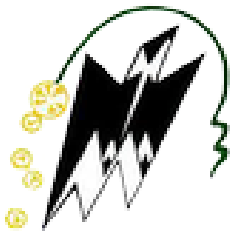
République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mouloud Mammeri de Tizi-Ouzou



Faculté De Génie Électrique et d'Informatique
Département de Télécommunications

Mémoire de Fin d'Etudes

de MASTER ACADEMIQUE
Filière :
Télécommunication
Spécialité :
Réseaux et Télécommunications

Par

CHERIFI Naoual
TOUZOUTI Narimane

Thème

Un mécanisme d'authentification sécurisé dans les réseaux VLANs

Devant le jury :

Président :	Mr. OUADAH MOHAMMED CHAMSE EDDINE	MCA	Univ. UMMTO
Promoteur :	Mr. AMIR MOUNIR	MCA	Univ. UMMTO
Examinatrice :	Mme. ABBA FAIZA	MCB	Univ. UMMTO

Année universitaire :2023/2024

Remerciements

Louange à Dieu , le miséricordieux, sans lui rien de tout cela n'aurait pu être.

Nous tenons tout d'abord à remercier l'entreprise Algérie Télécom de Tizi-Ouzou qui nous a permis de travailler dans un milieu professionnel. Merci à Mr. BAGHDAD, directeur de l'EMRC, ainsi qu'à toute son équipe, pour leur accueil, leur suivi, leur patience et leurs remarques constructives qui nous ont beaucoup aidés.

Nous remercions également Mr. AMIR, notre encadrant, pour son orientation efficace dans la réalisation de ce travail.

Nous exprimons également notre gratitude au président du jury, Mr. Ouadah Mohammed Chamse eddine, ainsi qu'à l'examinatrice, Mme Abba Faiza, qui ont honoré notre travail en acceptant de l'évaluer et de le corriger .

Enfin, nous exprimons notre gratitude à toutes les personnes qui ont contribué et soutenu ce projet, que ce soit de manière directe ou indirecte.

...

Dédicace

Je dédie ce projet à mes parents qui m'ont appris l'importance de l'excellence et de la persévérance, avec une grande reconnaissance et un grand amour pour eux.
Je dédie également ce projet à mes sœurs et à mon frère qui m'ont stimulé pour créer quelque chose de beau et de significatif.
Une spéciale dédicace à mes amis LOUIZA, MELLISSA, ATIKA, FEIROUZ, SELMA, RYMA.
Une dédicace spéciale à Monsieur BAGHDAD et son équipe.

...

Naoual

Dédicace

Avec une profonde reconnaissance et un amour sincère, je dédie ce projet à mes parents qui m'ont inculqué les valeurs de l'excellence et de la persévérance.
A mes sœurs HOUDA,DHRIFA et KHADIDJA que j'aime énormément.
Une dédicace spéciale à Monsieur BAGHDAD et Madame CHENNA pour leurs précieux conseils et leur soutien inestimable.
A mes copines FATMA et IMANE.
A toutes les personnes que j'aime.

...

Narimane

Abstract

It is crucial to manage network devices to prevent unauthorized takeover. Nowadays, remote access has become much more efficient and straightforward for network administrators, thus avoiding unnecessary travel. In this context, our project aims to establish a secure authentication mechanism within VLANs. With the assistance of the engineering team from Algeria Telecom, we have designed a network architecture for our telecommunication department in Tamda. In this regard, we have chosen to implement the AAA authentication protocol on a RADIUS server while segmenting the network into VLANs. This architecture provides consistent visibility, allowing the selection of authentication methods based on the required security level, while considering the network performance to be achieved.

Keywords : : authentication, AAA, Radius, VLAN.

Résumé

Il est essentiel de gérer les équipements réseau pour empêcher toute prise de contrôle non autorisée. De nos jours, l'accès à distance est devenu beaucoup plus efficace et simple pour les administrateurs réseau, évitant ainsi les déplacements inutiles.
Dans ce contexte, notre projet vise à mettre en place un mécanisme d'authentification sécurisé au sein des VLANs. Avec l'assistance du groupe d'ingénieurs d'Algérie Telecom, nous avons élaboré une architecture réseau pour notre département de télécommunication à Tamda. Dans cette optique, nous avons opté pour l'implémentation du protocole d'authentification AAA sur un serveur RADIUS tout en segmentant le réseau en VLANs. Cette architecture offre une visibilité cohérente permettant de choisir la méthode d'authentification en fonction du niveau de sécurité requis, tout en tenant compte des performances du réseau à atteindre.
Les mots clés : authentification, AAA, Radius, VLAN.

Table des matières

Table des figures

Liste des tableaux

LISTE DES ABREVIATIONS

ADSL	**A**symmetric**D**igital**S**ubscriber **L**ine
FO	**F**iber**O**ptic
BNG	**B**roadband **N**etwork**G**ateway
OLT	**O**ptical **L**ine**T**ermination
MSAN	**M**ulti **S**ervice**A**ccess**N**ode
PAN	**P**ersonal **A**rea **N**etwork
LAN	**L**ocal **A**rea **N**etwork
MAN	**M**etropolitan **A**rea **N**etwork
WAN	**W**ide **A**rea **N**etwork
OSI	**O**pen **S**ystems **I**nterconnection
ISO	**I**nternational **S**tandardization**O**rganization
TCP	**T**ransmission **C**ontrol **P**rotocol
ARPA	**A**dvanced **R**esearch**P**rojects**A**gency
UDP	**U**ser **D**atagram **P**rotocol
IP	**I**nternet **P**rotocol
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
HTTP	**H**ypertext **T**ransfer **P**rotocol
DNS	**D**omain **N**ame **S**ystem
MAC	**M**edia **A**ccess **C**ontrol
VLAN	**V**irtual **L**ocal **A**rea **N**etwork
VOIP	**V**oice**O**ver**I**nternet**P**rotocol
VTP	**V**lan **T**runking**P**rotocol
ID	**ID**entifiant
VPN	**V**irtual **P**rivate **N**etwork
AAA	**A**uthentication **A**uthorisation **A**ccounting
RADIUS	**R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice
NAT	**N**etwork **A**ddress **T**ranslation
ACL	**A**ccess **C**ontrol **L**ist
STP	**S**panning **T**ree **P**rotocol
SSH	**S**ecure **SH**ell
TELNET	**TEL**ecommunication **NET**work
SMTP	**S**imple **M**ail **T**ransfer**P**rotocol
QOS	**Q**uality **O**f**S**ervice
HTTP	**HT**ypertext**T**ransfer**P**rotocol

Introduction Générale

Le mot "réseau" est polyvalent, s'appliquant à divers domaines tels que :les télécommunications, la diffusion audiovisuelle, et plus répandu encore, les plateformes sociales contemporaines. En essence, un réseau permet d'interconnecter plusieurs entités, jouant un rôle crucial en informatique pour relier des ordinateurs, des imprimantes, des serveurs et divers autres équipements[1].

Parmi les composants les plus essentiels dans une entreprise, on retrouve les périphériques de terminaison, qui sont situés à l'extrémité de la chaîne. Pour établir un réseau, on utilise différentes méthodes d'interconnexion telles que : les câbles RJ45, la fibre optique, le Wi-Fi, avec des éléments intermédiaires tels que les commutateurs (switches) et les routeurs [1].

Avec l'évolution rapide de l'informatique et des systèmes de communication, les réseaux des entreprises sont de plus en plus vulnérables aux attaques potentielles perpétrées par des intrus.La preuve Lorsqu'un utilisateur tente d'utiliser les services réseau il doit s'y connecter physiquement ou via une borne wifi, ce qui met en danger la sécurité des ressources matérielles et logicielles de l'entreprise[3].

Afin d'éviter ces risques, l'administrateur réseau doit élaborer des stratégies de sécurité efficaces pour superviser les accès au réseau de son entreprise, garantissant ainsi à la fois un niveau de sécurité élevé, une simplicité pour l'utilisateur et une fiabilité des services.L'un des moyens pour réaliser ce contrôle est l'authentification des utilisateurs et l'application de droits utilisateurs[2].

Dans le cadre de notre projet de fin d'études, nous avons effectué un stage au sein de l'EMRC (Etablissement Maintenance Réseau Core) d'Algérie Télécom. Notre objectif était de développer une solution d'authentification garantissant la sécurité de l'accès à distance des utilisateurs au réseau du département de télécommunication à Tamda.

Initialement, l'accent était principalement mis sur la conception de l'architecture réseau du département.Par la suite les VLAN ont été déployés, fragmentant ainsi un réseau

physique en plusieurs segments logiques. En suivant cela, l'installation du protocole AAA sur le serveur RADIUS a été effectuée[4]. Ensuite, des listes de contrôle d'accès (ACL) ont été mises en place pour limiter l'accès à Internet, tandis que le protocole STP a été activé pour optimiser les itinéraires et éviter les boucles.

Notre mémoire est structuré en trois chapitres :

Chapitre 1 : La première partie se concentre sur la présentation de l'organisme d'accueil (Algérie Télécom). La seconde partie traite des concepts généraux des réseaux informatiques, en explorant les éléments fondamentaux nécessaires à la transmission de messages.

Chapitre 2 : La première section aborde la sécurité informatique en discutant des attaques courantes, tandis que la deuxième partie explore les solutions de sécurité proposées, telles que : les VLAN, le protocole AAA et le serveur RADIUS.

Chapitre 3 : Il se concentre sur la mise en place du service d'authentification et décrit les étapes de configuration nécessaires pour tester l'authentification des utilisateurs par le mécanisme de sécurité choisi.

Nous conclurons notre mémoire avec une conclusion et une bibliographie .

Bibliographie

[1] D.Salmi GH.Boudia,"Mise en place d'une infrastructure réseau sécurisé par Cloud Computing",mémoire de MASTER, Université Mouloud Maameri de Tizi-Ouzou,2014-2015.

[2] D.Tighilt, A.Hamoudi, "Mise en place d'une solution d'authentification RADIUS Cas :Cevital de Bejaia", Mémoire de Master,Université Abderrahmane Mira de Béjaia,2012-2013.

[3] Legrand Romain and Laurent Schalkwijk, Les reseaux avec Cisco : connaissances approfondies sur les reseaux, 3e édition. 11/10/2017.

[4] C. M. Cisco, "AAA PROTOCOLS : Authentication, Authorization, and Accounting for the Internet," p. 79, 1999.

Chapitre I

Généralités sur les réseaux informatiques

I.1 Introduction

Au sein de ce chapitre, nous allons d'abord examiner la présentation d'Algérie Telecom, en mettant l'accent sur le département de Maintenance Réseau Core de Tizi Ouzou (EMRC), ainsi que ses objectifs principaux en tant qu'entreprise de premier plan dans le domaine des télécommunications en Algérie. Ou nous avons eu la chance de nous plonger dans le fascinant domaine des télécommunications et de contribuer activement à la construction d'une infrastructure réseau solide et garantie.
Ensuite, nous aborderons les aspects généraux des réseaux informatiques, tels que les différents types de réseaux et leurs adresses, les modèles OSI et TCP/IP, l'architecture, les services et les topologies, etc.

I.2 Présentation de l'organisme d'accueil

Algérie Télécom est le leader sur le marché algérien des télécommunications qui connait une forte croissance, offrant une gamme complète de services de téléphonie fixe et d'internet aux clients résidentiels et professionnels. Cette position s'est construite par une politique d'innovation forte adaptée aux attentes des clients et orientée vers les nouveaux usages. Ses objectifs sont : Rentabilité, Efficacité, Qualité de service.

I.2.1 L'Établissement de Maintenance du Réseau Core d'Algérie Télécom(EMRC)

Est une installation chargée de la maintenance et de la gestion des équipements du réseau central de l'opérateur. Le réseau Core est le cœur du réseau de télécommunications, responsable du routage des données et de la gestion des appels téléphonique la surveillance, la maintenance préventive et corrective, ainsi que la gestion des équipements essentiels pour assurer le bon fonctionnement du réseau central. Cela inclut les commutateurs, les routeurs, les serveurs, les équipements de signalisation et d'autres infrastructures clés.

I.2.2 Fonctionnement du l'EMRC

On distingue deux types de clients ou abonnements qui sont accueillis par Algérie télécom sont : client ordinaire, client corporate.

Client ordinaire :

Qui utilisent un modem pour recevoir la connexion. Bien sûr, une fois qu'Algérie Télécom rédige un plan visant à transmettre l'internet vers la maison du client.
On commence par la fibre optique sortant d'Algérie Télécom jusqu'à la dernière destination, faisant usage d'un câble Ethernet (RJ45) s'il s'agit d'un modem ADSL. Dans ce cas, on a besoin d'un autre câble pour le téléphone fixe. Dans le cas où le modem est optique, on utilise également la fibre optique. Pour un modem 4G, on utilise un câble Ethernet ou une connexion sans fil captée par des ondes radioélectriques.

Client corporat (entreprise) :

— **1er cas :** la différence entre ADSL et SHDSL c'est la quantité de débit. L'ADSL passe par la boucle Metro par contre SHDSL va vers le BNG.

— **2eme cas :** qui utilise une liaison spécialisée (LS) via des équipements de transmission jusqu'à ce que cela se produise aux équipements Metro et PE situé chez Algérie télécom.

LS : la Liaison spécialisée est une liaison permanente réservée à l'usage exclusif d'un utilisateur. Elle offre la possibilité de transmission entre deux points de terminaison déterminés du réseau public.

Toutes ces procédures nécessitent des équipements pour les réalisés sont :

Modem 4G, ADSL (Asymmetric Digital Subsecriber Line), FTH.

MSAN (Multi Service Access Node) c'est une nouvelle technologie qui remplace DSLAM dans quelle mesure est-ce considéré comme le meilleur en termes de débit le plus élevé et aussi fusionne l'ADSL et la VOIX.

OLT (Optical Line Termination) (FTTH) transmit la voix et data aux clients qui utilisent la fibre optique avec un débit jusqu'à 1G bit/s.

Equipement de transmission : plusieurs équipements de transmissions sont placés sur une longue distance liés par des câbles pour atteinte la destination souhaitée.

Un schéma global : Ce schéma résume les trois façons existant pour conduire la connexion du client vers Alger.

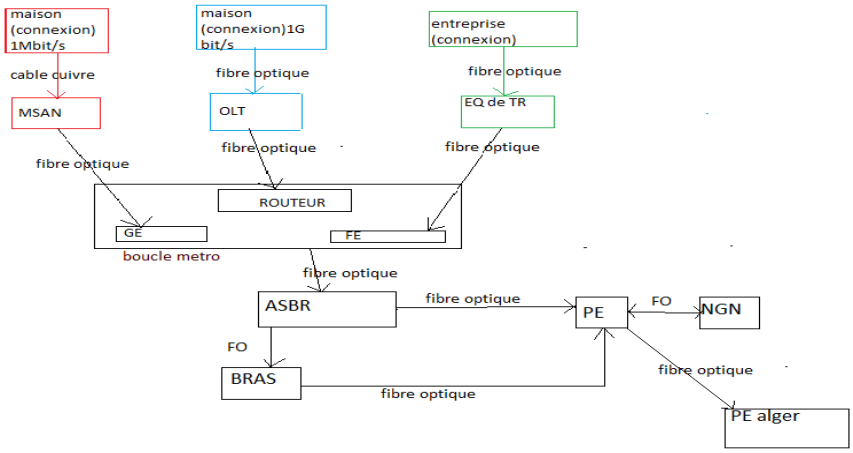


FIGURE I.1 – Le chemin du client vers Algérie Télécom

I.2.3 Les principales responsabilités de l'établissement de maintenance du réseau core peuvent comprendre

Surveillance du réseau :

L'établissement surveille en permanence les performances du réseau core, en utilisant des outils et des systèmes de surveillance avancés. Cela permet de détecter rapidement les problèmes potentiels et de prendre des mesures correctives.

Maintenance préventive :

Des tâches de maintenance planifiées sont effectuées régulièrement pour prévenir les pannes et les défaillances du réseau. Cela peut inclure des mises à jour logicielles, des

remplacements d'équipements obsolètes, des vérifications de la sécurité, etc.

Maintenance corrective :

En cas de panne ou de dysfonctionnement du réseau core, l'établissement intervient pour diagnostiquer et résoudre les problèmes. Cela peut impliquer des réparations d'urgence, des remplacements d'équipements défectueux, des reconfigurations du réseau, etc.

Gestion des mises à niveau et des nouvelles technologies :

L'établissement de maintenance du réseau core est également responsable de la mise en œuvre de mises à niveau technologiques et de l'introduction de nouvelles technologies dans le réseau. Cela peut inclure l'adoption de la fibre optique, le déploiement de réseaux 4G/5G, l'amélioration de la capacité du réseau, etc.

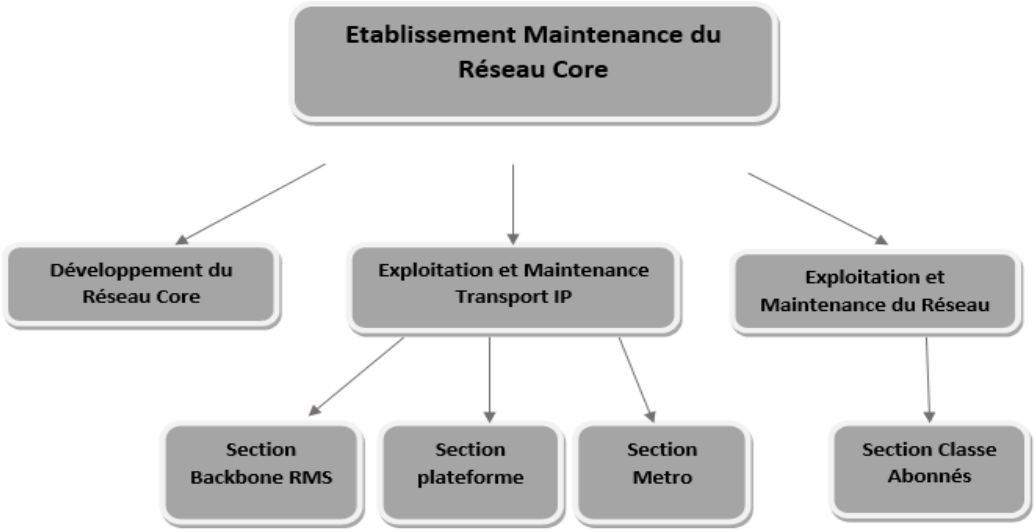


FIGURE I.2 – EMRC Tizi Ouzou

I.3 Réseau informatique

Est une structure qui a une réalité physique en utilisant des matériels ou des machines comme des ordinateurs, des serveurs, des téléphones fixe et portable et des modems ... etc, connecte entre eux par des câbles réseaux ou bien sans fil. Le monde entier utilise trop souvent le réseau afin de partager et communiquer avec n'importe qui à n'importe quel moment pour échanger des données des ressources matérielles, et pour établir cette connexion on doit suivre un ensemble de règles et de protocoles de communication intégrer dans le réseau[1].

I.3.1 Les types de réseaux informatiques

Selon l'importance de la couverture géographique, on classe les quatre types de réseaux PAN, LAN, MAN et WAN comme le montre cette figure 1-3 :

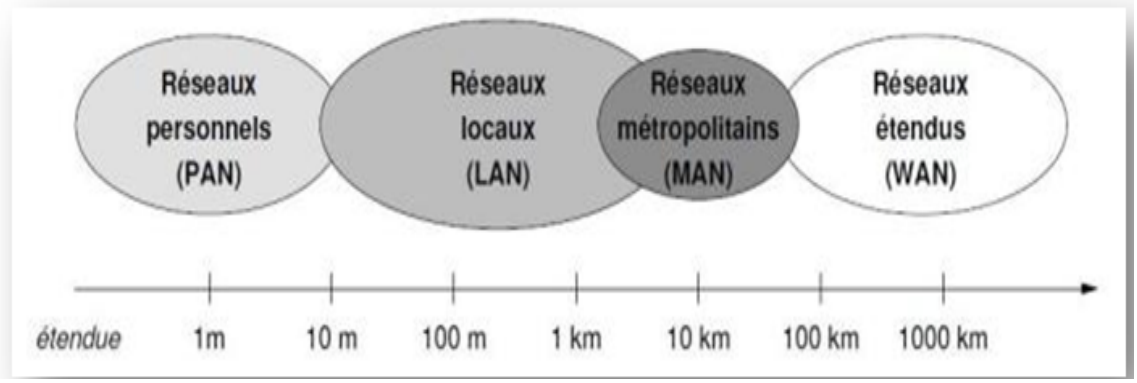


FIGURE I.3 – classement des types de réseaux informatiques[2]

I.3.1.1 PAN (Personal Area Network)

Est un réseau personnel qui relie des équipements positionnés à cote immédiat de l'utilisateur soit avec un câble dans la limite à quelque dizaine de mètres, soit sans fil ce type est destiné à un usage quotidien. Par exemple : un ordinateur bureau, Smartphone et tablette qui accède au réseau wi-fi domestique. . .etc[1].

I.3.1.2 LAN (Local Area Network)

Un réseau local se compose de plusieurs équipements connecter entre eux et positionner sur une surface pour partager des informations, il existe 2 types : Connexion WLAN (sans fil) qui peut atteindre quelques dizaines de mètres à plusieurs centaines de mètres en fonction des obstacles, et une connexion LAN câblés avec une portée maximale de quelques centaines de mètres à quelques kilomètres, et ça dépend de type de câble utilisé comme Ethernet. . .etc, à titre d'exemple de LAN une entreprise ou bien un bâtiment, un bureau, une maison. . .etc[2].

I.3.1.3 MAN (Metropolitan Area Network)

Réseau MAN (métropolitain area network) il couvre plusieurs réseaux locaux LAN (local area network) sur une zone métropolitaine qui peux s'étendre sur quelques dizaines de kilomètres.

I.3.1.4 WAN (Wide Area Network)

Les réseaux étendus (WAN) sont une forme de réseaux de télécommunication qui peuvent connecter des appareils de plusieurs endroits et à travers le monde. Le WAN est formé de nombreux petits réseaux informatiques comme le LAN (local area network) et le MAN (metropolitan area network) interconnecté entre eux. Sont les plus vastes et les plus étendues disponibles à ce jour pour transmettre des informations sur des milliers de kilomètres. Par exemple : internet c'est le plus grand réseau étendu car il relier tous les réseaux d'ordinateurs de monde entier pour qu'ils puissent échanger des informations via le protocole internet[3].

I.3.2 les Modèle référencier des réseaux informatiques

Il excite deux types de model de réseaux qui sont nécessaires pour la transmission des données qui sont les suivants :

I.3.2.1 Modèle OSI

Signifiait Open Système Interconnections est un modèle conceptuel utiliser pour montrer comment les applications communique sur un réseau.
Le modèle OSI permet le transfert de données d'un ordinateur à un autre malgré leurs utilisations des systèmes d'exploitation différentes (Windows, linux. . .etc).

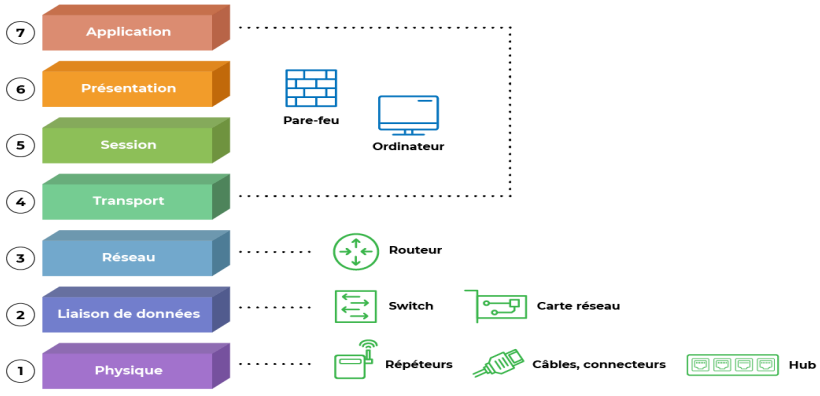


FIGURE I.4 – Modèle OSI[4]

Ce modelé est constitué de sept couches indépendantes qui sont :
• **Couche physique :** elle transfère les données sous forme de bits 1et 0 qui composent tout le code informatique.

Cette couche représente le support physique comme le câble Ethernet qui transforme les bits en format d'impulsions électriques, la fibre optique en format d'impulsion lumineuse, et le Wi-Fi sous forme d'onde radio.

• **Couche liaison de données :** elle gère les communications entre deux machines connectées entre elles ou connecté par un commutateur.

. Cette couche regroupe les bits en trames et les retransmettre.

. Détection des erreurs sur les bits.

. Utilise un système d'adresses qui est l'adresse MAC qui identifie d'une manière unique chaque carte réseau.

• **Couche réseau :** les données sont structurées en paquets, cette couche est responsable de choisissez le meilleur itinéraire à travers le réseau physique (le chemin le plus court) pour l'acheminement des paquets en utilisant les adresse IP pour les diriger vers leur destination.

• **Couche transport :** elle est responsable de la livraison de service à service en basant sur le numéro du port.

Cette couche traite également les problèmes de transport entre les hôtes et assure la fiabilité de transport de données.

La segmentation est de découpe les données en unité plus petites et assure le contrôle de flux pour que l'équipement récepteur reçoive juste la quantité de données dont il a besoin par l'équipement émetteur.

TCP orienté connexion et UDP orienté non connexion sont les deux protocoles nécessaires utilisés dans cette couche [5] [4].

• **Couche session :** elle permit d'initier une session avec la destination afin d'échanger des données c'est-à-dire elle réalise le lien entre les adresses logiques et les adresses physiques.

Elle est responsable de la synchronisation des informations provenant de différents source (synchronisation de la communication).

Elle se charge de l'authentification et de la connexion en cas d'interruption de réseau.

• **Couche présentation :** cette couche effective le traitement de syntaxe ou la conversion des données d'un format à un autre c'est-à-dire elle fait le déchiffrement des données qui devront être transmis à la couche inferieure.

• **Couche application :** la couche la plus proche de l'utilisateur final elle fournit des services réseau, ces services sont des protocoles qui fonctionne avec les données que le client utilise telle que le HTTP qui est utilisé avec des navigateurs web (Google chrome, Firefox et internet et explorer) et le SMTP est utilisé avec des applications comme (Outlook, Yahoo, et Gmail) et d'autres protocoles comme le DNS et le FTP...etc.

On peut dire que c'est une interface graphique qui permit de traduire les données dans notre langage.

I.3.2.2 Modèle TCP/IP

C'est un ensemble de protocole le plus utilisé pour la communication sur internet. C'est une version abrégée du modèle OSI et contient 4 couches comme le montre la figure suivante :

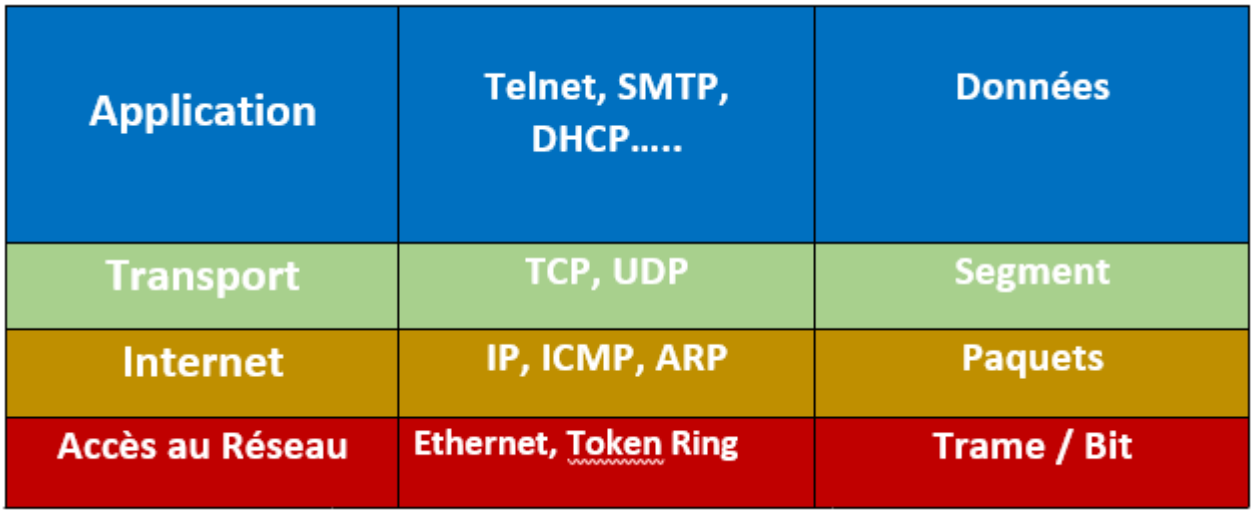


FIGURE I.5 – Les protocoles et les données associés aux couches TCP/IP[6]

• **Couche Application :** c'est l'interface entre l'utilisateur et le périphérique du réseau, parmi ces protocoles : HTTP, SMTP, DHCP. Elle rassemble les trois dernières couches de modèle OSI (session, présentation, application).
• **Couche Transport :** Permet l'acheminement de bout en bout entre les applications, elle utilise le protocole TCP pour une transmission fiable des données, tandis que le protocole UDP fournit un service de transfert de données plus rapide mais moins fiable.
• **Couche Internet :** responsable du routage des paquets, l'adressage et l'encapsulation en utilisant le protocole IP.
• **Couche Accès au Réseau :** définit la manière dont les données doivent être envoyer physiquement sur le réseau, parmi ces protocoles on trouve Ethernet, Token Ring etc.

I.3.3 les différents points entre le modèle OSI et TCP/IP

-Le modèle TCP/IP a été développé par l'ARPA (Advanced ResearchProjects Agency). Le plus utilisé pour les communications sur internet, décrit comment les données sont transmises de manière fiable vers d'autres réseaux à grande échelle. Combinaison de certaines couches par exemple la couche Accès au Réseau de tcp/ip combine les couches liaisons de données et physiques.

-Le modèle OSI a été développé par l'ISO (Organisation International de Normalisation). Utilisé comme une référence pour comprendre comment les différentes couches de communication interagissent entre elle, Contient 7 couches[4].

I.3.4 Architecture Réseau

I.3.4.1 Modèle client/serveur

Est un réseau qui utilise un périphérique central (Serveur) pour délivrer des informations et des ressources auprès des autres hôtes (clients).La plupart des protocoles de la couche application de tcp /ip opèrent conformément au modèle client/serveur[1].

I.3.4.2 Modèle pair-à-pair (Peer to Peer)

Est un réseau dans lequel une machine est à la fois client et serveur, c'est à dire elle peut envoyer des requêtes mais également à répondre. Sont souvent utilisé pour partager des fichiers illégaux ou des films cracker, car il n'y a pas de contrôle sur ces fichiers[5].

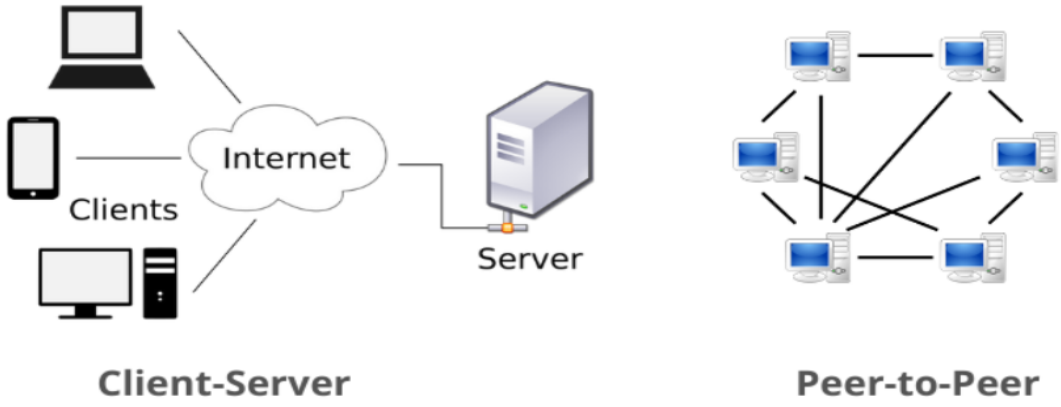


FIGURE I.6 – modèle client/serveur et Peer to Peer[4]

I.3.5 Les équipements du réseau informatique

Dans une topologie on distingue plusieurs équipements comme le Switch (commutateur), le routeur, le serveur, le modem, et la passerelle[4].

1 Routeur :

-Il relie entre plusieurs réseaux cela signifie qu'il associe des adresse réseaux différentes avec un masque sous réseau spécifier.

-Son rôle est l'examinassions de l'adresse IP de destination de paquet IP et envoyer sur la bonne interface.
-Il construit une table de routage pleine d'adresses IP de destination.
-Il fonctionne sur la couche 3 (réseau).

2 Switch (commutateur) :

Est un dispositif multiport pour interconnecter des ordinateurs et d'autres périphériques (serveur, imprimante...etc.) afin de former un réseau local.
-Il se base sur l'adresse MAC qui est un identifiant unique de chaque machine pour pouvoir envoyer les données au destinataire approprié.
-La trame Ethernet doit contenir l'adresse MAC source de l'ordinateur émetteur et celle de l'ordinateur récepteur puis il les inserts sur la table d'adresse MAC dans le commutateur.
-Il fonctionne sur la couche 2(liaison de données).

3 Serveur :

Est un gros ordinateur dont la fonction principale est de fournir des services autour des données pour les clients, souvent un serveur est nommé selon son utilisation.
Par exemple un serveur web va fournir l'accès aux pages web et un serveur mail va gérer les mails et un serveur de stockage de données en base de données...etc.

4 Modem :

Est un dispositif qui capte la connexion.
C'est l'abréviation de mot modulateur, démodulateur en effet il convertie les données analogiques en numérique pour être lisible sur l'écran du pc et inversement pour les transférer aux d'autre périphériques.

5 Passerelle :

C'est un dispositif qui achemine le trafic en dehors du réseau local, elle traduit les données échangées entre les deux protocoles d'un niveau différentes.

I.3.6 Topologies des réseaux

On trouve deux types, la topologie logique qui montre la manière dont les données sont transmises et contrôler par un ensemble de protocoles et des règles et la topologie physique décrit la manière dont les équipements sont connectés au réseau, il s'agit de sa structure. Parmi les topologies de base on trouve :

I.3.6.1 Topologie en bus

Facile a installé, tous les ordinateurs sont reliés à un câble qui se termine avec deux bouchons de terminaison, qui empêche les signaux de retourner sur le support de communication, en cas de rupture le réseau entier s'arrête.

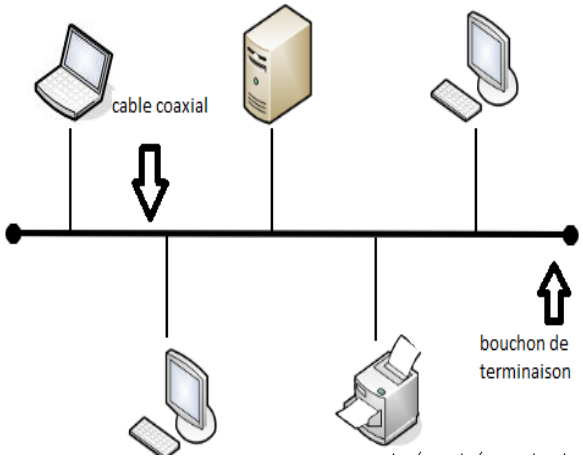


FIGURE I.7 – Topologie en Bus[7]

I.3.6.2 Topologie en étoile

Facile de localiser la panne, contiens un commutateur (Switch) central ou tous les périphériques sont connectés, c'est la topologie la plus utilisé dans les réseaux LAN.

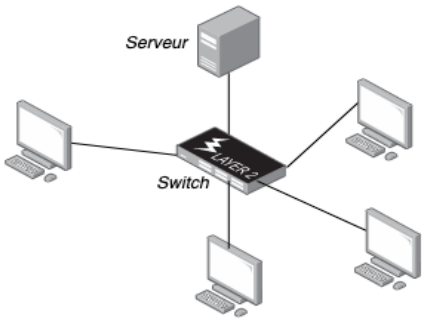


FIGURE I.8 – Topologie en étoile[7]

I.3.6.3 Topologie en anneau

Chaque hôte est connecté à son voisin en formant un anneau, la panne d'un seul périphérique affecte l'ensemble du réseau. Ya aussi la topologie en double anneau utilisé pour la redondance c'est à dire si le câble tombe en panne on utilisera le seconde câble de

secours comme ça le réseau ne tombera pas.

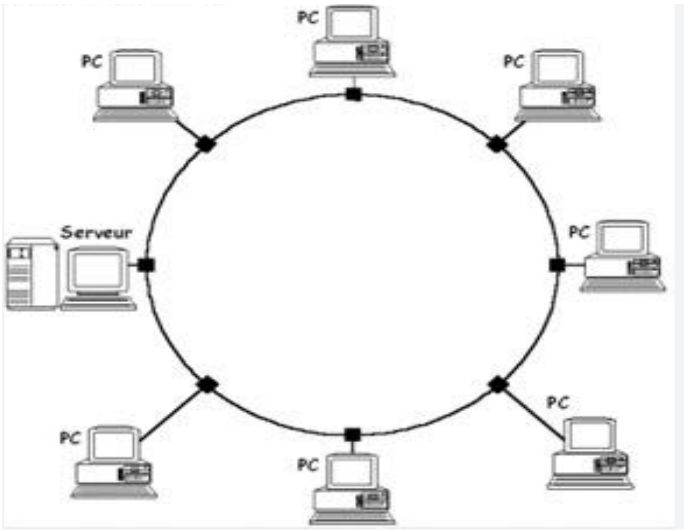


FIGURE I.9 – Topologie en Anneau[7]

I.3.7 Type d'adresse IP

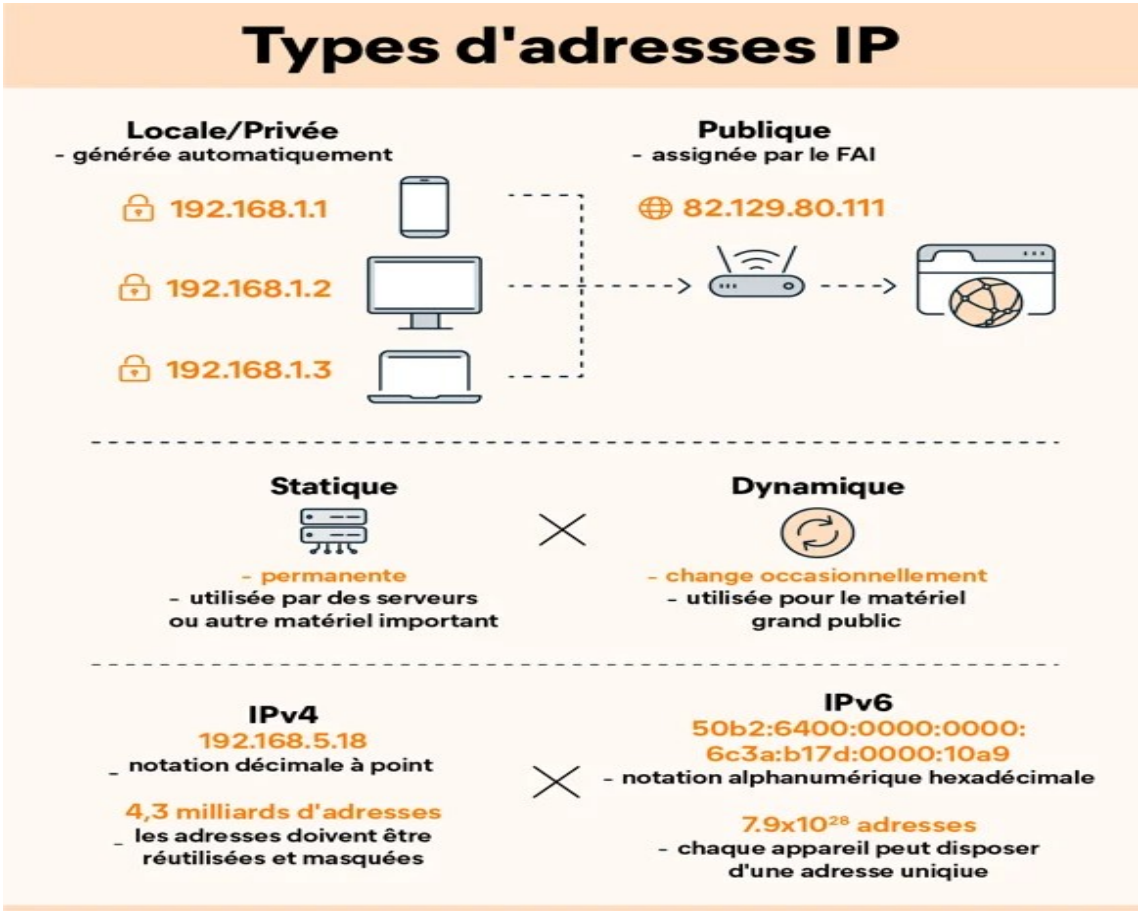


FIGURE I.10 – type d'adresses IP[8]

I.3.8 Les différences entre IPV4 et IPV6

	IPV4	**IPV6**
Adressage	32bits, 2°32 d'adresses uniques, basé sur les classes d'adresses.	128bits,2°128 d'dresses uniques, sans classes d'adresses.
Format d'adresse	Numérique décimal, séparé par des points (ex : 172.16.0.0).	Alphanumérique hexadécimal donc de (0-9) et de (A-F), séparé par des deux-points (ex : 2001 :db8 : :1).
En-tête de paquet	20 octets.	40 octets (simplifié, champs optionnels).
Multidiffusion	Facultative.	Est une spécification de base et en une seule opération permet la diffusion d'un paquet vers plusieurs destinations.
QOS	Qualité de service nécessite des technologies supplémentaires comme DiffServ pour atteindre un résulta similaire aux ipv6.	Qualité de service intégré.
Traduction d'adresse réseau (network address translation)	Utilise la traduction d'adresse réseau (NAT).	Elimination de la traduction d'adresse réseau (NAT).

TABLE I.1 – La différence entre IPV4 et IPV6[8]

I.3.9 Les services réseaux

Sur Internet, divers services sont en place, telles que l'accès à des sites web, la résolution de noms de domaine, l'envoi et la réception d'e-mails, ainsi que le transfert de fichiers. Chaque service doit définir les requêtes que le programme client peut envoyer au serveur, les réponses que le programme serveur peut renvoyer au client[8].
Parmi les services qui offrent les protocoles réseau on trouve :

1 HTTP :

Protocole de transfert hypertexte, utilisé pour accéder aux services Web. On a aussi le (HTTPS) sécurisé, permettant la transmission chiffrée des communications HTTP.

2 DNS :

Domain Name System c'est un service qui permet de convertir les noms de domaine en adresse IP.Il simplifie la mise à jour et la gestion des adresses IP, offrant la possibilité de modifier l'adresse IP associée à un nom de domaine sans nécessiter la mise à jour de tous les liens pointant vers ce nom de domaine[6].

3 EMAIL :

Service pour la messagerie électronique qui utilise les protocole SMTP (Simple Mail Transfer Protocol) st employé pour l'envoi d'e-mails, POP3 (Post Office Protocol version 3) est utilisé pour la réception d'e-mails.

4 DHCP (Dynamic Host Configuration Protocol)

Qui est utilisé afin de paramétrer de manière automatique les adresses IP, les masques de sous-réseau, leDNS, et les passerelles.

I.4 Conclusion

En conclusion, l'analyse de la structure organisationnelle et du fonctionnement d'Algérie Télécom nous éclaire sur la manière dont l'entreprise est organisée pour atteindre ses objectifs dans le secteur des télécommunications en Algérie. Cette analyse permet de mieux comprendre la façon dont les différentes composantes de l'entreprise interagissent pour assurer la prestation de services et le déploiement des infrastructures.

Ensuite nous avons abordé dans ce chapitre les fondements des réseaux informatiques, en mettant l'accent sur leur valeur et leur importance pour établir des communications à distance à l'aide d'équipements, de câbles et de systèmes. Cette infrastructure permet de créer des messages bien structurés et d'assurer leur transmission vers les destinations désirées. Il est essentiel de bien maîtriser ces concepts pour pouvoir avancer vers la prochaine étape, qui est la sécurité informatique.

Bibliographie

[1] R. Kalavathi, A. Y. Reddy, and amp; C. Swathi, “A COMPREHENSIVE ANALYSIS OF VIRTUAL LOCAL AREA NETWORK (VLAN) AND INTER-VLAN ROUTING STRATEGIES,”2017.

[2] Andrew S. Tanenbaum David J.Wetherall. ”Computer Networks Fifth Edition Pearson”. 2013.

[3] Legrand Romain and Laurent Schalkwijk, Les reseaux avec Cisco : connaissances approfondies sur les reseaux, 3e édition. 11/10/2017.

[4] Nesrine KHERNANE. ”cours : Cyber sécurité 1, chapitre 3 : Vulnérabilit´es des systèmes informatiqe et méthodes d’attaque”. Université Batna 2, 2021.

[5] C. CISCO, “CCNA1 Modules 1 – 3 : Examen Sur La Connectivité Des Réseaux De Base Et Les Communications Réponses,” 18/12/2021.

[6] C. CISCO, “CCNA1 :Introduction aux Réseaux – Modules 15,” 5/04/2023.

[7] Pr. Houssine Limouny, “ Support de Cours ‘chapitre2 : Réseaux et Transmission des données / Métrologie et Instrumentation,’” Meknès, Maroc.

[8] Huawei Technologies Co., Textbooks :DATA COMMUNICATIONS AND NETWORK. Hangzhou, China.

Chapitre II

La sécurité informatique : Etude des solutions proposées

II.1 Introduction

En 2018, 5 millions d'emails internes et externes de l'entreprise suisse Deloitte sont Potentiellement compromis, y compris des échanges avec des centaines de très gros clients tels que la FIFA et bien d'autres. Ces attaques ne représentent qu'une partie des dégâts causés par la cybercriminalité[1].
Donc Ce deuxième chapitre se concentre sur un aspect essentiel dans le domaine de l'informatique moderne : la sécurité réseau. Nous explorerons les défis et les solutions qui peuvent être mises en place pour renforcer la sécurité des réseaux, en mettant particulièrement l'accent sur l'authentification dans les réseaux VLAN.

II.2 Définition

La sécurité informatique consiste en différentes mesures prises pour prévenir et/ou réduire les pannes naturelles causées par l'environnement ou les défauts du système d'information, ainsi que les attaques malveillantes intentionnelles dont les conséquences sont catastrophiques[2]. Afin de protéger le mieux possible les données et l'accès aux équipements du réseau.

II.3 Les principaux objectifs

Voici quelques-uns des principaux objectifs de la sécurité :

•**Confidentialité :** signifie que les données ne sont accessiblesqu'aux personnes autorisées.

•**Intégrité :** l'assurance que les données consulter n'ont pas été modifié.

•**Disponibilité :** les données sont accessibles rapidement et régulièrement.

•**Authentification :** vérifierl'identité de l'utilisateur afin d'autoriser son accès au réseau.

•**Non-répudiation :** surveillance et enregistrement des actions exécutés pour les utilisateurs.

II.4 Les attaques réseau

Une attaque réseau se définit comme une intrusion dans une infrastructure de communication dans le but d'acquérir un accès non autorisé à des ressources ou d'exploiter des vulnérabilités existantes. Elle se compose généralement de deux phases distinctes : tout d'abord, une attaque passive qui consiste à analyser le trafic réseau afin de recueillir des informations sensibles ; ensuite, une attaque active, qui vise à perturber le fonctionnement du réseau[1][3].

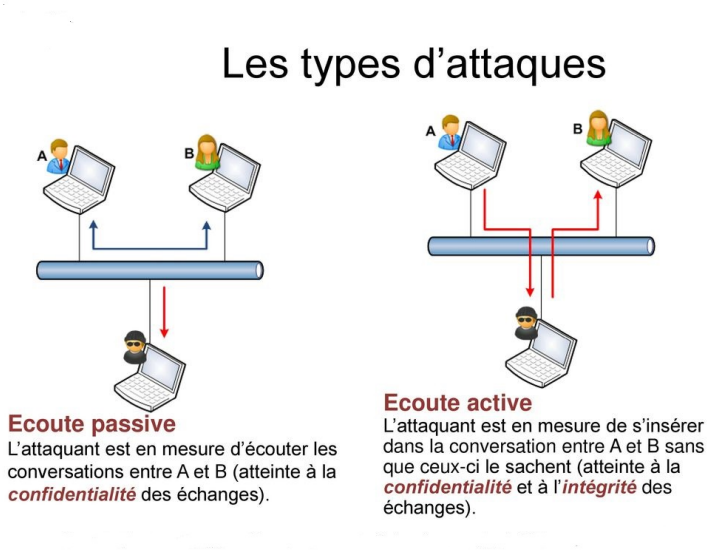


FIGURE II.1 – les types d'attaque [3].

II.5 Les solutions de sécurité proposées

Parmi les nombreuses solutions de sécurité disponibles on trouve :

•**Pare-feu (Firewall) :** c'est un mécanisme de filtrage des entrées de l'extérieur vers le réseau.

•**Chiffrement des données :** le processus de chiffrement implique de convertir un message en texte clair en un message illisible, généralement en utilisant un algorithme basé sur des clés. La cryptographie est divisée en deux types à savoir la cryptographie symétrique (DES) et la cryptographie asymétrique(AES).

•**Antivirus :** un logiciel antivirus examine les fichiers et les e-mails, ainsi que les secteurs de démarrage pour repérer les virus, en plus d'analyser la mémoire vive de l'ordinateur, les supports amovibles tels que les clés USB, les CD, les DVD, etc., ainsi que les données échangées sur les réseaux, y comprisInternet.

•**VPN :** un réseau privé virtuel est une technique très sécurisée permettant de prolonger un réseau privé à travers un réseau public tel qu'Internet. Grâce au VPN, les utilisateurs peuvent accéder aux données du réseau privé via Internet comme s'ils étaient directement connectés à ce réseau privé. Le VPN opère en utilisant un système de tunnelisation privée, où un tunnel est établi pour faire transiter toutes les communications et les données échangées, lesquelles sont cryptées[1].

- Dans notre projet, nous avons mis en place une solution qui intègre l'authentification AAA dans un serveur radius, les listes de contrôle d'accès (ACL), le NAT, et la segmentation réseau grâce à l'utilisation de VLANs.

II.5.1 les VLANs

a)Définition

Est un ensemble de périphériques logiques et d'utilisateurs sans contrainte de localisation physique, ce qui permet aux administrateurs de diviser logiquement différents utilisateurs du même LAN physique en différents domaines de diffusion selon les exigences réelles de l'application. Chaque VLAN contient un groupe d'ordinateurs ou de serveurs ayant les mêmes exigences, et ils communiquent entre eux comme s'ils étaient dans le même segment réseau. C'est pourquoi on l'appelle un réseau local virtuel. Les VLAN fonctionnent aux couches 2 et 3 du modèle de référence OSI, et un VLAN est un domaine de diffusion. La communication entre les VLAN doit passer par des dispositifs de couche 3 (routeurs ou commutateurs de couche 3)[4].

b)Les avantages

1. Contrôle de la portée de diffusion : un VLAN est un domaine de diffusion. Les trames de diffusion envoyées par des ordinateurs dans un VLAN ne se propageront pas à

d'autres VLAN, réduisant ainsi la plage d'impact d'émissions. En résumé, en contrôlant la portée de diffusion dans un réseau VLAN, on restreint la propagation des trames de diffusion à des ensembles spécifiques de périphériques. Ceci contribue à améliorer l'efficacité et la sécurité du réseau en réduisant les interférences entre ses divers segments[5].

2. La sécurité : différents VLAN peuvent être créés selon les exigences de sécurité et les ordinateurs avec les mêmes exigences de sécurité peuvent être mis dans le même VLAN. Par exemple, les ordinateurs avec des données sensibles sont isolés des autres les ordinateurs du réseau, réduisant ainsi la possibilité de fuite confidentielle information. Les ordinateurs des différents VLAN sont isolés les uns des autres à la couche de liaison de données, c'est-à-dire que les utilisateurs d'un VLAN ne peuvent pas communiquer directement avec les utilisateurs dans d'autres VLAN. Pour que les différents VLAN communiquent, ils doivent passer par Les périphériques de couche 3 tels que les routeurs ou les commutateurs de couche 3 et contrôlent le trafic sur Dispositifs de la couche 3[6].

3. Amélioration du rendement : division du réseau plat de la couche 2 en plusieurs groupes de travail logiques (diffusion domaines) peuvent réduire le trafic inutile sur le réseau et améliorer performance.

4. La simplification de la gestion : l'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement et simplement sans devoir manipuler les connexions physiques dans le local technique.

5. La technologie évolutive et à faible coût : la simplicité de la méthode d'accès et la facilité de l'interconnexion avec les autres technologies ont fait d'Ethernet une technologie évolutive à faible coût quelles que soient les catégories d'utilisateurs.

c)Type vlan : selon le principe de classification, il existe différents types de VLAN :

1. VLAN basés sur les ports : l'ID de VLAN d'un port physique est associé au port physique du commutateur, ce principe de classification est simple et intuitif, facile à mettre en œuvre, et relativement sûr et fiable.

2. VLAN basées sur les adresses MAC : une table de correspondance des adresses MAC et des identifiants de VLAN est établie et maintenue au sein du commutateur. Cependant, il convient de noter que la sécurité de ce type de VLAN est relativement faible, car il est facile pour certains ordinateurs malveillants de falsifier leurs adresses MAC.

3. VLAN basées sur les protocoles : il regrouper les trames en fonction de leur type de protocole Cela peut être bénéfique pour la gestion du trafic réseau et pour renforcer la sécurité.

II.5.2 Le protocole AAA

Le modèle AAA, qui englobe l'Authentification, l'Autorisation et la Comptabilité, représente un ensemble de mesures de sécurité pour contrôler l'accès au réseau. Il spécifie quels utilisateurs peuvent entrer dans le réseau et quels services et ressources sont disponibles pour ces utilisateurs autorisés[7].

• **Authentification :** le serveur AAA vérifie les identités des utilisateurs qui tentent d'accéder au réseau et détermine s'ils ont l'autorisation nécessaire. En comparant les informations d'authentification fournies par un utilisateur avec celles stockées dans une base de données, le serveur AAA valide l'identité de l'utilisateur. Si les informations correspondent, l'utilisateur réussit l'authentification et est autorisé à accéder au réseau. En revanche, si les informations ne correspondent pas, l'utilisateur échoue à l'authentification et se voit refuser l'accès au réseau. Les types d'informations d'authentification courants incluent le mot de passe, le nom d'utilisateur ainsi que le certificat numérique.

• **Autorisation :** les utilisateurs sont accordés des droits distincts afin d'accéder à des services spécifiques. Après qu'un utilisateur a réussi l'authentification d'identité, les éléments suivants sont autorisés à l'utilisateur : Commandes, Ressources, Informations. L'autorisation suit le principe du moindre privilège,Cela signifie que les utilisateurs ne se voient accorder que les permissions nécessaires à l'exécution des fonctions requises pour éviter tout comportement réseau accidentel ou malveillant[7].

• **Comptabilité :** enregistrer de manière exhaustive toutes les actions entreprises par un utilisateur pendant l'utilisation des services réseau, en incluant des détails tels que l'identité de l'utilisateur, le moment où les actions ont été effectuées et la nature de ces actions. La comptabilité enregistre les détails du service utilisé, l'heure de début de l'activité, ainsi que les données de trafic pour surveiller et enregistrer l'utilisation des ressources réseau par l'utilisateur Il est essentiel d'avoir ces informations pour mettre en œuvre une comptabilité basée sur le temps ou le trafic et pour assurer une surveillance efficace du réseau[7].

II.5.2.1 Le fonctionnement du protocole AAA

Un périphérique réseau peut opter pour deux modes afin de gérer l'authentification, l'autorisation et la comptabilisation des utilisateurs qui lancent l'accès administratif, on trouve :

-Mode interne : ce qui implique que le périphérique réseau vérifie et autorise l'utilisateur en se basant sur les informations de nom d'utilisateur et de mot de passe contenues dans sa base de données locale[7].

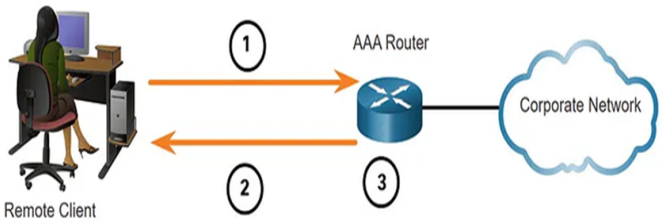


FIGURE II.2 – le protocole AAA en authentification local[8].

-Mode externe : ce mode exige un serveur qui contrôle le protocole AAA emploie la structure client/serveur, qui est simple, évolutive et facilite la gestion centralisée des informations utilisateur, les étapes de son fonctionnement sont les suivantes :

1- L'utilisateur établit une connexion avec le client AAA avant d'accéder au réseau.

2 -Le client AAA envoie les informations d'identification de l'utilisateur au serveur AAA.

3 -Le serveur AAA authentifie et autorise l'utilisateur en fonction des informations d'identification de l'utilisateur, puis renvoie les résultats d'authentification et d'autorisation au client AAA[9].

4 -Le client AAA détermine s'il doit permettre à l'utilisateur d'accéder au réseau en fonction des résultats d'authentification et d'autorisation reçus[7].

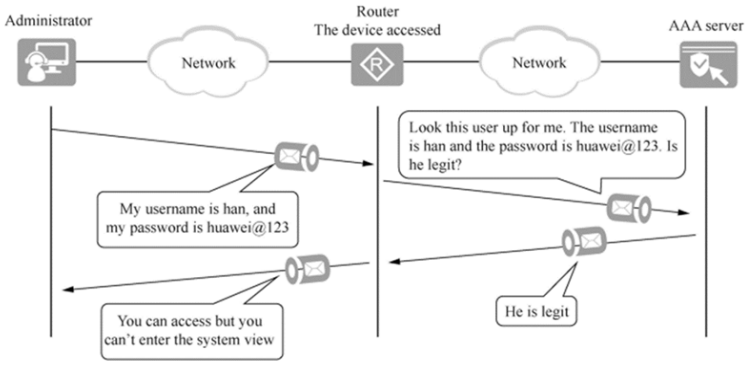


FIGURE II.3 – le fonctionnement de AAA avec le serveur local[6].

Pour que le protocole AAA fonctionne nécessite des protocoles de communications comme le RADIUS.

II.5.3 Le serveur RADIUS

RADIUS est un protocole standard largement soutenu par la plupart des principaux fournisseurs de dispositifs, ce qui en fait le plus couramment utilisé sur les réseaux en direct.

Dans RADIUS, l'authentification et l'autorisation sont définies dans le RFC 2865, tandis que la comptabilité est définie dans le RFC 2866. RADIUS a été conçu avant le modèle de framework AAA et intègre à la fois l'authentification et l'autorisation. Par conséquent, lorsqu'AAA est implémenté via RADIUS, les utilisateurs peuvent ne pas savoir si l'accès est refusé en raison d'une erreur d'authentification (par exemple, un mot de passe incorrect) ou d'une erreur d'autorisation (par exemple, l'utilisateur n'est pas autorisé)[7].

II.5.3.1 RADIUS authentification, autorisation, comptabilité

Un appareil qui fonctionne comme un client RADIUS collecte les informations d'un utilisateur, y compris le nom d'utilisateur et le mot de passe, et envoie les informations au serveur RADIUS. Le serveur RADIUS authentifie ensuite les utilisateurs selon les informations, et ensuite effectue l'autorisation et la compatibilité pour l'utilisateur. La figure 3 montre le processus d'échange d'informations entre un utilisateur, un client RADIUS et un serveur RADIUS.

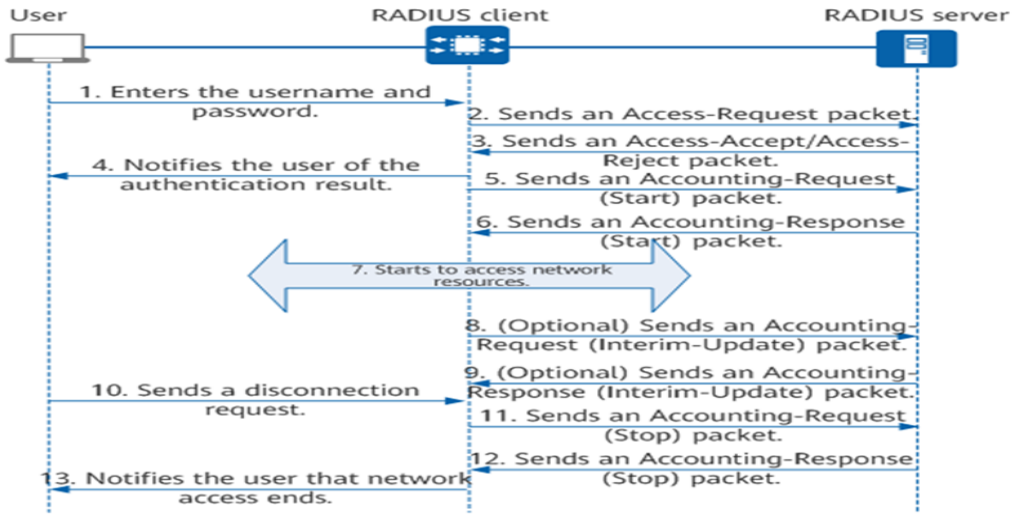


FIGURE II.4 – le fonctionnement de RADIUS[6].

1-Un utilisateur doit accéder à un réseau et envoie une demande de connexion contenant le nom d'utilisateur et le mot de passe au client RADIUS (dispositif).

2- Le client RADIUS envoie un paquet Access-Request RADIUS contenant le nom d'utilisateur et le mot de passe au serveur RADIUS.

3 -Le serveur RADIUS vérifie l'identité de l'utilisateur * Si l'identité de l'utilisateur est valide, le serveur RADIUS renvoie un paquet Access-Accept au client RADIUS pour permettre d'autres opérations pour l'utilisateur. Le paquet Access-Accept contient des informations d'autorisation car RADIUS fournit à la fois des fonctions d'authentification et d'autorisation.

*Si l'identité de l'utilisateur est invalide, le serveur RADIUS renvoie un paquet Access-Reject au client RADIUS pour rejeter l'accès de l'utilisateur.

4- Le client RADIUS notifie l'utilisateur si l'authentification est réussie.

5-Le client RADIUS permet ou rejette la demande d'accès de l'utilisateur en fonction du résultat de l'authentification. Si la demande d'accès est autorisée, le client RADIUS envoie un paquet Accounting-Request (Start) au serveur RADIUS, Pour initier une session de comptabilité avec l'utilisateur qui contient des détails tel que l'heure de début, le numéro du port, la taille des données et le nom d'utilisateur. . .etc. pour enregistrer l'utilisation dès le début de la connexion.

6- Le serveur RADIUS envoie un paquet Accounting-Response (Start) au client RADIUS pour indiquer qu'il a bien reçus le paquet Accounting-Resquest, et démarre la comptabilité.

7- L'utilisateur commence à accéder aux ressources réseau.

8-9-Accounting-Request (Interim-update) et Accounting-Response (Interim-update) sont deux requêtes facultatives, la première indique au RADIUS qu'il doit faire la mise à jour pour les informations traité par l'utilisateur (surveillance), la deuxième est envoyer par le RADIUS au client pour l'informer que la mise à jour est faite, Sont utilisé pour des opérations en temps réel.

10- L'utilisateur envoie une demande de déconnexion.

11- Le client RADIUS envoie un paquet Accounting-Request (Stop) au serveur RADIUS. Explication : Lorsqu'un utilisateur se déconnecte volontairement ou est déconnecté de force par le client RADIUS, ce dernier envoie un paquet contenant des détails sur l'utilisation des ressources du réseau (tels que la durée de la connexion et la quantité de données échangées), au serveur RADIUS, afin de demander l'arrêt de la comptabilisation.

12- Le serveur RADIUS envoie un paquet Accounting-Response (Stop) au client RADIUS et arrête la comptabilité.

13- Le client RADIUS notifie l'utilisateur du résultat du traitement, et l'utilisateur cesse d'accéder aux ressources réseau[7].

II.5.3.2 Format de paquet RADIUS

Code : Le champ Code, composé d'un octet, permet de déterminer le type de paquet RADIUS, avec une valeur variable selon le type de paquet, telle que 1 pour Access-Request et 2 pour Access-Accept.

Identifiant ID : est présent dans chaque requête, agissant comme un compteur simple pour identifier le paquet. Cela permet d'associer une réponse RADIUS à sa requête correspondante, car dans le protocole UDP, l'ordre des paquets peut varier entre l'émetteur et le récepteur.

Longueur : la taille d'un paquet RADIUS est déterminée par le champ Longueur,

qui est de deux octets. Il est important de considérer les octets situés en dehors de cette longueur comme du remplissage et de les ignorer lors de la réception. Tout colis inférieur à la longueur indiquée doit être renvoyé sans préavis.

Authentificateur : d'une longueur de 16 octets, sert à authentifier la réponse du serveur RADIUS et est essentiel dans le processus d'authentification, notamment dans l'algorithme de masquage des mots de passe.

Attribue : le champ Attribut, de longueur variable, contient des détails spécifiques liés à l'authentification, à l'autorisation, à la comptabilité et à la configuration dans les paquets de demande et de réponse du protocole RADIUS. Ce champ peut comporter plusieurs attributs, chacun étant constitué des éléments Type, Longueur et Valeur.

1.Type : le champ Type, d'un octet, spécifie l'identifiant de l'attribut RADIUS, avec une valeur comprise entre 1 et 255.

2.Longueur : le champ Longueur est d'un octet et indique la longueur de l'attribut RADIUS (y compris les champs Type, Longueur et Valeur). La longueur est mesurée en octets.

3.Valeur : la longueur maximale du champ Valeur est de 253 octets. Le champ Valeur contient des informations spécifiques à l'attribut RADIUS. Le format et la longueur du champ Valeur sont déterminés par les champs Type et Longueur.

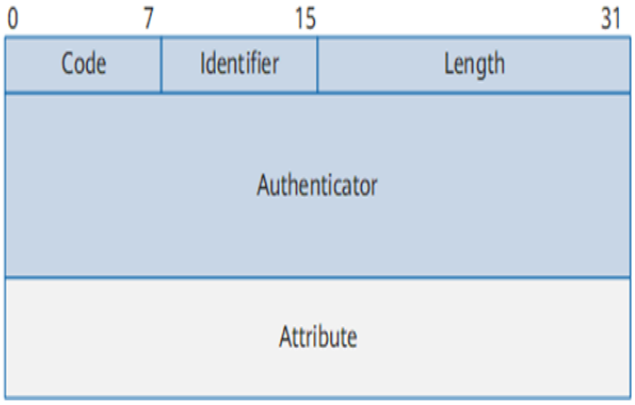


FIGURE II.5 – Format du paquet RADIUS [6]

II.5.4 Le NAT

La technologie de Traduction d'Adresse Réseau (NAT), est nécessaire pour que les ordinateurs qui utilise des adresses privées intranet puissent accéder à Internet (réseau public), en même temps il renforce la sécurité de l'intranet, le NAT soulage la pénurie d'adresses IPv4[10].

Il existe plusieurs types de NAT sont comme suite :

II.5.4.1 NAT statique

Il permet de traduit une seul adresse IP privé à une adresse IP publique, et cette dernière permet à l'adresse privé de sortir vers le WAN, et ce type de NAT ne sauvegarde pas les adresses IP publique.

II.5.4.2 NAT dynamique

On a plusieurs adresses IP privées (local) correspond à plusieurs adresses IP publiques, par exemple deux entreprises utilisent les mêmes adresses privées peuvent être fusionné.Elle est configurée d'une manière unique dont en doit créer d'abord une Access liste des PC ou de réseau autorisé à être translater, ensuite on déclare la plage d'adresse IP publique,à la fin on associer notre Access liste qui contient les IP privés avec le pool d'adresses publique,à partir de celui-ci un pc peut emprunter une adresse pour ce connecté à internet[10].

II.5.4.3 Port Adresse Translation (PAT)

En utilisant le PAT, toutes les adresses IP privées internes sont utilisées avec une adresse IP publique unique, mais chaque adresse IP privée reçoit un port distinct. Ce genre de NAT est aussi appelé surcharge NAT et est le type de NAT courant utilisé dans les réseaux actuels. La plupart des routeurs grand public le supportent même[11]. PAT vous offre la possibilité de gérer de nombreux hôtes en utilisant seulement quelques adresses IP publiques. Son fonctionnement repose sur la création d'un mappage NAT dynamique, où une adresse IP globale (publique) et un numéro de port unique sont choisi. Le routeur maintient une entrée de table NAT pour chaque combinaison unique d'adresse IP privée et de port, qui est traduite en adresse globale et en numéro de port unique[12]. Lorsque la surcharge est activée, le périphérique conserve suffisamment d'informations des protocoles de niveau supérieur (comme les numéros de port TCP ou UDP) pour effectuer la traduction entre l'adresse globale et l'adresse locale correspondante. Avec plusieurs adresses locales attribuées à une seule adresse globale, les numéros de port TCP ou UDP de chaque hôte interne permettent de distinguer les adresses locales.

Voici un exemple où la translation d'adresse de port (PAT) est démontrée dans l'image ci-dessous.

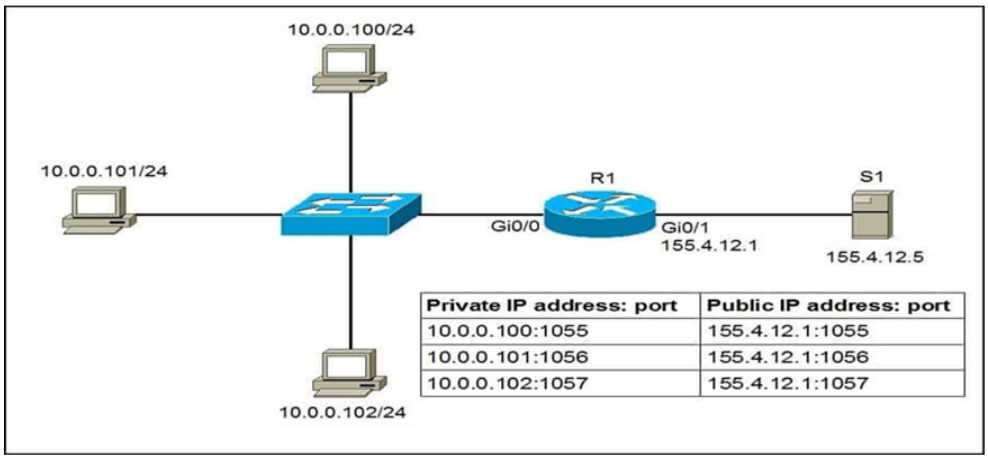


FIGURE II.6 – Le NAT surcharge (port addresse network)[12]

.

II.5.5 Les ACL

permet de renforcer la sécurité en limitant les ressources réseau accessibles aux terminaux selon une stratégie de sécurité définie. En effet, Les Access control List permettent d'appliquer des filtres sur les interfaces et d'indiquer au routeur les paquets qu'il doit accepter(permit) et ceux qu'il doit refuser(deny)[13].

on trouve deux type d'ACL :

II.5.5.1 Les ACL standard

Le trafic peut être analysé en fonction de l'adresse IP source, mais il est recommandé de l'appliquer le plus près possible de la destination en raison de leur méconnaissance.

II.5.5.2 Les ACL étendues

Permet d'analyser du trafic en fonction de l'adresse IP source, adresse IP destination, protocole (tcp, udp, icmp...,) Port source, port destination... sont à appliquer le plus proche possible de la source.

II.6 Conclusion

Ce chapitre nous a permis d'explorer une introduction à la sécurité informatique, en mettant particulièrement l'accent sur les différents types d'attaques auxquels les systèmes peuvent être confrontés. De plus, nous avons discuté des solutions de sécurité mises en œuvre dans notre projet, notamment la segmentation du réseau à l'aide de VLAN, ainsi que la mise en place d'un mécanisme d'authentification AAA au sein des VLAN. Un

élément clé de ce mécanisme est l'utilisation d'un serveur RADIUS, qui gère l'authentification, l'autorisation et la comptabilité des utilisateurs pour contrôler l'accès au réseau. En complément, l'utilisation de listes de contrôle d'accès (ACL) et de Network Adresse Translation (NAT) a contribué à organiser et à sécuriser efficacement notre réseau.

Bibliographie

[1] R. Boukharrou, Support de cours " Sécurité des réseaux",Université Abdelhamid Mehri - Constantine 2, 2019.

[2] A. Chouarfia,cour : "Introduction à la sécurité des réseaux et des systèmes d'information",USTO-MB Oran, Novembre 2010.

[3] Cours de sécurité "chapitre M33-2cyber attaque",université de grenoble, 2018.

[4] L. Huawei Technologies Co, Ed.,"VLAN," in HCNA Networking Study Guide, Singapore, 2016

[5] R. Elimanafe, Y. Suban Belutowe, P. Katemba,"Virtual Local Area Network (Vlan)" 2022.

[6] Huawei, support cours(Textbooks) :"DATA COMMUNICATIONS AND NETWORK," Hangzhou, China, 2023.

[7] D.C. Huawei, support de cours : "What Is AAA ? Three Elements of AAA".

[8] Ayush, magazine article : "AAA access control in networking",20/07/2020.

[9] S. Bordères,livres de Serge Bordère " Authentification réseau avec Radius", édition EYROLLES,2006.

[10] Journal of Applied Computer Science Methods, J.Konikiewicz, Wojciech Markowski, Marcin. "Analysis of Performance and Efficiency of Hardware and Software Firewalls"2017.

[11] TP CISCO, "Configuration de la traduction d'adresses de port (PAT)," 2014.

[12] TP CISCO, "Configuring NAT for IP Address Conservation", 2006.

[13] Charles Dracoulides,Mémoire de master d'ingénieur CNAM,"La sécurité informatique. Cryptographie et sécurité",2015.

Chapitre III

Mise en oeuvre et simulation

III.1 Introduction

Dans ce chapitre on a utilisé le simulateur Cisco, nous avons élaboré une topologie visant à résoudre les problèmes liés à l'authentification des clients et à l'autorisation d'accès à Internet. Nous avons commencé par créer des VLANs, gérés par l'administrateur via le VLAN management, permettant ainsi un accès libre. En définissant des ACL, nous avons établi des limites pour contrôler cette admission. De plus, pour aborder l'autre moitié de la question nous avons intégré le protocole AAA pour l'authentification.

III.2 Présentation de packet tracer

Packet Tracer, développé par Cisco, est un logiciel de simulation de réseaux informatiques qui offre une approche pratique pour l'apprentissage et la compréhension des concepts clés des réseaux. Dans Packet Tracer, les équipements réseau sont représentés de manière réaliste, permettant aux étudiants d'interagir avec eux en personnalisant les configurations, en les activant ou en les désactivant, et en observant la circulation des données entre les différents appareils[1].

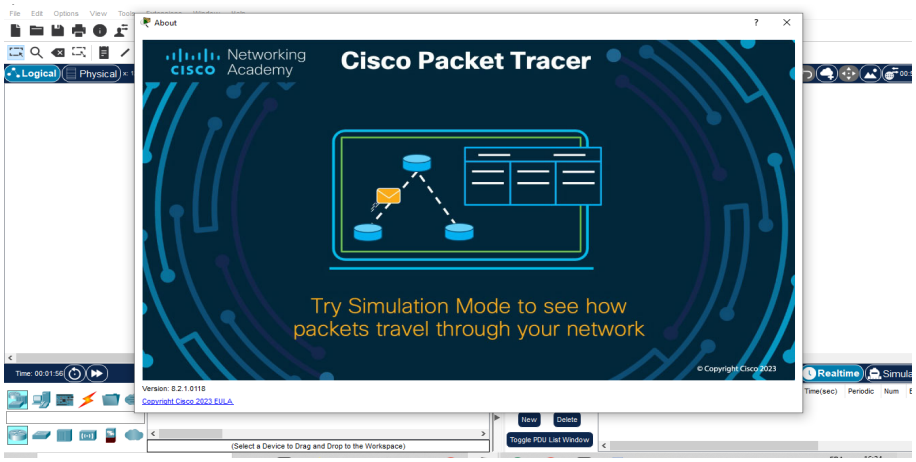


FIGURE III.1 – Le simulateur Packet Tracer CISCO [1]

III.3 Présentation de l'architecture de département

Voici au-dessous l'architecture :

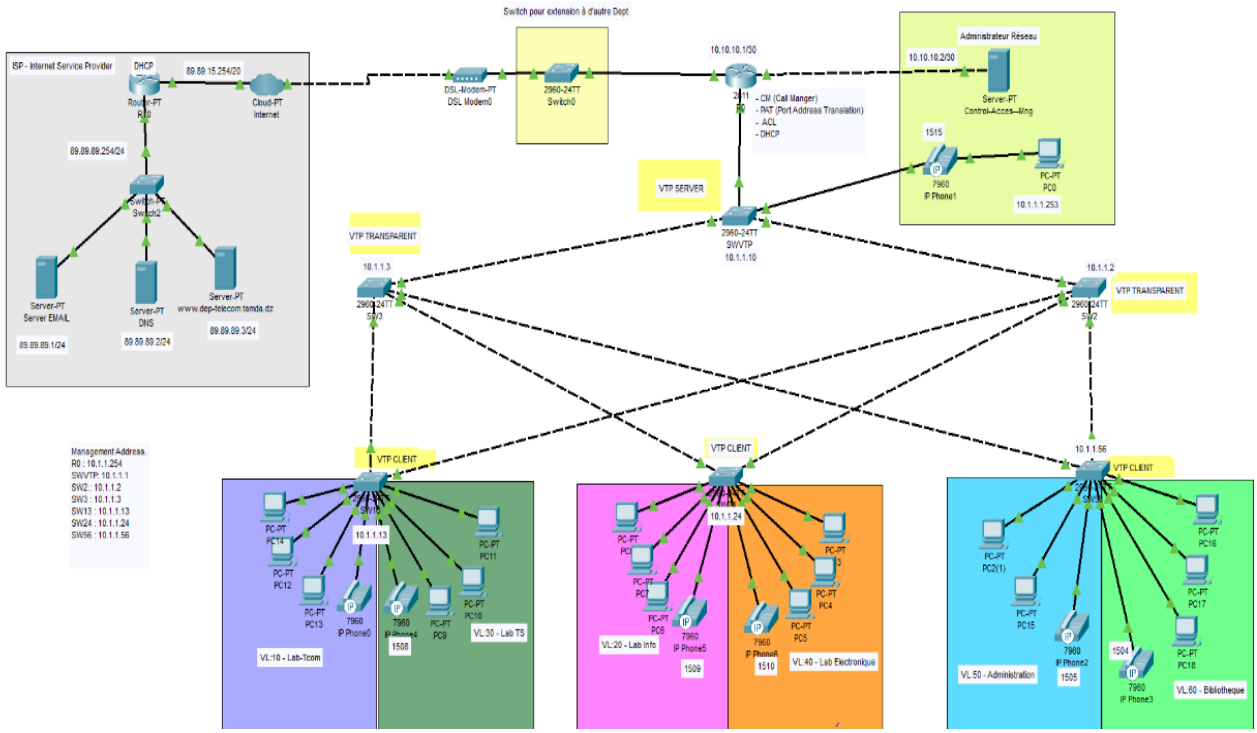


FIGURE III.2 – architecture réseau du département de télécommunication-TAMDA

III.3.1 Le principe de l'architecture

La configuration du département de télécommunication est illustrée par sa topologie, comprenant une bibliothèque, une administration, et quatre laboratoires au rez-de-

chaussée : télécommunications, informatique, traitement du signal, et électronique.
La topologie démarre avec un routeur central qui connecte les trois composantes essentielles de cette structure via trois ports.

• Le routeur et relier avec l'interface Fa1/0 est configurer avec l'adresse 10.10.10.1/30 au serveur spécifique de AAA qui contrôle l'authentification des utilisateurs.

• Le routeur est connecté au switch via l'interface Fa0/0 configurée avec l'adresse 89.89.89.254/24. Le switch est relié à un fournisseur d'accès internet, situé chez Algérie Télécom, et est composé de trois serveurs, chacun représentant un protocole : DNS, HTTP, et Email. Ce routeur est également connecté via l'interface Fa1/0, configurée avec l'adresse 89.89.15.254/20 (cette adresse est attribuée par le protocole DHCP), à un nuage(cloud) internet, qui est à son tour connecté au modem DSL.

• Le routeur est relié à un switch serveur avec l'interface Fa0/1 par l'adresse réseau 192.168.0.0/16 configurer via le protocole DHCP et un routage inter-vlan qui va diviser l'adresse réseau en plusieurs adresse.
* Ce switch serveur distribuera les VLANs aux deux switches transparents qui, à leur tour, achemineront ces VLANs vers les switches clients. Chaque switch client comportera deux VLANs.
* Une interface Fa0/1 de switch serveur est sortie vers un téléphone puis vers un pc de l'administrateur sa configuration est faite dans le routeur avec le vlan management par l'adresse 10.1.1.254, est utilisé pour administrer le trafic entre les commutateurs et les ordinateurs ainsi que pour améliorer la sécurité et les performances du réseau, et chaque switch est également configuré avec un vlan management sont les suivant :
Switch serveur : l'adresse de vlan management 10.1.1.1
Switch SW2 : l'adresse de vlan management 10.1.1.2
Switch SW3 : l'adresse de vlan management 10.1.1.3
Switch SW13 : l'adresse de vlan management 10.1.1.13
Switch SW24 : l'adresse de vlan management 10.1.1.24
Switch SW56 : l'adresse de vlan management 10.1.1.56

III.3.2 les composantes nécessaires

Switch :
- 6 Switch étaient mis en œuvre.
- Marque : Cisco.
- Image : Cisco IOS c2960-lanbasek9-mz.122-46.SE.bin.

- 24 interfaces de Fast Ethernet.
- 2 gigabits Ethernets.

Routeur :

- 1 routeur mis en service qui représente la base de la topologie.
- Marque : Cisco.
- Image : c 1811-advipservicesk9-mz. 124-24.T1.bin.
- 2 interfaces de Fast Ethernet.
- 1 serial interface.
- Pour ajouter des ports on intègre des cartes externes par exemple :
  - HWIC-2T : intégrer deux ports sériels.
  - NM-1 E : intégrer un seul port Ethernet.
  - NM-1FE-FX : intégrer un seul port de Faste Ethernet.

Un serveur RADIUS :

- Une base de données d'authentification pour stocker les noms des utilisateurs.
- Clients radius.
- Protocole UDP.

III.4 La configuration de la partie réseau

III.4.1 présentation des VLANs

Un VLAN est en effet une méthode de segmentation d'un réseau local physique en plusieurs réseaux logiques, Chaque VLAN peut avoir un identifiant unique (ID), un nom, une adresse IP et des sous-interfaces, comme indiqué dans le tableau ci-dessous :

Nom de Switch	Nom de vlan	ID	L'adresse réseau	Sous-interface
SW56 /SW13	IP-Voice	11	172.16.255.0/24	Fa0/0.11
SW13	Lab-Tcom	10	192.168.10.0/24	Fa0/0.10
SW13	Lab-Ts	30	192.168.30.0/24	Fa0/0.30
SW24	Lab-Info	20	192.168.20.0/24	Fa0/0.20
SW24	Lab-Electronique	40	192.168.40.0/24	Fa0/0.40
SW56	Administration	50	192.168.50.0/24	Fa0/0.50
SW56	Bibliothèque	60	192.168.60.0/24	Fa0/0.60

TABLE III.1 – nomination des VLANs et affectation d'adresse IP et sous-interface

Voix IP : Dans le but d'optimiser notre architecture réseau et de garantir l'accessibilité à tous les services, nous envisageons d'intégrer la téléphonie IP à notre infrastructure afin de simplifier les opérations.

1- Nous allons générer des numéros de téléphone et assigner des boutons DN aux téléphones (ephones) dans le routeur, comme illustré dans le schéma ci-dessous. De plus, nous aurons la possibilité de configurer d'autres paramètres tels que le nom du téléphone et les paramètres de sonnerie.

```
telephony-service
max-ephones 40
max-dn 40
ip source-address 172.16.255.254 port 2000
auto assign 1 to 40

ephone-dn 1
number 1501

ephone-dn 2
number 1502
```

FIGURE III.3 – la configuration de la téléphonie IP (VoIP) sur R0

```
ephone 1
 device-security-mode none
 mac-address 0010.11E2.6953
 type 7960
 button 1:1
```

FIGURE III.4 – la configuration de la téléphonie IP (VoIP) sur R0

2-configuré le vlan voice sur les switch :

```
SWVTP(config)#interface fa0/1
SWVTP(config-if)#switchport mode access
SWVTP(config-if)#switch port voice vlan 11
SWVTP(config-if)#exit
```

FIGURE III.5 – Configuration de l'interface vlan voice

3- Nous effectuerions un appel téléphonique de l'administration vers le téléphone de la bibliothèque afin de tester la connectivité du téléphone IP.

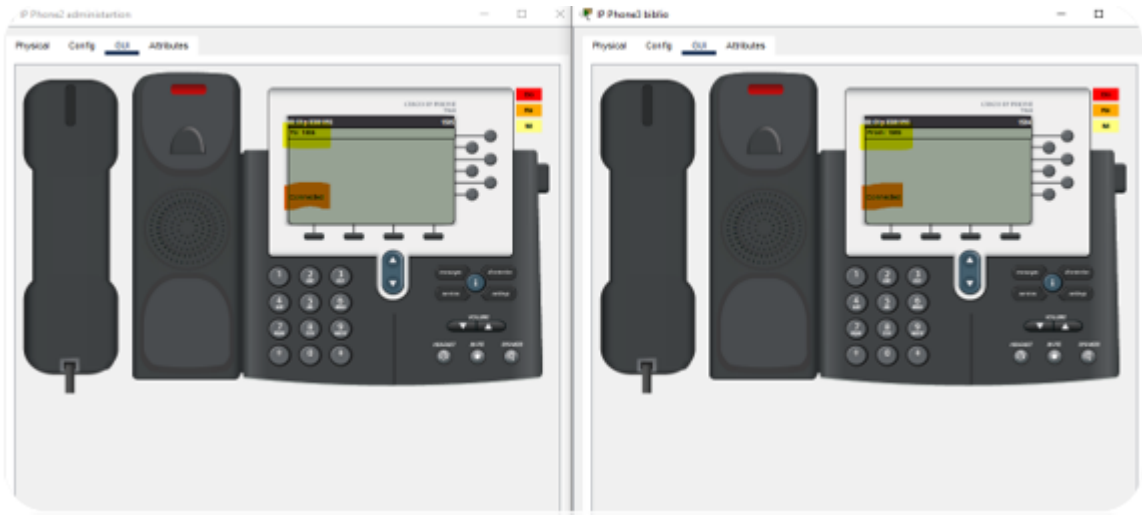


FIGURE III.6 – test d'appel entre la bibliothèque et l'administration

III.4.2 Configuration des Switches

Ci-dessous est exposée la configuration initiale pour créer des VLAN à l'aide du protocole VTP, qui facilite la distribution des opérations de création, suppression ou modification de VLAN sur l'ensemble des commutateurs de notre réseau à partir d'un seul commutateur.

III.4.2.1 Vtp serveur

Nous débuterons en définissant le Switch (SWVTP) central en tant que serveur VTP, Où il permet à l'administrateur d'effectuer des modifications sur les VLANs et de les propager automatiquement à tous les commutateurs du réseau.

```
SWVTP(config)#vtp mode server
Device mode already VTP SERVER.
SWVTP(config)#vtp ?
  domain    Set the name of the VTP administrative domain.
  mode      Configure VTP device mode
  password  Set the password for the VTP administrative domain
  version   Set the adminstrative domain to VTP version
SWVTP(config)#vtp dom
SWVTP(config)#vtp domain ?
  WORD  The ascii name for the VTP administrative domain.
SWVTP(config)#vtp domain switching
Changing VTP domain name from NULL to switching
SWVTP(config)#vtp ?
  domain    Set the name of the VTP administrative domain.
  mode      Configure VTP device mode
  password  Set the password for the VTP administrative domain
  version   Set the adminstrative domain to VTP version
SWVTP(config)#vtp ver
SWVTP(config)#vtp version ?
  <1-2>  Set the adminstrative domain VTP version number
SWVTP(config)#vtp version 2
```

FIGURE III.7 – configuration du VTP serveur

```
Switch#show vtp ?
  counters  VTP statistics
  password  VTP password
  status    VTP domain status
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 21
Maximum VLANs supported locally : 255
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : switching
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xEF 0x86 0x66 0x7D 0xCC 0x1F 0x48 0x77
Configuration last modified by 10.1.1.10 at 3-1-93 00:41:42
Local updater ID is 10.1.1.10 on interface Vl1 (lowest numbered VLAN interface found)
Switch#
```

FIGURE III.8 – Information sur VTP serveur

-Nous allons créer et configurer les vlan sur le VTP serveur :

```
SWVTP(config)# vlan 10
SWVTP(config-vlan)# name lab-TS
SWVTP(config-vlan)# exit
SWVTP(config)# interface vlan 10
SWVTP(config-if)# ip address 192.168.10.0 255.255.255.0
switch(config-if)# end
```

FIGURE III.9 – configuration des vlan sur vtp serveur

III.4.2.2 VTP client

Il traite les informations reçues et les transmets aux autres commutateurs. On l'a activée sur SW3, SW24, SW56, voici sa configuration :

```
vtp domain switching
vtp mode client
vtp version 2
!
```

FIGURE III.10 – configuration du VTP client

III.4.2.3 Vtp transparent

Agissant comme une passerelle, son rôle est de transmettre les VLAN aux commutateurs clients auxquels il correspond. Nous l'avons activée sur SW3, SW2, voici sa configuration :

```
!
vtp domain switching
vtp mode transparent
vtp version 2
!
```

FIGURE III.11 – configuration du VTP transparent

III.4.3 Activation des liaisons Trunk et Access

III.4.3.1 liaison Trunk

C'est un lien de communication entre deux commutateurs pour transporter le trafic de plusieurs VLANs sur une seule liaison. Il permet de marquer l'en tête du paquet de chaque VLAN avec un identifiant spécifique avant de l'envoyer vers un autre périphérique[2].

```
SWVTP(config)#interface fastEthernet 0/24
SWVTP(config-if)#swi
SWVTP(config-if)#switchport mo
SWVTP(config-if)#switchport mode trun
SWVTP(config-if)#switchport mode trunk

SWVTP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/24, changed state to up

SWVTP(config-if)#
SWVTP(config-if)#
```

FIGURE III.12 – activation de la liaison trunk

III.4.3.2 liaison Access

Elle relie des périphériques terminaux comme des ordinateurs, des imprimantes et des téléphones IP à un commutateur réseau, pour transporte le trafic d'un seul VLAN.

```
SWVTP(config)#interface fastEthernet 0/1
SWVTP(config-if)#des
SWVTP(config-if)#description LAN-MANAGER
SWVTP(config-if)#swi
SWVTP(config-if)#switchport mode a
SWVTP(config-if)#switchport mode access
SWVTP(config-if)#
```

FIGURE III.13 – activation de la liaison Access

III.4.4 configuration de routeur

III.4.4.1 DHCP

Dans notre configuration, le protocole DHCP a été mis en place sur le routeur afin de distribuer des adresses IP aux ordinateurs des clients.

```
R0(config)#ip dhcp pool LAN1
R0(dhcp-config)#netw
R0(dhcp-config)#network 192.168.10.0 255.255.255.0
R0(dhcp-config)#defaul
R0(dhcp-config)#default-router 192.168.10.254
R0(dhcp-config)#dns
R0(dhcp-config)#dns-server 89.89.89.2
R0(dhcp-config)#exit
R0(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
R0(config)#ip dhcp excluded-address 192.168.10.254
R0(config)#
```

FIGURE III.14 – la configuration du DHCP

- Activons cette commande pour permettre de définir une plage d'adresse qui contienne

des adresses IP disponible pour être distribuer aux clients.

```
R0(configue)#ip dhcp pool LAN1
```

- Nous avons impliqué cette commande pour éliminer des adresses IP, Dans ce cas, neuf adresses ont été retirées.

```
R0(configue)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
```

```
ip dhcp pool LAB-TCOM-V10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.254
 dns-server 89.89.89.2
ip dhcp pool LAB-INFO-V20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.254
 dns-server 89.89.89.2
ip dhcp pool IP-Voice
 network 172.16.0.0 255.255.0.0
 default-router 172.16.255.254
 option 150 ip 172.16.255.254
ip dhcp pool LAB-TS
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.254
 option 150 ip 172.16.255.254
 dns-server 89.89.89.2
ip dhcp pool LAB-ELECTRONIQUE
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.254
 dns-server 89.89.89.2
ip dhcp pool ADMINISTRATION
 network 192.168.50.0 255.255.255.0
 default-router 192.168.50.254
 option 150 ip 172.16.255.254
 dns-server 89.89.89.2
ip dhcp pool BIBLIO
 network 192.168.60.0 255.255.255.0
 default-router 192.168.60.254
 option 150 ip 172.16.255.254
 dns-server 89.89.89.2
```

FIGURE III.15 – création des pools d'adresses

III.4.4.2 Routage inter-vlan

Il est créé pour permettre la communication entre les différents VLAN configurés sur divers appareils réseau centralisés par un routeur.

```
R0(config)#interface fa0/1
R0(config-if)#no shu
R0(config-if)#no shutdown

R0(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

R0(config-if)#int
R0(config-if)#interface fa0/1.10
R0(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/1.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.10, changed state to up

R0(config-subif)#enca
R0(config-subif)#encapsulation dot
R0(config-subif)#encapsulation dot1Q 10
R0(config-subif)#ip ad
R0(config-subif)#ip address 192.168.10.254 255.255.255.0
R0(config-subif)#
```

FIGURE III.16 – activation du routage inter vlan

- Cette commande est activée pour entrer en sous interface.

R0(configue-if)#interface fa0/1.10

- Grâce à cette commande, nous avons pu mettre en place configurer le routage de plusieurs VLANs via un seul lien physique, où chaque VLAN possède une sous-interface et une adresse IP distincte.

- Les trames Ethernet seront marquées avec des étiquettes VLAN (tag) contenant des informations sur le VLAN auquel la trame appartient.

R0(configue-subif)#encapsulation dot1Q 10

III.4.4.3 PAT

Une configuration est mis en oeuvre sur le routeur pour que plusieurs utilisateurs puissent accéder à internet avec une seule adresse publique.

```
R0(config)#interface Fa0/1
R0(config-if)#ip nat inside
R0(config-if)#interface Fa0/0
R0(config-if)#ip nat outside
R0(config-if)#exite
R0(config)#access-list 1 permet 192.168.0.0 0.0.255.255
R0(config)#ip nat inside source list 1 interface Fa0/0 overload
```

FIGURE III.17 – la configuration du PAT

- Ces deux commandes sont activées pour définir l'interface Fa0/1 comme l'interface associée à l'adresse privée, c'est-à-dire l'interface connectée au réseau interne.

```
R0(configue)#interface fastEthernet fa0/1
R0(configue-if)#ip nat inside
```

- La configuration de ces deux commandes indique que l'interface fa0/0 est connectée à l'extérieur vers internet. Elle spécifie que tout paquet sortant par cette interface doit être traduit, cela implique que son adresse IP privée sera modifiée en une adresse IP publique avant d'être transmis à l'extérieur.

```
R0(configue-if)#interface fa0/0
R0(configue-if)#ip nat outsie
```

- Nous avons implémenté cette commande afin de créer une liste permettant au trafic provenant de cette plage d'adresses de passer à travers le routeur, identifiée par le numéro 1.

```
R0(configue)#access-list 1 permet 192.168.0.0 0.0.255.255
```

- Cette commande est activée pour les adresses IP internes. Précisant qu'elle adresse doit être traduite pour accéder à Internet via l'interface fa 0/0. L'option "Overload" permet de regrouper plusieurs adresses privées en une seule adresse publique.

```
R0(configue)#ip nat inside source liste 1 interface fastEthernet 0/0 overload
```

III.4.5 Les tests

III.4.5.1 DHCP

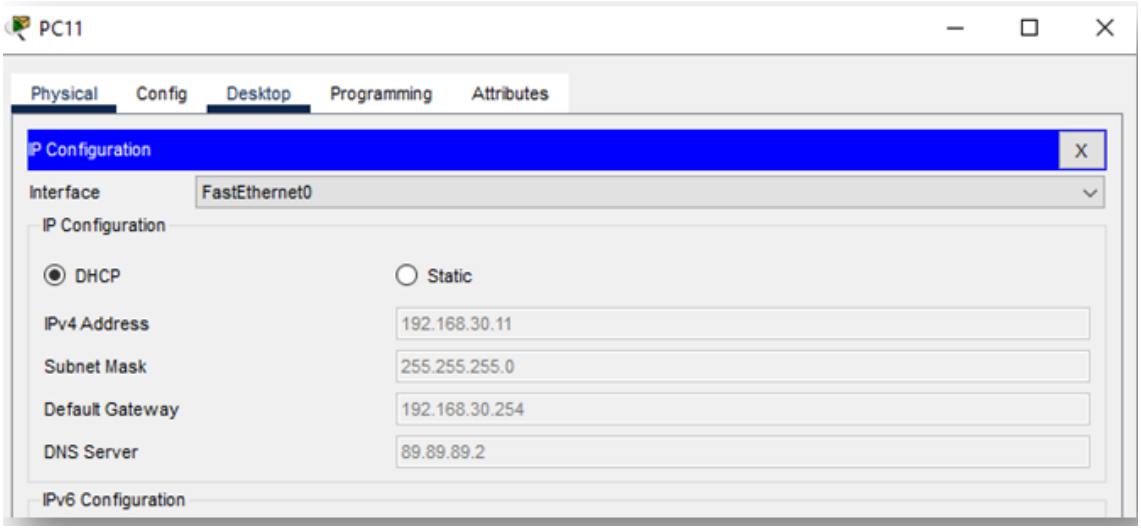


FIGURE III.18 – illustre le résultat de DHCP

III.4.5.2 Routage inter vlan

Nous testons la connectivité entre deux emplacements en utilisant la commande ping.

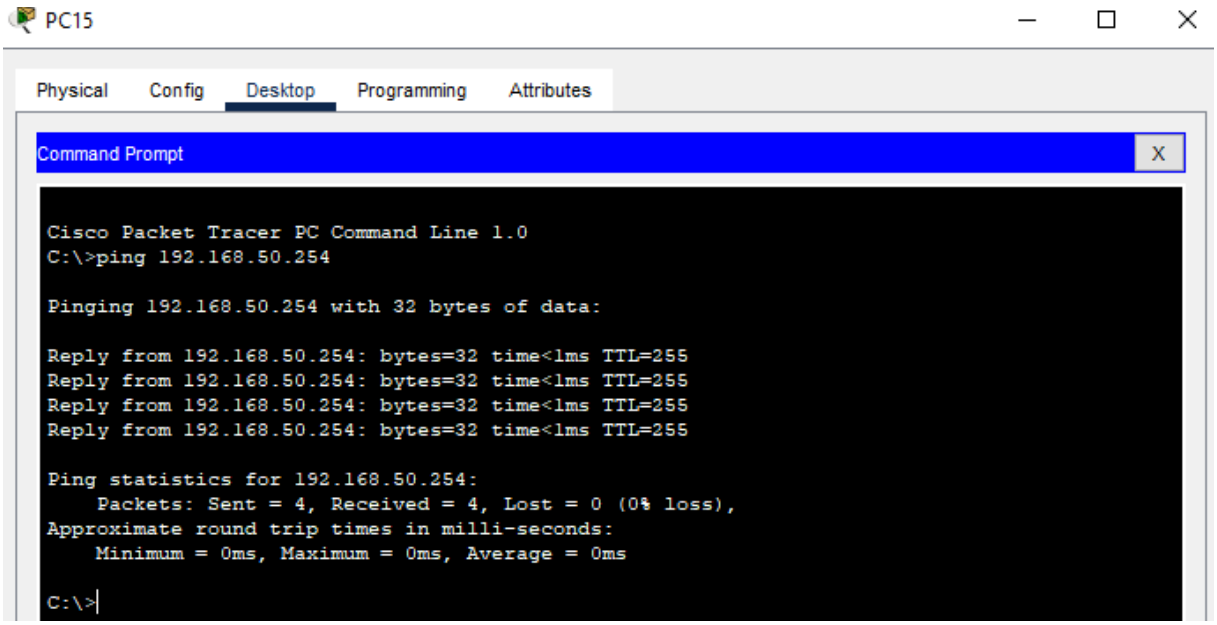


FIGURE III.19 – illustre le ping entre pc administration et le routeur

Ensuite un ping entre un pc d'un client et le routeur.

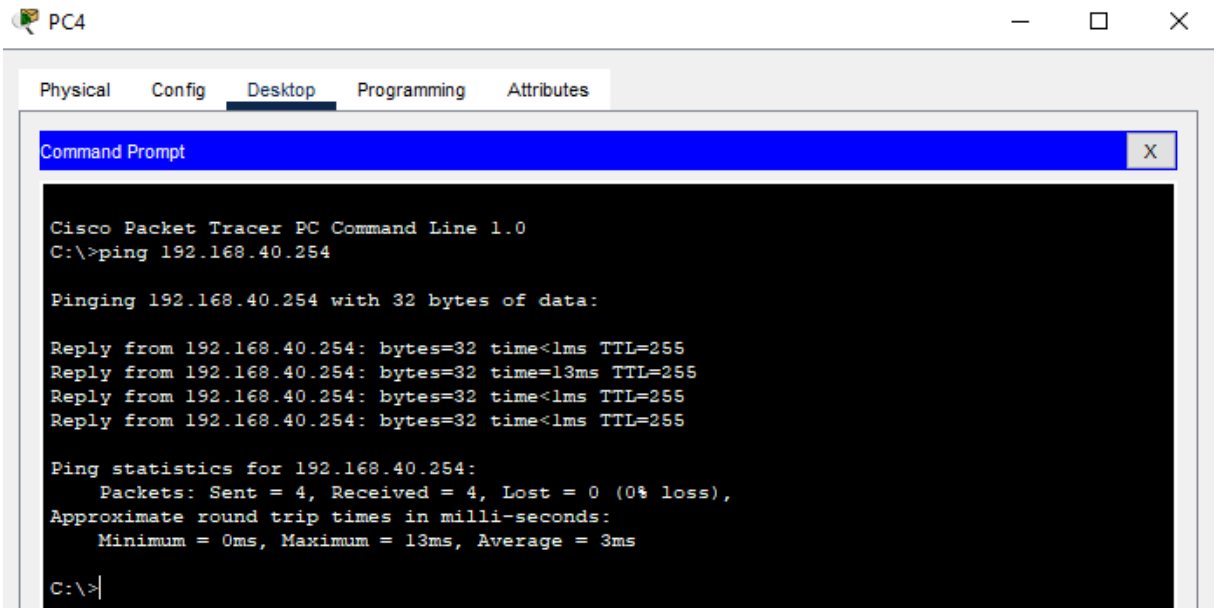


FIGURE III.20 – illustre le ping entre pc client et le routeur

III.4.5.3 PAT

Pour vérifier le bon fonctionnement du PAT, on utilise la commande ping à partir du routeur situé chez le fournisseur d'accès Internet. On envoie des paquets vers un PC client qui possède une adresse IP privée. Cela nous permet de confirmer que la translation d'adresse se fait correctement et que le PC client reçoit les paquets de manière appropriée.

```
R0#ping 89.89.15.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 89.89.15.254, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 59/66/82 ms

R0#
```

FIGURE III.21 – Démonstration du fonctionnement du PAT

III.5 Mettre en œuvre le protocole AAA dans un serveur RADIUS

III.5.1 configuration du protocole AAA dans les périphériques

-Activez le modèle AAA en saisissant la commande suivante : **"aaa new model"**.

```
R0(config)#aaa new-model
```

-Configure l'authentification par défaut pour les connexions de terminal en utilisant d'abord le serveur RADIUS, puis la base de données locale du routeur avec la commande suivante :**" aaaauthentication login default group radius local"**.

```
R0(config)#aaa authentication login default group radius local
```

-Activez le serveur RADIUS en spécifiant son adresse IP, le numéro de port et en fournissant une clé partagée :

```
R0(config-radius-server)#address ipv4 10.10.10.2 auth-port 4000
R0(config-radius-server)#key azerty
```

-Accéder à la configuration des lignes de terminal virtuel (VTY) qui limiter le nombre de sessions simultanées autorisées, Cela permet de contrôler qui peut se connecter au périphérique :

```
R0(config-radius-server)#line vty 0 4
R0(config-line)#
```

-Indiquer la méthode d'authentification par défaut pour vérifier les informations d'identification de l'utilisateur :

```
R0(config-line)# login authentication default
R0(config-line)#end
```

III.5.2 configurations du serveur RADIUS :

III.5.2.1 Attribution d'une adresse IP statique au serveur :

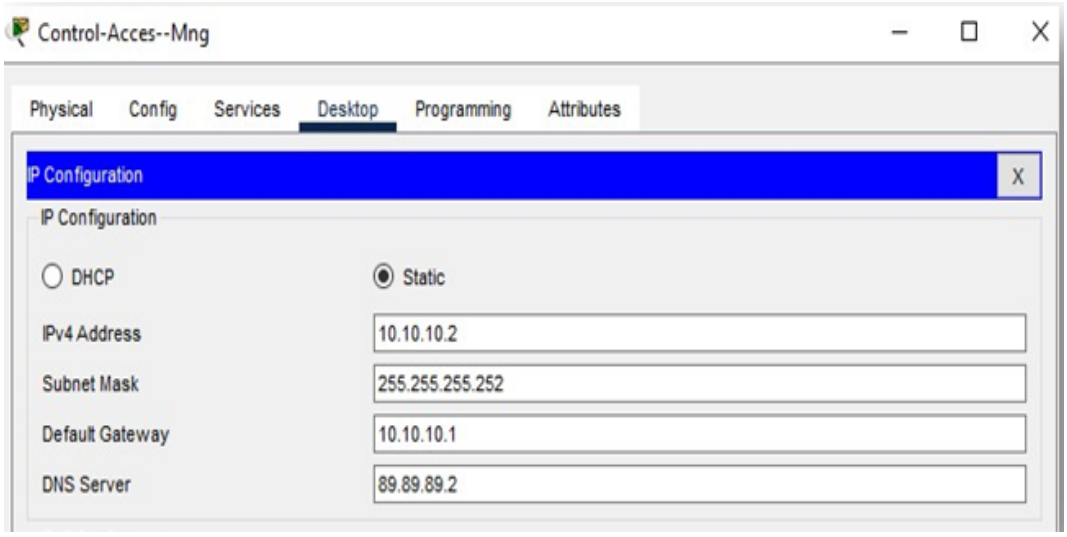


FIGURE III.22 – Attribution d'une adresse statique au serveur

III.5.2.2 création des clients radius dans le serveur

Nous allons ajouter les noms des périphériques ainsi que leurs adresses IP :

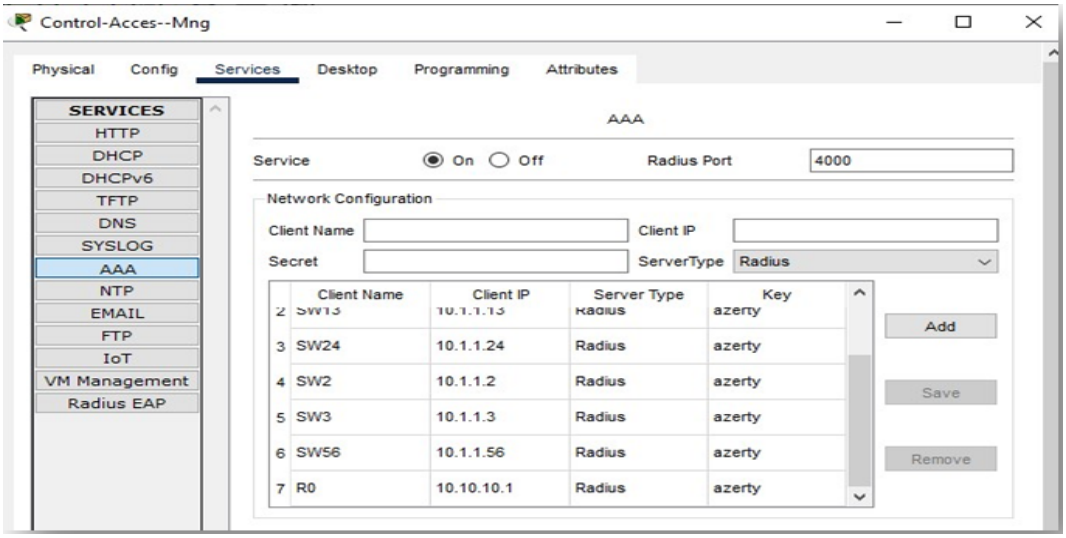


FIGURE III.23 – création des clients RADUIS

III.5.2.3 création des administrateurs dans le serveur :

Nous allons ajouter les admins et leurs mots de passe :

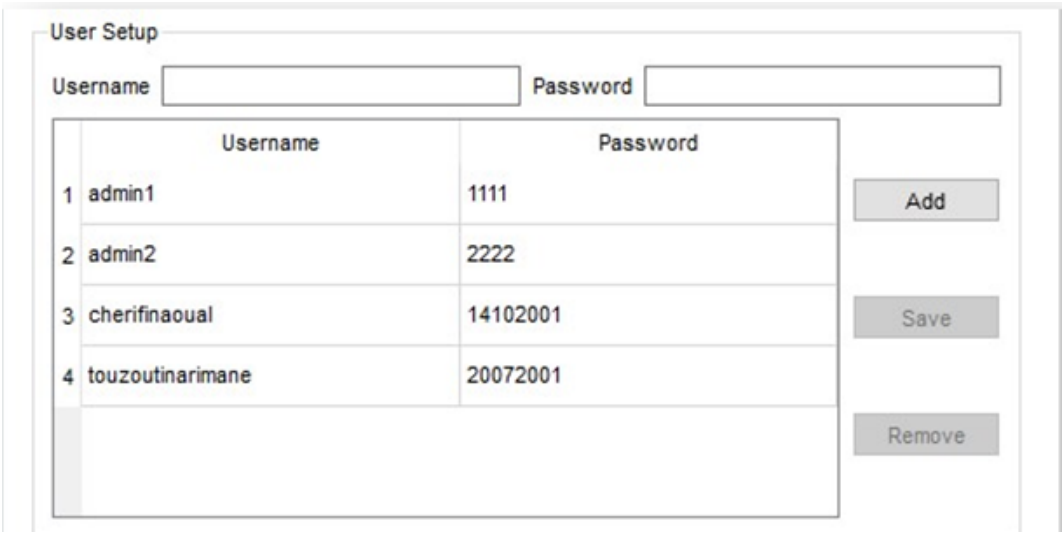


FIGURE III.24 – création des administrateurs réseau et leurs mots de passe

III.5.3 Les testes d'authentification

III.5.3.1 Vérification d'accès des admins

On test l'accès des utilisateurs dans les périphériques réseau :

FIGURE III.25 – vérification de l'accès pour les utilisateurs

Si un utilisateur n'appartient pas dans le groupe des admins créés dans le serveur RADUIS alors :

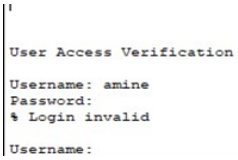


FIGURE III.26 – Utilisateur n'appartenant pas au serveur RADUIS

III.5.3.2 vérifier l'authentification à distance

Nous avons effectué des tests en faisant appel à :

Telnet : c'est un protocole qui permet d'ouvrir et administrer une session sur une machine distante.

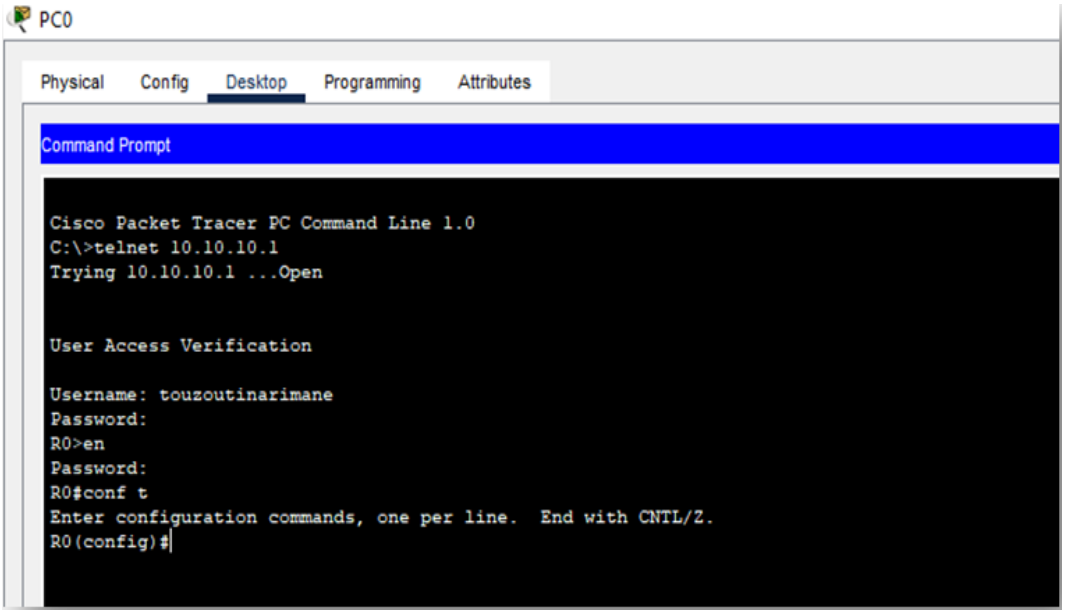


FIGURE III.27 – Accéder au routeur via telnet

SSH : est utilisé pour établir un accès sécurisé à distance, contrairement au Telnet qui transmit en clair les mots de passes des utilisateurs, le SSH utilise des algorithmes de chiffrement tel que RSA[3].

-d'abord on doit configurer le protocole SSH dans les périphériques :

```
R0(config)#ip domain-name mondomaine.com
R0(config)#cryp
R0(config)#crypto key gen
R0(config)#crypto key generate rs
R0(config)#crypto key generate rsa
The name for the keys will be: R0.mondomaine.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]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R0(config)#ip ssh ve
*Mar 1 0:16:46.296: %SSH-5-ENABLED: SSH 1.99 has been enabled
R0(config)#ip ssh version 2
R0(config)#linevt
R0(config)#line vty 0 15
R0(config-line)#trans
R0(config-line)#transport inp
R0(config-line)#transport input ssh
R0(config-line)#wr
```

FIGURE III.28 – configuration du SSH

-accéder à distance avec SSH :

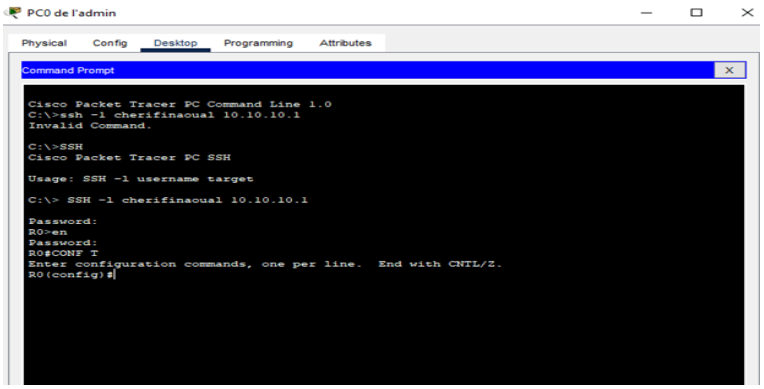


FIGURE III.29 – Accéder au routeur via SSH

III.6 ACL

Pour restreindre l'accès à Internet pour les VLANs de laboratoire, les ACL sont configurées comme décrit ci-dessous :

```
R0#show access-lists
Standard IP access list 1
    10 permit 192.168.0.0 0.0.255.255
Standard IP access list 10
    10 permit 192.168.10.0 0.0.0.255
    20 deny any
Standard IP access list 30
    10 permit 192.168.30.0 0.0.0.255
    20 deny any
Standard IP access list 20
    10 permit 192.168.20.0 0.0.0.255
    20 deny any
Standard IP access list 40
    10 permit 192.168.40.0 0.0.0.255
    20 deny any
Standard IP access list 70
    10 permit host 10.1.1.253
```

FIGURE III.30 – configuration des ACL

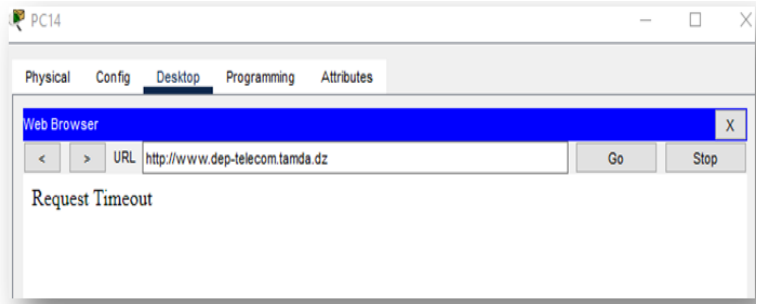


FIGURE III.31 – page web bloqué par les ACL

III.7 Le STP

C'est un protocole utilisé pour empêcher la formation de boucle dans le réseau, et cela en combinant plusieurs liens physiques en un seul lien logique afin d'augmenter la bande passante et d'améliorer la redondance du réseau, cela s'appelle « la technologie d'agrégation de liens » qui assure une meilleure gestion du trafic[4].

Nous avons rencontré un échec où une requête "not found" a été reçue lors du téléchargement de la page web et l'envoie des emails, pour cela on a activé le protocole STP dans tous les machines .

```
spanning-tree mode pvst
```

FIGURE III.32 – activer le protocole STP

Après activation du protocole STP, voici le résultat obtenu :

FIGURE III.33 – test page web

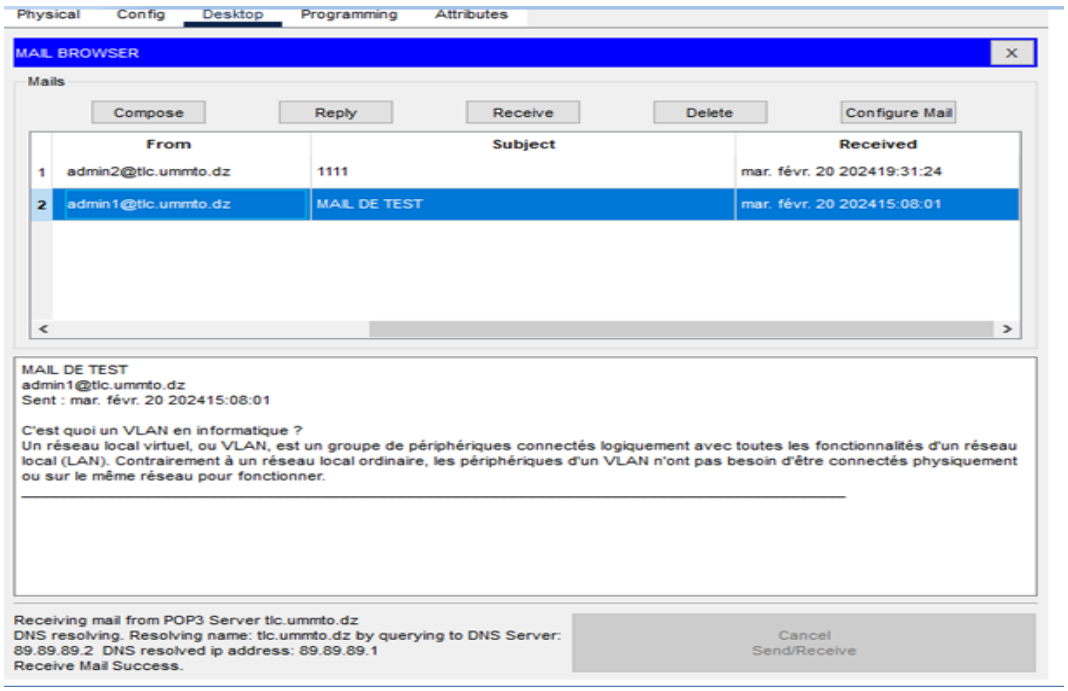


FIGURE III.34 – test email

III.8 conclusion

Ce chapitre met en pratique les idées explorées précédemment, nous permettant ainsi d'atteindre l'objectif initial de notre projet. Nous avons réalisé une topologie sur le simulateur Packet Tracer dédié au département réseaux et télécommunications, et nous avons mis en place un mécanisme d'authentification des utilisateurs à distance à l'aide d'un serveur RADIUS c'est une solution offre une gestion robuste et flexible de l'authentification, de l'autorisation et de la comptabilisation des utilisateurs sur le réseau, renforçant ainsi la sécurité et la gestion des accès au sien des VLANs. À la fin de notre projet, nous avons effectué des tests, y compris la validation de la page HTML et l'envoi d'e-mails.

Bibliographie

[1] CISCO, “support de cours : Networking Academy Becoming A Cisco Networking Academy Frequently Asked Questions,” 2021.

[2] R. Kalavathi, A. Y. Reddy, and amp; C. Swathi, “A COMPREHENSIVE ANALYSIS OF VIRTUAL LOCAL AREA NETWORK (VLAN) AND INTER-VLAN ROUTING STRATEGIES,”2017.

[3] Ibrahim HAJJEH, Mohamad BADRA, support cours :“Le protocole SSH,” .

[4] huawei, support cours(Textbooks) :"DATA COMMUNICATIONS AND NETWORK,” Hangzhou, China, 2023.

Conclusion Générale

Quand on pense sur la sécurité informatique on trouve que les ingénieures en réseaux informatiques sont entraine d'essayer d'innover un protocole ou de créés un autre plus efficace, pour mettre en contrôle leurs architecteurs et leurs travails, pour les protégés contre les menaces quel que soit une tentative d'interception ou bien de modification provenant de diverses sources comme des pirates informatique des cybercriminels. . .etc.

Dans notre étude, nous nous concentrons sur l'authentification de notre topologie développée pour le département de Tamda. Nous avons exposé les différentes étapes de mise en œuvre des protocoles, chacun configuré pour accomplir les tâches d'un autre.

Plusieurs protocoles ont été mis en place dans cette topologie afin de garantir la réussite de l'authentification dans les VLANs. Pour accomplir cela, une solution a été développée, qui consiste en une suite de protocoles qui analysent chaque problème pour le détecter.

L'intégration des VLANs, y compris la gestion des VLANs, a permis de rétablir l'accès entre les laboratoires, l'administration et la bibliothèque. Ensuite, nous avons configuré un protocole NAT pour permettre la connexion à tous les secteurs. Toutefois, l'emploi du VLAN management et du protocole NAT a engendré un souci car les VLAN se connectaient librement entre eux. Afin de résoudre ce problème, nous avons choisi le protocole ACL, qui permet de définir des limites entre les VLANs. Notre architecte met en place un protocole STP afin d'éviter les boucles.

En revenant à notre but, le processus d'authentification AAA est composé de deux parties : une première partie locale, puis une seconde partie avec un serveur RADIUS. Ce dernier permet à l'utilisateur d'accéder après confirmation et définit également les tâches à accomplir pour chaque client une fois que le protocole est réussi, garantissant ainsi un accès distant réel.