REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA BOUMERDES

FACULTE DE TECHNOLOGIE

Département : Ingénierie des systèmes électriques

Filière : Télécommunications

Mémoire de projet de fin d'études pour l'obtention du

Diplôme de Master

Spécialité : Réseaux et Télécommunications

Thème

Organisation d'un réseau local et sécurisation au niveau de l'accès

---

Etudié et réalisé par :

Oualah Mohamed bachir

Encadreur/Co-Encadrant :

Mme GUERBAI Y.

Mr Tarek Benarabi

Soutenu, le 03/07/2023, devant le jury composé de :

MESSAOUDI	Noureddine	MCA	UMBB	Président
BELKACEM	SAMIA	MCA	UMBB	Examinateur
GUERBAI	Yasmine	MCA	UMBB	Encadrant

Année universitaire : 2022/2023

Remerciement

Je remercie ALLAH le tout puissant de m'avoir donné La santé et la volonté d'entamer et de terminer ce mémoire Et bien sûr mon soutien moral et source de joie et De bonheur, celui qui s'est toujours sacrifié pour me voir Réussir, que ALLAH te garde et te protège Mon père Et la lumière de mes jours, la source de mes efforts, ma vie et mon bonheur ma mère

Tout d'abord, je souhaite remercier chaleureusement Madame Guerbai, mon encadratrice à l'Université de UMBB, Faculté de Technologie. Sa patience, son expertise et ses conseils avisés ont été d'une grande aide tout au long de mon parcours académique. Je lui suis reconnaissante pour son soutien et son dévouement.

Je tiens également à exprimer ma reconnaissance envers l'ingénieur Tarek Benarabi de Sonatrach Aïn Salah, mon encadrant de stage. Je lui suis reconnaissant pour son accompagnement tout au long du stage.

Je souhaite également remercier l'ingénieur Abdel Rahime pour son assistance et son soutien précieux. Sa contribution a été très appréciée et a eu un impact positif sur mon travail.

Mes amis proches, Belkebir Mohamed Ahmed Amine, benhenia Redah, Mohammou Mehamed Khalile et issiakhem Amel i ont été une source de soutien et d'encouragement tout au long de ce parcours. Leur amitié sincère a été précieuse pour moi, et je les remercie de tout cœur pour leur présence et leur soutien.

Je tiens à exprimer ma reconnaissance envers toute l'équipe du service Data Center chez Sonatrach-BP et l'ensemble de l'équipe de la société "Sonatrac Aïn Salah Gaz". Leur collaboration et leur expertise ont contribué à la réussite de mon mémoire, et je les remercie pour leur précieuse contribution.

Dédicaces

A Dieu le tout puissante, source de toute connaissance, qui m'a donné
La force et la volonté pour achever ce modeste travail.

A ma mère celle qui m'a donnée la vie, le symbole de tendresse et qui S'est sacrifiée pour mon bonheur et ma réussite.

A mon père, école de mon enfance, celui qui a été mon ombre durant Toutes mes années d'études, et qui a veillé tout au long de ma vie à M'encourager et à me donner l'aide.

Que Dieu les Garde et les Protège.

Table des matières

Liste des figures

Liste des tableaux

Liste d'abréviation

MDA: pour Mail Delivery Agent

ACL : Access Control List

FTP : File Transfer Protocol

SMB : Server Message Block

NFS: Network File System

NCP : Netware Core Protocol

BPDU : Bridge Protocol Data Units

DHCP : Dyanmic Host Control Protocol

DMZ : Dé-Militarized Zone

DNS : Domain Name System

ESP : Encapsulating Security Payload

FTP : File Transfer Protocol ixListe des abréviations

FW : FireWall

HMAC : keyed-Hash Message Authentication Code

Http : HyperText Transfer Protocol

HTTPS : HyperText Transfer Protocol Secure sockets

IDEA : International Data Encryption Algorithm

IIS : Internet Information Services

IKE : Internet Key Echange

IP : Internet Protocole

IPSec : Internet Protocole Sécurité

IPv4 : Internet Protocole Version 4

ISO : International Standardization Organization

L2TP : Layer 2 Tunneling Protocol

LAN : Local Area Network

LAC Layer 2 : Tunneling Protocol Access Concentrator

LNS Layer 2 : Tunneling Protocol Network Server

MAC : Medium Access Control

MAN : Métropolitain Area Network

MD5 : Message Digest 5

NAT : Network Address Translation

OSI Open : Systems Interconnection

PC : Personnel Computer

PPTP : Point to Point Tunneling Protocol xListe des abréviations

PPTPAC : Point to Point Tunneling Protocol Access Concentrator

PPTPNS : Point to Point Tunneling Protocol Network Server

RC5 : Ron's Code ou Rivest's Cipher

RJ45 : Registered Jack 45

SADB : Sécurity Association Data Base

SARL : Société A Responsabilité Limité

SHA-1 : Secure Hash Algorithm-1

SMTP : Simple Mail Transfer Protocol

SPA : Société Par Actions

SPI : Serial Peripheral Interface

SSH : SHell SSL Secure Socket Layer

STP :Shielde Twisted Paire

TCP : Transmission Control Protocol

TLS : Transport Layer Security

UDP : User Datagram Protocol

USB : Universal Serial Bus

PVST + : Per VLAN Spanning Tree Plus

UTP : Unshielded Twisted Pair

VLAN : Virtual Local Area Network

VPN : Virtual Private Network

VTP : Vlan Truking Protocol WAN Wide Area Network

Résume

ملخص :

تتناول هذا الأطروحة تنظيم وتأمين الشبكات المحلية. من خلال التركيز على

، التحكم في العاصفة، أمان المنافذ، تنظيم الشبكACL ، قوائمDHCP ، تطفلARP تغليف

تهدف المذكرة إلى تعزيز حماية الشبكات من التهديدات المتزايدة كما تغطي جوانب نظرية وعملية لتحليل الهجمات وممارسات الأمان باستخدام برامج مثل

Packet Tracerو Kali Linux

الهدف هو توفير أساس قوي لتطوير استراتيجيات أمان فعالة لمحاكاة الهجمات وتكوين آليات الأمان للشبكات المحلية

Résume :

Ce mémoire examine l'organisation et la sécurisation des réseaux locaux en environnement d'accès en neveux de port. En mettant l'accent sur des mesures telles que dynamique ARP inscription le DHCP Shopping, les ACL, le Storm Control, la sécurité des ports et l'organisation du réseau, il vise à renforcer la protection des réseaux contre les menaces croissantes. L'étude des attaques et des pratiques de sécurisation se fait à la fois sur le plan théorique et pratique. Des outils Kali Linux pour appliquer quelques attaques et Packet Tracer pour simuler notre réseau et notre sécurité. L'objectif est de fournir une base solide pour l'élaboration de stratégies de sécurité efficaces dans les réseaux locaux en neveux de port.

Resume:

This thesis examines the organization and securing of local networks in the context of neveux access environment. By focusing on measures such as ARP encapsulation, DHCP snooping, ACLs, Storm Control, port security, and network organization, it aims to enhance network protection against growing threats. The study covers both theoretical and practical aspects of attack analysis and security practices. Tools such as Kali Linux and Packet Tracer are utilized for simulating attacks and configuring security mechanisms. The goal is to provide a strong foundation for the development of effective security strategies in local networks.

Introduction générale

Les réseaux informatiques jouent un rôle essentiel dans notre société moderne, reliant les utilisateurs, les appareils et les ressources à travers le monde. Avec l'augmentation constante de la dépendance aux technologies de l'information, il devient crucial d'organiser et de sécuriser efficacement les réseaux locaux. Ce mémoire se concentre sur l'organisation d'un réseau local et la sécurisation des niveaux d'accès.

Le chapitre 01, "Généralités sur les réseaux informatiques", pose les bases nécessaires pour comprendre les principes fondamentaux des réseaux. On y explore le modèle OSI (Open Systems Interconnection) et le protocole TCP/IP (Transmission Control Protocol/Internet Protocol), qui sont les fondements des communications réseau. De plus, les différents types de réseaux tels que les réseaux locaux (LAN), les réseaux étendus (WAN) et les réseaux métropolitains (MAN) sont examinés, tout comme les équipements de réseau essentiels tels que les commutateurs (switches), les routeurs et les câbles réseau.

Le chapitre 2, intitulé "La Sécurité et les attaques des réseaux locaux", aborde les défis liés à la sécurité des réseaux locaux. Les attaques courantes telles que l'ARP spoofing, le DHCP spoofing et le MAC flooding sont explorées en détail, mettant en évidence les vulnérabilités potentielles auxquelles sont confrontés les réseaux locaux. En outre, des techniques de sécurité essentielles telles que le DHCP snooping, la sécurisation des ports, le chiffrement ARP dynamique et les listes de contrôle d'accès (ACL) sont présentées comme des mesures de prévention et de protection.

Le chapitre 3, intitulé "Conception et Réalisation", propose une approche pratique de la mise en œuvre des mesures de sécurité dans un réseau local. Une simulation est réalisée pour mettre en évidence les concepts abordés dans le chapitre précédent. L'organisation du réseau local est présentée, en mettant en avant les méthodes de sécurité telles que le DHCP snooping, la sécurisation des ports et l'authentification du serveur. De plus, la sécurisation des paquets et l'analyse des traces (packet tracing) sont abordées pour renforcer la sécurité globale du réseau.

Ce mémoire vise à fournir une compréhension approfondie de l'organisation des réseaux locaux et de la sécurisation des niveaux d'accès. En explorant les aspects théoriques et pratiques de la gestion des réseaux, il vise à offrir des recommandations et des bonnes pratiques pour garantir la sécurité et l'efficacité des réseaux locaux.

Après l’étude du réseau informatique de Sonatrach ain salah nous avons remarqué que ce réseau nécessite des améliorations comme la sécurité des données et des services. Dans notre étude nous essayons de répondre à la problématique suivante : Comment Configurer et sécuriser le réseau Local de la direction central-informatique et système information de l’entreprise Sonatrach ?

Chapitre 01 : Généralités sur les réseaux informatique

Chapitre 01 : Généralités sur les réseaux informatique

Introduction

Pour mener à bien notre projet qui est de proposer des solutions de sécurité pour le réseau LAN, nous devons commencer par expliquer le fonctionnement des réseaux informatiques. Nous allons aborder les concepts de bases des réseaux informatiques.

1. Définition d'un réseau :

D'une manière générale, un réseau n'est rien d'autre qu'un ensemble d'objets ou de personnes connectés ou maintenus en liaisons et dont le but est d'échanger des informations ou des biens matériels.

2. Les types de réseaux :

Nous distinguons différents types de réseaux classifiés selon leurs tailles, leurs vitesses de transfert des données, ainsi que leurs étendues [1].

2.1. Les réseaux locaux Local Area Network (LAN) :

Un réseau local est un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau dont la taille est de quelque kilomètres [1].

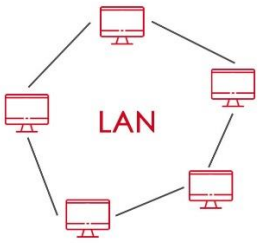


Figure 1. 1: réseaux locaux (LAN).

2.2. Les réseaux métropolitains : Métropolitains Area Network (MAN) :

Un réseau MAN interconnecte plusieurs LAN géographiquement proches (au maximum quelques kilomètres) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens de hauts débits (généralement de fibres Optiques) [1].

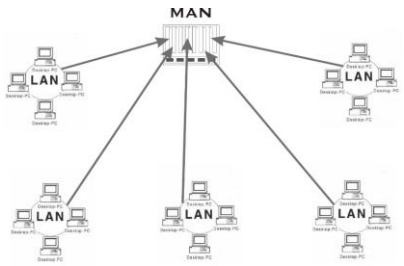


Figure 1. 2: Réseau étendu (MAN).

2.3 Les réseaux distants : Wide Area Network (WAN) :

Les réseaux WAN interconnectent plusieurs LAN à travers de grandes distances géographiques. Les débits disponibles sur un MAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles contrairement aux WAN qui fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau [1].

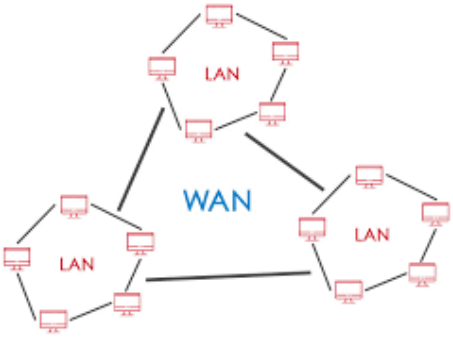


Figure 1. 3: Réseau étendu (WAN).

2.4. Caractéristiques des réseaux locaux (LAN) :

Un réseau local se caractérise principalement par sa topologie (physique et logique), les médias utilisés pour le transport, ainsi que le mode transmission [2].

a. Media de transmission : Dans les réseaux locaux, nous pouvons trouver plusieurs médias de transport, et parmi ces médias nous citons :

- Le câble coaxial.
- La paire torsadée.
- La fibre optique.
- Les ondes hertziennes.

b. Mode de transmission : Selon le sens des échanges, nous distinguons trois modes de transmission :

• La liaison simplex.

• La liaison half-duplex.

• La liaison full-duplex [2].

3. Les topologies d'un réseau :

Pour pouvoir utiliser un réseau, Il faut définir, en plus du type de réseau, une méthode d'accès entre les ordinateurs, ce qui nous permettra de connaître la manière dont les informations sont échangées.

Il existe deux types de topologies : topologie physique et topologie logique [1].

3.1. La topologie physique :

La topologie physique est la façon dont les équipements sont connectés physiquement les uns aux autres grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels (cartes réseau, etc.) [1].

a. Topologie en bus :

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau. Cette topologie a pour avantages d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui sera affecté [1].

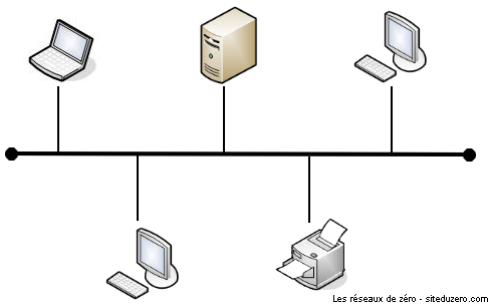


Figure 1. 4: Topologie en bus.

b. Topologie en étoile :

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé hub ou concentrateur. Il s'agit d'une boîte comprenant un certain nombre de jonctions

auxquelles nous pouvons connecter les câbles en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions [1].

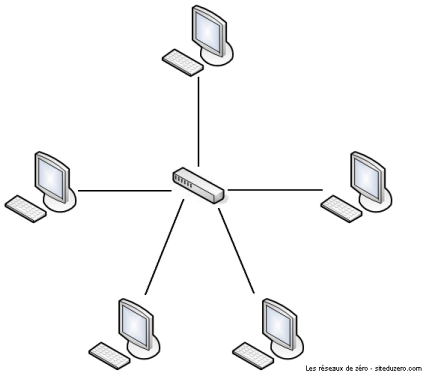


Figure 1. 5: Topologie en étoile.

c. Topologie en anneau :

Dans un réseau en topologie en anneau, les ordinateurs communiquent chacun à leur tour, nous avons donc une boucle d'ordinateurs sur laquelle chacun d'entre eux va avoir la parole successivement.

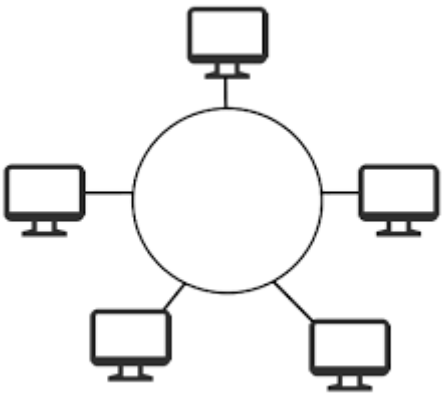


Figure 1. 6: Topologie en anneau.

En réalité les ordinateurs d'un réseau en topologie anneau ne sont pas reliés en boucle, mais sont reliés à un répartiteur appelé MAU (Multi station Access Unit) qui gère la communication entre les ordinateurs qui lui sont reliés en accordant à chacun d'entre eux un temps de parole [1].

d. Topologie en arbre :

Dans une topologie en arbre le réseau est divisé en niveaux. Il existe un hôte principal à la tête du réseau. Cet hôte est lui-même connecté à d'autres hôtes de niveaux inférieurs, créant une hiérarchie [3].

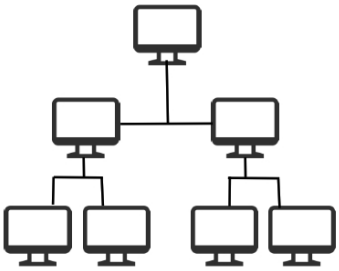


Figure 1. 7: Topologie en arbre.

Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence [3].

e. Topologie en maillée :

Dans une topologie maillée les dispositifs sont connectés avec de nombreuses interconnexions redondantes entre les nœuds du réseau. Une unité réseau peut avoir (1, N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres [3].

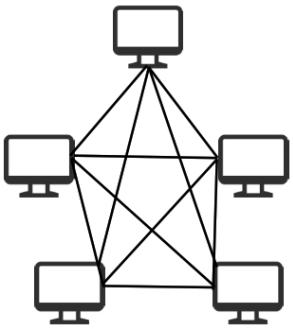


Figure 1. 8: Topologie en maillée.

4. type de communication (Architecture des réseaux) :

4.1. Communication post à post :

Dans une architecture d'égal à égal (ou poste à poste), contrairement à une architecture de réseau de type client-serveur, il n'y a pas de serveur dédié. Ainsi, chaque ordinateur dans un tel réseau est un peu serveur et un peu client. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources. Un ordinateur relié à une imprimante pourra donc éventuellement la partager afin que tous les autres ordinateurs puissent y accéder via le réseau [4].

4.2. Communication client-serveur :

De nombreuses applications fonctionnent selon un environnement client-serveur. Cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur

qui leur fournit des services, programmes fournissant des données telles que l'heure, des fichiers, une connexion... [4].

5. Conception de base d'un réseau Informatique :

5.1 Modèle OSI (Open System Interconnexion) :

Le modèle OSI est un modèle conceptuel. Il a pour but d'analyser la communication en découpant les différentes étapes en 7 couches, chacune de ces couches remplissant une tâche bien spécifique. Afin de connaitre les services de chaque couche on va les présenter ci-dessous l'une après l'autre.

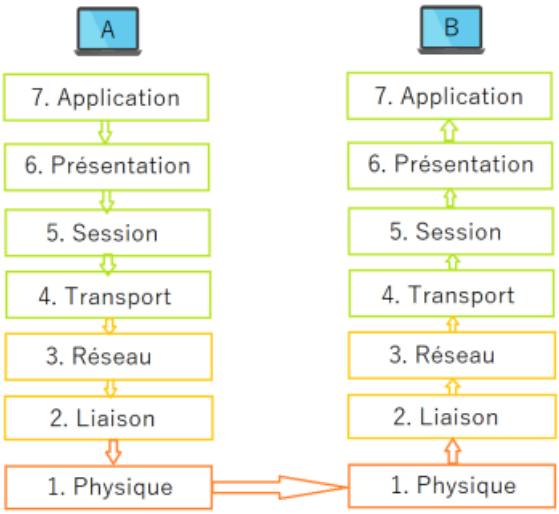


Figure 1. 9: Modèle OSI.

5.2 Rôle des différentes couches :

Chaque couche réseau définie par le modèle a un rôle bien précis, qui va du transport du signal codant les données à la présentation des informations pour l'application destinataire [5].

a. La couche Physique

Cette couche traite de la transmission physique des données, tels que les niveaux de tension, les câbles et les connecteurs [5].

Définissant le mode de propagation des signaux, elle géré au besoin les circuits physiques. Des matériels comme les modems (modulateur/démodulateur), les répéteurs ou la connectique des cartes réseaux, RJ45 par exemple, se placent à ce niveau [5].

b. Couche Liaison de données :

Cette couche assure le transfert de données fiable sur une liaison physique, en détectant et en corrigeant les erreurs qui se produisent dans la couche physique [5].

c. Couche Réseau :

Cette couche fournit des services de routage et d'adressage, permettant le transfert de données entre différents réseaux [5].

d. Couche Transport :

Cette couche assure la fiabilité et le contrôle de flux de bout en bout de la communication, en segmentant les données en paquets et en fournissant des mécanismes de récupération d'erreur [5].

e. La couche Session

Cette couche gère la communication entre les applications sur des systèmes différents, en établissant, en maintenant et en terminant des connexions de session [5].

f. Couche Présentation :

Cette couche assure la compatibilité des formats de données entre les différentes plates-formes, en convertissant les données en un format commun [5].

g. Couche Application :

Cette couche fournit des services d'application aux utilisateurs, tels que la messagerie électronique, le transfert de fichiers, le partage de fichiers, etc [5].

6. Le Modèle TCP/IP :

TCP/IP est un protocole de liaison de données utilisé sur Internet. Son modèle est divisé en quatre couches distinctes. Utilisées ensemble, elles peuvent également être appelées une suite de protocoles [6].

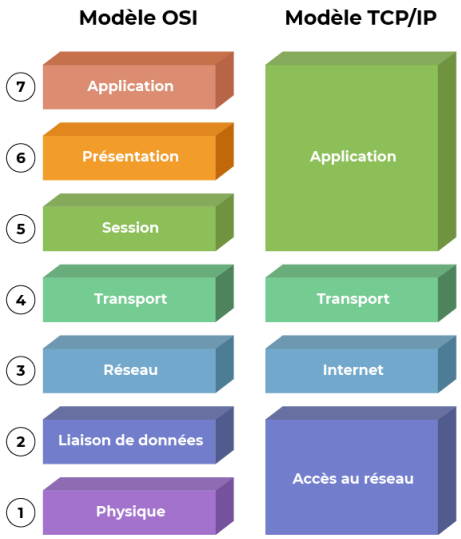


Figure 1. 10: Correspondance OSI, TCP/IP.

6.1 Les rôles des différentes couches :

6.1.1) La couche Accès réseau :

La couche accès réseau est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau [6].

6.1.2) Couche Internet :

La couche Internet, également appelée couche réseau, contrôle le mouvement des paquets sur le réseau [6].

6.1.3) Couche transport :

La couche transport fournit une connexion des données fiable entre deux appareils. Elle divise les données en paquets, accuse réception des paquets qu'elle a reçus de l'autre appareil et s'assure que ce dernier accuse réception des paquets qu'il reçoit [6].

6.1.4) Couche application :

La couche application est le groupe d'applications nécessitant une communication réseau. Il s'agit généralement de l'application avec laquelle l'utilisateur interagit, comme les e-mails et la messagerie. Parce que les couches inférieures gèrent les détails de la communication, les applications n'ont pas besoin de s'en préoccuper [6].

7. Adressage IP :

7.1. Définition :

Sur Internet, les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol), qui utilise des adresses numériques, appelées adresses IP C'est l'l CANN (Internet Corporation for Assigned Names and Numbers), remplaçant l'lANA Internet Assigned Numbers Agency depuis 1998) qui est chargée d'attribuer des adresses IP publiques. C'est-à-dire les adresses IP des ordinateurs directement connectés sur le réseau public Internet [1].

7.2 Le format des adresses IP :

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

7.2.1) Adresse IP de version 4 (IPv4) :

IPv4 (Internet Protocol version 4) Une adresse IP de version 4 est représentée avec 4 octets. On utilise, pour cela, la notation décimale pointée, c'est-à-dire que cheque octet est affiché, séparé par un point :

132.148.67.2

Suivant la valeur du premier octet, il est possible de connaitre la classe de l'adresse IP, c'est-à-dire le nombre d'octets utilisés pour le numéro de réseau et ceux restant pour l'hôte. La plage d'attribution s'étend de 0.0.0.0 à 255.255.255.255, sachant qu'il existe certaine adresse qui ne sont pas utilisées parce qu'elles sont soit réservées [7].

7.2.2) Adresse IP de version 6 (IPv6) :

IPv6, ou IP Next Génération (NG), est la nouvelle version du protocole IP (Internet Protocol). Elle devrait remplacer le protocole IPv4. Cette migration est extrêmement progressive mais doit maintenant être réalisée très rapidement. IPv6 conserve les principales caractéristiques de son prédécesseur, tout en comblant ses lacunes. Ainsi, de nouvelles fonctions ont été ajoutées. Tout d'abord, l'espace d'adressage est passé de 4 octets (32 bits) à 16 octets (128 bits).

Cela était un des objectifs majeurs de cette nouvelle mouture au début. En effet, il n'était pas prévu que IPv4 ait un tel succès, Iié a celui d'internet [7].

7.3) Différence entre IPv4 et IPv6 :

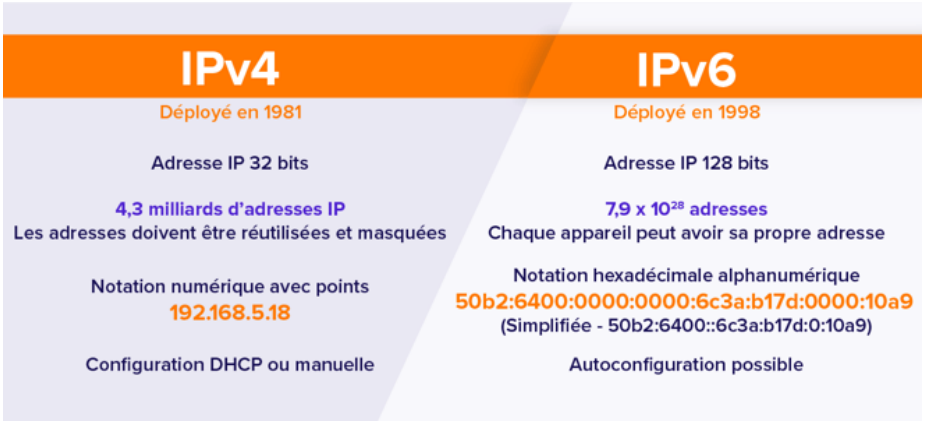


Figure 1. 11: Différence entre IPv4 et IPv6

7.4. Classe d'adresse IP :

La division des adresses IP en classes a pour but de faciliter la recherche d'un ordinateur sur le réseau. En effet, avec cette notation, il est possible de rechercher d'abord le réseau à atteindre et ensuite de rechercher un ordinateur sur celui-ci. Ainsi, l'attribution des adresses IP se fait en fonction de la taille du réseau. En effet, il y a 5 classes d'adresses IP, à savoir : classe A, classe B, classe C, classe D et classe E, de sorte que chaque classe a un format spécial de son adresse IP.

A- La Classe A :

Dans une adresse IP de classe A, le premier octet représente le réseau. Le bit de poids (le premier bit, celui de gauche) est à Zéro, ce qui signifie qu'il y a 2^7 (00000000 à 01111111) possibilités de réseaux, soit 128 possibilités. Toutefois, le réseau 0 (bts Valant 00000000) n'existe pas et le nombre 127 est réservé pour désigner votre machine.

Les réseaux disponibles en classe A sont donc les réseaux allant de 1.0.0.0 à 126.0.0.0 (les derniers octets sont des zéros ce qui indique qu'il S'agit bien de réseaux et non d'ordinateurs) [8].

B- La Classe B :

Dans une adresse IP de classe B les deux premiers octets représentent le réseau les deux premiers bits 1 et 0, ce qui signifie qu'il y a 2^14 (1000000 00000000 à 10111111 11111111) Possibilités de réseaux soit 16384 réseaux disponibles en classe B sont donc les réseaux possibles. Les réseaux disponibles en classe B sont donc les réseaux allant 128.0.0.0 à 191.255.0.0 [8].

C- La Classe C :

Dans une adresse IP de classe C, les trois premiers octets représentent le réseau. Les représentent le réseau. Les trois premiers bits sont 1, 1 et 0, ce qui signifie qu'il y a 2^21 possibilités de réseaux, c'est-à-dire 2 097 152. Les réseaux disponibles en classe C sont donc les réseaux allant de 192.0.0.0 à 223.255.255.0 [8].

7.5 Le masque réseau :

Le masque de réseau est utilisé pour séparer les parties réseau et hôte d'une adresse. L'adresse réseau est trouvée en effectuant un ET logique entre une adresse complète et le masque de réseau [8].

7.6 La passerelle par défaut :

La passerelle par défaut, c'est l'adresse de l'élément qui va permettre la discussion entre deux hôtes, par exemple un routeur, serveur ou une boxe internet [9].

7.7 L'adresse de diffusion :

Chaque réseau possède une adresse particulière dite de diffusion. Tous les paquets avec cette adresse de destination sont traités par tous les hôtes du réseau local [9].

8. Câblage

Le câblage des bureaux et des entreprises nécessite des sommes souvent importantes. Lors de l'évaluation de ce cout, il faut prendre en compte non seulement le support mais aussi les équipements situés aux deux extrémités du câble. Il faut en outre évaluer les besoins afin de sélectionner et d'installer le bon câble une fois pour toutes [10].

8.1 Câble coaxial :

Le câble coaxial (en anglais coaxial câble) a longtemps été le câblage de prédilection, pour la simple raison qu'il est peu coûteux et facilement manipulable (poids, flexibilité, ...). Un câble coaxial est constitué d'une partie centrale (appelée âme), c'est-à-dire un fil de cuivre, enveloppé dans un isolant, puis d'un blindage métallique tressé et enfin d'une gaine extérieure [10].

Figure 1. 12: câble coaxial.

8.2 Câble à paire torsadée :

Dans sa forme la plus simple, le câble à paire torsadée (twisted-pair cable) est constitué de deux brins de cuivre entrelacés en torsade et recouverts d'isolants.

Un câble est souvent fabriqué à partir de plusieurs paires torsadées regroupées et placées à l'intérieur de la gaine protectrice. L'entrelacement permet de supprimer les bruits (interférences électriques) dus aux paires adjacentes ou autres sources (moteurs, relais, transformateur).

La paire torsadée est donc adaptée à la mise en réseau local d'un faible parc avec un budget limité, et une connectique simple. Toutefois, sur de longues distances avec des débits élevés elle ne permet pas de garantir l'intégrité des données (c'est-dire la transmission sans perte de données) [10].

Il existe cinq types de paires torsadées :

a- Paire Torsadée Non Blindée (UTP) :

La paire torsadée non blindée ou UTP (Unshielded twisted pair) n'est pas entourée d'un blindage protecteur. C'est le type de câble souvent utilisé pour le téléphone et certains réseaux informatiques [11].

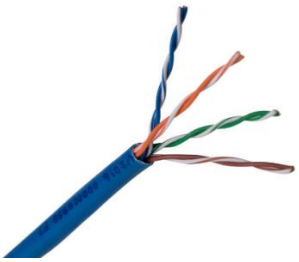


Figure 1. 13: Câble UTP

b- Paire Torsadée écrantée (FTP) :

Les paires torsadées ont un blindage général assuré par une feuille d'aluminium. L'écran est disposé entre la gaine extérieure et les 4 paires torsadées. Elle est utilisée pour le téléphone et les réseaux informatiques [11].

Figure 1. 14: Câble FTP

c- Paire Torsadée Blindée (STP) :

Chaque paire torsadée blindée (ou STP pour Shielded twisted pairs) est entourée d'une couche conductrice de blindage, de façon similaire à un câble coaxial. Cela permet une meilleure protection contre les interférences. Elle est communément utilisée dans les réseaux token ring.

Figure 1. 15: Câble STP

d- Paire Torsadée écrantée et Blindée (SFTP) :

Câble doté d'un double écran commun à l'ensemble des paires (feuille métallisé et tresse) [11].

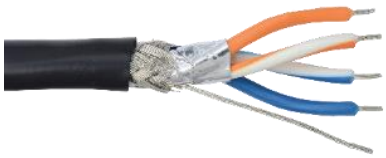


Figure 1. 16 : Câble SFTP

e- Paire Torsadée Blindée et Générale Blindée (SSTP) :

Câble STP doté en plus d'un écran commun entre la gaine extérieure et les 4 paires 2 [11].

Figure 1. 17 : Câble SSTP

8.3 Les catégories de câbles :

Catégorie	Cat.5	Cat.6	Cat.6A	Cat.7	Cat.7a	Cat.8.1	Cat.8.2
Classe	D	E	EA	F	FA	I	II
Fréquence max.	100 MHz	250 MHz	500 MHz	600 MHz	1 GHz (1000 MHz)	2 GHz (2000 MHz)	2 GHz (2000 MHz)
Débit de données max. (Ethernet)	1 Gbit/s	1 Gbit/s	10 Gbit/s	10 Gbit/s	10 Gbit/s	40 Gbit/s (y compris 25 Gbit/s)	40 Gbit/s (y compris 25 Gbit/s)
Longueur de câble max.	100 m	100 m	100 m	100 m	100 m	30 m	30 m
Nombre de connecteurs dans le canal (Channel)	Jusqu'à 4	Jusqu'à 4	Jusqu'à 4	Jusqu'à 4	Jusqu'à 4	Max. 2	Max. 2
Câblage blindé / non blindé	Les deux	Les deux	Les deux	Blindé	Blindé	Blindé	Blindé
Connecteur	RJ45	RJ45	RJ45	Autre que RJ45	Autre que RJ45	RJ45	Autre que RJ45

Figure 1. 18 : catégorie des câbles

8.4 Fibre optique :

La fibre optique consiste en un noyau de verre central entouré de plusieurs couches matériaux de protection. Il émet de la lumière plutôt que des signaux électroniques, éliminant ainsi le problème des interférences électriques. Cela le rend idéal pour certains environnements contenant de nombreuses interférences électriques Il est construit également pour la connexion de réseaux entre bâtiments, en raison de son immunité aux effets de l'humidité et de la lumière.

Les câbles à fibres optiques ont la capacité de transmettre des signaux sur des distances beaucoup plus longues que les paires coaxiales et torsadées a également la capacité de transporter des informations à des vitesses beaucoup plus grandes. Cette capacité élargit les possibilités de communication pour inclure des services tels que la vidéoconférence et les services interactifs.

Il existe deux types courants de fibres optiques – monomodes et multimodes. Le câble multimode a un diamètre plus grand ; Pourtant, les deux câbles fournissent une bande passante élevée à des vitesses élevées. Le mode simple peut fournir plus de distance, mais il est plus cher [11].

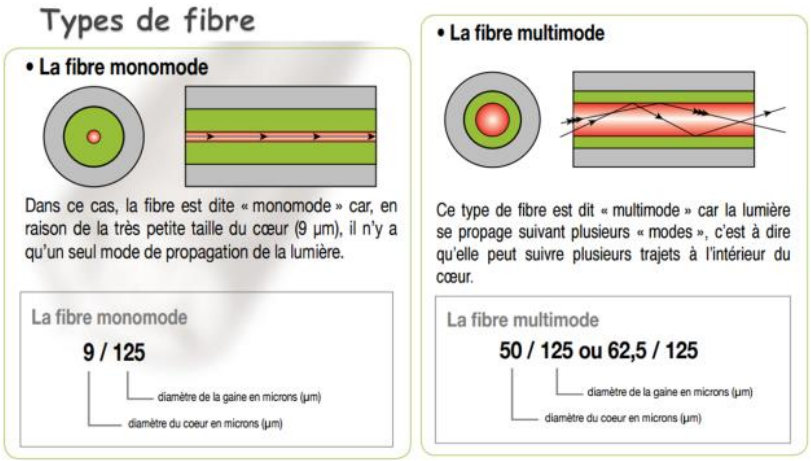


Figure 1. 19: type Cable Fibre Optique.

8.5 La connectique :

Elle permet l'interconnexion des câbles, mais aussi le raccordement aux équipements actifs (PC, switch, routeurs, etc.) [11].

A) RJ45 :

La connectique généralement utilisée est le connecteur RJ45, il est défini par la norme CEI 60603-7.

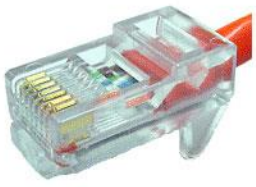


Figure 1. 20: Connectique Rj45.

B) Connecteur murale :

Figure I.21 : Connectique Murale de Rj-45.

Figure 1. 21: Connectique Murale de Rj-45.

C) connecteur de fibre optique :

Type connecteur	Standards / Normes	Système de montage	Couleur du corps	Couleur du manchon	Férule
SC	IEC 61754-4	Push-Pull	SM APC : vert SM PC : bleu MM PC : beige	SM APC : vert SM UPC : noir MM PC : noir	Zirconia ZrO2
LC	IEC 61754-20	Push-Pull	SM APC : vert SM UPC : bleu MM PC : beige	SM APC/UPC et MM PC : blanc	Zirconia ZrO2
ST	IEC 61754-2	Baïonnette	Corps métallique Al/Zn	SM APC/UPC et MM PC : noir	Zirconia ZrO2
FC	UPC: IEC 61754.13 APC: IEC 61754.20	Vis	Corps métallique Al/Zn	UPC: noir APC: vert	Zirconia ZrO2
MTRJ	IEC 61754-18	Push-Pull	SM et MM : noir	SM APC/UPC et MM PC : noir	Plastique
MU	IEC 61754-6	Push-Pull	SM APC : vert SM UPC et MM PC : marron	SM APC : vert SM UPC et MM PC : lavande	Zirconia ZrO2
EC	IEC 60874-13-1	Push-Pull	Gris – Polysulfone PBT	Gris	Cuivre / Nickel
VFO	-	Vis	Corps métallique - Laiton nickelé	Gris	Zirconia ZrO2

Figure 1. 22: connecteur de fibre optique.

9. Equipement de base d'un réseau informatique :

9.1. Carte Réseau :

La carte réseau (appelée Network Interface Card en anglais et notée NIC) constitue l'interface entre l'ordinateur et le câble du réseau. La fonction d'une carte réseau est de préparer, d'envoyer et de contrôler les données sur le réseau [12].

Figure 1. 23 : Carte Réseau.

9.2. Switch :

Un switch, ou commutateur en français, est un équipement réseau qui permet de connecter plusieurs appareils sur un même réseau local (LAN). Le switch agit comme un centralisateur, en interconnectant les différents appareils sur le réseau et en acheminant les données d'un appareil à un autre.

Le switch fonctionne en utilisant l'adresse MAC (Media Access Control) des appareils connectés pour diriger le trafic réseau vers le destinataire approprié. Il peut également être configuré pour segmenter le réseau en plusieurs sous-réseaux, ce qui permet une gestion plus efficace du trafic et une meilleure sécurité du réseau. Les switches peuvent être utilisés dans diverses applications, telles que les réseaux d'entreprise, les centres de données, les réseaux résidentiels, etc [13].

Figure 1. 24: Switch.

9.3. Le Routeur :

Un routeur est un équipement de réseau qui permet de connecter plusieurs réseaux informatiques différents (par exemple, Internet et un réseau local d'entreprise) et de faire transiter les données entre eux.

Le routeur agit comme une passerelle entre les réseaux, en utilisant des adresses IP pour diriger le trafic réseau vers sa destination appropriée. Il peut également être configuré pour effectuer des fonctions de sécurité, telles que le filtrage des paquets, la mise en place de pare-feu, etc.

Le routeur est donc un équipement crucial pour l'acheminement efficace des données sur Internet, ainsi que pour la sécurisation des réseaux. Il est souvent utilisé dans les environnements professionnels, tels que les entreprises, les organisations gouvernementales et les centres de données, ainsi que dans les foyers pour la connexion à Internet et la gestion du réseau domestique [13].

Figure 1. 25: Routeur.

9.4. Pont :

Un pont (ou bridge en anglais) est un équipement réseau qui permet de connecter deux segments de réseau local (LAN) afin de les faire communiquer ensemble comme s'il s'agissait d'un seul et même réseau.

Le pont fonctionne en analysant les adresses MAC des paquets de données qui circulent entre les deux segments de réseau, et en apprenant les adresses MAC de chaque appareil connecté à chaque segment. Cette information est ensuite utilisée pour diriger le trafic réseau de manière optimale, en évitant de saturer inutilement les deux segments de réseau [13].

Figure 1. 26: Pont

10.Les serveurs réseaux :

A) Un serveur HTTP (Hypertext Transfer Protocol) : serveur web HTTP est un logiciel qui reçoit les requêtes HTTP des clients, tels que les navigateurs web, et renvoie les réponses correspondantes. Il permet de fournir des ressources telles que des pages web, des images, des fichiers CSS, etc. Le serveur web est responsable de la gestion de ces requêtes, de l'identification des ressources demandées et de l'envoi des réponses appropriées aux clients.

B) serveur DNS : serveur DNS, ou serveur de noms de domaine, est un serveur informatique qui assure la traduction des noms de domaine en adresses IP. Il agit comme un répertoire pour Internet, permettant aux utilisateurs d'accéder à des sites Web et à des services en saisissant un nom de domaine (par exemple, www.example.com) plutôt que l'adresse IP correspondante. Lorsqu'un utilisateur saisit un nom de domaine dans un navigateur Web, le serveur DNS est chargé de résoudre ce nom de domaine en adresse IP afin que les ressources demandées puissent être accessibles. Il agit comme un intermédiaire entre les utilisateurs et les serveurs en fournissant les informations nécessaires pour établir une connexion.

C) serveur DHCP (Dynamic Host Configuration Protocol) : serveur DHCP est un serveur qui attribue automatiquement des adresses IP aux appareils connectés à un réseau. Il facilite la configuration réseau en fournissant aux appareils les informations nécessaires, telles que l'adresse IP, la passerelle par défaut et les serveurs DNS, sans nécessiter une configuration manuelle. Le serveur DHCP simplifie le processus d'attribution des adresses IP et facilite la connexion des appareils à un réseau.

D) serveur FTP (File Transfer Protocol) : Un serveur FTP (File Transfer Protocol) est un logiciel qui permet le transfert de fichiers entre des ordinateurs via un réseau. Il permet aux utilisateurs de télécharger des fichiers depuis un serveur FTP vers leur ordinateur local ou d'envoyer des fichiers depuis leur ordinateur local vers le serveur FTP distant. Le serveur FTP offre des fonctionnalités pour la gestion des fichiers, la création de répertoires, le renommage de fichiers, etc. Les clients FTP se connectent au serveur à l'aide d'un nom d'utilisateur et d'un mot de passe pour accéder aux fichiers et aux répertoires disponibles.

10.Conclusion :

Ce chapitre nous a permis de découvrir les différents éléments des réseaux informatiques et de mieux comprendre les notions et les aspects élémentaires des réseaux informatiques, où nous avons commencé par la définition des réseaux informatique et ces fonctionnalités, puis on a vu les conceptions de base, type, topologie, et l'architecteur des réseaux informatique, puis on a parlé sur l'adressage et le câblage, et enfin on a parlé sur les composants et équipements des réseaux informatiques.

Introduction sur chapitre 02 :

En chapitre 02 en a examiné d'une manière Générale la sécurité des réseaux informatiques, les différentes attaques réseau ainsi que les moyens et technologies qui permettent de faire face à ces attaques.

Chapitre 02 : La Sécurité Des Réseaux Locaux

Chapitre 02 : La Sécurité Des Réseaux Locaux

II.1. Introduction

Aujourd'hui, la sécurité informatique dans les entreprises est un domaine légitime, même si les frontières de ce qu'elle recouvre restent floues Elle fait en tout cas figure d'évidence sur le plan général. Si les méthodes qui lui sont dédiées et le périmètre qui lui est réservé sont évidemment discutés et débattus, personne en revanche ne défend l'idée qu'il ne faudrait pas sécuriser les échanges, les machines ou les réseaux de communication. Pourtant, hormis quelques rares, les politiques sécuritaires restent largement ignorées par les chercheurs qui s'intéressent à la place des technologies de communication dans les organisations. Et si l'on connaît les grandes lignes des principaux discours médiatiques qui décrivent les enjeux de la sécurité informatique, on sait mal comment, au jour le jour, le souci sécuritaire s'actualise dans les entreprises, quelles formes il prend. On ne sait pas non plus ce qu'il fait des technologies et de leurs usagers, alors même qu'il est une des sources importantes d'encadrement des pratiques professionnelles. [14]

La sécurité des réseaux devient alors une problématique essentielle tant pour les individus que pour les entreprises ou les Etats. Il est donc important de définir une politique de sécurité pour ces réseaux et de veiller à son respect. Néanmoins les mécanismes de sécurité préventifs mis en place ne sont pas incontournables. Il est nécessaire, de mettre en œuvre des outils permettant de détecter toute violation de la politique de sécurité, c'est-à-dire toute intrusion. Tout au long de ce chapitre, notre intérêt se porte sur les principales menaces pesant sur la sécurité des réseaux ainsi que les mécanismes de défense.[15]

La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Nous allons maintenant parler de la sécurité informatique, ses objectifs et de son impact sur les réseaux

II.2. Les attaques réseau :

Les attaques réseau sont aujourd'hui si nombreuses qu'il serait illusoire de prétendre les décrire toutes. Il est cependant possible de dresser une typologie des faiblesses de sécurité afin de mieux appréhender ces attaques, qui ont pour point commun d'exploiter des faiblesses de sécurité. L'objectif de ce chapitre est de présenter les faiblesses les plus couramment exploitées par les attaques et de détailler les mécanismes de ces attaques. Nous espérons de la sorte faire comprendre les dangers qui menacent les réseaux, et non de susciter des vocations de piraterie, au demeurant réprimandées par la loi. Comme tout effet a une cause, les attaques réseau s'appuient sur divers types de faiblesses, que l'on peut classifier par catégorie, comme illustré à la figure 1. Les protocoles réseau sont encore jeunes, et aucun d'eux n'a été conçu pour tenir compte des problèmes de sécurité. Le protocole IP, par exemple, ne comporte pas de couche sécurité. La plupart des protocoles utilisés dans un réseau, tels SNMP (Simple Network Management Protocol) pour la supervision ou BGP (Border Gateway Protocol) pour le routage, n'implémentent pas de véritable couche de sécurité et s'exposent à diverses attaques, comme les attaques par fragmentation, déni de service, etc. De même, les protocoles réseau n'ont prévu aucun mécanisme d'authentification véritable et subissent des attaques qui s'appuient sur ces faiblesses d'authentification, comme les attaques de type spoofing, man-in-the-middle, etc. [16]

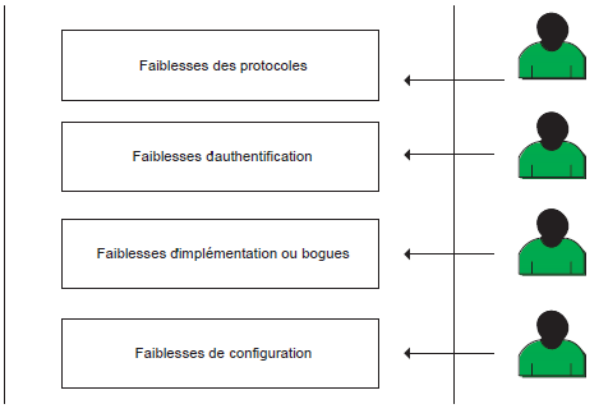


Figure 2. 1: Typologie des Faiblesses de sécurité

Nous décrivons dans ce chapitre un ensemble d'attaques classées en fonction des objectifs des pirates et reposant sur des faiblesses protocolaires, d'authentification ou d'implémentation [16].

II.2.1. Les types attaques réseau

II.2.1.1. Attaques permettant d'écouter le trafic réseau

Cette technique est généralement utilisée par les pirates pour capturer les mots de passe. Lorsqu'on se connecte à un réseau qui utilise le mode broadcast, toutes les données en transit arrivent à toutes les cartes réseau connectées à ce réseau. En temps normal, seules les trames destinées à la machine sont lues, les autres étant ignorées [16].

a) Attaque par sniffing :

Lorsque l'on parle d'attaque par sniffing réseau dans le monde de la cyber-sécurité, cela fait référence à une technique de piratage informatique : cela consiste à créer un faux réseau Wi-Fi se faisant passer pour un vrai réseau Wi-Fi public, pour écouter les communications afin de récupérer le contenu transmis. Bien que ces réseaux aient l'air authentique – ils utilisent des noms de lieux proches (par exemple Starbucks Wi-Fi) – ils sont en réalité directement connectés au pirate informatique.

L'hacker se connecte à internet pour que vous puissiez naviguer comme si tout était normal, sans vous rendre compte de quoi que ce soit d'anormal. De son côté, l'hacker peut analyser et récupérer tout ce que vous tapez, que ce soit sur votre ordinateur ou sur votre mobile connecté à ce faux réseau.

Le pirate cherche ainsi à dérober vos identifiants et vos fameux mots de passe. Il utilise pour cela un outil spécialement conçu. C'est la raison pour laquelle il est crucial de vous connecter uniquement à des réseaux que vous connaissez et auxquels vous pouvez faire confiance. Tous ces réseaux doivent avoir un mot de passe afin que vous connexions soient cryptées. Ne vous connectez jamais à un réseau public ouvert qui ne requiert pas de mot de passe au risque d'être épié, comme nous venons de le décrire.

Dans cette vidéo, Jason Hart, ancien hacker au chapeau blanc qui travaille désormais pour Gemalto, explique comment un pirate informatique peut créer une attaque par sniffing réseau dans le but de voler vos informations personnelles [17.1].

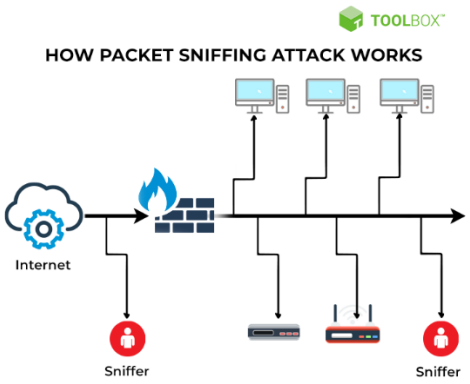


Figure 2. 2: Écoute sur un réseau local

b) Attaque de commutateur (Switch Attack) :

Le commutateur (switch) a pour fonction de permettre la cohabitation de différents sous réseaux physiques, qui ne communiquent pas nécessairement entre eux, sur le même équipement. Pour atteindre cet objectif, le principe du VLAN (Virtual LAN) a été développé. À la base, un port du commutateur est assigné à un VLAN particulier, et seuls les ports du même VLAN peuvent s'échanger de l'information. Dans le but d'améliorer le confort pour l'administrateur et la qualité de service (redondance, etc.) des fonctionnalités supplémentaires ont vu le jour, avec leurs faiblesses. Ainsi, une attaque ARP spoofing peut permettre à une machine de recevoir des données qu'elle n'est pas censée recevoir [16].

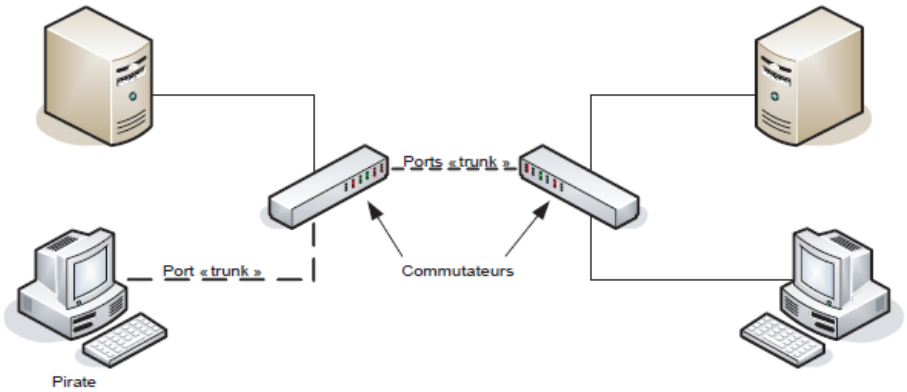


Figure 2. 3: L'attaque VLAN Hopping

Si l'attaque réussit, le port par lequel le pirate est attaché au commutateur devient un port « trunk ». À ce titre, il reçoit une copie de tous les paquets en transit sur tous les VLAN du commutateur [16].

II.2.1.2. Attaques permettant d'utiliser des accès distants Wi-Fi :

La technologie sans fil Wi-Fi (IEEE 802.11) s'appuie sur les ondes hertziennes pour établir les communications entre les équipements. Il suffit de se trouver dans la zone de couverture des émetteurs pour écouter les données. Compte tenu du risque intrinsèque.

D'une telle méthode de communication, des protocoles ont été développés afin de pallier cette insécurité. Ainsi, le protocole WEP (Wired Equivalent Privacy) est censé améliorer la confidentialité des flux réseau échangés. WEP est un protocole de sécurité défini dans le standard IEEE 802.11b. Il est chargé d'assurer un niveau de sécurité équivalent à celui des réseaux filaires en chiffrant les données transitant sur les ondes radio afin de réduire le risque d'écoute.[16]

Les attaques permettant d'utiliser des accès distants Wi-Fi sont des méthodes utilisées pour compromettre la sécurité des réseaux sans fil. Voici quelques exemples :

a) Attaque par modification de paquet :

Une attaque par modification de paquet" est un type d'attaque qui cible les réseaux informatiques, dans laquelle les paquets de données qui sont envoyés sur le réseau sont modifiés afin de les rediriger, les altérer, les détruire ou obtenir des informations sensibles. Cela peut être effectué en apportant des modifications aux en-têtes ou au contenu des paquets, et peut être réalisé en utilisant des outils spécialisés ou en exploitant les vulnérabilités du logiciel ou du matériel utilisé dans le système. Ces attaques sont l'un des types les plus courants d'attaques électroniques et sont couramment exécutées sur les réseaux locaux et Internet.[16]

b) Attaque par envoi de paquet ou par répétition :

Une attaque par envoi de paquet ou par répétition" est une méthode d'attaque utilisée dans les réseaux informatiques, où des paquets de données sont envoyés en grand nombre ou répétitivement dans le but de surcharger le système cible et de rendre les ressources réseau indisponibles pour les utilisateurs légitimes. Cette technique est également connue sous le nom d'attaque par déni de service (Dos). Les attaquants utilisent souvent des botnets, qui sont des réseaux d'ordinateurs infectés et contrôlés à distance, pour générer et envoyer des paquets de données malveillants à partir de multiples sources, afin d'amplifier l'impact de l'attaque et de rendre sa détection et sa prévention plus difficiles. Les attaques par envoi de paquet ou par répétition sont une menace sérieuse pour la sécurité des réseaux et nécessitent des mesures de sécurité efficaces pour les contrer.[16]

c) Attaque par redirection d'adresse IP :

Cette attaque nécessite que le point d'accès permette l'accès au réseau Internet, ce qui est fréquemment le cas. Elle suppose en outre que le pirate contrôle un ordinateur sur Internet. La séquence des événements est la suivante :

-Le pirate modifie l'intégrité d'un paquet en remplaçant l'adresse IP destination par l'adresse de l'équipement qu'il contrôle. Il s'appuie pour cela sur un paquet capturé et la méthode dite du « bit flipping ».

-Il garde une copie du paquet chiffré.

-Le paquet est déchiffré par le point d'accès puis envoyé en clair sur le réseau vers L'adresse IP destination (donc l'ordinateur sous contrôle du pirate), laquelle reçoit la version en clair du paquet de données.

-Le pirate récupère cette version en clair.

Le pirate possédant la version chiffrée et déchiffrée du paquet, il peut commencer une attaque de type « texte déchiffré connu » pour trouver la clé WEP [16].

Bien que l'accès sans fil distant puisse offrir confort et liberté aux utilisateurs, il représente également un risque de sécurité important. Il est donc important de suivre les mesures de sécurité nécessaires pour protéger les réseaux informatiques et les informations sensibles [16].

II.2.1.3. Attaques permettant d'interface avec une session réseau :

La plupart des protocoles réseau n'ayant prévu aucun mécanisme d'authentification véritable, ils subissent des attaques qui s'appuient sur ces faiblesses d'authentification, au premier rang desquelles les attaques ARP spoofing et man-in-the-middle.

a) Attaque ARP spoofing :

Lorsqu'un système désire communiquer avec ses voisins sur un même réseau (incluant la passerelle d'accès à d'autres réseaux), des messages ARP sont envoyés afin de connaître l'adresse MAC des systèmes voisins et d'établir ainsi une communication avec un système donné.

Sachant que chaque système possède localement une table de correspondance entre les adresses IP et MAC des systèmes voisins, la faiblesse d'authentification du protocole ARP permet à un système pirate d'envoyer des paquets ARP réponse au système cible indiquant que la nouvelle adresse MAC correspondant à l'adresse IP d'une passerelle est la sienne.

Le système du pirate reçoit donc tout le trafic à destination de la passerelle. Il lui suffit d'écouter ou de modifier passivement le trafic et de router ensuite les paquets vers leur véritable destination [16].

b) Attaque IP spoofing :

L'attaque IP spoofing consiste à se faire passer pour un autre système en falsifiant son adresse IP. Le pirate commence par choisir le système qu'il veut attaquer. Après avoir obtenu le maximum de détails sur ce système cible, il détermine les systèmes ou adresses IP autorisés à se connecter au système cible. Le pirate procède ensuite aux étapes illustrées à la figure II.4 pour mener à bien son attaque sur le serveur cible en utilisant l'adresse IP de la machine A [16].

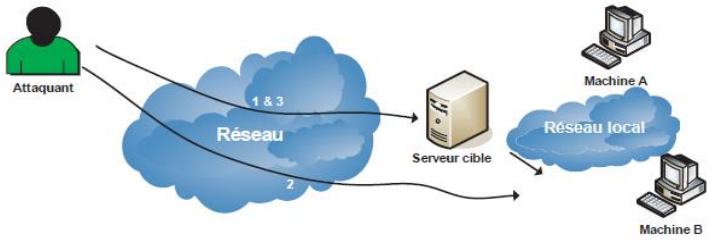


Figure 2. 4: L'attaque IP spoofing

c) Attaque man-in-the-middle:

L'attaque man-in-the-middle consiste à faire passer les échanges réseau entre deux systèmes par le biais d'un troisième, sous le contrôle du pirate. Ce dernier peut transformer à sa guise les données à la volée, tout en masquant à chaque acteur de l'échange la réalité de son interlocuteur. Pour mettre en œuvre l'échange réseau approprié, il faut soit que la machine du pirate se trouve physiquement sur le chemin réseau emprunté par les flux de données, soit que le pirate réussisse à modifier le chemin réseau afin que sa machine devienne un des points de passage [16].

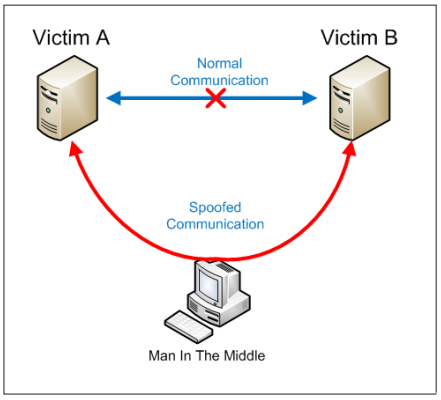


Figure 2. 5: attaque the man in the middle

d) Attaque man-in-the-middle par modification du routage :

Une des méthodes permettant à un pirate de se placer dans la configuration de l'homme au milieu repose sur la modification du routage. Par diverses méthodes, selon le protocole de routage visé, le pirate peut influencer le comportement du réseau afin que les flux de celui-ci transitent par son ordinateur.

**Modification par routage à la source :*

Le routage à la source vise à forcer un routage particulier pour un échange de données. Son principe de fonctionnement est des plus simple : les paquets sont envoyés avec le chemin qu'ils doivent emprunter.

. Une machine A échangé des données avec une machine B. Normalement, cet échange de flux se fait par le biais des routeurs 1 et 2 (ligne en pointillés).

. L'agresseur envoie ses paquets vers la machine B en usurpant l'adresse IP source de la machine A et en utilisant un routage à la source.

. La machine B reçoit les données et renvoie les réponses via le chemin précisé dans le routage à la source.

. La machine de l'agresseur reçoit les données comme les aurait reçues la véritable machine A.

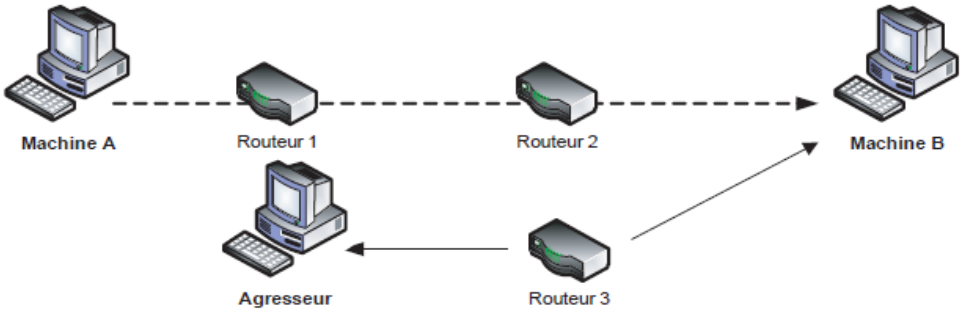


Figure 2. 6 : Attaque par routage à la source

**Modification par ICMP redirect :*

Une variante de l'attaque précédente consiste à utiliser le type redirect du protocole ICMP. Le principe de fonctionnement de cette attaque est le suivant (voir figure II.6) :

. Une machine A échangé des données avec une machine B.

. Normalement, cet échange de flux s'effectue par le biais des routeurs 1 et 2 (ligne en pointillés).

. L'agresseur s'installe entre les routeurs 3 et 4.

. Il convainc le routeur 1 que le meilleur chemin consiste à passer par le routeur 3 en lui envoyant des paquets ICMP redirect.

. Le routeur 1 envoie les paquets destinés à la machine B via le routeur 3.

. L'agresseur est placé en goulet d'étranglement entre les routeurs 3 et 4. [16].

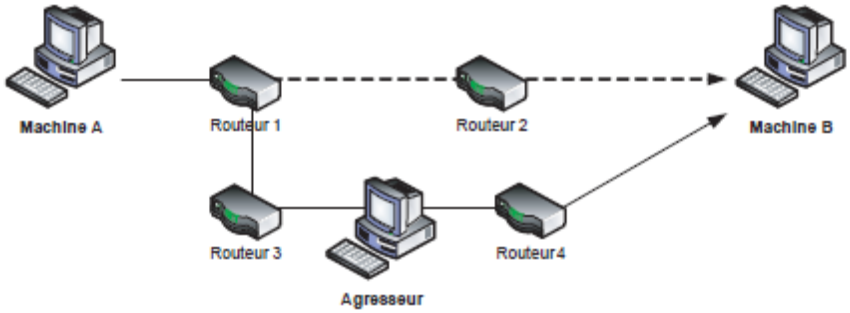


Figure 2. 7: Attaque par ICMP redirect

II.2.1.4. Attaques permettant de modifier le routage réseau :

Tous les protocoles de routage ont pour objectif de maintenir les tables de routage du réseau dans un état intègre et cohérent. Pour y parvenir, les protocoles diffusent des informations de routage aux autres systèmes du réseau afin de transmettre les modifications des tables de routage. Ces protocoles réceptionnent en contrepartie les informations de routage d'autres systèmes du réseau afin de mettre à jour les tables de routage [16].

a) Attaques de détournement de route (route hijacking) :

Ces attaques visent à rediriger le trafic réseau vers des destinations incorrectes en manipulant les tables de routage. Les attaquants peuvent utiliser des techniques telles que le BGP hijacking pour annoncer de fausses informations de routage et diriger le trafic vers des passerelles compromises.

b) Attaques de falsification de paquets (packet spoofing) :

Ces attaques consistent à falsifier l'adresse IP source d'un paquet pour tromper les routeurs et les systèmes de sécurité. En falsifiant l'adresse source, un attaquant peut modifier le routage du trafic et faire en sorte que les réponses reviennent vers une autre destination [16].

II.3. La sécurité des Réseaux informatique :

II.3.1.1. Sécurité Physiques d'équipement réseau LAN/WLAN :

La sécurité physique est un aspect fondamental de tout type de sécurité pour garantir l'intégrité, la confidentialité et la disponibilité des informations. Si quelqu'un réussit à accéder au système informatique de l'entreprise, il peut l'endommager ou même le détruire. La sécurité physique consiste aussi en l'usage de barrières, alarmes, serrures et autres contrôles physiques permettant de conditionner l'accès physique aux locaux, aux ordinateurs et aux équipements. Ces mesures sont nécessaires pour protéger les ordinateurs, leur contenu et les autres ressources matérielles contre l'espionnage, le vol et la destruction accidentelle ou intentionnelle. L'eau représente une menace aussi pour les ordinateurs, les supports magnétiques et même pour le papier. Que l'accident ait lieu dû à l'environnement naturel (sources d'eau, pluies abondantes) ou artificiel (rupture des tuyaux, fuites, état des locaux …), l'entreprise doit prévoir des mesures de sécurité qui protègent le matériel contre l'humidité et les pertes partielles ou totales des ressources physiques [17].

II.3.1.2. Sécurité Logique de Réseau LAN/WLAN :

La sécurité logique dépôt sur la config utilise pour contrôle d'Access aux réseaux comme VLAN, ACL, STP …etc. on peut distinguer deux types de sécurité logique pour les réseaux locaux, en raison de deux types de connexion, par câble (LAN) ou par Wifi (WLAN). De plus, ces deux types de sécurité peuvent se diviser en deux modes, statique ou dynamique, selon les technologies et les équipements utilisées dans chaque mode [17].

II.4. Sécurité logique de réseau LAN en mode statique :

II.4.1. Les VLANs :

Un VLAN (Virtual Local Area Network) est un réseau local virtuel créé en regroupant des périphériques réseau appartenant à des segments de réseau différents, mais qui ont des besoins de communication similaires.

En d'autres termes, un VLAN permet de séparer un réseau physique en plusieurs réseaux logiques, isolant ainsi le trafic entre les différents groupes de périphériques. Cela permet de mieux gérer le trafic sur le réseau, de contrôler les accès, de garantir la sécurité des données et d'optimiser les performances en évitant la diffusion inutile de paquets.

Les VLANs sont largement utilisés dans les réseaux d'entreprise pour segmenter les utilisateurs et les applications en fonction de leur rôle et de leur niveau de sécurité [18].

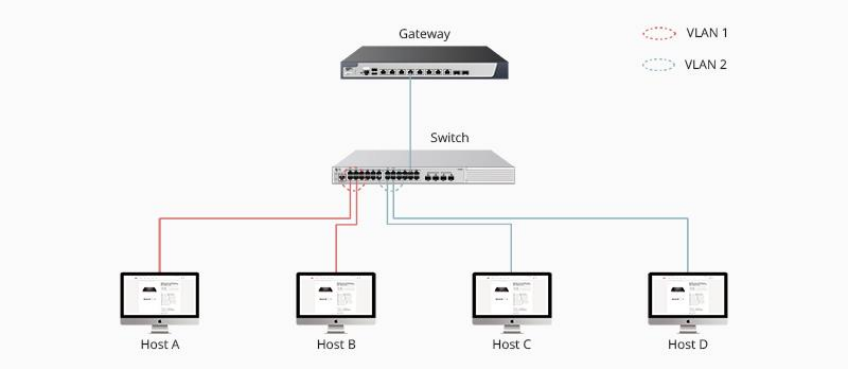


Figure 2. 8: vlan

a) VLAN basé sur le port :

Un VLAN basé sur le port est un type de VLAN dans lequel les ports du commutateur sont associés à un VLAN spécifique. Les paquets qui sont reçus sur un port particulier sont transmis uniquement aux autres ports qui appartiennent au même VLAN [18].

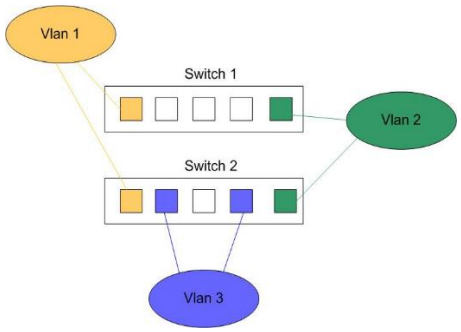


Figure 2. 9: vlan niveaux 1 (par port).

b) VLAN par adresse MAC :

Le Vlan de niveau segmente le réseau en fonction de l'adresse MAC de l'utilisateur. On associe ainsi des adresses à des VLANs pour permettre à un utilisateur de se déplacer sans pour autant changer de profil. Ce type de Vlan est généralement utilisé pour regrouper les utilisateurs par service [18].

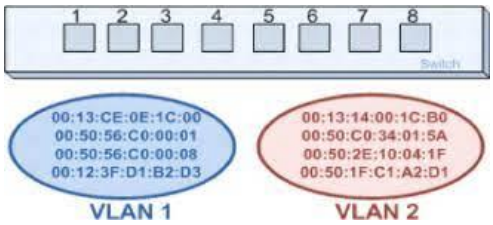


Figure 2. 10: VLAN par adresse MAC

c) VLAN basé sur le protocole :

Dans ce type de VLAN, les paquets sont regroupés en fonction de leur protocole de couche 3 (par exemple, IP, IPX) [18].

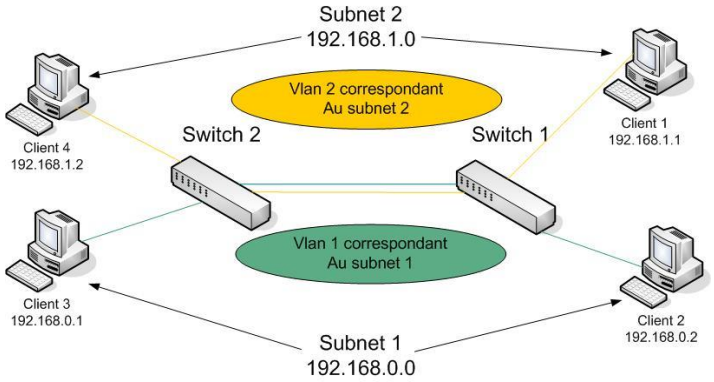


Figure 2. 11: VLAN par adresse MAC

II.4.2. Le protocole VTP :

Le protocole VTP de **Cisco** est un protocole propriétaire de la couche 2. Son principal avantage est la possibilité de propager automatiquement les VLAN configurés sur un commutateur en mode "serveur" vers d'autres commutateurs configurés en mode "client". Dans un réseau complexe qui comprend plusieurs commutateurs, le protocole VTP est un atout car il permet une configuration centralisée et facilite la gestion des VLAN sur l'ensemble du réseau [19].

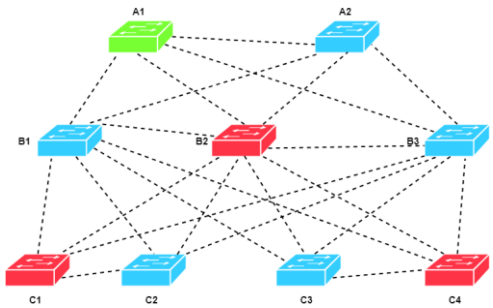


Figure 2. 12: Le protocole VTP.

VTP permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur (le serveur) qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau (clients). VTP permet ainsi d'éviter toute incohérence de configuration des VLAN sur l'ensemble d'un réseau local. Selon le rôle du protocole vtp, nous distinguons les trois types suivants :

a) VTP Server : Le switch en mode Server permet à l'administrateur de faire toute modification sur les VLANs et de propager automatiquement ses modifications vers tous les switches du réseau [20].

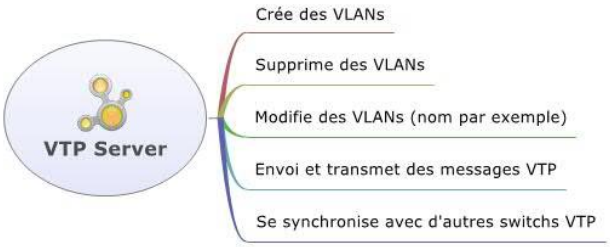


Figure 2. 13: VTP Server

b) VTP Client : Le switch en mode Client ne permet pas à l'administrateur de faire des modifications sur les VLANs. Vous recevez un message d'erreur quand vous essayez de créer un VLAN [20].

Figure 2. 14 : VTP Transparent

c) VTP Transparent : Le switch en mode Transparent permet à l'administrateur de faire toute modification sur les VLANs en local uniquement et donc ne propage pas ses modifications vers tous les switchs du réseau. Très pratique pour des maquettes ! [7].

Figure 2. 15: VTP Transparent

II.4.3. Access Control List ou ACL :

Une ACL (Access Control List) est une liste de règles qui spécifie les types de trafic autorisés ou interdits à passer à travers un point de contrôle de sécurité, comme un routeur ou un pare-feu. Les ACL sont souvent utilisées pour contrôler l'accès au réseau en limitant les types de trafic qui sont autorisés à traverser des points de contrôle spécifiques.

Les règles d'une ACL peuvent être basées sur différents critères tels que l'adresse IP source et de destination, le port source et de destination, le protocole, etc. Les ACL peuvent être configurées pour permettre ou bloquer des paquets spécifiques en fonction de ces critères.

En résumé, une ACL est un mécanisme de contrôle d'accès qui permet de limiter l'accès au réseau en spécifiant les règles pour autoriser ou bloquer le trafic réseau.

ACL est une collection d'instructions ayant comme objectif de permettre ou d'interdire la commutation des paquets en fonction d'un certain nombre de conditions ou de critères, tels que :

- Adresses de source et de destination
- Les protocoles de couches supérieures tel que UDP ; et le numéro de port tel que 67,
- Des paramètres dynamiques basés sur le temps : 2 heures sur une période de 24 heures. [21].

Les ACL réseau gèrent l'accès à un réseau. Pour ce faire, elles fournissent des instructions aux commutateurs et aux routeurs quant aux types de trafic autorisés à s'interfacer avec le réseau. Elles dictent également ce que chaque utilisateur ou appareil peut faire une fois qu'il est à l'intérieur du réseau [22].

Il existe deux types principaux de listes de contrôle d'accès (ACL) :

a) Les ACL standard : ce type d'ACL utilise uniquement l'adresse IP source comme critère pour autoriser ou bloquer le trafic. Les ACL standard peuvent être utilisées pour autoriser ou bloquer le trafic en fonction de l'adresse IP source, mais elles ne peuvent pas être utilisées pour filtrer le trafic en fonction d'autres critères tels que les ports source ou de destination.

b) Les ACL étendues : contrairement aux ACL standard, les ACL étendues utilisent plusieurs critères pour autoriser ou bloquer le trafic. Les critères incluent l'adresse IP source et de destination, les ports source et de destination, le type de protocole, etc. Les ACL étendues sont plus puissantes que les ACL standard car elles offrent un plus grand contrôle sur le trafic autorisé ou bloqué [23].

c) Composants d'une ACL :

Voici une liste complète des composants d'une liste de contrôle d'accès (ACL) :

Numéro d'ACL : chaque ACL est identifiée par un numéro unique qui est utilisé pour la référencer lors de la configuration.

Type d'ACL : les deux types d'ACL les plus courants sont les ACL standard et les ACL étendues.

Critères de filtrage : les critères utilisés pour filtrer le trafic peuvent inclure l'adresse IP source et de destination, les ports source et de destination, le type de protocole, etc.

Action : l'action à effectuer lorsque le trafic correspond aux critères de l'ACL peut être de permettre le trafic ou de le bloquer.

Emplacement de l'ACL : l'emplacement de l'ACL peut être soit à l'entrée soit à la sortie d'une interface du routeur ou du pare-feu.

Interface : l'interface sur laquelle l'ACL est appliquée.

Masque de sous-réseau : un masque utilisé pour identifier un sous-réseau.

Priorité : une valeur numérique utilisée pour classer les ACL en ordre de priorité.

Durée de validité : une période de temps pendant laquelle l'ACL est active [23].

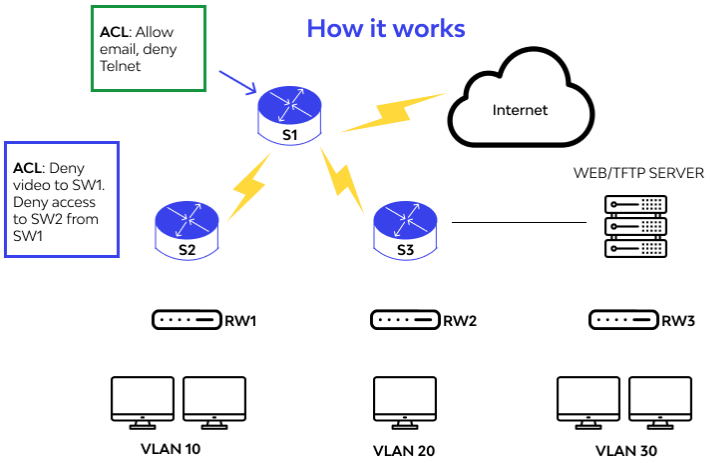


Figure 2. 16: Accès Control List

II.4.4 Serveur d'authentification RADIUS (Remote Authentication Dial-In User Service) :

Le serveur d'authentification RADIUS est un serveur qui permet de gérer l'authentification et l'autorisation d'accès à un réseau informatique. RADIUS signifie Remote Authentication Dial-In User Service. Il s'agit d'un protocole de réseau utilisé pour la gestion de l'authentification, de l'autorisation et de la comptabilisation (AAA) pour les utilisateurs qui se connectent à un réseau distant. Le serveur RADIUS permet de centraliser l'authentification des utilisateurs et des équipements réseau, tels que les routeurs, les commutateurs et les points d'accès sans fil. Lorsqu'un utilisateur tente de se connecter à un réseau, le serveur RADIUS vérifie ses informations d'identification et détermine si elle est autorisée à accéder au réseau. Si l'utilisateur est autorisé, le serveur RADIUS envoie un message d'autorisation aux équipements réseau appropriés pour permettre l'accès.

Le serveur RADIUS est souvent utilisé dans les environnements d'entreprise et les fournisseurs de services Internet (FAI) pour gérer l'accès à leurs réseaux. Il offre un moyen centralisé de gérer les accès et d'appliquer des politiques de sécurité pour les utilisateurs et les équipements réseau [24].

Le AAA (Authentification, Autorisation et Comptabilisation) est un ensemble de fonctions de sécurité informatique qui permettent de contrôler et de gérer l'accès des utilisateurs à des ressources informatiques. Le AAA est souvent utilisé dans les réseaux d'entreprise, les systèmes de gestion de contenu, les services d'hébergement, les systèmes de gestion de base de données, etc.

a) L'Authentification : est la première étape du processus AAA. Elle consiste à vérifier l'identité de l'utilisateur qui tente de se connecter au système en demandant des informations d'identification, telles que le nom d'utilisateur et le mot de passe. L'authentification peut également impliquer l'utilisation d'autres formes d'authentification, telles que des jetons d'accès, des cartes à puce, des codes de vérification à deux facteurs, etc.

b) L'Autorisation : est la deuxième étape du processus AAA. Elle consiste à déterminer les autorisations et les privilèges accordés à l'utilisateur après l'authentification. L'autorisation peut être basée sur le rôle de l'utilisateur, les politiques de l'entreprise ou les règles de sécurité.

c) La Comptabilisation : est la troisième étape du processus AAA. Elle consiste à suivre et à enregistrer les activités de l'utilisateur, telles que le temps de connexion, la durée de la session, les ressources accédées, etc. Ces informations sont utilisées pour l'analyse du trafic, la facturation, la gestion des performances et la conformité réglementaire [25].

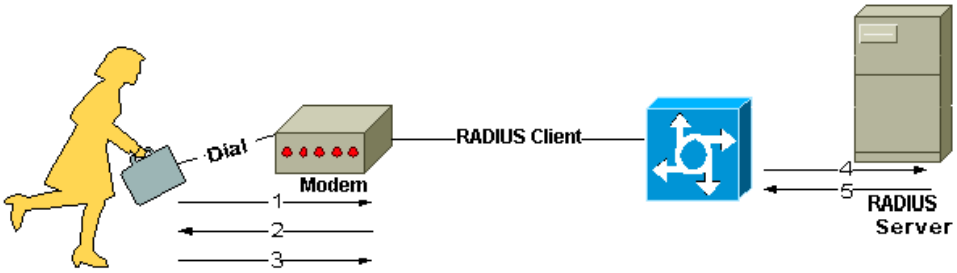


Figure 2. 17: server d'authentification radius

II.4.5. Port sécurité :

Le port de sécurité, également connu sous le nom de port sécurisé, est un mécanisme de sécurité utilisé pour protéger un réseau informatique contre les attaques malveillantes en limitant l'accès aux ports réseau non autorisés. Les ports sont des canaux de communication logiques utilisés pour transférer des données entre différents périphériques connectés à un réseau. Les ports de sécurité aident à bloquer les ports non autorisés pour éviter les attaques.

a) **Port de sécurité par défaut :** Ce type de port est configuré par défaut pour être sécurisé et bloqué pour tout trafic entrant.
b) **Port de sécurité dynamique :** Ce type de port est utilisé pour les connexions temporaires, qui sont autorisées pour une durée limitée avant d'être bloquées.
c) **Port de sécurité fixe :** Ce type de port est configuré de manière permanente pour être sécurisé et bloqué pour tout trafic entrant.

Le rôle principal du port de sécurité est de protéger le réseau informatique contre les attaques malveillantes en limitant l'accès aux ports non autorisés. Les ports non autorisés peuvent être

utilisés pour des attaques telles que la récupération de données sensibles, la propagation de logiciels malveillants et la perturbation du réseau.

En bloquant les ports non autorisés, les ports de sécurité empêchent également les attaques telles que les attaques de déni de service (DDoS) et les attaques de force brute, qui peuvent compromettre la sécurité du réseau en surchargeant les ressources du réseau [26].

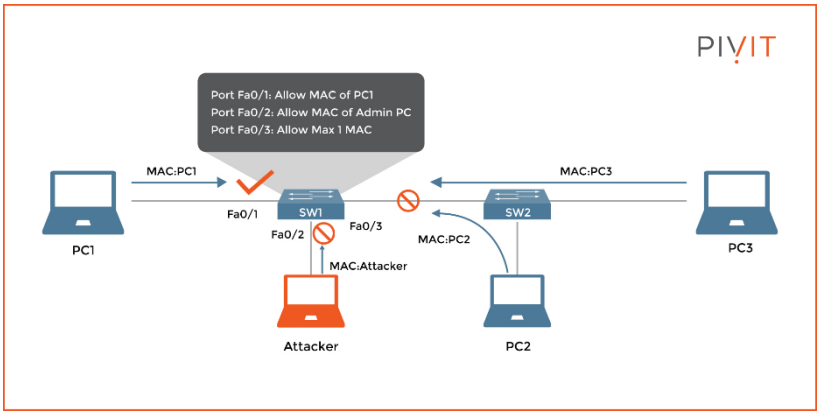


Figure 2. 18: port sécurité

II.4.6. Dynamic ARP Inspection :

Dynamic ARP Inspection (DAI) est une fonctionnalité de sécurité réseau qui permet de protéger contre les attaques de type ARP Spoofing, qui sont une forme courante d'attaques de type Man-In-The-Middle (MITM). L'ARP Spoofing consiste à envoyer de fausses adresses MAC dans les trames ARP (Address Resolution Protocol), qui sont utilisées pour résoudre les adresses IP en adresses MAC sur le réseau. Les attaquants peuvent utiliser cette technique pour intercepter et modifier le trafic sur le réseau, ainsi que pour mener des attaques de type Denial-of-Service (DoS).

Le rôle de Dynamic ARP Inspection est de vérifier les trames ARP entrantes sur un réseau, de valider l'adresse MAC de l'émetteur et de la comparer à la table ARP du switch. Si l'adresse MAC est conforme, le switch transmet la trame ARP à sa destination. Si l'adresse MAC n'est pas valide ou correspond à une adresse MAC déjà utilisée par une autre machine, la trame ARP est considérée comme suspecte et est soit supprimée, soit envoyée à un emplacement spécifié pour une analyse ultérieure. De cette manière, DAI peut détecter les attaques ARP Spoofing et protéger contre les attaques MITM [27].

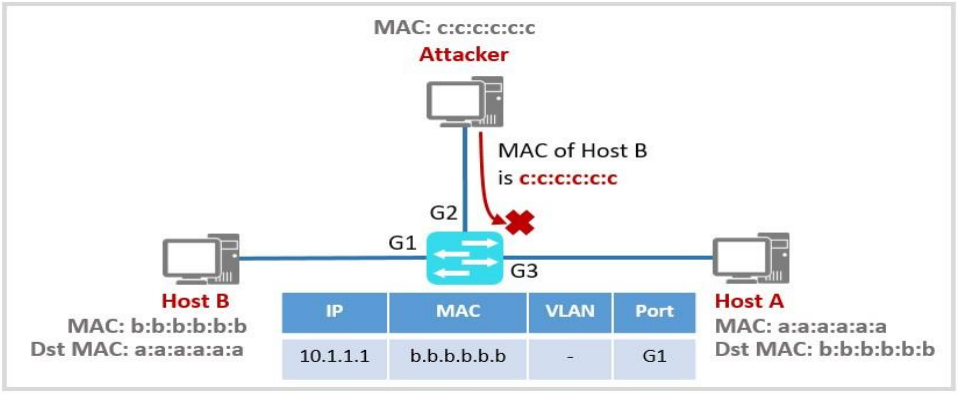


Figure 2. 19: DAI (Dynamic ARP inspection)

II.4.7. DHCP Snooping:

Le DHCP snooping est une fonctionnalité de sécurité qui joue un rôle important dans la protection des réseaux contre les attaques telles que les attaques par déni de service (DoS), les attaques d'usurpation d'adresse IP, les attaques de type Man in the Middle (MITM) et les attaques de type Spoofing.

Le DHCP snooping fonctionne en surveillant les messages DHCP échangés entre les serveurs DHCP et les clients DHCP sur le réseau. Il permet de vérifier l'authenticité des messages DHCP et d'associer les adresses IP aux adresses MAC des périphériques.

Lorsqu'un commutateur réseau est configuré avec le DHCP snooping, il enregistre les informations relatives aux adresses IP, aux adresses MAC et aux interfaces associées. Il utilise ces informations pour valider les messages DHCP entrants et sortants. Si un message DHCP est reçu sur une interface non autorisée ou provenant d'une adresse MAC non autorisée, le DHCP snooping peut prendre des mesures pour bloquer le trafic suspect, telles que la suppression du message DHCP ou la mise en quarantaine du périphérique.

Le DHCP snooping protège contre les attaques en empêchant les serveurs DHCP non autorisés ou malveillants d'attribuer des adresses IP aux clients du réseau. Les attaquants peuvent tenter de déployer un serveur DHCP frauduleux pour distribuer des adresses IP incorrectes ou pour lancer des attaques MITM. Le DHCP snooping peut détecter ces serveurs DHCP non autorisés en vérifiant les adresses IP sources et les adresses MAC des paquets DHCP [28].

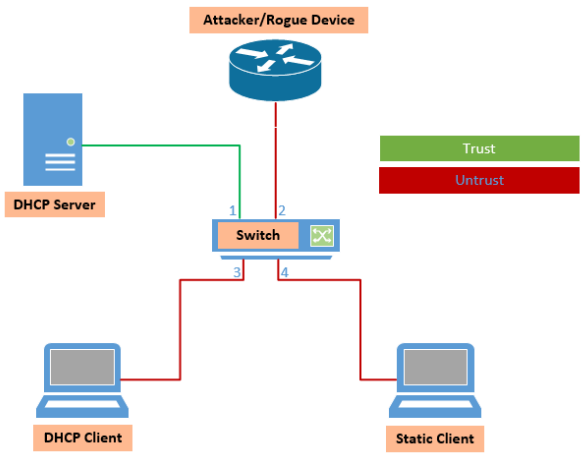


Figure 2. 20: fonctionnalité de DHCP Snooping

II.4.8. Storm control :

Le "Storm Control" est une fonctionnalité utilisée dans les réseaux informatiques pour contrôler la propagation excessive du trafic de diffusion, aussi appelé "broadcast Storm" ou

"multicast Storm". Cette fonctionnalité vise à prévenir les problèmes de saturation du réseau causés par une surcharge de trafic multicast ou broadcast.

Lorsqu'un réseau est confronté à un flux excessif de paquets multicast ou broadcast, il peut entraîner des performances médiocres, des ralentissements, voire une indisponibilité du réseau. Le "Storm Control" est conçu pour détecter et gérer ces situations en appliquant des seuils de limitation au trafic de diffusion.

Le fonctionnement du "Storm Control" peut varier selon les équipements réseau et les protocoles utilisés, mais voici les principes de base :

a) Surveillance du trafic : Les commutateurs réseau surveillent le trafic entrant sur chaque port pour détecter les niveaux de trafic de diffusion. Cela peut être réalisé en comptant le nombre de paquets multicast/broadcast par seconde ou en mesurant la bande passante utilisée.

b) Seuils de déclenchement : Des seuils de trafic sont configurés pour chaque port. Lorsque le trafic dépasse ces seuils, le "Storm Control" est activé.

c) Actions de contrôle : Lorsque le "Storm Control" est activé, différentes actions peuvent être entreprises pour gérer la tempête de diffusion :

- **Mode de protection :** Certains commutateurs offrent un mode de protection qui permet de bloquer temporairement ou définitivement le trafic de diffusion lorsque le seuil est atteint. Cela permet de protéger le réseau contre une surcharge due à un trafic excessif.
- **Limitation de trafic :** Une autre approche consiste à limiter la bande passante allouée au trafic de diffusion dépassant le seuil. Par exemple, le commutateur peut limiter le trafic multicast/broadcast à un pourcentage prédéfini de la bande passante totale disponible.
- **Notification d'alarme :** Certains commutateurs peuvent également générer des notifications d'alarme ou des journaux pour informer les administrateurs réseau de l'activité de la tempête de diffusion.

d) Rétablissement automatique : Une fois que le trafic de diffusion est revenu en dessous du seuil défini, le "Storm Control" peut désactiver les actions de contrôle et rétablir le trafic normal.

Remarque : Il est important de configurer correctement les seuils de déclenchement du "Storm Control" pour éviter des faux positifs ou des faux négatifs. Des seuils trop bas peuvent entraîner une activation fréquente et inutile du contrôle de tempête, tandis que des seuils trop élevés peuvent ne pas détecter une véritable tempête de diffusion [29].

II.4.8. Conclusion :

Chaque système informatique dans un réseau local a besoin d'implémenter des techniques de sécurités, afin de garantir le bon fonctionnement de ce réseau. Dans ce chapitre nous avons défini quelques techniques qu'on peut utiliser pour faire face à quelques attaques provoquées. Le chapitre suivant sera la partie réalisation de ces techniques de sécurité.

Chapitre 03 : simulation et Réalisation

Chapitre 03 : simulation et Réalisation

Introduction

Dans ce chapitre, nous allons passer à la dernière étape qui est la configuration et la sécurisation de réseaux local Au niveau de la direction central informatique et système

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

1. Les étape de Configuration de Réseaux Local :

1.1. Présentation générale du modèle type :

Notre modèle type se compose d'un réseau local (LAN) compose deux Switch-coeur, avec des Switches d'accès.

Pour assurer la disponibilité et la continuité de fonctions, le Switch- coeur1 est lié avec le Switch- coeur2 et ce dernier avec tous les Switch d'accès.

Nous allons également mettre en place :

-Un serveur DHCP pour une affectation dynamique d'adresses IP.

-Un serveur FTP pour la transmission des ficher.

-Un serveur DNS pour d'associer à site web.

-Un server http pour accéder les web site.

- Serveur d'authentification RADIUS pour sécurisation l'Access

1.2. Présentation des équipements utilisés pour la simulation :

Les équipements réseau utilisées sont présentés dans le tableau qui suit :

Les équipements	La marque et le type

Switch- coeur	Cisco Catalyst 3560
Switch d'accés	Cisco Catalyst 2960
Server	Server-PT

Tableau 3. 1: Présentation des équipements

1.3. Nomination des équipements et des VLAN :

Nous allons nominer les équipements utilisés et les différents VLANs dont nous aurons besoin.

1.3.1- Nomination des équipements :

Nous nominons les équipements par des noms significatifs pour faciliter la conception de l'architecture du réseau local.

Le switch d'accès seront nominés selon leur emplacement par exemple : switch Finance (SW-FIN), switch Mangement (SW-MNGT).

Switch principale	Switch d'accès	Serveur
SW-CORE1	SW1-ITC	SEV-DHCP
	SW2-IMP	SEV-FTP
	SW3-RHU	SEV-DNS
	SW4-RXT	SEV-HTTP
	SW5-MANGT	SEV- RADIUS

Tableau 3. 2: Les noms des équipements

1.3.2- Nomination des VLANs :

Pour notre réseau nous avons choisie l'adresse 172.16.0.0/24 que nous allons utiliser pour la segmentation du réseau en VLANs par port (Tableau III.5.).

Nom	**Numéro**	**Adresse IP**	**Masque Réseau**
SERVER	VLAN 1	172.16.10.1	255.255.255.0
ITC	VLAN 20	172.16.20.1	255.255.255.0
IMP	VLAN 30	172.16.30.1	255.255.255.0
RHU	VLAN 40	172.16.40.1	255.255.255.0
RXT	VLAN 50	172.16.50.1	255.255.255.0
MANGT	VLAN 60	172.16.60.1	255.255.255.0

Tableau 3. 3: Nomination des VLAN.

1.4. Les protocole VTP :

Le protocole VTP assure la cohérence de la configuration VLAN en gérant l'ajout, la suppression et le changement de nom des réseaux locaux virtuels sur plusieurs commutateurs d'un réseau.

Switch	**Mode VTP**
SW-CORE1	Serveur
SW1-ITC	Client
SW2-IMP	Client
SW3-RHU	Client
SW4-RXT	Client
SW5-MANGT	Client

Tableau 3. 4: les modes VTP

1.5. Désignation des interfaces :

Les interfaces sur les équipements sont indiquées dans le tableau suivant (Tableau III.5) :

Local Device	**Remote Device**	**Interface Local**
Multilayer Switch 01	SW1-ITC	F0/2
	SW2-IMP	F0/3
	SW3-RHU	F0/4
	SW4-RXT	F0/5
	SW5-MANGT	F0/6
	SEV-DHCP	F0/1
	SEV-DNS	F0/7
	SEV-WEB (HTTP)	F0/8
	SEV-FTP	F0/9
	SEV- RADIUS	F0/10
SW1-ITC	LAPTOP 0	F0/2
	PC 7	F0/3
	PRINTER 0	F0/4
SW2-IMP	PC 8	F0/2
	PC 9	F0/4
SW3-RHU	PC 10	F0/2
	LAPTOP 1	F0/3
	PRINTER 1	F0/4
SW4-RXT	PC 11	F0/2
	PC 12	F0/3

SW5-MANGT	PC 13	F0/2
	LAPTOP 2	F0/3
	PRINTER 2	F0/4

Tableau 3. 5: Désignation des interfaces

2. Présentation du simulateur Cisco Packet Tracer, et le système d'exploitation KALI LINUX :

2.1 Pecket tracer :

Packet Tracer est un logiciel développé par Cisco Systems qui est utilisé pour la simulation de réseaux informatiques. Il permet aux étudiants, aux professionnels de l'informatique et aux ingénieurs réseau de créer des topologies de réseau virtuelles et d'expérimenter avec différents équipements réseau, tels que des routeurs, des commutateurs, des pares-feux, des serveurs, etc. Nous avons utilisé dans notre travail la version 8.2.0.

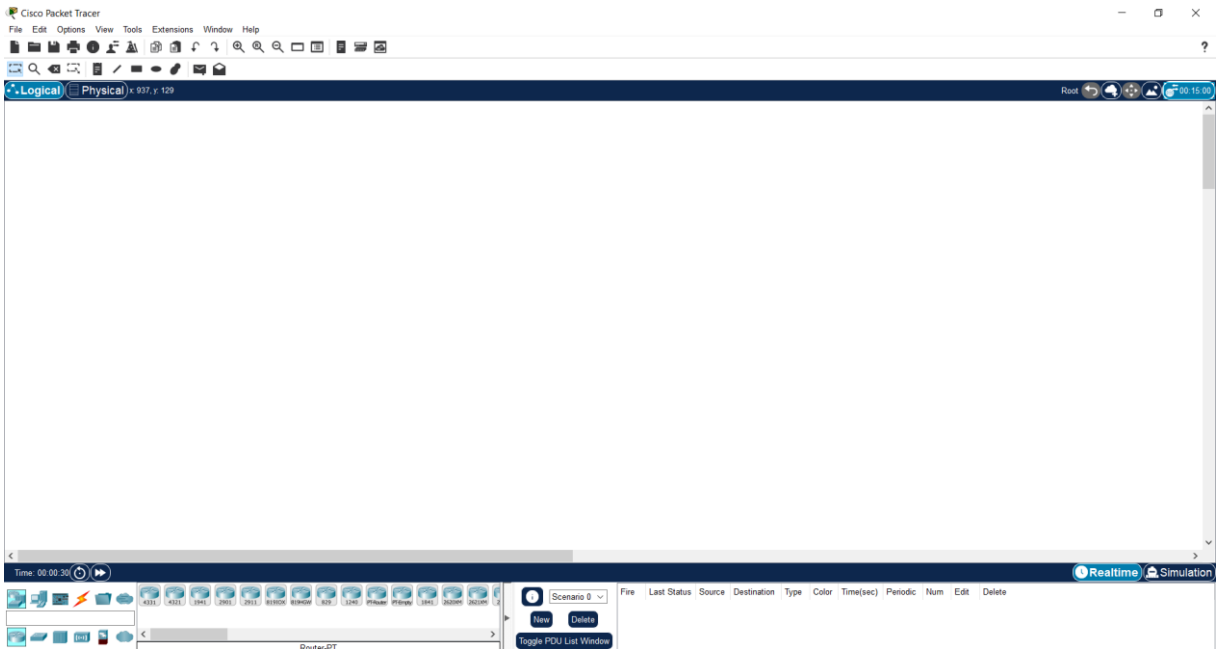


Figure 3. 1: Interface Pecket Tracer

2.2 Kali Linux :

Kali Linux est une distribution Linux basée sur Debian spécifiquement conçue pour les tests de pénétration, la sécurité informatique et les activités d'hacking éthique. Elle est utilisée par les professionnels de la sécurité, les chercheurs en sécurité et les passionnés de la sécurité informatique.

Figure 3. 2: kali linux

3. Configuration et sécurisation des équipements :

Toutes les configurations des équipements du réseau seront réalisées au niveau de la CLI (Commande Langage Interface) (Figure III.3). CLI est une interface de simulateur Cisco Packet Tracer qui permet la configuration des équipements du réseau à l'aide d'un langage de commandes.

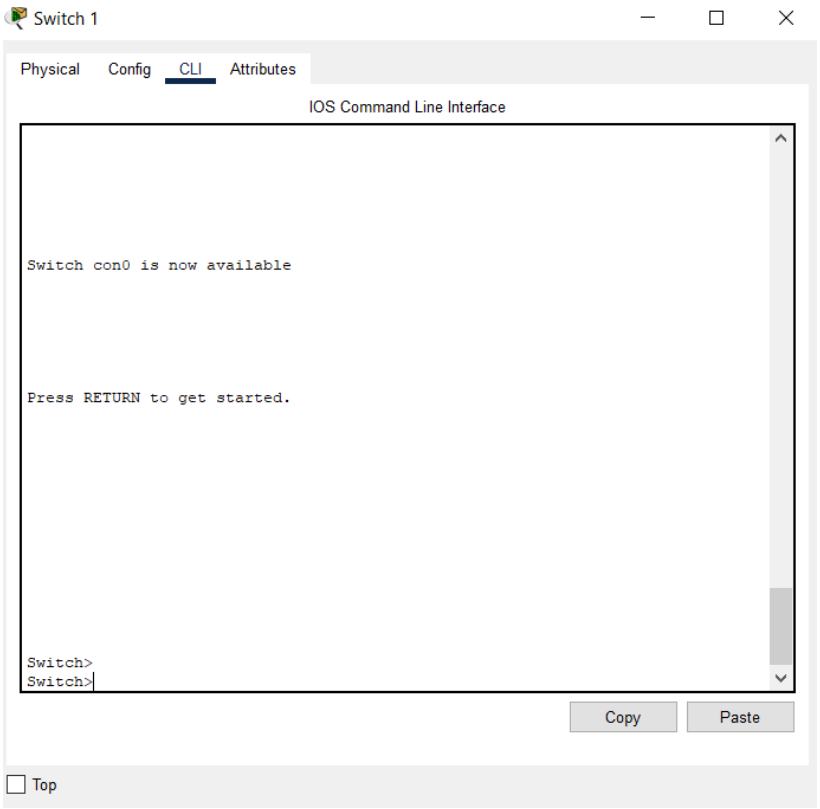


Figure 3. 3: interface CLI

Nous allons lancer des séries des configurations sur tous les équipements du réseau. Dans ce qui suit, tout en montrant des exemples de chaque configuration.

En commence par la Création des VLANs :

#Enable

#Config terminal

#Vlan 10

#Name SERVER

#Exit

#Exit

La fonction de cette commande et de créer et nommer les VLANs et cree le pro La (figure III.10) montre les commandes :

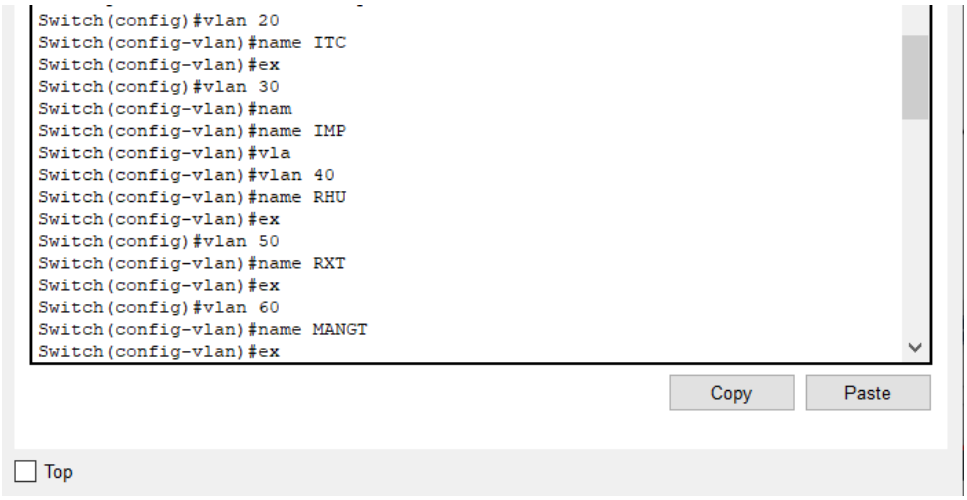


Figure 3. 4: Création des VLANs sur Multilayer Switch 01.

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

1) Configuration des mots de passe.

2) Configuration de VTP.

3) Configuration des VLANs

4) Configuration des interfaces

5) Configuration de Spanning-Tre

6) Insertion des ACL

7) configuration la sécurisation de DHCP snooping

8) configuration la sécurisation Dynamic ARP Inspection (DAI)

9) configuration la sécurisation port Security

10) configuration la sécurisation Storm control

3.1. Configuration des mots de passe :

a) Sécuriser : l'accès à la ligne de console, l'accès au mode privilégié, Configurez un mot de passe chiffré pour sécuriser l'accès au mode privilégié, Chiffrement du mot de passe :

- Notre choix c'est porté sur « st0000 » comme mot de passe via console, l'exemple que nous prendrons est "Multilayer Switch 01
- Pour sécuriser l'accès au mode privilégié, nous avons choisi le mot de passe « st00000 ».
- Le mot de passe d'activation (enable) doit être remplacé par le mot de passe secret chiffré à l'aide de la commande # enable secret. Nous avons choisi « st000000 » en tant que mot de passe secret actif.

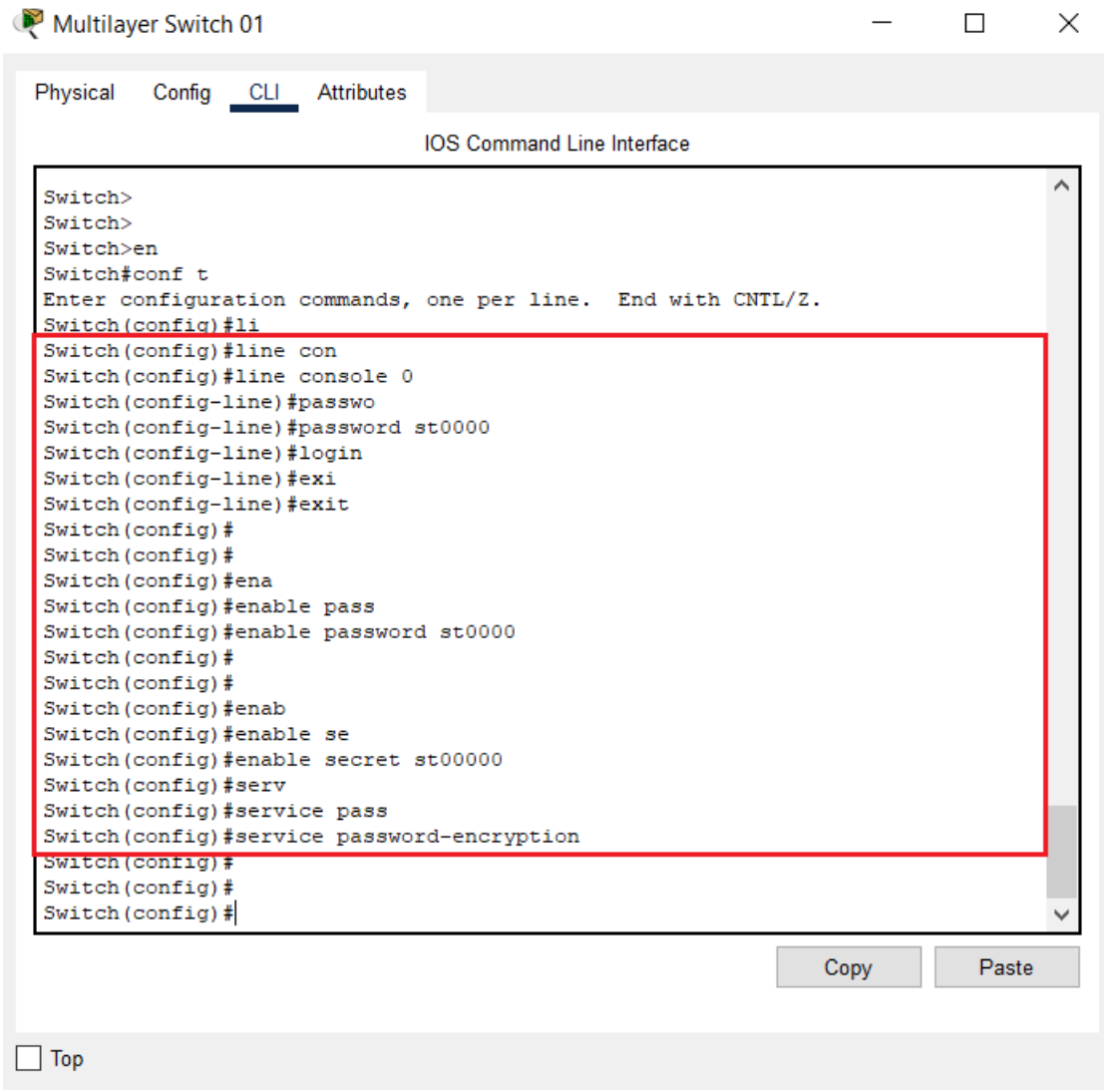


Figure III.10: Sécuriser l'accès à la ligne de console, l'accès au mode privilégié,

Figure 3. 5: Sécuriser l'accès à la ligne de console, l'accès au mode privilégié,

Configurez un mot de passe chiffré pour sécuriser l'accès au mode privilégié, Chiffrement les mots de passe

Remarque : Est bien sue en a configure cette configuration en les switches 1,2,3,4,5

b) Sécuriser l'accès à distance avec protocole SSH :

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

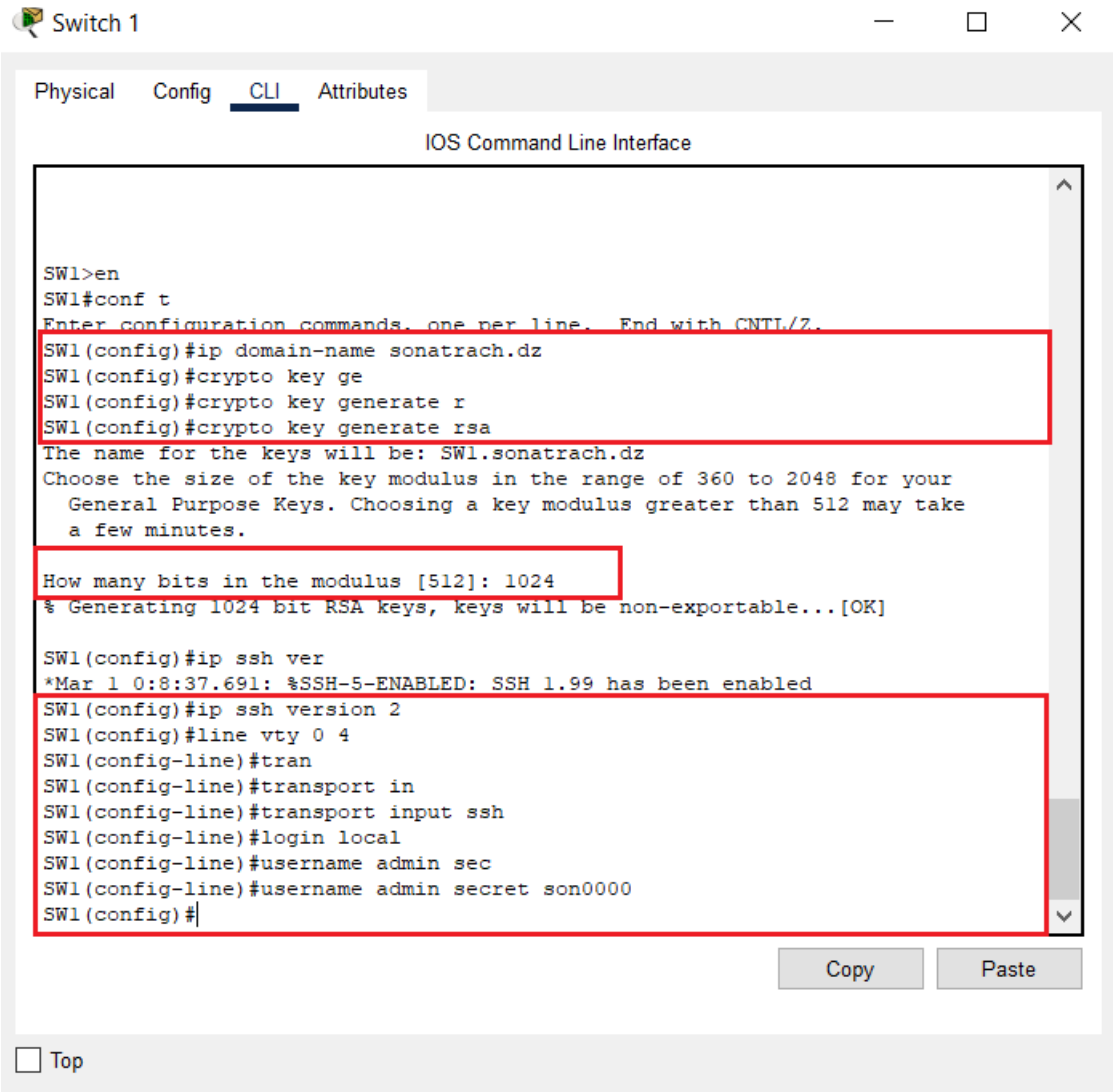


Figure III.11 : Sécuriser l'accès SSH sur un switch.

Figure 3. 6: Sécuriser l'accès SSH sur un switch.

Remarque : Est bien sue en a configure cette configuration en les switches 1,2,3,4,5

3.2. Configuration du protocole VTP :

Maintenant nous allons configurer le protocole VTP, le Multilayer Switch 01 sera configuré en mode serveur à l'aide de la commande

#VTP mode server

#VTP domaine sonatrach

#vtp password

(Figure III.12), (Figure III.13) montre la commande de configuration de protocole vtp sur le Switch-coeur1 et les switchs d'accès en **#vtp mode client**. Nous prendrons le switch admission comme exemple (III.14), la même chose sera appliquée aux autres commutateurs.

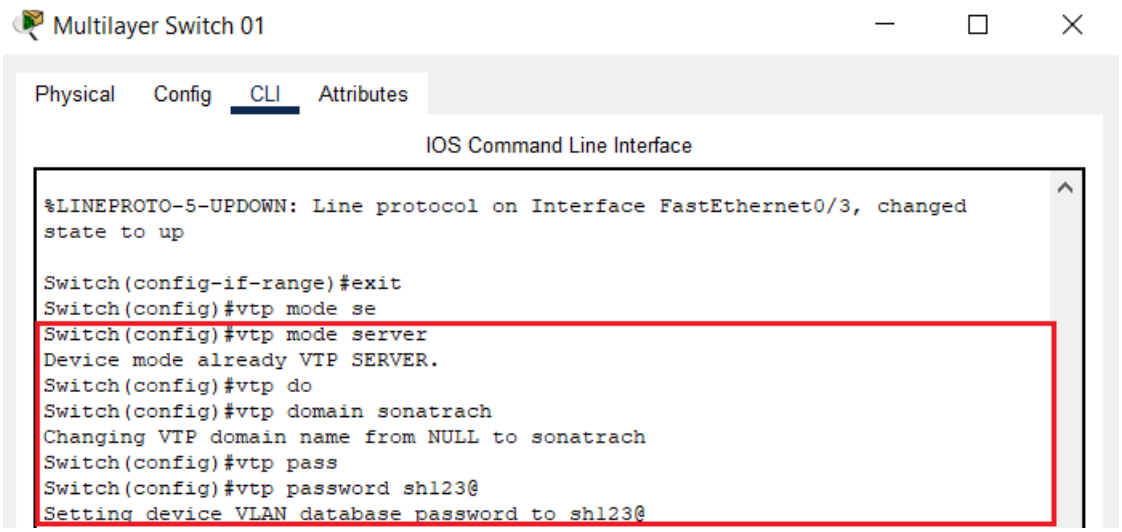


Figure III.12 : active le mode VTP serveur le Multilayer Switch 01

Figure 3. 7: active le mode VTP serveur le Multilayer Switch 01

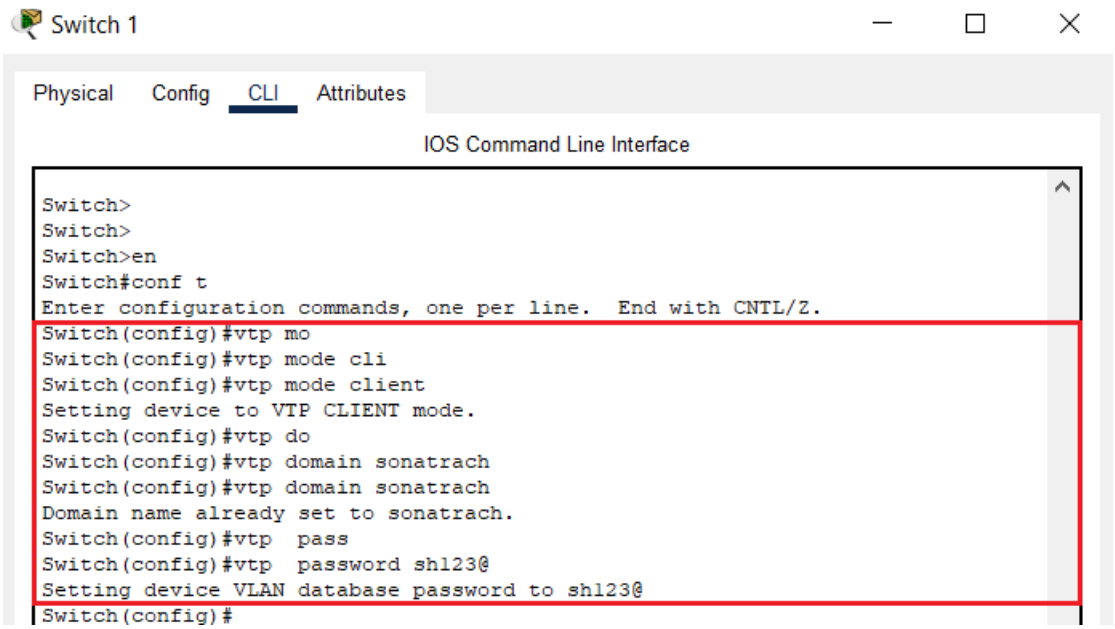


Figure III.13 : active le mode VTP client en switch 1 de ITC

Figure 3. 8: active le mode VTP client en switch 1 de ITC

Et bien sûr en a activé le mode VTP mode client en les switches 2,3,4,5 les switches de ITC, IMP, RXT, RUH, MANGT.

Remarque : Est bien sue en a configure cette configuration en les switches 1,2,3,4,5

3.3 Configuration des VLANs :

Dans cette partie de configuration nous allons attribuer les adresses IP de passerelle pour chaque VLAN au niveau du Switch-coeur1 et, nous allons également utiliser la commande « IP helper » pour donner l'adresse du serveur DHCP à chaque VLAN et la commande « ip adresse » pour donner les VLANS des adresse ip. Comme illustré dans la figure suivante

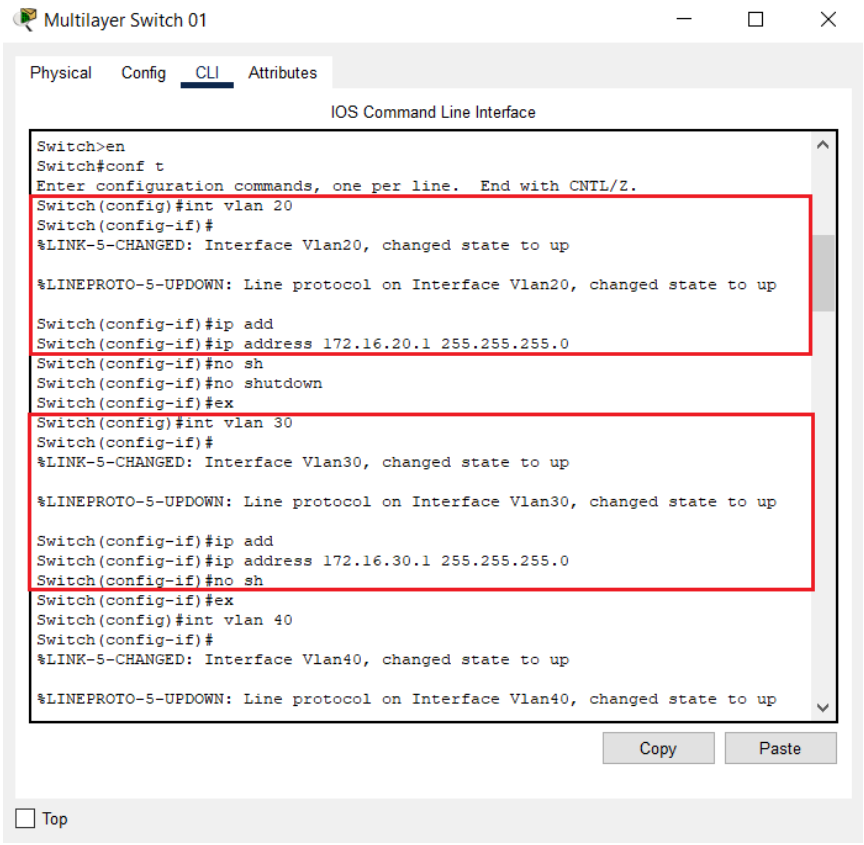


Figure III.14 : donner les VLANS des adresse ip

Figure 3. 9: donner les VLANS des adresse ip

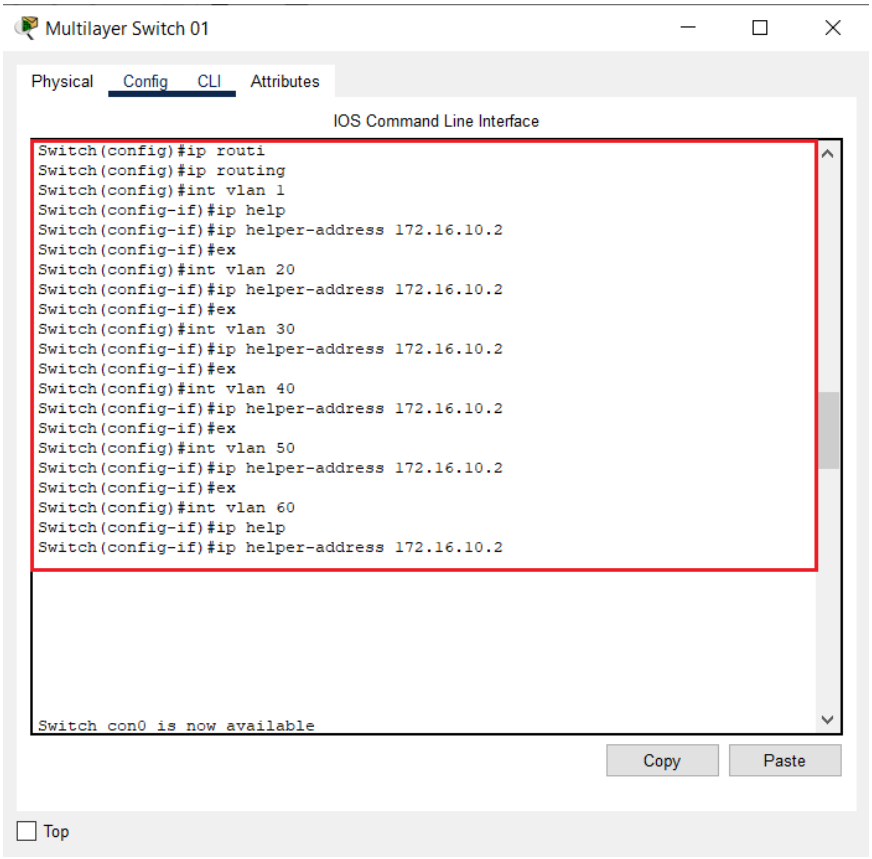
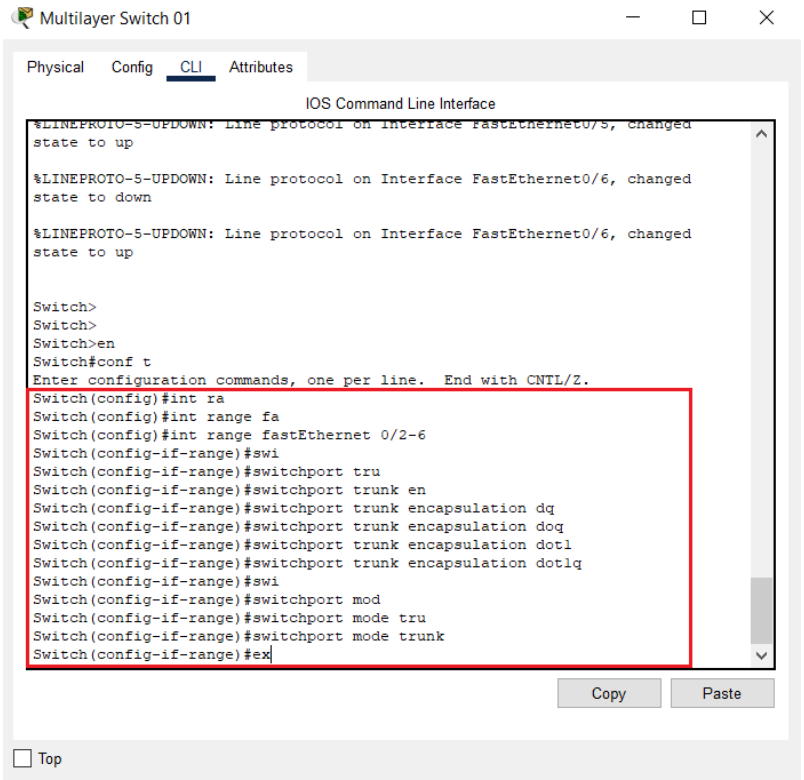


Figure 3. 10: donner les VLANS des adresse ip halper

3.4. Configuration des interfaces : Nous allons configurer les liaisons entre les commutateurs en mode truck et active mode encapsulation et mode IP config



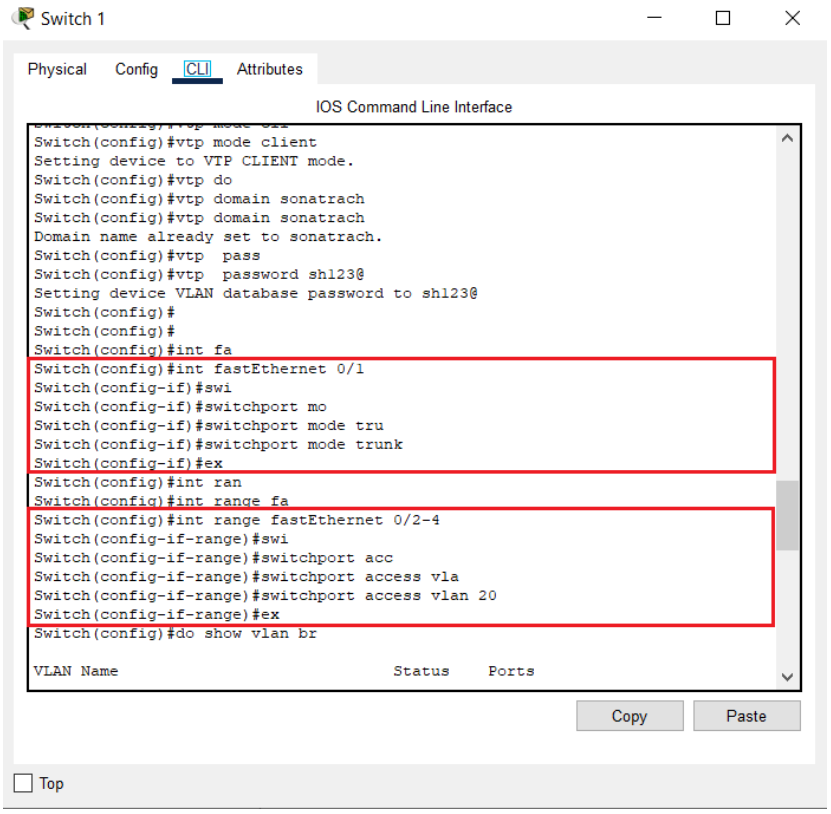


Figure 3. 11: Activation de mode encapsulation au niveau du Multilayer Switch 01 et mode trunk.

Remarque : Est bien sûr en a configure cette configuration de mode trunk pour les intrefaces f0/1 des switches et switchport access vlan les switch 1,2,3,4,5

3.5. Configuration de Spanning-Tree :

Maintenant nous allons configurer le protocole Spanning-Tree pour définir le Switch-coeur1 en tant que switch racine par la commande swivante : #spanning-trre vlan 1 20 30 40 50 60 root primary

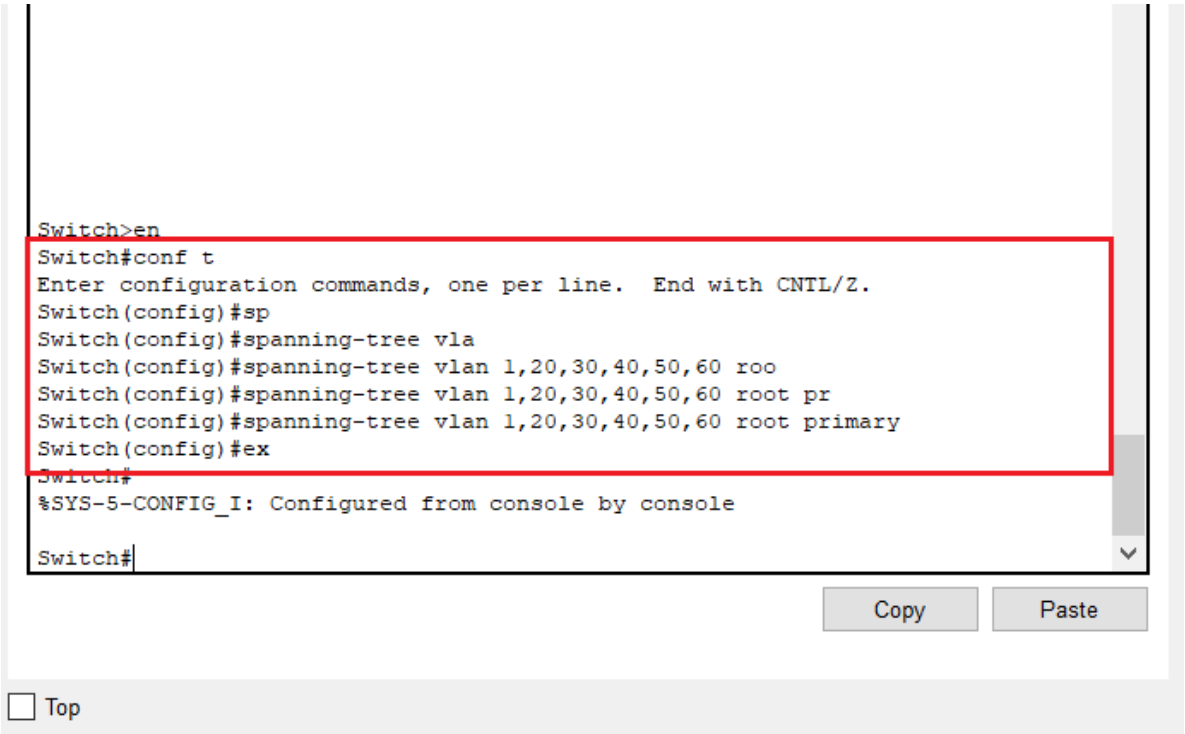


Figure 3. 12: Configuration de Spanning-Tree Multilayer Switch 01.

3.6. Insertion des ACL :

Nous allons maintenant utiliser les listes des contrôles d'accès afin de limiter la communication entre certains VLANs à l'aide de la commande suivante :

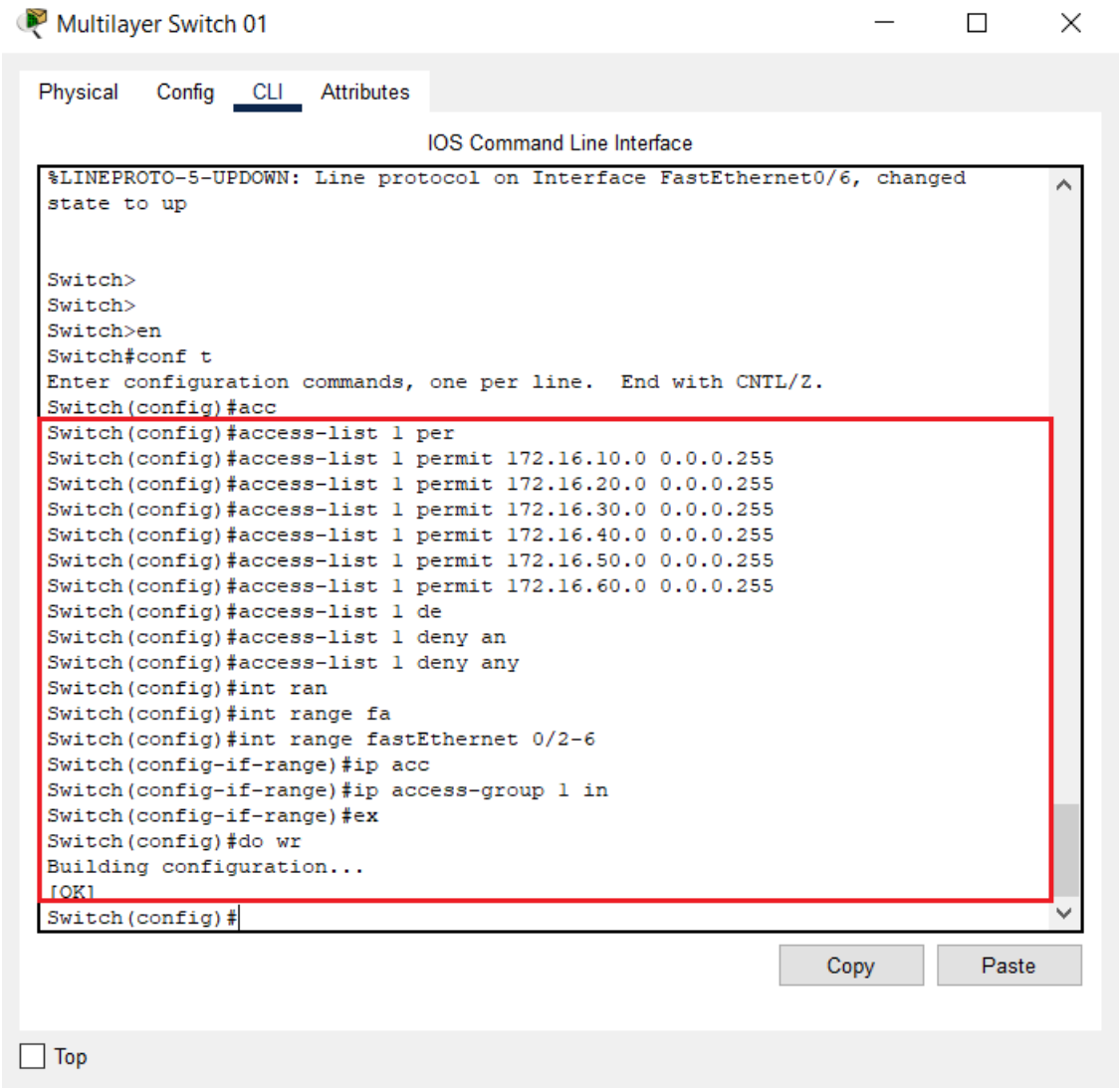


Figure 3. 13: Création des ACL Sur le SWCORE1

3.7 Configuration les serveur DHCP/FTP/DNS/HTTP :

Dans cette étape de configuration nous allons configurer le serveur DHCP et les PC et imprimante pour une attribution automatique d'adresses IP et nous allons configurer aussi le serveur FTP qui permettre depuis un PC de copier des fichiers vers un autre PC du réseau, ou encore de supprimer ou de modifier des fichiers et nous allons configurer Le serveur DNS est utilisé pour résoudre un nom de machine FQDN en adresse IP. Cela nous permet de réussir à trouver et se connecter à des sites et services Internet et nous allons configurer http/s pour accéder les navigateur Web et pour établir sécuriser la transmission avec le web server.

3.7.1) Configuration DHCP :

Pour configurer le serveur DHCP, nous devons créer des pools d'adresses qui comporteront les noms des VLANs tout en introduisant les gateway et le nombre maximum d'adresses, ensuite nous allons attribuer une adresse IP statique au serveur DHCP, les figures suivantes montrent les étapes de configuration

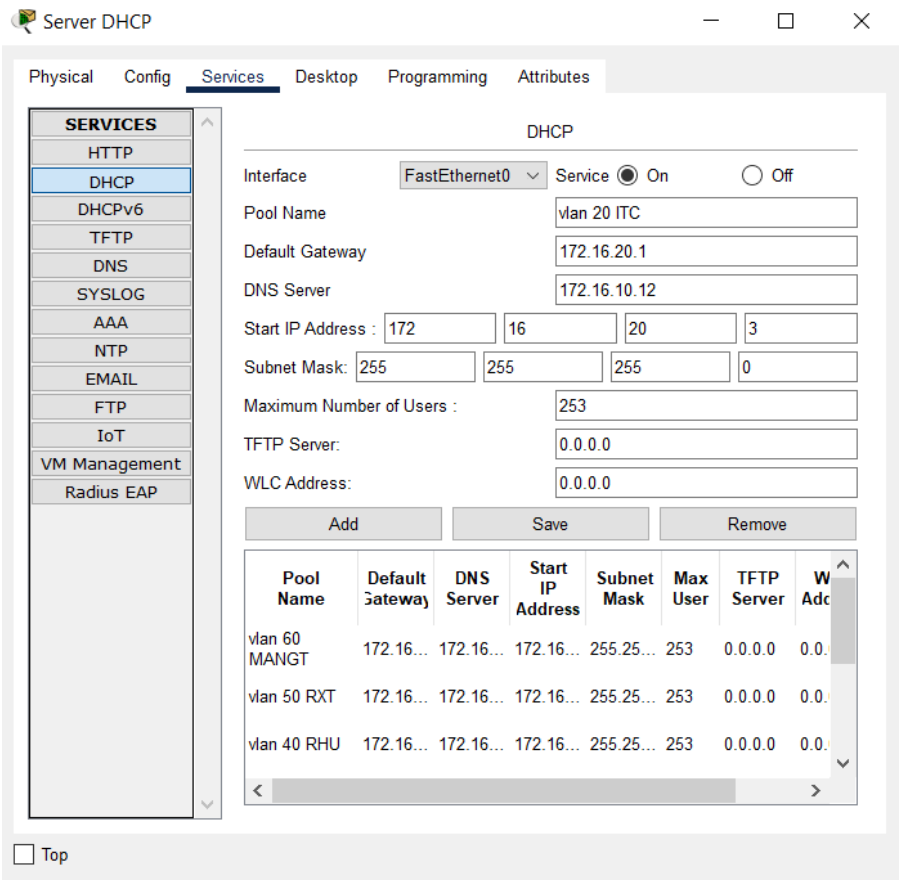


Figure 3. 14: Création des Pool d'adresses

Configuration PC et les imprimantes :

La configuration des PC passe par l'attribution d'une adresse IP dynamiquement comme le montre la figure suivante.

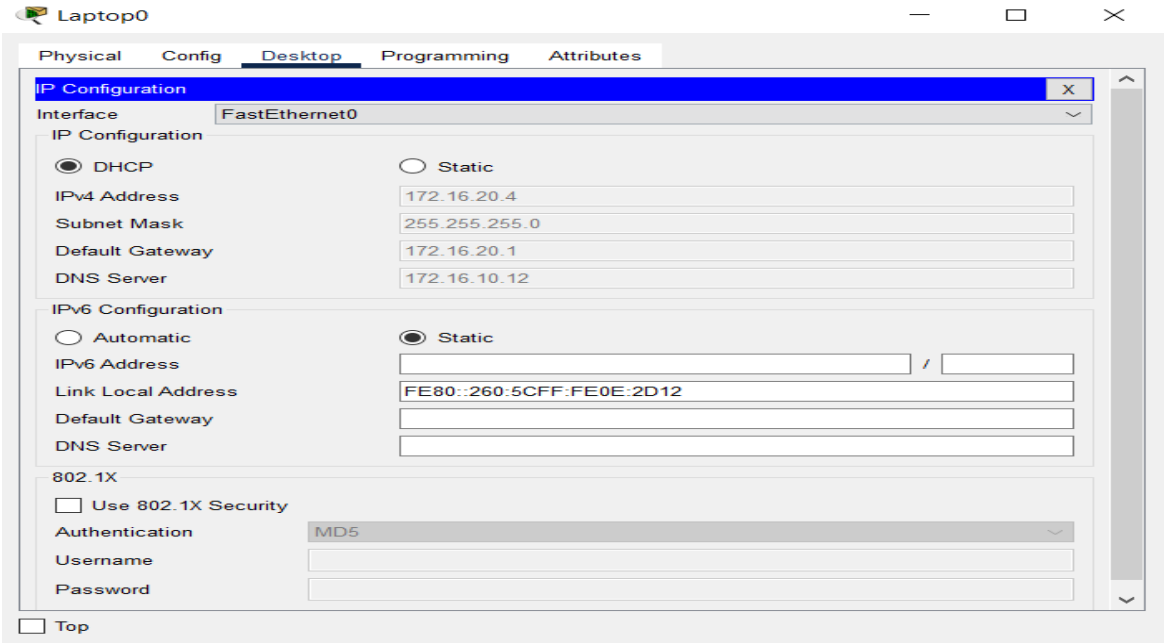


Figure 3. 15: Attribution dynamique d'une adresse à un PC.

3.7.2) Configuration FTP

Pour configurer le serveur FTP, nous allons attribuer une adresse de connexion IP statique au serveur FTP ensuite nous devons créer un identifiant et le mot de passe et en active les droits d'accès. Les figures suivantes montrent les étapes de configuration.

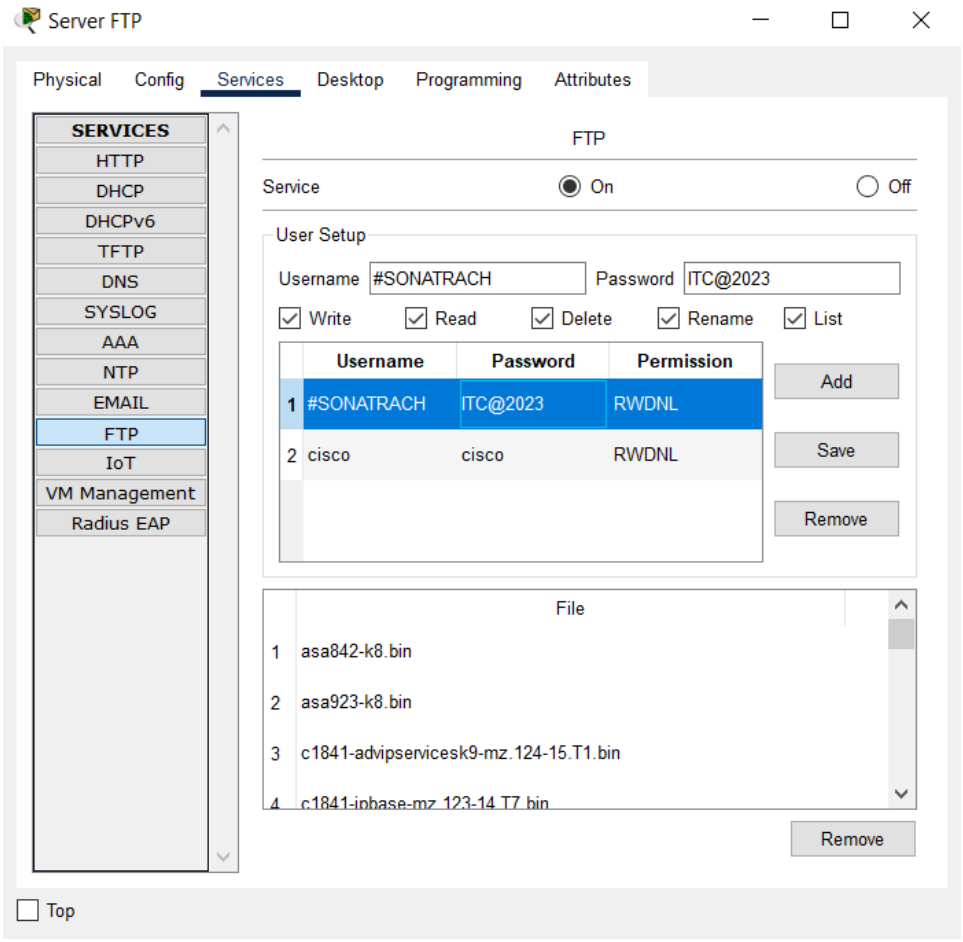


Figure 3. 16: Création d'identifiant.

3.7.3) Configuration DNS :

Pour configurer le serveur DNS, nous allons attribuer une adresse de connexion IP statique au serveur DNS ensuite Sur le serveur en clique sur l'onglet Services et choisissez le service DNS en active le service (clique sur ON) et tapez le nom des enregistrements de ressources de votre page Web, dans mon cas est www.sonatrach.dz tapez dans le champ Adresse adresse IP de notre serveur DNS 172.16.10.12 et cliquez sur le bouton Ajouter, Les (figures III.24)suivantes montrent les étapes de configuration.

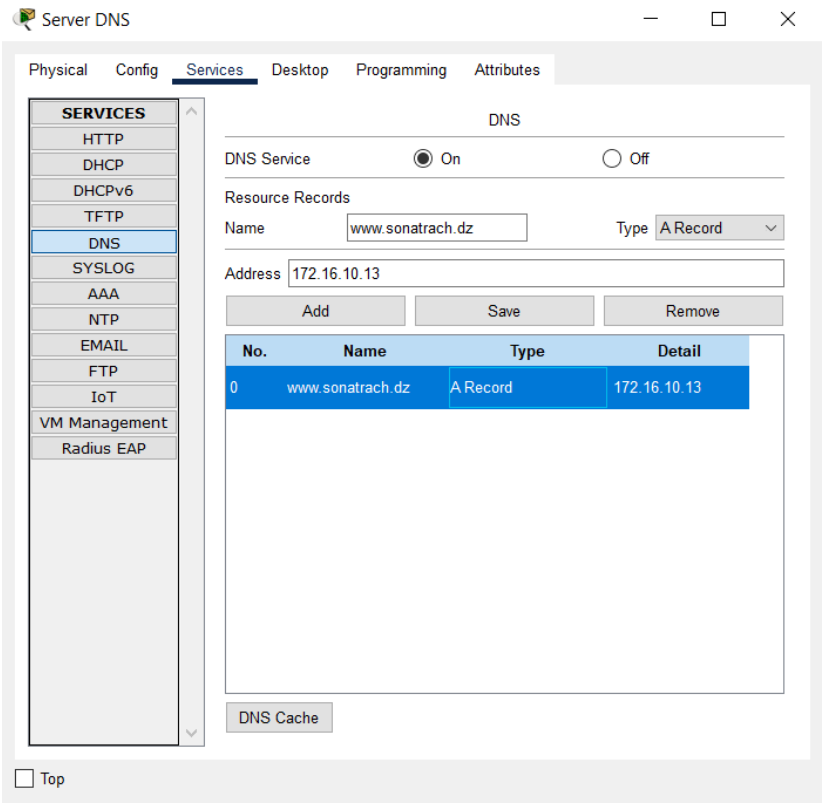


Figure 3. 17: Création ressources de page web.

3.7.4) Configuration HTTP :

Pour configurer le serveur HTTP, nous allons attribuer une adresse de connexion IP statique au serveur HTTP ensuite Sur le serveur en clique sur l'onglet Services et choisissez le service HTTP et HTTPS en active les service (clique sur ON) ensuite nous devons créer un nouveau index(.html), Les figures suivantes montrent les étapes de configuration.

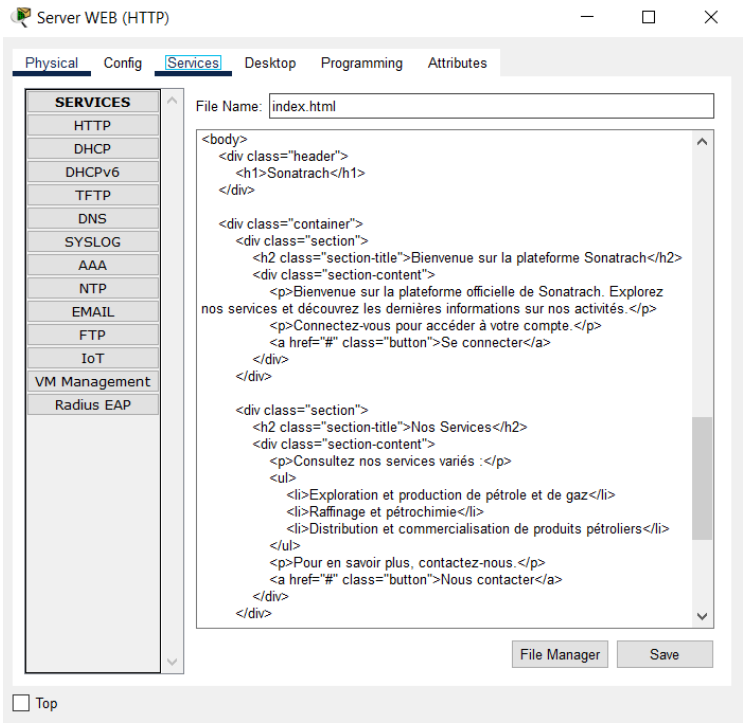


Figure 3. 18: Création index.html

3.7.5) serveur Serveur d'authentification RADIUS :

Pour configure le serveur radius en a entre en service de serveur et click sur AAA âpre en à Remplir les formules de network configuration (cline name, client ip, secret (key)…) âpre en crier des user name et passwrod pour notre users pour chaque vlan.

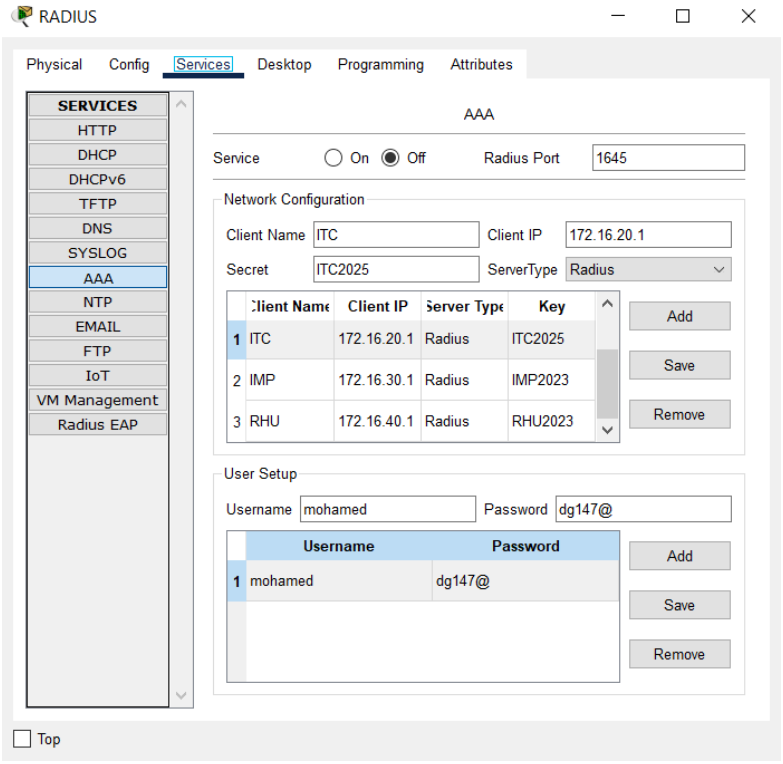


Figure 3. 19: Configuration de serveur radius

- Le prencipe comment ça marche de Serveur d'authentification RADIUS

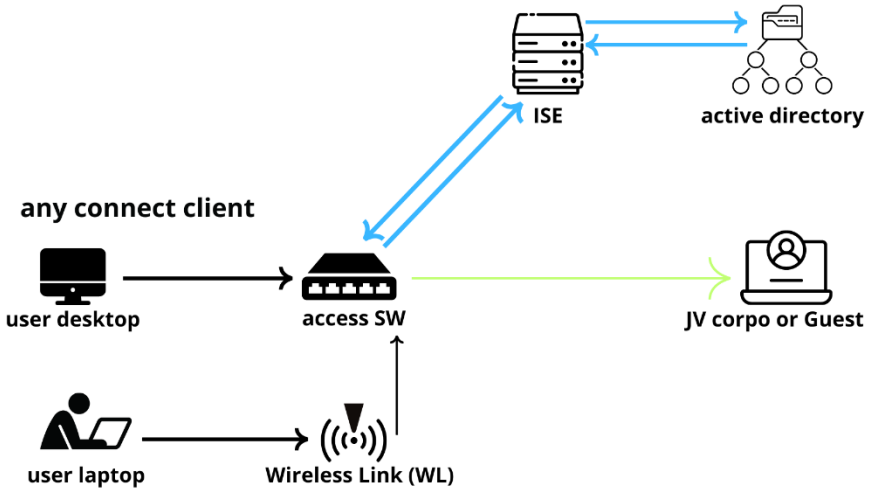


Figure 3. 20: le presncipe de serveur radius

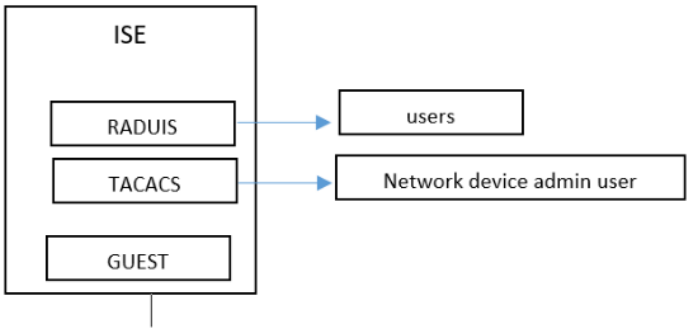


Figure 3. 21: serveur ISE (référence à l'Identity Services Engine)

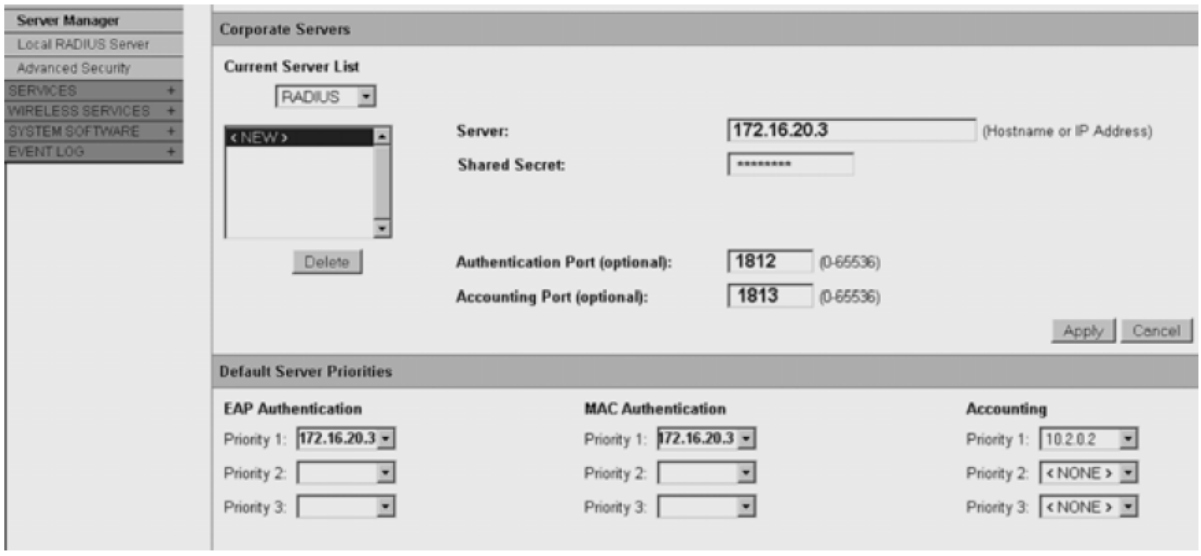


Figure 3. 22: Déclaration des serveurs Radius dans une borne Cisco

4) configuration la sécurisation de DHCP snooping :

Nous allons maintenant configure DHCP snooping et DHCP limite pour protecte notre réseau contre les attaques de DHCP spoofing et DHCP Discover packet.

Pour configurer le DHCP snooping sur les commutateurs ITC, IMP, RHU, RXT et MANGT à l'interface FastEthernet 0/1, vous pouvez utiliser les étapes suivantes :

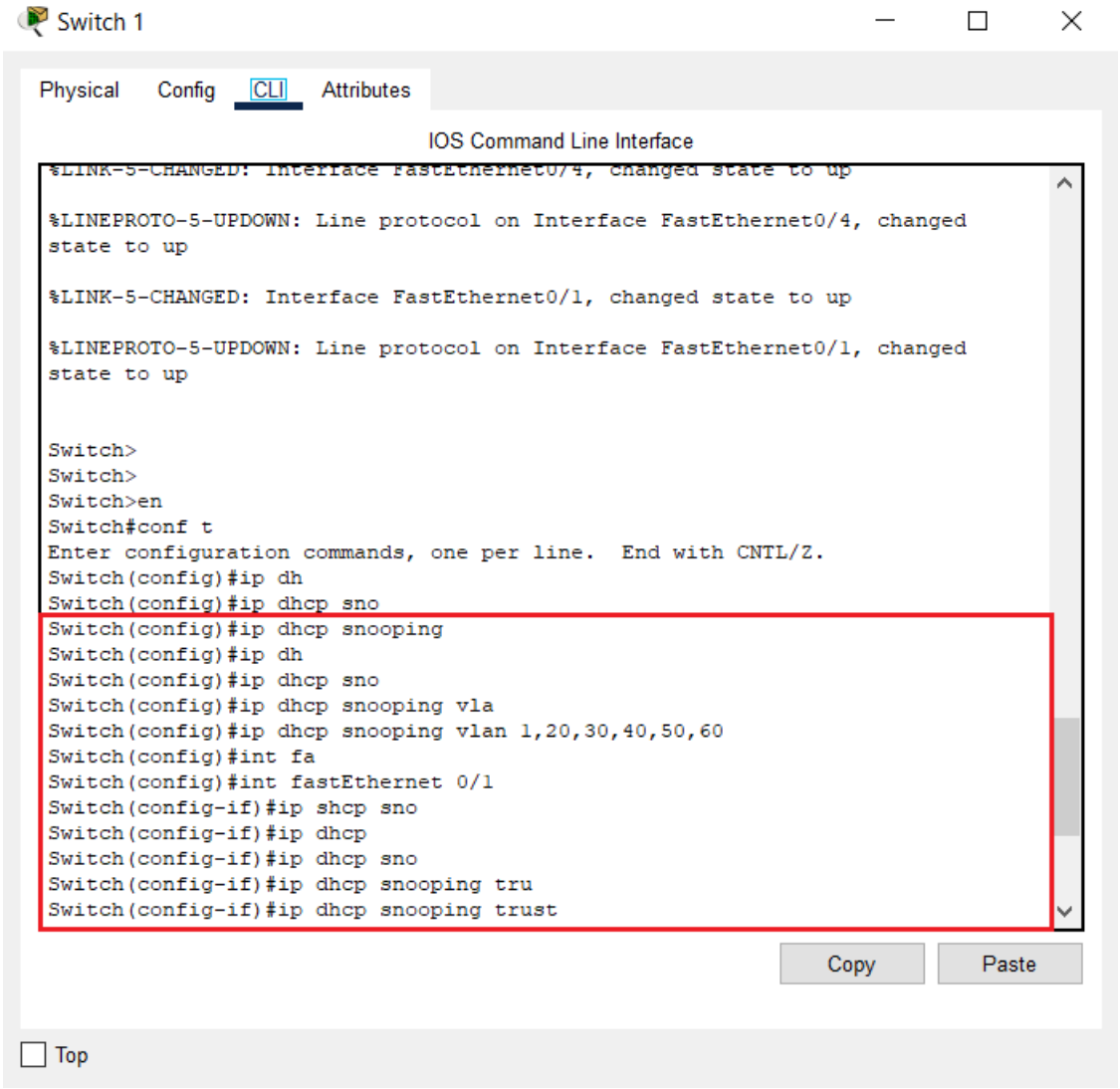
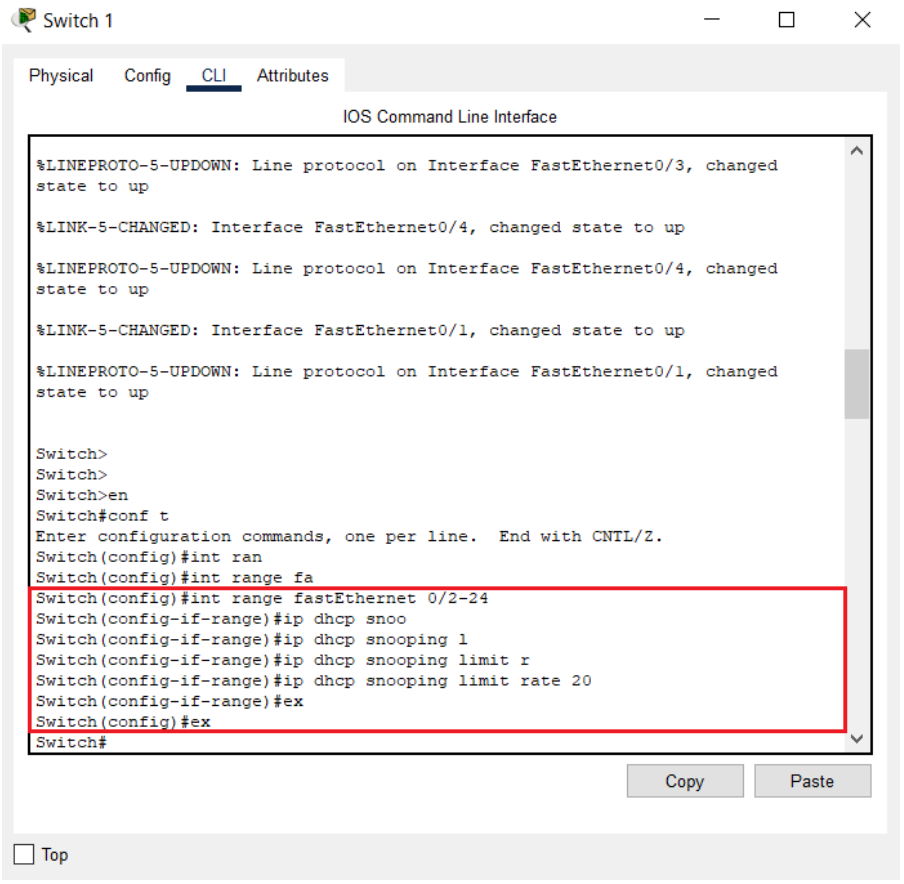


Figure 3. 23: configuration de DHCP snooping.

Nous activons cette configuration de dhcp snooping et DHCP discover packet sur tous les switches de ITC, IMP, RHU, RXT et MANGT.



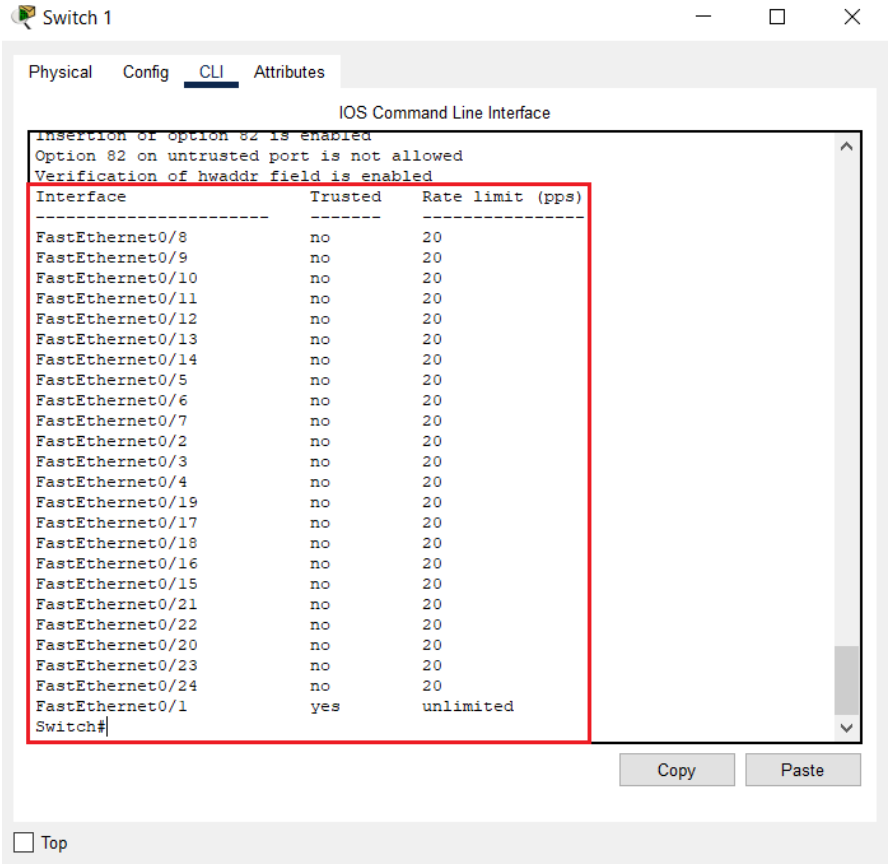


Figure 3. 24: active DHCP snooping limit et show les interface

5) configuration la sécurisation Dynamic ARP Inspection (DAI) :

Nous allons maintenant configure Dynamic ARP Inspection (DAI) pour protecte notre réseau contre l'attaque d'ARP spoofing

Pour configurer Dynamic ARP Inspection (DAI) sur les commutateurs ITC, IMP, RHU, RXT et MANGT à vous pouvez utiliser les étapes suivantes :

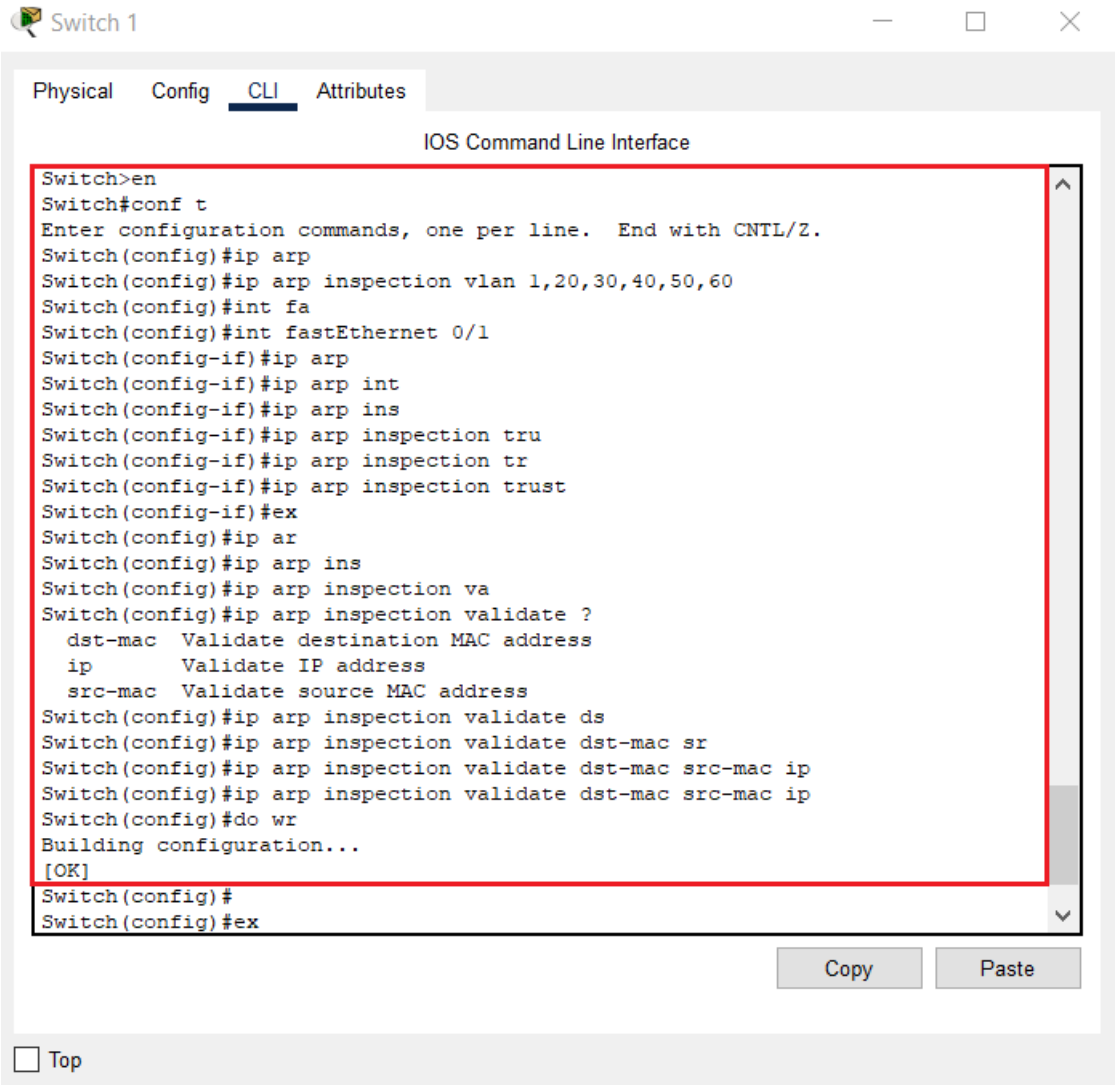


Figure 3. 25: configuration de DAI en le switch 01

Remarque :

Nous activons cette configuration de Dynamic ARP Inspection (DAI) sur tous les switches de ITC, IMP, RHU, RXT et MANGT.

6) configuration la sécurisation port Security :

Nous allons maintenant configure port Security pour protecte notre réseau contre l'attaque comme attaque MAC flooding

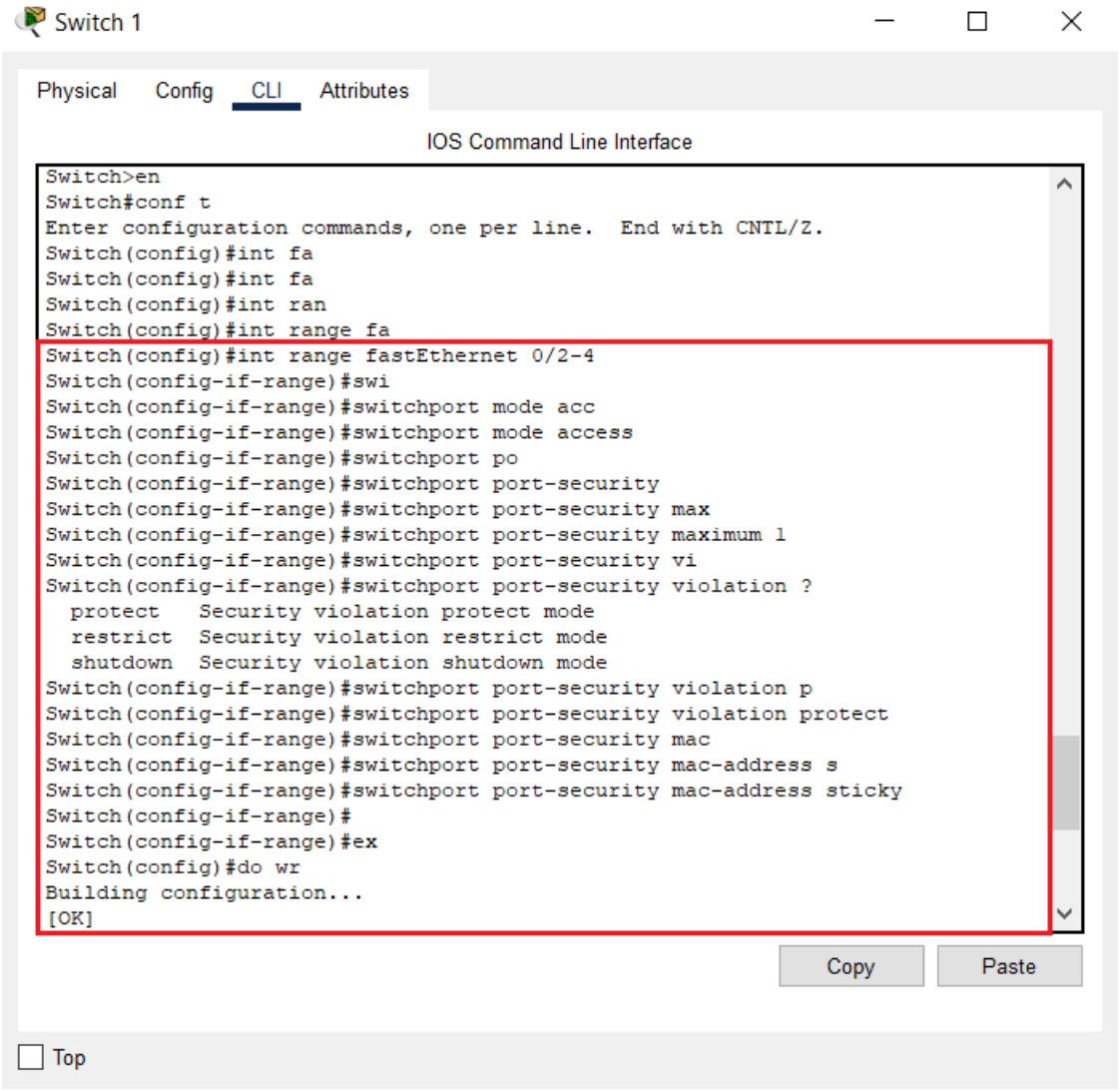


Figure 3. 26: configuration de port Security en switch 01

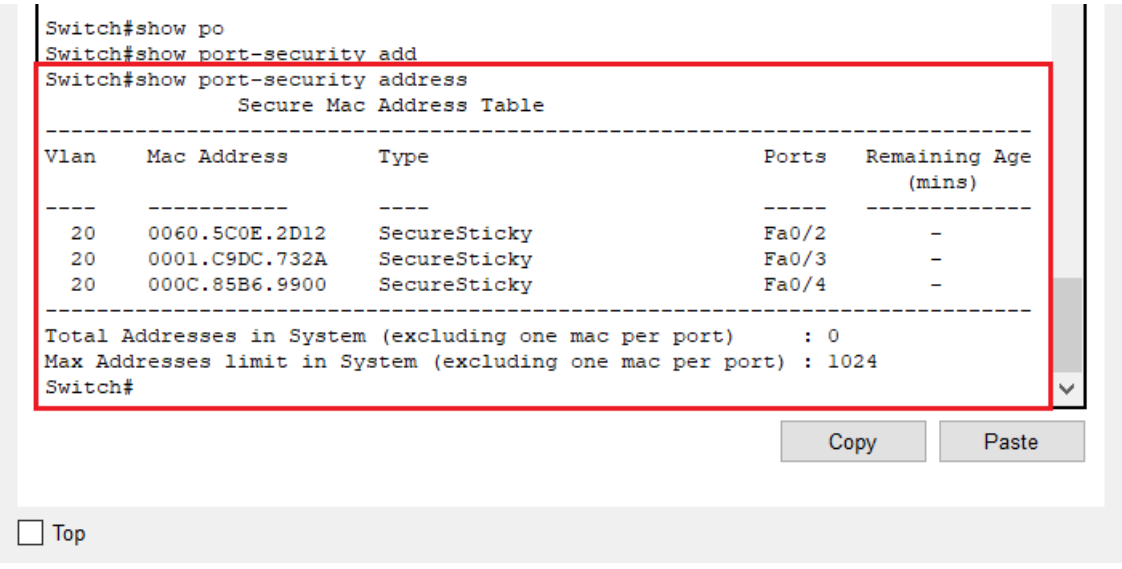


Figure 3. 27: le tableau de port Security adresse

Remarque :

Nous activons cette configuration de port Security sur tous les switches de ITC, IMP, RHU, RXT et MANGT

7) configuration la sécurisation Storm control :

Nous allons maintenant configure Storm control pour protecte notre réseau contre

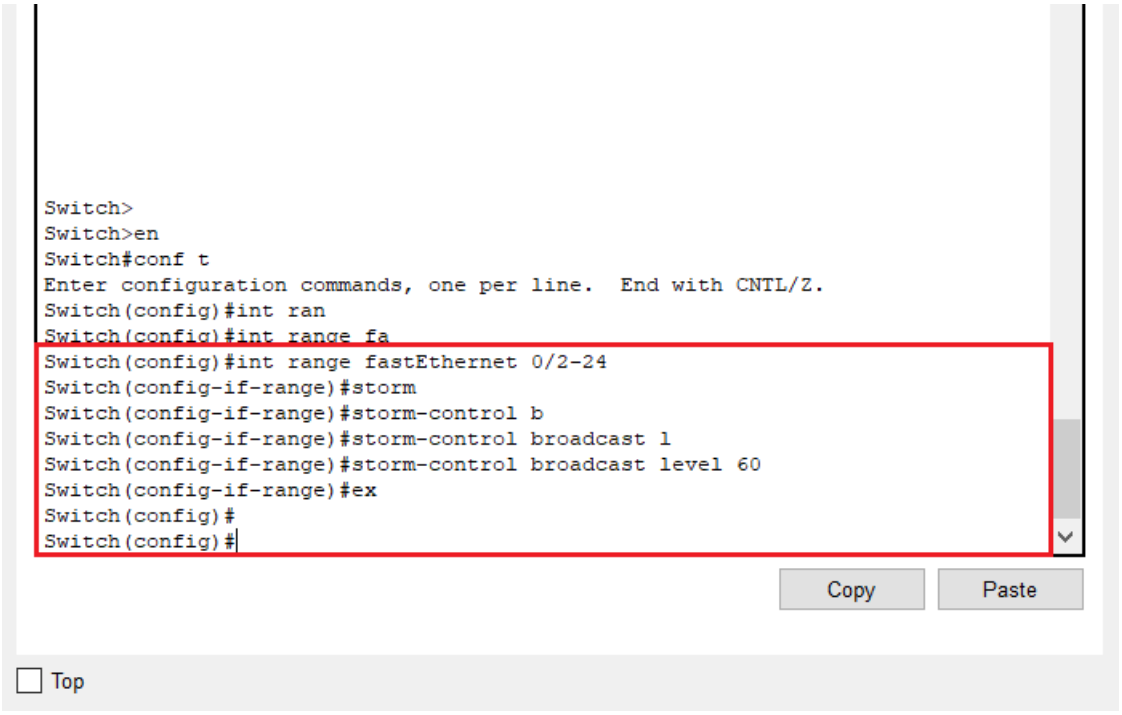


Figure 3. 28: configuration de storm control en switch ITC

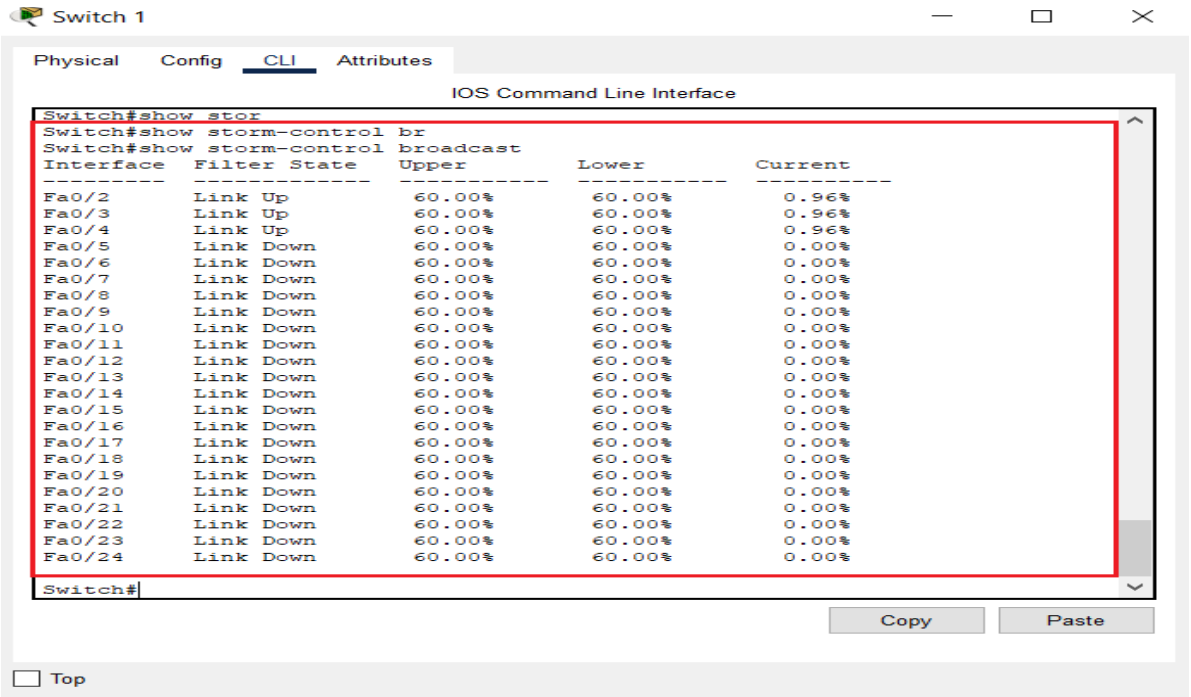


Figure 3. 29: le tableau de storm control en switch 01 de ITC

```
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#int fa 0/1
Switch(config-if)#sho
Switch(config-if)#tro
Switch(config-if)#stor
Switch(config-if)#storm-control ?
  action     Action to take for storm-control
  broadcast  Broadcast address storm control
  multicast  Multicast address storm control
  unicast    Unicast address storm control

Switch(config-if)#storm-control b
Switch(config-if)#storm-control broadcast l
Switch(config-if)#storm-control broadcast level 80 50
Switch(config-if)#storm-control broadcast level 80
Switch(config-if)#stom
Switch(config-if)#sto
Switch(config-if)#storm-control ac
Switch(config-if)#storm-control action ?
  shutdown  Shutdown this interface if a storm occurs
  trap      Send SNMP trap if a storm occurs

Switch(config-if)#storm-control action
% Incomplete command.

Switch(config-if)#storm-control action s
Switch(config-if)#storm-control action shutdown
Switch(config-if)#end
Switch#
Switch#
Switch#
*Jan  2 00:05:23.548: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch#
```

Figure 3. 30: la configuration de storm control en switch cisco 2960 real

Remarque :

Nous configurons cette configuration de storm control sur tous les switches de ITC, IMP, RHU, RXT et MANGT.

8) Test et valdiation de la configuration et sécurisation de notre réseaux :

8.1) Tests de VLAN's :

8.1.1) Test de création des VLANs et Test intra-VLAN :

Dans cette partie nous allons vérifier la création des VLANs et les communications entre tous les équipements en utilisant la commande « Ping ». Ces tests sont faits entre équipements (PC, Switchs et Switch-coeur1), inter-VLANs, Il est à noter que la commande Ping aide à vérifier la connectivité au niveau IP.

A l'aide de la commande «do show vlan brief », nous pouvons voir les différents VLANs créés. La (figure III.36) montre les VLANs crées au niveau du MULTI LAYER SWITCH 01.

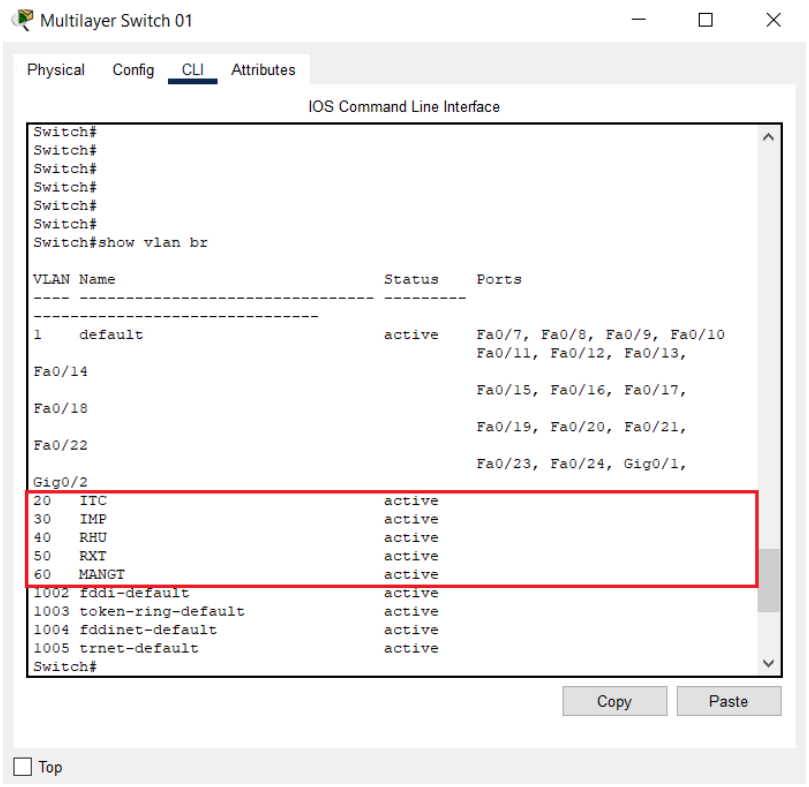


Figure 3. 31: Test de création des VLANs.

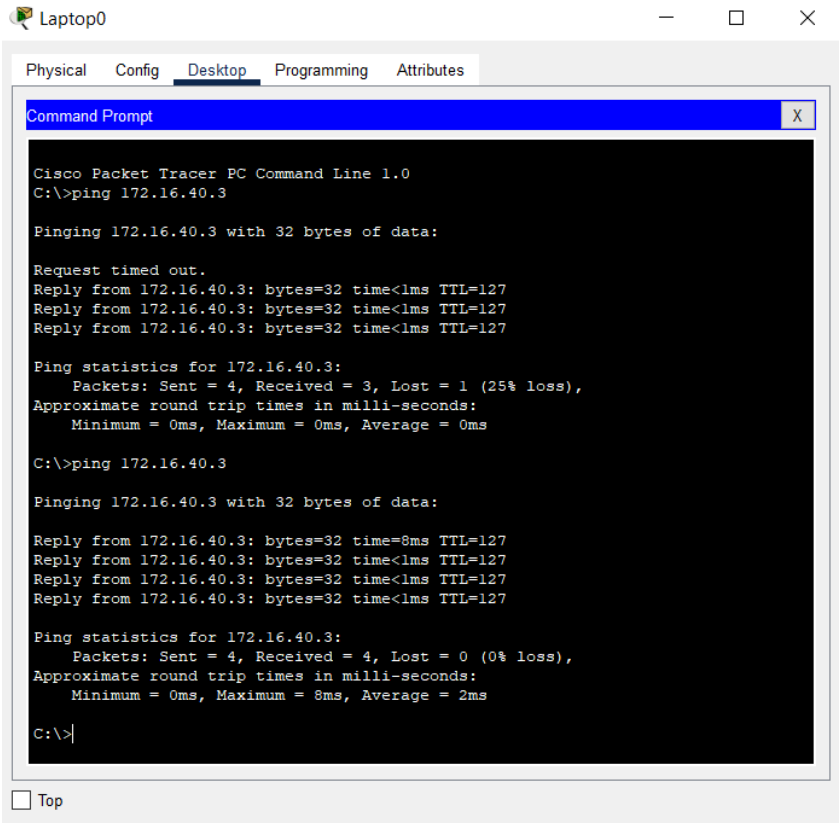
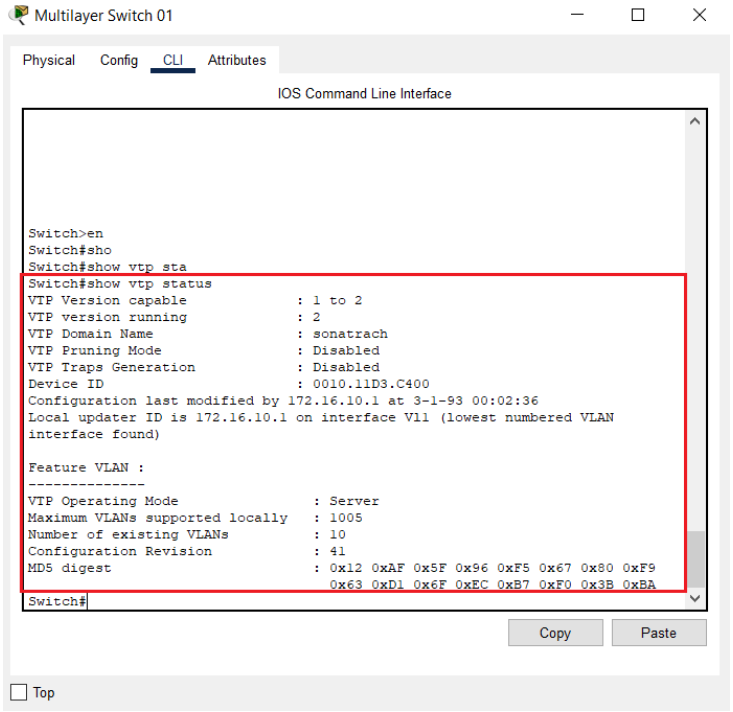


Figure 3. 32 : Ping réussi entre USER1-ITC et USER5-RHU.

8.2) Vérification de la création de VTP

- Vérification de la création de VTP server et VTP client :

A l'aide de la commande «do show vtp status », nous pouvons voir le vtp creé La (figure III.37) montre les VLANs crées au niveau du MULTI LAYER SWITCH 01, A l'aide de la commande «do show vtp status », nous pouvons voir le vtp creé La (figure IV.38) montre les VLANs crées au niveau du SW1-FIN



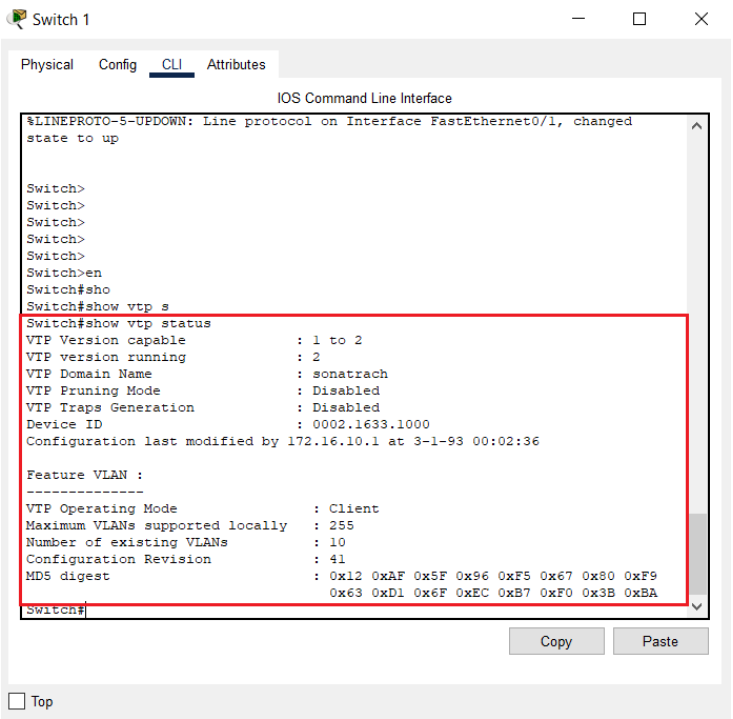


Figure 3. 33: Vérification de la création de VTP server et VTP client.

8.3) Test les serveurs FTP, WEB, DNS :

8.3.1) serveur FTP :

La vérification de server ftp À partir de l'invite de commande de l'ordinateur (USER1-ITC) envoyez un FTP au serveur à l'aide de l'adresse IP du serveur en tapant:<< ftp 172.16.10.20>> Fournissez le nom d'utilisateur (#SONTRACH) et le mot de passe (ITC@2023) pour la connexion ftp.

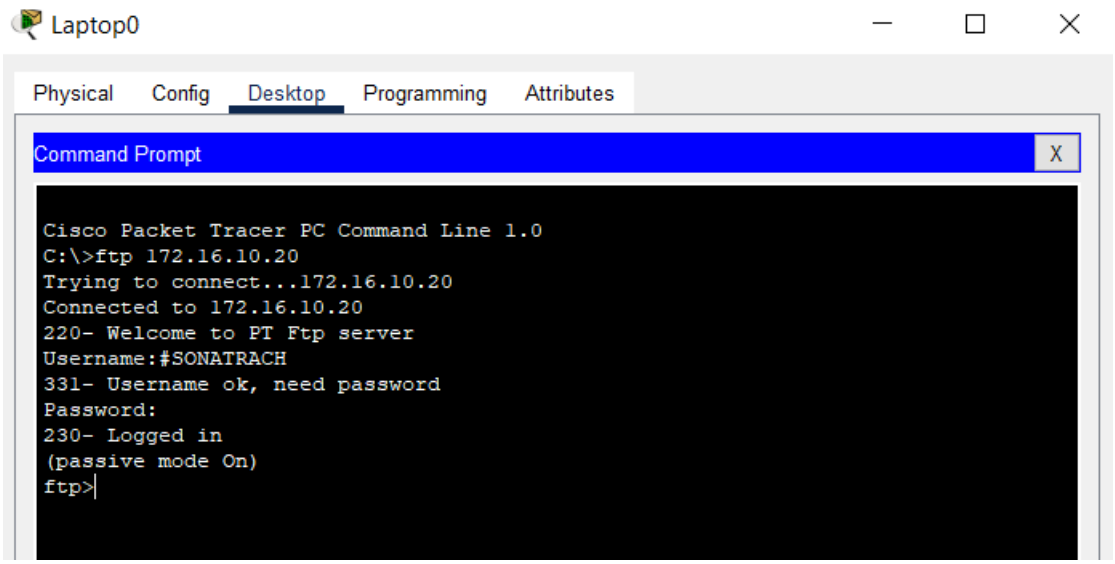


Figure 3. 34: Test de Fonctionment de Server FTP.

Créez un fichier dans PC8-IMP, puis téléchargez-le sur le serveur via FTP Pour se faire, ouvrez l'éditeur de texte dans l'ordinateur portable, créez un fichier et donnez-lui le nom de votre choix. Tapez n'importe quel texte dans l'éditeur puis enregistrez votre.

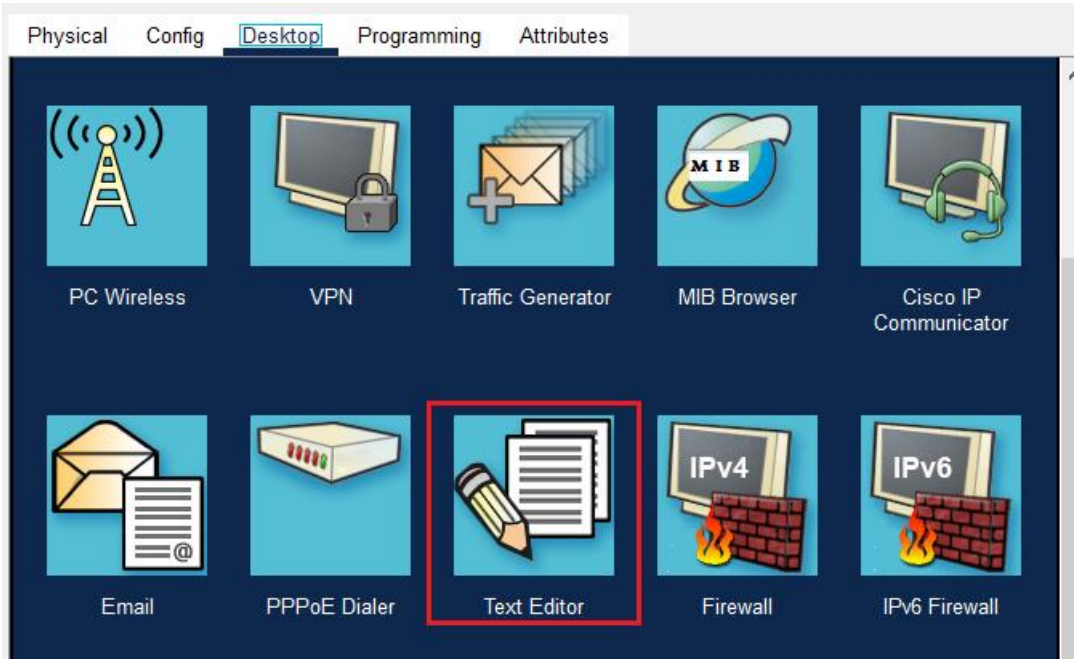


Figure 3. 35: interface de USER1-FIN.

Par exemple : test-serveur.txt.

Téléchargez maintenant le fichier de l'ordinateur portable vers le serveur via FTP.

(Une connexion FTP doit d'abord être démarrée. Mais c'est ce que nous avons fait à l'étape 3) Donc, pour effectuer un téléversement FTP, nous allons taper : put test-serveur.txt

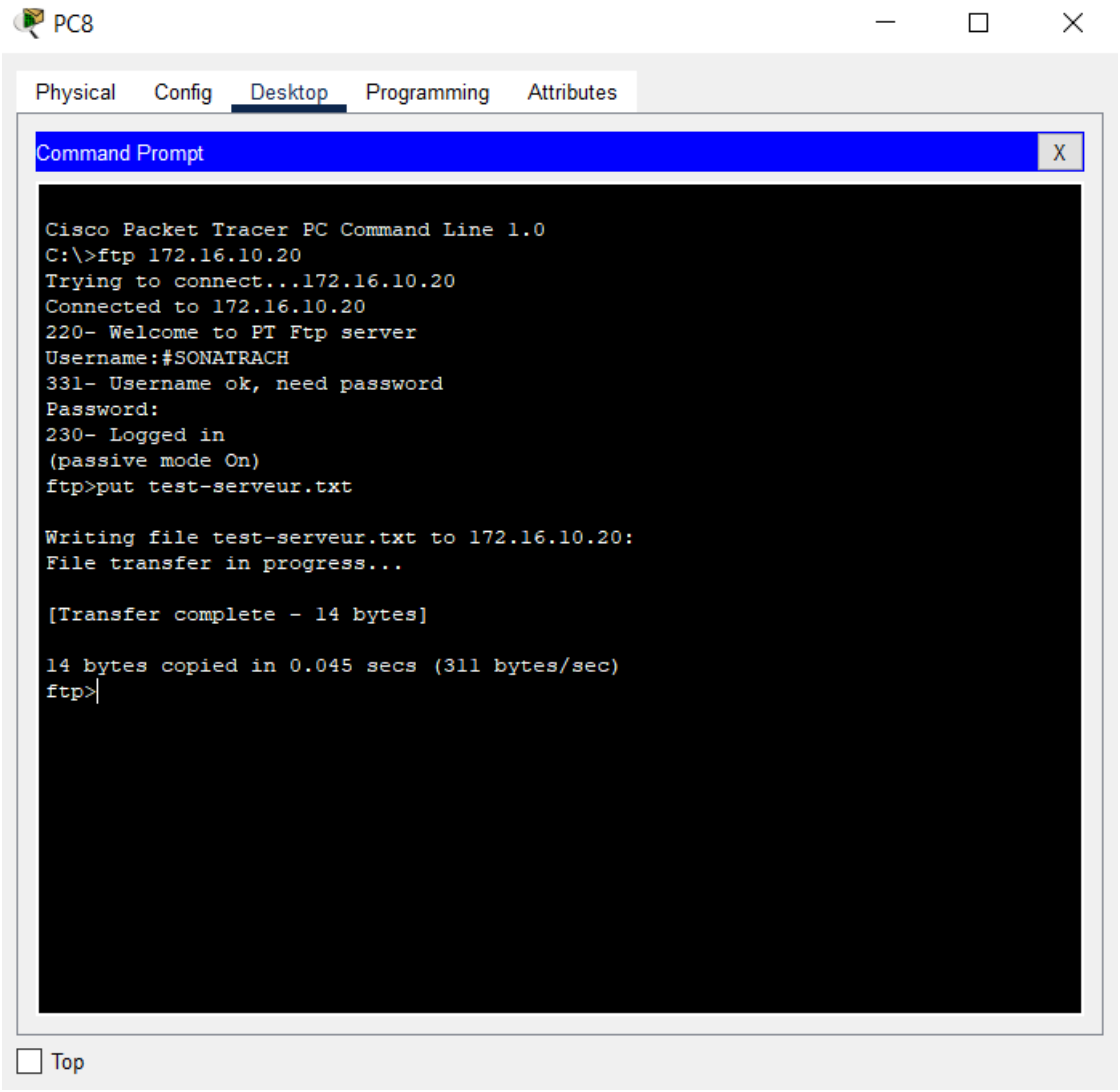


Figure 3. 36 : La Création de fichier dans PC8-IMP.

8.3.2) Test de server DNS :

La vérification de server DNS À partir de l'invite de commande de l'ordinateur (USER1-FIN) en tapant : « ping 172.16.10.20 »

Dans l'interface de l'ordinateur (USER1-ITC) en click sue le buton web browser en tapant l'adresse 172.16.10.13.

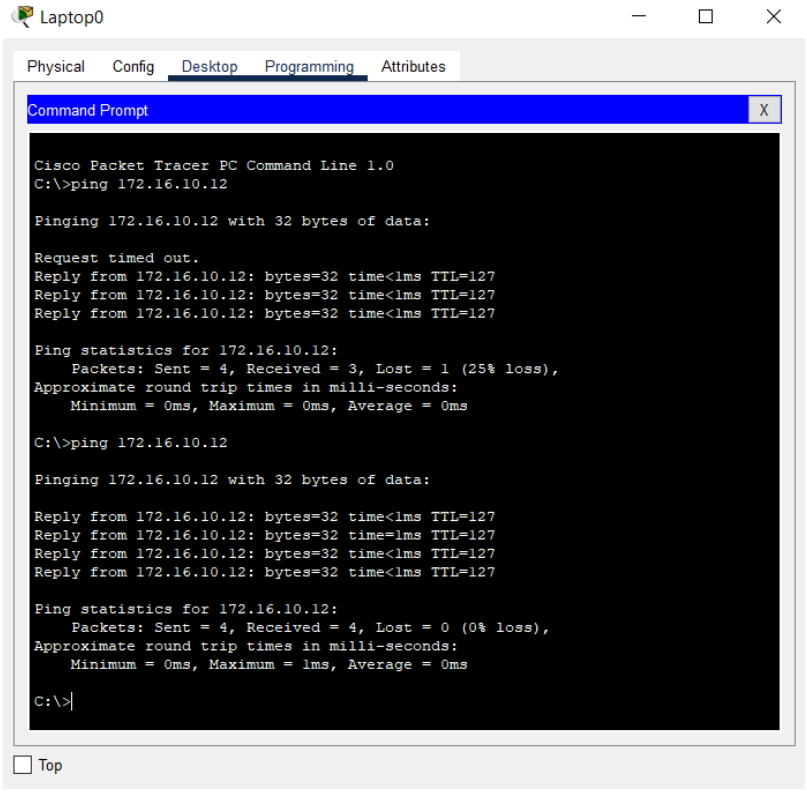


Figure 3. 37: Ping l'adresse de server DNS.

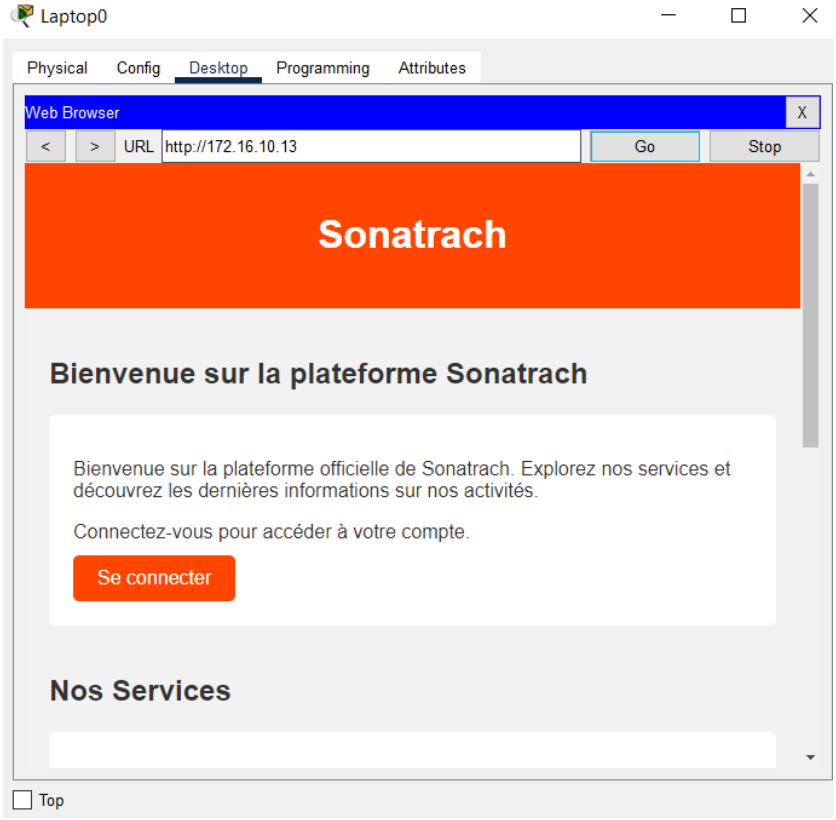


Figure 3. 38: Test web page sur USER1-ITC.

8.3.3) Test server WEB (HTTP):

La vérification de server http à partir de l'ordinateur (USER1-ITC)

Dans l'interface de l'ordinateur (USER1-ITC) en click sue le buton web browser en tapant l'adresse www.sonatrach.dz .

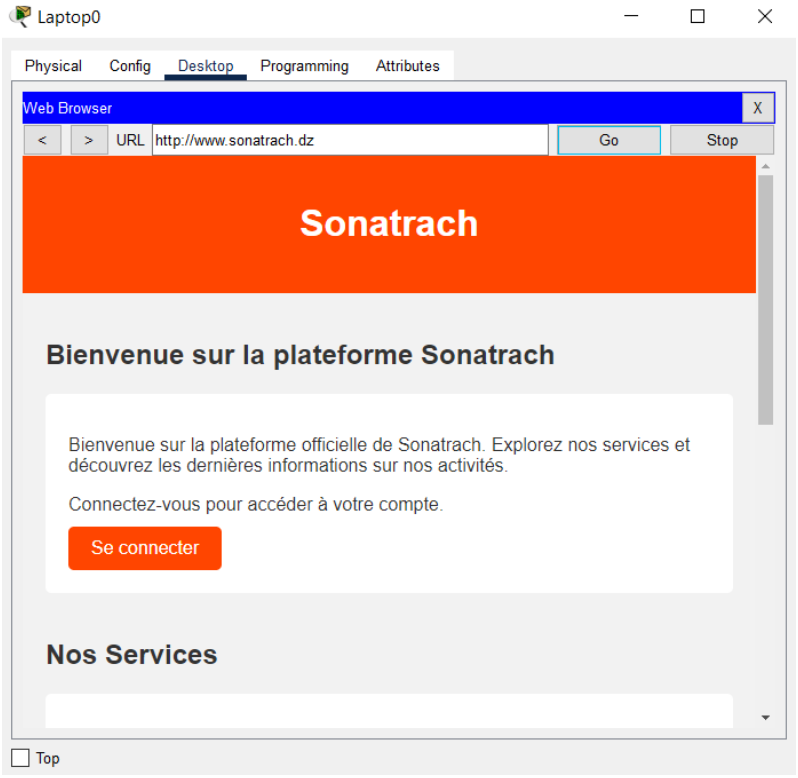


Figure 3. 39: Test l'adresse de server web(http).

8.4) Test la sécurité de DHCP snooping :

La vérification de DHCP snooping ce l attaqueur avent et âpre active la DHCP spoofing

8.4.1) Avent dative DHCP snooping:

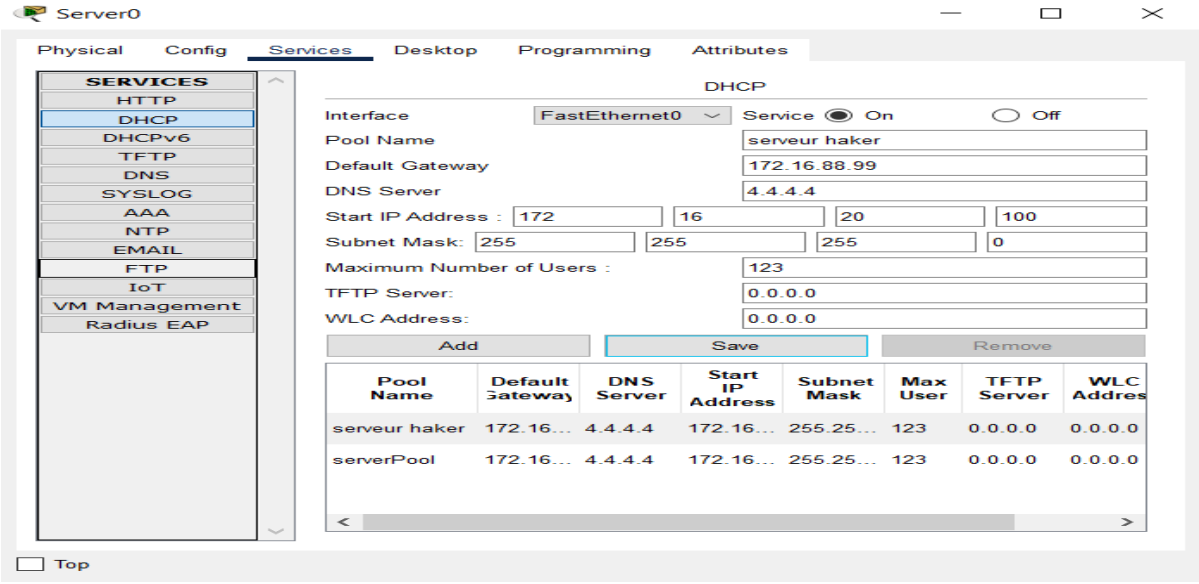


Figure 3. 40: serveur et le pool d'attaqueur

Ena remarque que default gateway et 172.16.88.99 (la address de serveur haker)

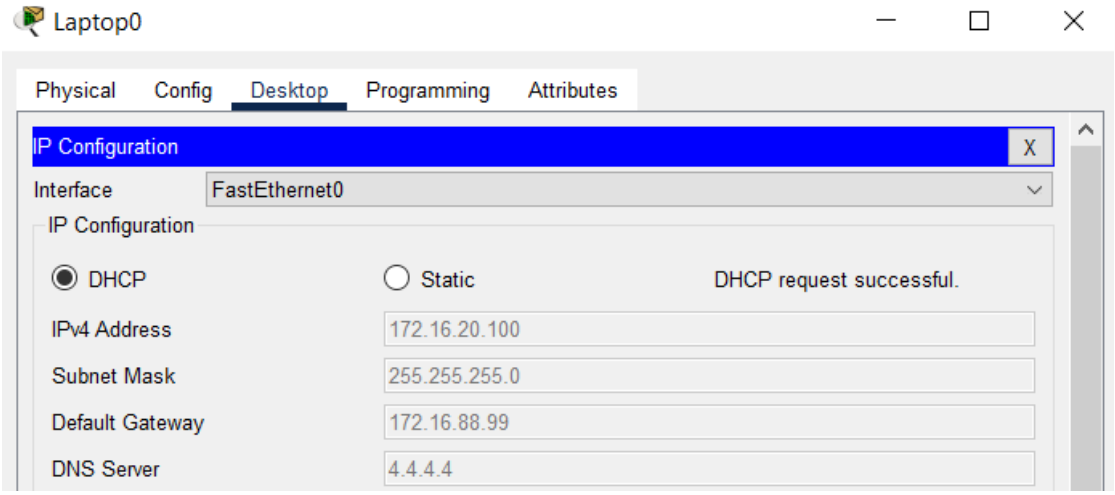


Figure 3. 41: default Gateway de USER 1 de switch ITC est change a 172.16.88.99

8.4.2) âpre d'active DHCP snooping donne le switch ITC :

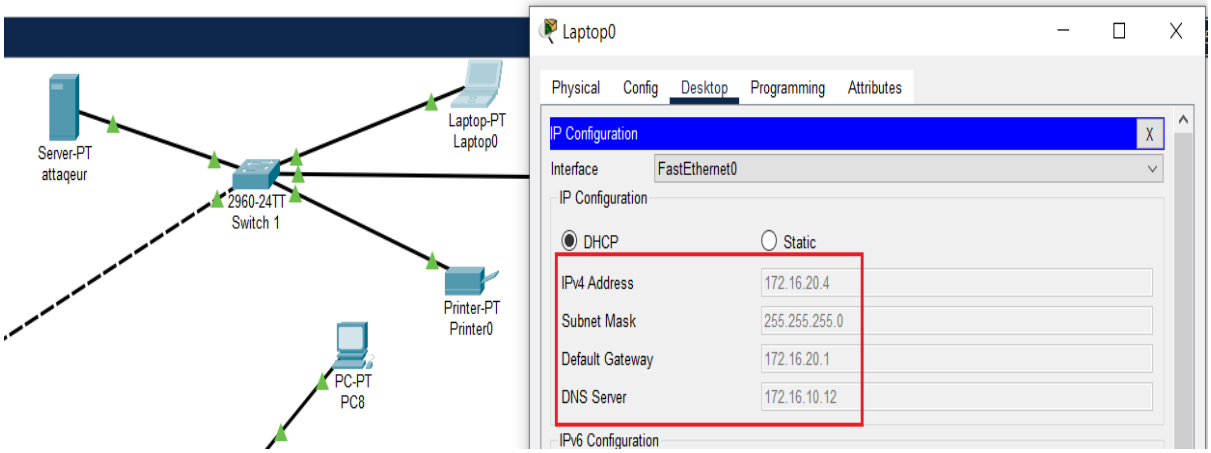


Figure 3. 42: default Gateway de USER 1 de switch ITC est change a 172.16.20.1

8.5) Test la sécurité de port sécurité :

En a place un pc d'adresse ip et Gateway de vlan 20 a la même interface (fa 0/2) de laptop 0 (user 1) et ping a la pc 7 d'adresse 172.16.20.5

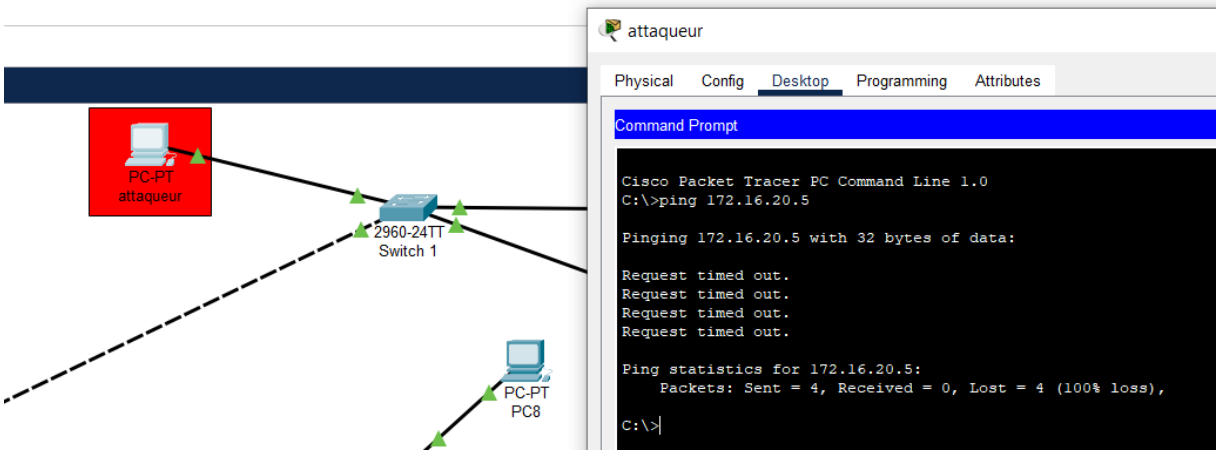


Figure 3. 43: place le pc attaqueur en l'interface de fa 0/2

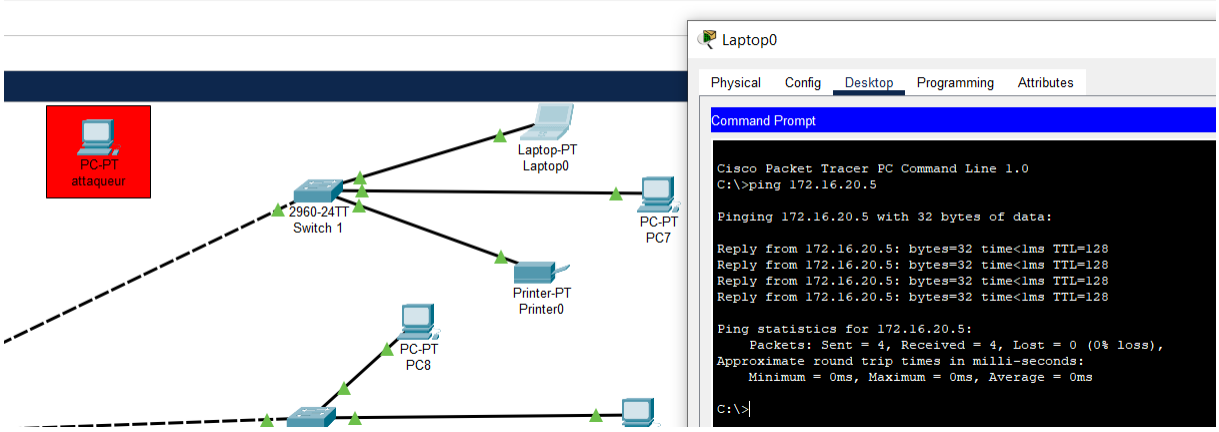


Figure 3. 44: place le pc de laptop 0 user 1 et ping a 172.16.20.5

Remarque :

Pour le test de « dynamique ARP inspection » et « Storm control » ne peut pas fait avec notre le programme pecket tracer.

9.Architecture réalisée :

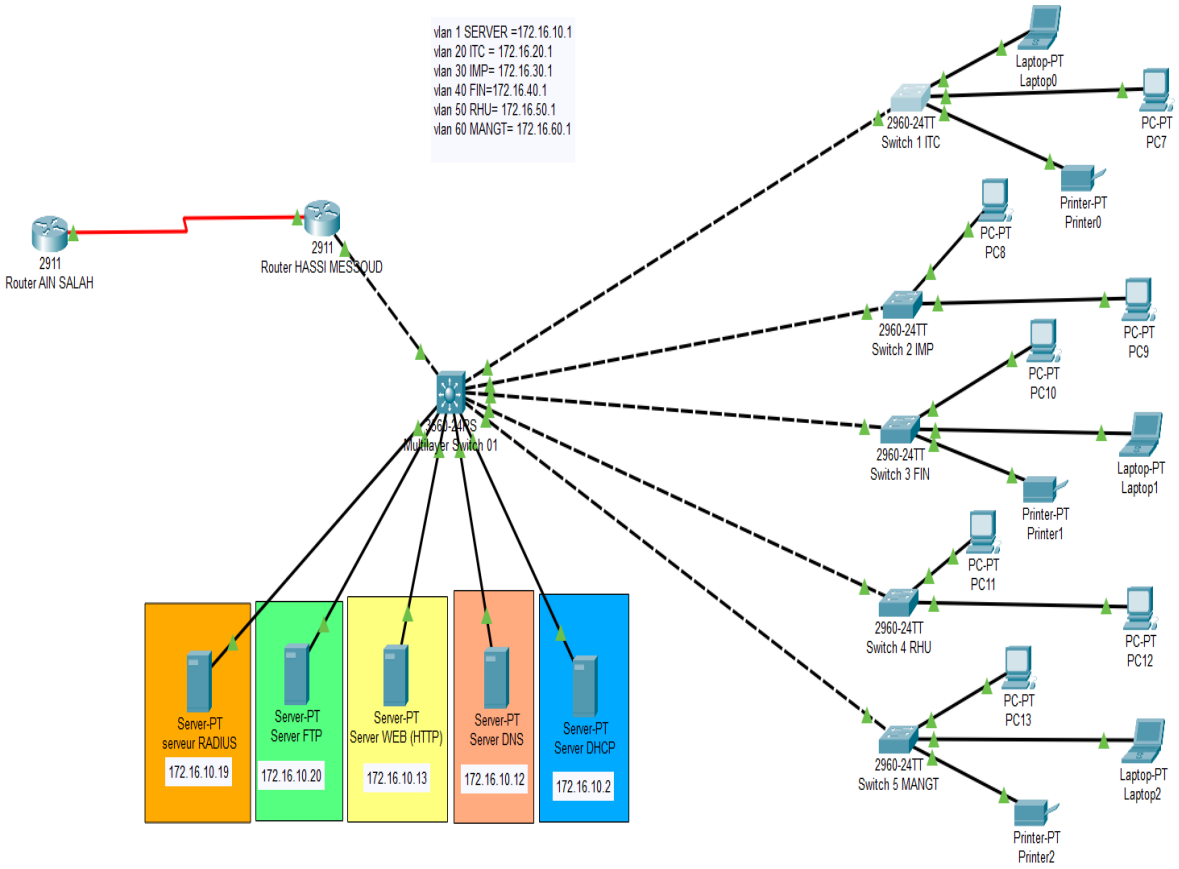


Figure 3. 45: Architecture réalisée.

Conclusion :

La sécurité des réseaux locaux peut être définie avec plusieurs manières, cette diversité dépend de l'architecture de chaque réseau. En revanche, nous ne pouvons pas dire que les techniques de sécurité que nous avons configurée sont suffisantes, mais dans notre cas, elles peuvent mettre fin à plusieurs problèmes de sécurité que nous avons cités dans la problématique.

Conclusion générale

En conclusion générale, Nous avons essayé à travers ce mémoire d'apporter une solution pour sécuriser le réseau Local de Sonatrach. Comme nous l'avons constaté, Sonatrach-BP Ain Salah gaz est constituée de plusieurs service à savoir le service des Finance, la direction générale, Management, ressources humaines, etc. Alors nous avons opté pour une solution basée sur les réseaux virtuels en procédant à la segmentation

En conclusion générale, mon mémoire aborde trois chapitres clés dans le domaine des réseaux informatiques. Dans le premier chapitre, j'ai présenté une vue d'ensemble sur les réseaux informatiques, en abordant des sujets tels que les systèmes OSI et TCP/IP, les réseaux LAN, WAN et MAN, ainsi que les équipements de réseau tels que les commutateurs, les routeurs et les câbles de réseau.

Le deuxième chapitre se concentre sur la sécurité et les attaques des réseaux locaux. J'y ai exploré des attaques courantes telles que l'ARP spoofing, le DHCP spoofing et le MAC flooding, ainsi que des mesures de sécurité telles que le DHCP snooping, la sécurité des ports, l'encapsulation ARP dynamique et les listes de contrôle d'accès (ACL).

Dans le troisième chapitre, intitulé "Conception et Réalisation", j'ai réalisé une simulation et organisé un réseau local. J'ai mis en pratique les méthodes de sécurité abordées dans le chapitre précédent, telles que le DHCP snooping, la sécurité des ports et l'authentification du serveur, pour assurer la sécurité des paquets transitant sur le réseau.

ce mémoire a permis d'explorer en détail les différents aspects des réseaux informatiques, en mettant l'accent sur la sécurité des réseaux locaux. Les connaissances acquises tout au long de cette étude sont essentielles pour comprendre, concevoir et mettre en œuvre des réseaux sécurisés et fiables. En combinant les aspects théoriques avec des mises en pratique concrètes, il est possible d'assurer une protection adéquate contre les attaques et les vulnérabilités potentielles, garantissant ainsi l'intégrité et la confidentialité des données échangées sur les réseaux informatiques.

Les références :

[1] JF. PILLOU, Fabrice LEMAINAQUE, Tout sur les réseaux et internet, 4eme édition Dunod,3 juin 2015, page 12

[2] G. Pujolle. LES RESEAUX. Paris, 4 Edition 9 2014, pages 15-16.

[3] https://www.proconcept-service.com/installation-reseau/ ,14/03/2023, 14 :53

[4] G. Pujolle. LES RESEAUX. Paris, 5 Edition ,2020 page 7 et 10.

[5] Philippe ATELIN, Réseaux informatiques notion fondamentales. Paris, 3eme édition 1 Janvier 2009, page 55-57

[6] https://www.avast.com/fr-fr/c-what-is-tcp-ip, 18/03/2023, 11 :16

[7] Philippe ATELIN, Réseaux informatiques notion fondamentales. Paris, 3eme édition 1 Janvier 2009, page 274-275

[8] JF. PILLOU, Fabrice LEMAINAQUE, Tout sur les réseaux et internet, 4eme édition Dunod,3 juin 2015, page 41-42

[9] https://www.inetdoc.net/articles/adressage.ipv4/adressage.ipv4.format.html, 19/03/2023, 8 :00

[10] JF. PILLOU, Fabrice LEMAINAQUE, Tout sur les réseaux et internet, 4eme édition Dunod,3 juin 2015, page 32-33

[11] https://waytolearnx.com/2019/06/differents-types-de-cablage-informatique.html , 20/03/2023, 7 :25

[12] https://web.maths.unsw.edu.au/~lafaye/CCM/pc/carte-reseau.htm , 27/03/2023, 18 :54

[13] G. Pujolle. LES RESEAUX. Paris, Edition 2014, page 125-126.

[14] Article : Dans Réseaux 2012/1 (n° 171), pages 161 à 187

[15] mimoire de "Proposition et implémentation d'une solution sécurité pour un réseau LAN", page 4

[16] C. Llorens L. Levier D. Valois. Tableaux de bord de la sécurité. Groupe Eyrolles Edition 2

Page 12-13-17-18-19

[17]]https://www.securiteinfo.com/conseils-cybersecurite/securite-physique-et-logique-du- materiel-informatique.shtml , 16/05/2023, 17 :11

[17.1] Jason Hart, hacker éthique, https://justaskthales.com/fr/attaque-reniflage-reseau-sniffing-cest-quoi-jason-hart-hacker-ethique-nous-explique-tout/

[18] http : //www-igm.univ-mlv.fr type de vlan, 18/04/2023, 21 :26

[19] https://www.connecthostproject.com/vtp.html 14/03/2023, 17 :21

[20] https://reussirsonccna.fr/vtp-vlan-trunking-protocol 15/03/2023 07:41

[21] https://www.connecthostproject.com/acl.html 15/03/2023 15 :00

[22] https://www.fortinet.com/resources/cyberglossary/network-access-control-list 15/03/2023 15 :10

[23] https://www.connecthostproject.com/acl.html , 29/04/2023, 15 :20

[24] https://fr.theastrologypage.com/authentication-server, 30/04/2023, 19 :35

[25] https://formip.com/securite-radius-tacacs/ , 29/04/2023, 18 :15

[26] https://cisco.goffinet.org/ccna/ethernet/switchport-port-security-cisco-ios/ , 29/04/2023, 19 :30

[27] https://forum.huawei.com/enterprise/en/dynamic-arp-inspection/thread/841135-867?page=1 , 08/05/2023, 17 :54

[28] https://www.networkacademy.io/ccna/ , 29/04/2023, 21 :18

[29] https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-5-0E/15-21E/configuration/guide/config/bcastsup.pdf , page 02, 10/05/2023, 18 :45