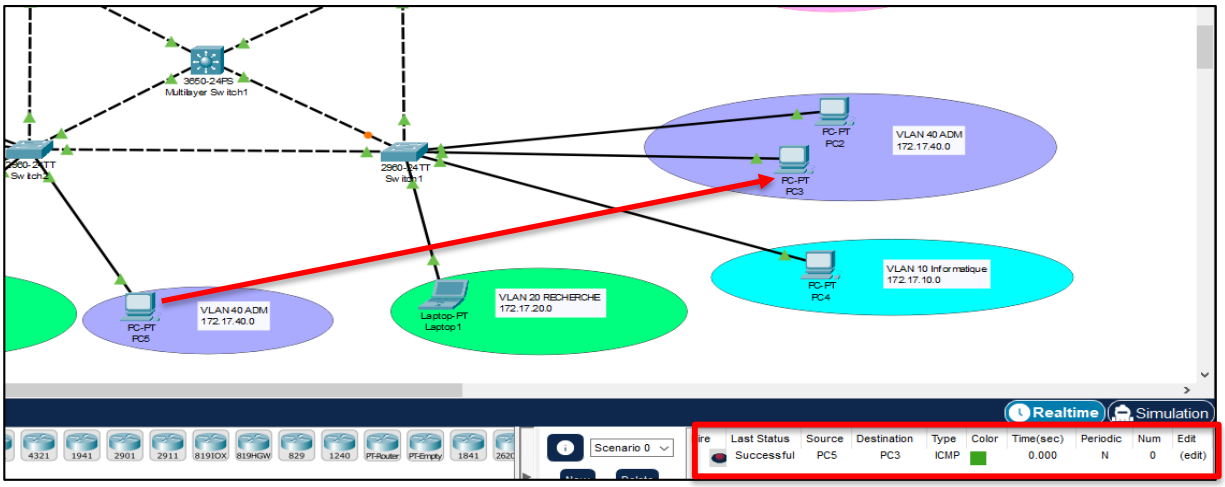

figure IV.27 : Ping entre le PC5 et le PC3

La réponse au Ping a été reçue avec succès.

Donc en bloquant le routage inter-VLAN avec des ACLs, nous optimisons la gestion de la bande passante en limitant le trafic entre les VLANs, ce qui réduit la charge de routage sur nos équipements réseau. Cette approche permet une meilleure utilisation des ressources, une optimisation des performances réseau et renforce la sécurité en isolant efficacement le trafic entre les différents segments VLAN. De plus, cette configuration peut être facilement ajustée et réactivée selon les besoins spécifiques de notre réseau.

6 Conclusion

Dans ce chapitre, nous avons amélioré notre réseau en y ajoutant des switchs et en créant des VLANs. Nous les avons configurés dans chaque switch et avons également mis en place le routage inter-VLAN dans le switch multicouche.

De plus, nous avons configuré des ACL pour contrôler le routage inter-VLAN et mis en place le protocole SSH pour l'accès à distance, renforçant ainsi la sécurité du réseau.

Grâce à ces améliorations, notre infrastructure est désormais mieux protégée contre les menaces potentielles et offre une gestion optimisée des flux de données.

Conclusion Générale

Nous avons exploré en profondeur dans ce mémoire l'utilisation des Virtual Local Area Networks (VLANs) et du routage inter-VLAN pour améliorer la sécurité et la gestion des réseaux locaux (LANs). À partir de l'étude que nous avons réalisée au sein du département technologie d'information de Sonatrach à Boumerdes sur le réseau informatique LAN, nous avons pu identifier et résoudre des défis spécifiques liés à la sécurité et à la gestion des réseaux.

Pour ce faire, dans un premier temps, nous avons présenté les bases théoriques en définissant les réseaux informatiques et en introduisant les concepts fondamentaux tels que les modèles OSI et TCP/IP, ainsi que les principes de routage et de gestion du trafic. Ensuite, nous avons mis en évidence le concept de la sécurité informatique en analysant les critères de sécurité, les risques potentiels, les contre-mesures et les protocoles de sécurité essentiels.

La partie centrale de notre analyse s'est concentrée sur les VLANs, en examinant en détail leurs divers types, leur classification, ainsi que les avantages substantiels qu'ils offrent en termes de segmentation du réseau et de gestion efficace du trafic. Nous avons également étudié de près le routage inter-VLAN, en mettant en évidence ses mécanismes de fonctionnement et les approches pour résoudre les défis liés à sa configuration.

Pour vérifier le fonctionnement du LAN avec les protocoles de sécurité et de gestion, nous avons utilisé l'environnement de simulation Packet Tracer pour illustrer la mise en œuvre pratique des VLANs et du routage inter-VLAN. Selon les simulations que nous avons réalisées, incluant les configurations des switchs, des PCs et d'un switch multicouche, des tests de connectivité ont ensuite été effectués pour vérifier le bon fonctionnement du réseau, démontrant ainsi les capacités et les bénéfices de ces technologies dans un contexte réel.

Dans le cahier de charge de l'entreprise, il n'est pas indiqué la communication via internet. Comme indiqué précédemment, nous avons résolu le problème d'intercommunication entre les différents blocs constituant le LAN. La connexion de ce LAN avec internet nécessite l'implémentation d'autres protocoles qui permettent de garantir une bonne gestion et une sécurité. La perspective de ce travail peut être orientée dans cet optique.

Références

[1] https://technologiecycle4stgab.jimdofree.com/5%C3%A8me/probl%C3%A9matique-2/

[2] https://www.camerecole.org/classes/1441-configuration-d-un-reseau-informatique.html

[3] https://cisco.goffinet.org/ccna/fondamentaux/composants-reseau/, consulté en 5 avril 2024.

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

[5] P. Latu, "Technologie RNIS," 2000.

[6] https://sti2d.ecolelamache.org/ii_rseaux_informatiques___7_topologie_des_rseaux.html

[7] https://www.researchgate.net/figure/Topologie-en-etoile_fig7_350340759

[8] https://www.researchgate.net/figure/Figure-5-7-Topologie-en-anneau_fig34_349641743

[9] https://www.researchgate.net/figure/Topologie-maillee-Topologie-arborescente-offre-des-liens-dedies-qui-permettent-de_fig6_350340759

[10] P. Atelin, "Réseaux informatiques : Notions fondamentales (Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, Wi-Fi,...)," Editions ENI, 2009.

[11] https://www.frameip.com/tcpip/#google_vignette. consulté en 15 avril 2024

[12] https://www.frameip.com/tcpip/#google_vignette. consulté en 15 avril 2024.

[13] Avast, "Qu'est-ce qu'une adresse IP ? | Définition d'une adresse IP," consulté en15 avril 2024.

[14] https://linux-note.com/modele-osi-et-tcpip/

[15] Netacad, "Introduction aux Réseaux - Structure de l'adresse IPv4," consulté en 20 avril 2024.

[16] Netacad, "Introduction aux Réseaux - Structure de l'adresse IPv4," consulté en 20 avril 2024.

[17] https://ccnareponses.com/introduction-aux-reseaux-modules-11-adressage-ipv4/

[18] FrameIP, "Protocole TCP/IP," https://www.frameip.com/tcpip/#google_vignette, consulté en 21 avril 2024.

[19] IONOS, "IPv6 : C'est quoi le protocole IPv6 et quels sont les avantages ?," consulté en 21 avril 2024.

[20] IONOS, "IPv6 : C'est quoi le protocole IPv6 et quels sont les avantages ?," consulté en 21 avril 2024.

[21] Llorens, C., Levier, L., & Valois, *D., avec la contribution de Salvatori, O. (2006).* Tableaux de bord de la sécurité *(2eme. Éd.). Eyrolles.*

[22] Llorens, C., Levier, L., & Valois, *D., avec la contribution de Salvatori, O. (2006).* Tableaux de bord de la sécurité *(2eme. Éd.). Eyrolles.*

[23] https://www.securiteinfo.com/attaques/hacking/typesattaques.shtml consulté en 13 mai 2024.

[24]http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2002ttnfa03/Vasseur-Marcq/Attaques/Types_attaques.html

[25]http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2002ttnfa03/Vasseur-Marcq/Attaques/Types_attaques.html

[26]http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2002ttnfa03/Vasseur-Marcq/Attaques/Types_attaques.html

[27] https://www.kaspersky.fr/resource-center/definitions/firewall consulté en 14 mai 2024.

[28] https://www.wixxim.fr/fiches/le-pare-feu-ou-firewall.

[29] https://culture-informatique.net/cest-quoi-un-serveur-proxy/.

[30] Belhadj Belaid, et Yacine Hamadouche. "Étude et sécurisation d'une infrastructure DMZ avec ASA Cisco5510." Mémoire de fin d'étude, Université Mouloud Mammeri de Tizi Ouzou (UMMTO), 2015

[31] https://www.it-connect.fr/informatique-cest-quoi-une-dmz/

[32] https://www.cloudflare.com/fr-fr/learning/access-management/what-is-ssh/ consulté en 21 mai 2024.

[33] https://aws.amazon.com/fr/what-is/ipsec . Consulté en 21 mai 2024.

[34] https://www.fortinet.com/fr/resources/cyberglossary/what-is-https consulté en 30 mai 2024.

[35] Blanc J., «les réseaux locaux virtuels»,T MRIM-MOTAUBAN,Technologie, Décembre2007

[36] VLAN-Réseaux virtuels (unsw.edu.au) / consulté en 25mai 2024.

[37] CHABANE Farid,MEHALLA Youba «Etude du réseau téléphonique de Hassi R'mel» 2008/2009

[38] https://igm.univ-mlv.fr/~dr/XPOSE2006/SURZUR-DEFRANCE/vlanport.html

[39] https://particular-course.blogspot.com/2014/11/reseau-haut-debit-2.html

[40] https://particular-course.blogspot.com/2014/11/reseau-haut-debit-2.html

[41] https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c03323978. consulté en 25 mai 2024.

[42] https://www.researchgate.net/figure/IEEE-8023-and-8021Q-Ethernet-frame-formats-from-21_fig2_368533522

[43] https://www.cisco.com/c/fr_ca/support/docs/lan-switching/8021q/17056-741-4.html. consulté en 28 mai2024.

[44] https://packetsdropped.wordpress.com/2011/01/26/ethernet-frame-types-part-1/

[45] https://www.cisco.com/c/fr_ca/support/docs/lan-switching/vtp/10558-21.html. consulté en 1juin 2024.

[46] https://reussirsonccna.fr/vtp-vlan-trunking-protocol/

[47] https://reussirsonccna.fr/vtp-vlan-trunking-protocol/

[48] https://reussirsonccna.fr/vtp-vlan-trunking-protocol/

[49] [Cours] Le routage Inter-VLAN – FingerInTheNet Consulté juin 2024

[50] https://reussirsonccna.fr/trunk-802-1q-et-isl-ce-quil-faut-savoir-pour-le-ccna/

[51] P. C. Rollins, "Virtual Local Area Networks and Wireless Virtual Local Area Networks," 3 mai 2001.

[52] https://www.formip.com/pages/blog/routage-inter-vlan. consulté en 3juin 2024.

[53] https://webusers.i3s.unice.fr/~deneire/cours/courses/5-Routage-inter-VLAN.pdf

[54] https://ofppt.info/#google_vignette

[55] https://ccnareponses.com/notions-de-base-sur-la-commutation-le-routage-et-sans-fil-modules-4-routage-inter-vlan/. consulté en 8 juin 2024.

[56] https://ccnareponses.com/notions-de-base-sur-la-commutation-le-routage-et-sans-fil-modules-4-routage-inter-vlan/. consulté en 8 juin 2024.

[57] "Problèmes liés aux ports de commutateur," OFPPT, consulté en mai 2024. [En ligne]. Disponible sur: [samba.pdf].

[58] https://ccnareponses.com/4-5-2-travaux-pratiques-mise-en-oeuvre-du-routage-inter-vlan/

[59] BENAISSA Adil, «Etude et simulation du Routage Inter VLAN », 2014/2015

[60] https://ccnareponses.com/modules-14-16-concepts-de-routage-et-examen-de-configuration-reponses/

[61] https://ccnareponses.com/modules-14-16-concepts-de-routage-et-examen-de-configuration-reponses/

[62] https://ccnareponses.com/modules-14-16-concepts-de-routage-et-examen-de-configuration-reponses/