REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A.MIRA-BEJAIA

Faculté des Sciences Exactes

Département d'informatique

Projet de fin de cycle

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

Option : Administration et Sécurité des Réseaux

Thème :

Conception et déploiement d'une Architecture réseau sécurisée à la Direction de la Sécurité Aéronautique de Bejaia

Réalisé par :

BOUDIAB Sabiha

BOUDJAIDI Siham

Soutenu le 18 juin 2023 devant les jury composés de :

Président	**Mr**	**BEDJOU Khaled**	**MAA**	**U. A/Mira Bejaia**
Encadrant	**Mr**	**MOKTEFI Mohand**	**MCB**	**U. A/Mira Bejaia**
Encadrant	**Mme**	**NEDJADI Chafika**		**ENNA Bejaia**
Examinatrice	**Mme**	**HOCINI Kenza**	**MAB**	**U. A/Mira Bejaia**

Année Universitaire : 2022 / 2023

Remerciements

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

Et nous adressons nos vifs remerciements et notre gratitude

Â :

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

Nous tenons à adresser nos plus profonds et sincères remerciements à notre encadreur ***Mr. MOKTEFI****, pour nous avoir encadrés et guidés tout au long de ce projet, pour tous ses conseils et ses encouragements, pour sa disponibilité et sa compréhension.*

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

Nous tenons à remercier également notre encadreur de stage ***Mme. NEDJADI Chafika*** *et tout le personnel de l'ENNA pour leur orientation et accueil sympathique durant la période de stage.*

Aussi à tous les enseignants et employés du département Informatique à qui on doit notre avancement.

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

Dédicaces

Je dédie ce modeste travail :

A mes très chers parents qui m'ont tout donné ;

Soucieux de m'offrir une meilleure éducation et de me garantir un bon avenir.

Sans lesquels je ne saurai pu progresser et en arriver a l'achèvement de ce travail ; mes très chers frères et sœurs.

A mes chers cousins et cousines

A mes sœurs de cœur : Anais, Milida ,Akila, Wissam, Feriel, Massinta.

À mon binôme et amie Sabiha et à sa famille.

A tous ceux qui m'ont encouragé et soutenu dans mon parcours.

SIHAM

Dédicaces

Je dédie ce modeste travail à :

À la lumière de mes jours, Maman, je te dois ce que je suis aujourd'hui et ce que je serai demain et je ferai toujours de mon mieux pour rester ta fierté et ne jamais te décevoir.

À mon très cher papa, autant de phrases et d'expressions aussi éloquentes soient-elles ne sauraient exprimer ma gratitude et ma reconnaissance, que dieu le tout puissant te préserve t'accorde santé, bonheur, quiétude de l'esprit et te protège de tout mal.

À mon très cher frère que j'aime beaucoup et que j'ai trouvé à mes côtés.

À mon binôme et amie Siham et à sa famille.

À tout ma famille, mes amies pour leur soutien tout au long de mon parcours universitaire, que ce travail soit l'accomplissement de vos vœux tant allégués et le fruit de votre soutien infaillible.

SABIHA

Table des matières

Chapitre II Etude de l'architecture existante et proposition de solutions

Liste des figures

Liste des tableaux

Liste des abréviations

AD	Active Directory.
AD DS	Active Directory Domain Services.
ADSL	Asymmetric Digital Subscriber Line.
AP	Access Point.
ARP	Address resolution protocol.
BGP	Border Gateway Protocol.
BSS	Extented Service Set.
CDMA	Code Division Multiple Access.
CMD	Command Prompt
CSMA /CD	Carrier sense multiple access/Collision Detection
CVSS	Common Vulnerability Scoring System.
DHCP	Dynamic Host Configuration Protocol.
DNS	Domain Name System.
DS	Distribution System.
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer.
ENNA	Etablissement National de la Navigation Aérienne
EPON	Ethernet Passive Optical Network.
FAI	Fournisseur d'Accès à Internet.
FTTB	Fiber-to-the-building.
FTTC	Fiber-to-the-cabinet.
FTTH	Fiber-to-the-home.
GNS3	Graphical Network Simulator 3
GPO	Group Policy settings.
GPON	Gigabit Passive Optical Network.
GSM	Global System for Mobile Communications.
HDSL	High-Speed Digital Subscriber Line.
IEEE	International Electronical and Electronics Engineers.
IP	Internet Protocol.
LAN	Local Area Network.
LCC	Logical Link Control.
LDP	Label Distribution Protocol.

LSP	Label Switched Path.
LSR	Label Switching Routers.
MAC	Media Access Control.
MAN	Metropolitan Area Network.
NG-PON2	Next Generation Passive Optical Network 2.
NTDS	Naval Tactical Data System
OLT	Optical Line Terminal.
ONU	Optical Network Unit
OSI	Open System Interconnection.
OSPF	Open Shortest Path First.
OU	Organisation Unit.
PING	Packet Internet Groper.
QoS	Qualité de Service.
SYSVOL	System Volume
SDSL	Symmetric Digital Subscriber Line.
SMB	Server Message Block.
SSH	Secure Shell.
TCP	Transmission Control Protocol.
TTL	Time To Live.
VDSL	Very high-speed rate Digital Subscriber Line.
VLAN	Virtual Local Area Network ou Réseau Local Virtuel.
VPN	Virtual Private Network.
WAN	Wide Area Network
WIFI	WIreless Fidelity Internet.
WIMAX	Worldwide Interoperability for Microwave Access.
XG-PON	10 Gigabit Passive Optical Network.
XPON	X Passive Optical Network
3G	Troisième génération.
4G	Quatrième génération.
5G	Cinquième génération.

Introduction générale

Ces dernières années, le domaine des réseaux informatiques a connu une évolution technologique sans précédent, permettant une utilisation de plus en plus répandue dans les entreprises et chez les particuliers. Les réseaux informatiques sont devenus une composante essentielle pour les entreprises, augmentant leur productivité et leur efficacité tout en assurant la sécurité et la protection des données confidentielles [2].

Cependant, la sécurité des réseaux informatiques est devenue une préoccupation majeure pour les entreprises, notamment dans les secteurs sensibles tels que l'aéronautique. La Direction de Sécurité Aéronautique de Béjaïa, où nous avons effectué notre stage, doit garantir la confidentialité, l'intégrité et la disponibilité de ses données critiques tout en assurant une connectivité optimale à tous les niveaux de son organisation.

Le stage que nous avons effectué à la Direction de Sécurité Aéronautique de Béjaïa nous a permis de découvrir son réseau et de comprendre la nécessité d'une architecture réseau sécurisée pour garantir la sécurité de ses données. Notre travail vise à améliorer l'infrastructure de l'ENNA en intégrant une solution de contrôle d'accès pour les utilisateurs et une meilleure gestion du partage des ressources, et pour réaliser notre projet et atteindre nos objectifs fixés, nous avons subdivisé ce travail en trois chapitres distincts :

Dans le premier chapitre, nous allons examiner les différents types de réseaux d'entreprise ainsi que les technologies qui les sous-tendent. Cela nous permettra de mieux comprendre le fonctionnement de ces réseaux et les enjeux auxquels ils sont confrontés.

Le deuxième chapitre est consacré à la présentation de l'organisme d'accueil où nous avons effectué notre stage, en mettant l'accent sur ses besoins en matière de sécurité informatique. Ensuite nous allons présenter le système CVSS qui nous permettra d’évaluer la gravité des vulnérabilités de réseau existant pour élaborer une politique de sécurité plus claire.

Enfin, dans le troisième chapitre, nous allons mettre en pratique toutes les connaissances et solutions proposées dans les chapitres précédents en réalisant des étapes pratiques telles que la configuration des VLANS, l'installation de l'Active Directory, la mise en place des services de stockage, d'impression et le serveur de messagerie, ainsi que la vérification des résultats.

Enfin, nous terminerons par une conclusion générale résumant les éléments clés abordés dans ce mémoire afin de fournir une vision d'ensemble des points importants.

Chapitre I : Généralités sur les réseaux d’entreprise.

1 Introduction

Le domaine des réseaux informatiques a connu une évolution technologique significative ces dernières années, avec une utilisation répandue à travers le monde. Les réseaux informatiques sont aujourd'hui très prisés pour augmenter la productivité et l'efficacité, tout en garantissant la sécurité des données de l'entreprise. Dans ce chapitre, nous allons examiner les réseaux d'entreprise ainsi que les technologies qui les sous-tendent.

2 Définition d'un réseau entreprise

Un réseau entreprise est l'épine dorsale de communication d'une entreprise qui permet de connecter des ordinateurs et des périphériques associés à travers les départements et les réseaux de groupe de travail, facilitant la compréhension et l'accessibilité des données. Un réseau d'entreprise réduit les protocoles de communication, facilite l'interopérabilité des systèmes et des appareils, ainsi qu'une meilleure gestion des données internes et externes de l'entreprise.

Son objectif principal est d'éliminer les utilisateurs et les groupes de travail isolés. Tous les systèmes devraient être capables de communiquer et de fournir et de récupérer des informations. [1]

Les réseaux d'entreprise peuvent être de différentes tailles et configurations, allant des petits réseaux locaux (LAN) pour des entreprises de petite taille aux réseaux étendus (WAN) pour les grandes entreprises avec des succursales partout dans le monde. La figure 1-1 illustre les réseaux LAN, MAN, WAN :

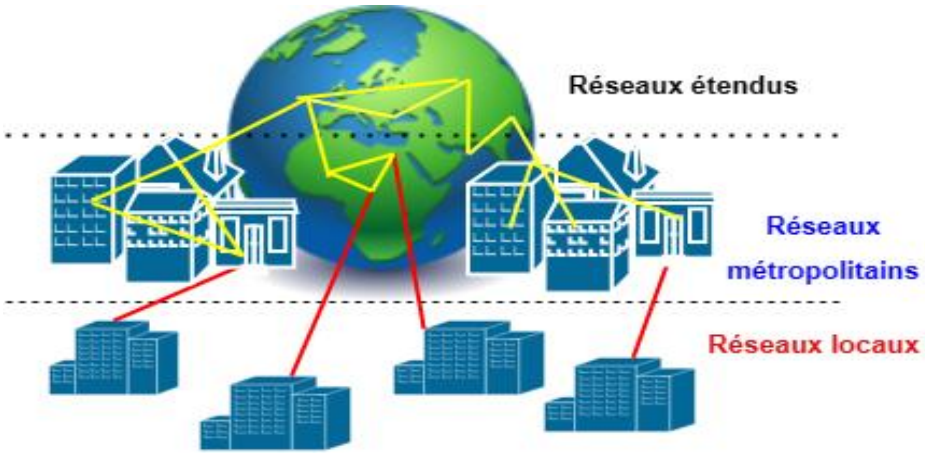

Figure 1-1 : Réseaux LAN, MAN, WAN

3 Réseaux locaux d'entreprise

Les réseaux locaux d'entreprise (LAN) sont des réseaux informatiques qui permettent à des ordinateurs et à d'autres périphériques de se connecter et de communiquer dans un environnement limité, tel qu'un bureau, un bâtiment ou un campus. Les LAN sont généralement utilisés pour faciliter l'échange de données, l'accès aux ressources partagées et la communication entre les employés.

Les réseaux locaux d'entreprise peuvent être configurés en utilisant différents types de technologies de connexion, telles qu'Ethernet, Wi-Fi ou Fibre optique. Ils sont également souvent accompagnés de solutions de sécurité telles que des pare-feu, des VPN et des outils de gestion de réseau pour garantir la confidentialité des données et la disponibilité des ressources. [2]

3.1 Technologie Ethernet commuté

La technologie Ethernet, développée par DGital, Intel et Xerox, initialement conçue pour l'accès au réseau via CSMA/CD et le transport en mode diffusion d'un payload avec un simple contrôle d'erreur, ne prévoyait pas de services tels que la retransmission ou le mode connecté.

Cependant, le groupe 802.3 de l'IEEE a normalisé l'utilisation de la couche LLC dans la technologie Ethernet. Cette normalisation a entraîné l'implémentation de deux standards IEEE différents, 802.3 pour la sous-couche MAC et 802.2 pour la sous-couche LLC.

Les différents services demandés nécessitent l'utilisation de différents formats de trames Ethernet avec ces implémentations variables. [3]

3.1.1 Architecture de la technologie Ethernet

Deux types d'équipement sont utilisés dans la technologie Ethernet: le hub et le switch. Le hub permet un accès partagé à une ressource en simulant un bus commun pour tous les utilisateurs. En tant que répéteur, il régénère le signal originaire d'une station et le diffuse à tous les accès. Le switch, quant à lui, résout les problèmes de collision en utilisant des mémoires tampons pour stocker les trames entrantes, plutôt que de créer un bus partagé. [4]
Ethernet utilise des techniques de multiplexage de bande de base. L'algorithme CSMA/CD est utilisé pour la communication entre les équipements. La figure 1-2 présente l'architecture de la technologie Ethernet :

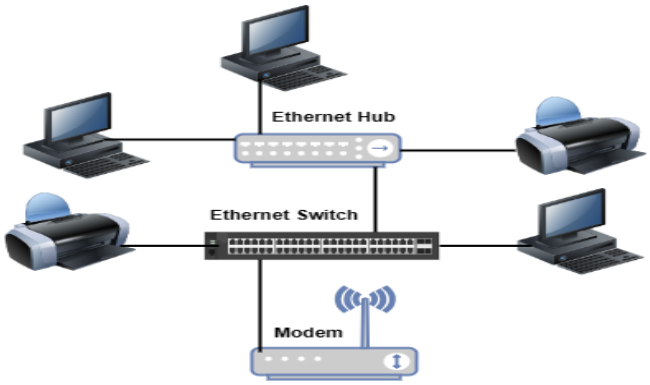

Figure 1-2 : Architecture d'Ethernet.

3.1.2 Variantes de la technologie Ethernet

Le protocole Ethernet, également appelé IEEE 802.3, est une technologie de réseau local qui repose sur une architecture où toutes les machines du réseau sont reliées à une ligne de communication unique, composée de câbles cylindriques.

On distingue différentes variantes de technologie Ethernet suivant le diamètre des câbles utilisés [5] :

- 10 Base-2 : le câble utilisé est un câble coaxial de faible diamètre.
- 10 Base-5 : le câble utilisé est un câble coaxial de gros diamètre.
- 10 Base-T : le câble utilisé est une paire torsadée, le débit atteint est d'environ 10 Mbps.
- 100 Base-TX : comme 10 base-T mais avec une vitesse de transmission beaucoup plus importante (100 Mbps). Le tableau 1-1 présente les différentes variantes de la technologie Ethernet :

Technologie	Type de câble	Vitesse	Portée
10 Base-2	câble coaxial de faible diamètre	10 MB/s	185 m
10 Base-5	câble coaxial de gros diamètre	10 MB/s	500 m
10 Base-T	double paire torsadée	10 MB/s	100 m
100 Base-TX	double paire torsadée	100 MB/s	100 m
1000 Base-SX	fibre optique	100 MB/s	500 m

Tableau 1-1 : Variantes de technologie Ethernet. [5]

3.1.3 Caractéristique de la technologie Ethernet

Voici quelques-unes des principales caractéristiques de la technologie Ethernet : [6]

- **Vitesse de transmission** : Ethernet est capable de transmettre des données à des

vitesses allant de 10 Mbps à plusieurs Gbps, selon la version du protocole utilisée.

- **Support de la norme IEEE** : Ethernet est normalisé selon la norme IEEE 802.3, ce qui permet une interopérabilité entre les équipements de différents fabricants.
- **Topologies de réseau :** Ethernet peut être utilisé dans différents types de topologies, y compris les réseaux en étoile, en bus et en anneau.
- **Fiabilité :** Ethernet est considéré comme une technologie de réseau fiable, avec un faible taux de perte de données.
- **Sécurité :** Ethernet offre des fonctionnalités de sécurité telles que des adresses MAC uniques pour chaque appareil, ainsi que des mécanismes de cryptage pour protéger les données en transit.

3.1.4 Avantages et inconvénients de la technologie Ethernet

Le tableau 1-2 présente les avantages et les inconvénients de la technologie Ethernet :

Avantages	Inconvénients
• Gigabit Ethernet peut fournir une vitesse maximale de 1 Gbps, ce qui est plus de 10 fois plus rapide que Fast Ethernet. • La mise en place d'Ethernet est relativement peu coûteuse, avec un coût total faible. • Dans un réseau Ethernet, tous les nœuds ont des privilèges équivalents plutôt que de suivre une architecture client-serveur. • Grâce à sa résistance au bruit, la qualité de transfert des informations via Ethernet n'est pas dégradée, ce qui assure une bonne qualité de transfert des données.	• Il permet une communication hors ligne sur le réseau. • Tandis que le destinataire est incapable de transmettre des données après réception des paquets. • En cas de dysfonctionnement de l'Ethernet, identifier le câble ou le nœud du réseau à l'origine de la panne est compliqué. • Pour la version 100 Base-T4, le mode de communication en duplex intégral n'est pas pris en charge.

Tableau 1-2 : Avantages et inconvénients de la technologie Ethernet. [7]

Ethernet est utilisé dans une grande variété de contextes, que ce soit dans les réseaux domestiques, les environnements professionnels ou les centres de données. elle a largement

évolué depuis sa création, avec l'émergence de nouvelles normes, malgré quelques inconvénients, l'Ethernet offre des avantages significatifs en termes de vitesse, de fiabilité, de compatibilité et de sécurité. Il reste une technologie très répandue et utilisée dans de nombreux domaines.

3.2 Technologie Wi-Fi

Le standard international IEEE 802.11, également connu sous le nom de Wi-Fi, spécifie les propriétés d'un réseau local sans fil (WLAN) qui relie des ordinateurs portables, des équipements de bureau et des appareils personnels tels que des PDA. Ce réseau sans fil couvre une distance d'environ quelques dizaines de mètres et permet une mobilité à faible vitesse.

3.2.1 Architecture Wi-Fi

Deux types d'architecture définissent un réseau Wi-Fi :

- **Le réseau d'infrastructure** : Les communications passent par un point d'accès (AP) pour couvrir une zone radioélectrique appelée Cellule BSS (Basic Service Set). La BSS est reconnaissable grâce au BSSID, généralement l'adresse MAC de l'AP. L'ensemble des points d'accès forme le réseau ESS (Extended Service Set), qui est identifié par un SSID. Ce réseau est connecté à un commutateur LAN (DS - Distribution System) via une connexion Ethernet 100Base-TX. [4]

La figure 1-3 présente le mode infrastructure :

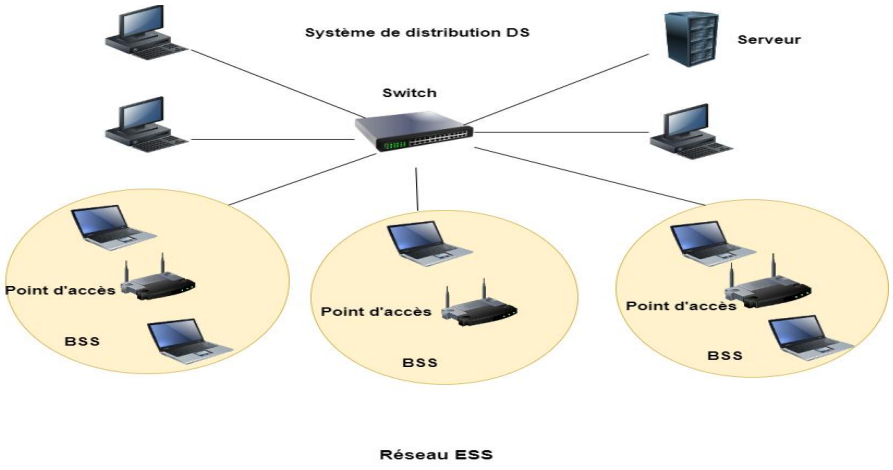

Figure 1-3 : Architecture de réseau infrastructure. [4]

- **Le réseau ad-hoc :** pour lequel les communications s'effectuent directement entre les stations. Ce modèle simplifié permet une exécution rapide de communication entre deux stations sans fil. [4]

La figure 1-4 présente le mode ad-hoc :

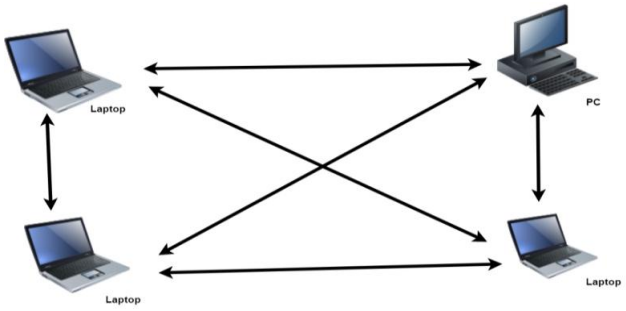

Figure 1- 4 : Architecture du réseau ad-hoc.

3.2.2 Différentes normes Wi-Fi

La norme initiale IEEE 802.11 proposait des débits de 1 ou 2 Mbps. Cependant, des modifications ont été apportées pour optimiser ce débit, notamment avec les normes physiques 802.11a, 802.11b et 802.11g. D'autres ajustements ont été faits pour renforcer la sécurité ou faciliter l'interopérabilité. Le tableau suivant présente les différentes révisions de la norme 802.11 et leur signification. [3]

Le tableau 1-3 présente les différentes technologie Wi-Fi :

Norme	Bande de fréquence	Débit théorique	Portée
IEEE 802.11a	5 GHz (5,7 à 5.8 GHz en Guinée)	54 Mbit/s	10 m
IEEE 802.11b	2.4 GHz (2,4 à 5,5 GHz en Guinée)	11 Mbit/s	300 m
IEEE 802.11g	2.4 GHz (2,4 à 5,5 GHz en Guinée)	54 Mbit/s	300 m
IEEE 802.11n	2.4 GHz ou 5 GHz (2,4 à 5,8 Ghz en Guinée)	450 Mbit/s	100 m

Tableau1- 3 : Technologie Wi-Fi- IEEF 802.11. [3]

3.2.3 Equipements de la technologie Wi-Fi

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil Wi-Fi

- **Les adaptateurs sans fil ou cartes d'accès :** Les adaptateurs sans fil, également appelés cartes d'accès ou NIC (network interface controller en anglais), sont des cartes réseau respectant la norme 802.11 qui permettent à un équipement de se connecter à un réseau sans fil. Les équipements équipés d'une telle carte sont appelés des stations. A noter que les composants Wi-Fi sont devenus des standards sur les ordinateurs portables grâce au label Centrino d'Intel.

- **Les points d'accès** : Les points d'accès sont des boîtiers centraux ayant le même rôle que les hubs dans les réseaux Ethernet. Ils permettent la connexion d'autres ordinateurs équipés d'une carte Wi-Fi et proposent souvent des connexions Ethernet RJ-45 pour se connecter à un réseau filaire. Certains modèles disposent également d'un modem ADSL pour se connecter à Internet. [8]
- **Les antennes :** En pratique, chaque carte Wi-Fi est munie d'une antenne interne mobile uniquement si la station elle-même est mobile. Les points d'accès Wi-Fi sont équipés d'antennes qui émettent des ondes radios. Les antennes Wi-Fi directionnelles, utilisées pour augmenter la portée et la qualité du signal, émettent des ondes radios sur une plus grande distance en fonction de leur gain. [9]

3.2.4 Avantages et inconvénients de la technologie Wi-Fi

Le tableau 1-4 présente les avantages et les inconvénients de la technologie Wi-Fi :

Les avantages	Les inconvénients
• **Mobilité** : En se connectant au réseau sans fil, il est possible de se déplacer aisément dans la zone de couverture disponible. • **Facilité** : Lorsqu'un réseau Wi-Fi est correctement configuré et que l'on dispose de l'autorisation nécessaire, il est extrêmement facile de s'y connecter, et il est généralement suffisant de se trouver dans la zone de couverture pour être connecté. • **Souplesse** : La flexibilité d'installation du Wi-Fi offre la possibilité d'ajuster aisément la zone de couverture selon les exigences. En cas de signal faible à partir du point d'accès, il est possible d'installer des répéteurs pour étendre la portée. • **Coût** : En général, la plupart des composants du réseau Wi-Fi tels que les points d'accès, les répéteurs ou les antennes	• **Qualité et continuité du signal :** En règle générale, un réseau Wi-Fi correctement installé et configuré offre une fiabilité et une qualité constantes. • **Sécurité** : Comme le Wi-Fi est un réseau sans fil, il est accessible sans avoir besoin d'intervenir sur des équipements physiques. Cependant, il est important de prendre des mesures adéquates pour sécuriser le réseau et éviter ainsi la présence d'indésirables ou la fuite d'informations sensibles.

peuvent être facilement installés sans utiliser d'outils particuliers. Ainsi, l'installation peut être réalisée sans recourir à une main-d'œuvre spécialisée, ce qui permet de réduire les coûts. • **Evolutivité :** Grâce à la flexibilité de l'expansion ou de la réduction du réseau, il est possible d'avoir une couverture Wi-Fi qui répond en permanence aux besoins réels.	

Tableau 1- 4 : Avantages et les inconvénients de la technologie Wi-Fi. [10]

Malgé que Wi-Fi offre une connectivité sans fil pratique et polyvalente, mais il est important de prendre en compte ses limitations en termes de portée, d'interférences, de sécurité et de vitesse pour une expérience optimale.

3.3 Technologie VLAN

Grâce à la technologie VLAN (Virtual Local Area Network), il est possible de créer des réseaux logiques indépendants au sein d'un même réseau physique. Cela permet de segmenter le réseau en différents groupes virtuels afin d'optimiser la gestion des ressources et d'améliorer la sécurité du réseau.

3.3.1 Types de la technologie VLAN

Plusieurs types de VLAN sont définis, en fonction des critères de commutation et du niveau auquel le VLAN est implémenté [11]:

- **VLAN par port :** aussi appelés VLAN de niveau 1, sont adaptés aux réseaux avec une seule station raccordée sur chaque port du switch. Ils sont simples à utiliser pour des petits réseaux.
- **VLAN par adresse MAC :** Les VLAN par adresse MAC, ou VLAN de niveau 2, sont plus souples car ils permettent de définir l'appartenance à un VLAN pour chaque station, indépendamment de sa situation géographique dans le réseau. Cependant, ils sont plus complexes à administrer en raison de la difficulté à gérer les adresses MAC des utilisateurs.
- **VLAN par protocole :** Les VLAN par protocole, ou VLAN de niveau 3, regroupent

toutes les stations utilisant le même protocole de niveau 3 ou appartenant au même réseau logique (subnet) et sont plus simples à administrer puisqu'ils travaillent sur des adresses de niveau 3 bien connues des exploitants de réseaux.

- **Les VLAN sur critères applicatifs :** les VLAN sur critères applicatifs sont associés aux VLAN de niveau 3 et permettent d'optimiser ou de personnaliser les VLAN pour des applications particulières.

3.3.2 Applications du VLAN

Les applications des VLAN peuvent se résumer comme suit [12] :

- Créer des VLAN dans un bâtiment permet de regrouper les utilisateurs en fonction de leurs catégories, même s'ils sont situés à différents endroits.
- Prioriser les flux en fonction des catégories d'utilisateurs.
- Offrir un réseau d'administration.
- Créer un réseau de quarantaine pour isoler les stations qui manifestent une activité anormale afin de limiter la propagation de la contamination et de prévenir la pollution de l'intranet par du trafic inutile.

3.3.3 Avantages et inconvénients de la technologie VLAN [13]

Le tableau 1-5 présente les avantages et les inconvénients de la technologie VLAN :

Les avantages	Les inconvénients
• Une bande passante large et une vitesse de données élevée. • Une amélioration de la sécurité grâce à la protection des ressources et l'isolement de certains groupes. • Des performances accrues en limitant les domaines de diffusion. • Les utilisateurs qui déménagent ont toujours les mêmes droits d'accès aux ressources LAN sans que l'équipe d'exploitation ait besoin d'intervenir.	• Il est possible que d'autres réseaux sans fil et dispositifs à micro-ondes interfèrent avec le fonctionnement de ce système. • De plus, une bande passante limitée peut survenir lorsque plusieurs utilisateurs sont connectés simultanément. • Le coût initial de déploiement est élevé. • Il existe également un manque de normalisation internationale complète.

Tableau 1- 5 : Avantages et les inconvénients de la technologie VLAN.

La technologie VLAN présente des avantages significatifs tels que la segmentation du réseau, la flexibilité et la gestion efficace des ressources. Cependant, elle nécessite une configuration complexe, peut entraîner une charge de travail supplémentaire, présenter des risques de sécurité et avoir des limitations de scalabilité. Il est donc important de peser soigneusement les avantages et les inconvénients avant de mettre en place des VLAN dans un environnement réseau.

4 Réseaux métropolitains d'entreprise

Les réseaux métropolitains d'entreprise MAN sont des réseaux privés de télécommunication à haut débit qui interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) il permet à deux équipements distants de communiquer comme s'ils faisaient partie d'un même réseau local. Ces réseaux offrent une connectivité rapide et sécurisée entre les différentes sites et locaux d'une entreprise, ce qui permet de renforcer la collaboration, la coordination et la productivité des employés. [2]

4.1 Technologie WiMAX

Le WI-MAX, un acronyme pour Word Interoperability for Microwave Access, est un réseau de communication sans fil qui permet des débits allant jusqu'à plusieurs dizaines de mégabits par seconde sur une zone de couverture maximale de quelques dizaines de kilomètres. Cette technologie est standardisée par l'IEEE sous la norme 802.**16.** Sa principale utilité est de fournir un accès à Internet à haut débit aux zones mal desservies par les réseaux filaires à cause de contraintes économiques ou géographiques. [13]

4.1.1 Architecture de la technologie WiMAX

Le système WiMAX est constitué majoritairement de deux types de stations : les stations de base (BS ou base station) et les stations mobiles (SS ou subscriber station). La station de base a pour fonction de servir d'antenne centrale pour transmettre des données aux stations mobiles qui, à leur tour, fournissent aux clients un accès à large bande via Wi-Fi ou Adsl.

La figure 1-5 illustre l'architecture générale de la technologie WiMax [14] :

Figure 1- 5 : Exemple d'un réseau WiMAX. [14]

4.1.2 Différentes normes de WiMAX

Le WiMax regroupe différentes normes permettant d'établir des connexions radio à haut débit. Le tableau ci-dessous explique les spécificités techniques du développement des normes 802.16, dont la version la plus avancée et la plus attrayante est le standard IEEE 802.16e. Cette dernière offre la possibilité de se connecter en déplacement. [15]

Le tableau 1-6 présente les différentes normes de la technologie WiMAX :

Standard	Description	Publié	Statut
IEEE std 802.16-2001	définit des réseaux métropolitains sans fil utilisant des fréquences supérieures à 10 GHz (jusqu'à66 GHz).	8 avril 2002	obsolètes
IEEE std 802.16c-2002	définit les options possibles pour les réseaux utilisant les fréquences entre 10 et 66 GHz.	15 janvier 2003	obsolètes
IEEE std 802.16a-2003	amendement au standard 802.16 pour les fréquences entre 2 et 11 GHz.	1 er avril 2003	obsolètes /actifs
IEEE std 802.16-2004 (également désigné 802.16d)	il s'agit de l'actualisation (la révision) des standards de base 802.16, 802.16a et 802.16c.	1 octobre 2004	obsolètes /actifs
IEEE 802.16e (également désigné IEEE std	apporte les possibilités d'utilisation en situation mobile du standard, jusqu'à 122 km/h.	7 décembre 2005	actifs

802.16e2005)			
IEEE 802.16f	Spécifie la MIB (Management Information Base), pour les couches MAC (Media Access Control) et PHY (Physical).	22 janvier 2006	actifs

Tableau 1- 6 : Normes d'IEEE 802.16X. [15]

4.1.3 Aapplications de WIMAX

Le caractère de mobilité ainsi que les coûts d'installations réduits, ouvre la voie à de nombreuses applications pour le WIMAX [16] :

- Offres commerciales grand public triple play : données, voix, télévision ;
- Couvertures conventionnelles de zones commerciales (« hot zones ») : zones d'activité économique, parcs touristiques, centres hôteliers... ;
- Déploiements temporaires : chantiers, festivals, infrastructure de secours sur une catastrophe naturelle... ;
- Gestion de réseaux de transports intelligents ;
- Zone hospitalière étendue (lieu médicalisé) ;
- Sécurité maritime et sécurité civile ;
- Systèmes d'information géographique déportés ;
- Métrologie (télémesure, pilotage à distance, relevés géophysiques...).

4.1.4 Avantages et inconvénients du WiMAX

Le tableau 1-7 présente les avantages et les inconvénients de la technologie WiMAX :

Les avantages	Les inconvénients
• Une capacité de transmission de données rapide et une bande passante étendue. • Des connexions réseau performantes et à grande portée. • Une accessibilité accrue à Internet pour les utilisateurs en dehors des zones urbaines. • Une grande évolutivité facilitant l'expansion du réseau.	• Il y a des risques d'interférences avec d'autres réseaux sans fil et des dispositifs utilisant des micro-ondes. • La bande passante est limitée lorsqu'il y a un grand nombre d'utilisateurs connectés simultanément. • La mise en place initiale est coûteuse. Il n'y a pas de standardisation internationale complète

• Des options de déploiement économiques en comparaison à la fibre optique.	

Tableau 1-7 : Avantages et les inconvénients du WiMAX.[17]

Le WiMAX présente des avantages tels que sa large portée, sa vitesse élevée et son interopérabilité, ce qui en fait une solution attrayante pour les zones mal desservies. Cependant, il est important de prendre également en considération les inconvénients tels que les coûts d'infrastructure élevés, les interférences potentielles, la latence et la réduction du débit avec la distance.

5 Réseaux étendus d'entreprise

Le réseau WAN d'entreprise est un réseau informatique qui relie des ordinateurs et des périphériques situés dans des sites géographiquement distants, tels que des bureaux, des succursales ou des centres de données, à l'aide de technologies de communication à longue portée.

Les réseaux WAN d'entreprise permettent aux utilisateurs de partager des ressources telles que des fichiers, des imprimantes et des applications, et facilitent également la communication entre les employés. [18]

5.1 Technologie XDSL

La technologie XDSL ou Digital Subscriber Line (DSL) est une famille de technologies qui permettent de fournir une connexion Internet haut débit via les lignes téléphoniques existantes. Elle utilise des fréquences plus élevées que celles utilisées pour les appels téléphoniques afin d'envoyer et de recevoir des données à des vitesses plus élevées. Les différents types de technologies DSL incluent ADSL, VDSL, et SDSL, qui offrent des vitesses et des capacités de bande passante variables en fonction des besoins de l'utilisateur. [19]

IL existe deux sortes de XDSL identifiées par leurs modes de transmission: [20]

- Celle utilisant une transmission symétrique : c'est-à-dire le débit est identique dans le 2 sens de transmission « HDSL, SDSL ».
- Celle utilisant une transmission asymétrique : c'est-à-dire les débits sont différents dans le 2 sens de transmission « ADSL, VDSL, RADSL »

5.1.1 Variantes de la technologie XDSL

- **ADSL (Asymmetric Digital Subscriber Line) :** Cette technologie utilise une ligne téléphonique existante pour proposer une connexion haute débit asymétrique. Elle permet une vitesse de téléchargement plus rapide que la vitesse de téléversement.
- **VDSL (Very high-speed Digital Subscriber Line) :** Cette technologie offre des vitesses de téléchargement et de téléversement plus élevées que l'ADSL et est idéale pour les applications gourmandes en bande passante telles que la diffusion en continu de contenu vidéo ultra haute définition.
- **SDSL (Symmetric Digital Subscriber Line) :** Cette technologie offre une vitesse de téléchargement et de téléversement symétrique, ce qui signifie que la vitesse de téléversement est également rapide que la vitesse de téléchargement. Elle est idéale pour les entreprises qui ont besoin de télécharger et de téléverser de gros volumes de données.
- **HDSL (High bit-rate Digital Subscriber Line) :** Cette technologie a été conçue pour les connexions professionnelles et peut offrir des débits allant jusqu'à 2,048 Mbps. Elle est symétrique et nécessite une paire de fils en cuivre spécialement réservée à l'abonné.

Le tableau 1-8 présente Les différentes technologies de XDSL :

Nom	Technologie	Débit descendant	Débit montant	Distance max
SDSL	Sym	2 Mbits/s	2Mbits/s	2,4 Km
ADSL	Asym	0,5 à 9 Mbits/s	16 à 640 Kbits/s	5,4 Km
ReADSL	Asym	0,6 à 7 Mbits/s	128 à 1024 Kbits/s	5,4 Km
VDSL	Asym	13 à 53 Mbits/s	1,5 à 8 Mbits/s	1,5 Km
VDSL	Sym	30 Mbits/s	30 Mbits/s	1,5 Km
VDSL2	Asym	34 à 100 Mbit/s	1,5 à 8 Mbit/s	5,4 Km
VDSL2	Sym	50 Mbit/s	50 Mbit/s	5,4 Km

Tableau 1- 8 : Description des différentes technologies. [21]

5.1.2 Comparaison des technologies VDSL1, VDSL2, ADSL2+

Avec une bande de fréquence encore plus large et un encodage plus efficace, le VDSL very high bitrate DSL et le VDSL2 (portée et débit largement supérieurs) offrent des débits plus élevés, ainsi qu'une possibilité de symétrie. La plupart des opérateurs européens ont annoncé des déploiements VDSL2 à grande échelle. [22]

La figure 1-6 illustre une comapraison entre les technologies VDSL1, VDSL2, ADSL2+ :

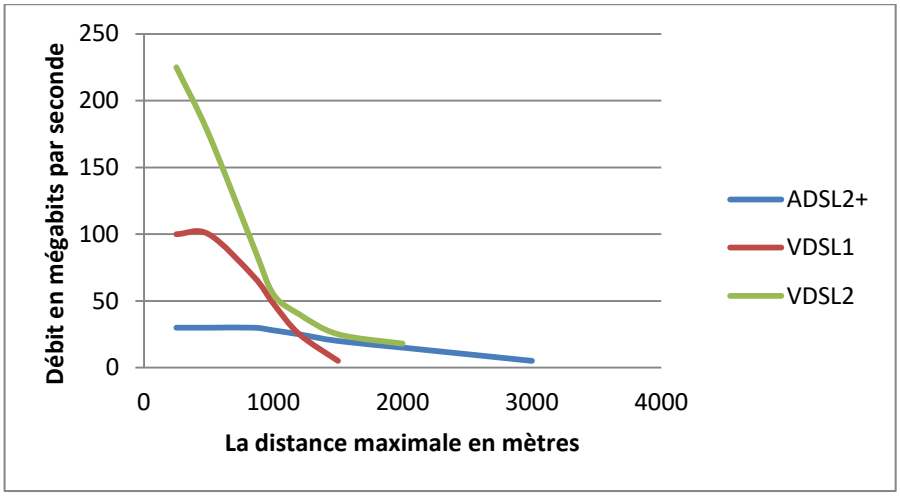

Figure 1- 6 : Comparaison des technologies VDSL1, VDSL2, ADSL2+

5.1.3 Architecture de la technologie XDSL

L'architecture de la technologie xDSL comprend plusieurs éléments, voici une liste non-exhaustive: [23]

- **Le modem xDSL :** il est installé chez l'utilisateur et se connecte à la ligne téléphonique de l'utilisateur. Il traite les signaux de données entre le réseau et l'utilisateur.
- **Le câblage :** il est utilisé pour connecter l'interface de ligne xDSL et le modem xDSL à la ligne téléphonique de l'utilisateur.
- **Les protocoles de communication :** ils permettent la communication entre l'interface de ligne xDSL et le modem xDSL.
- **Les équipements d'infrastructure réseau :** ils sont utilisés pour transmettre les signaux de données entre les différents réseaux.
- **DSLAM :** est un dispositif qui regroupe les lignes d'abonné individuelles en une liaison montante à haut débit. Ces liaisons montantes, telles que ATM (Asynchronous Transfer Mode) ou Gigabit Ethernet, connectent les abonnés à leur fournisseur d'accès Internet (FAI). Les DSLAM sont généralement situés dans des centraux téléphoniques ou des points de distribution. Ils permettent d'utiliser les lignes de cuivre existantes pour la transmission à haut débit de la technologie DSL (Digital Subscriber Line) qui utilise ces lignes de cuivre déployées pour le téléphone dans les années **1950.** [24]
- **Filtre :** est un petit dispositif électronique qui est utilisé pour séparer les signaux vocaux des signaux haut débit transitant sur une ligne téléphonique xDSL. Ce filtre

est connecté entre la prise murale téléphonique et les équipements haut débit tels que les modems ADSL ou les routeurs. [25]

La figure 1-7 illustre un exemple d'une architecture ADSL :

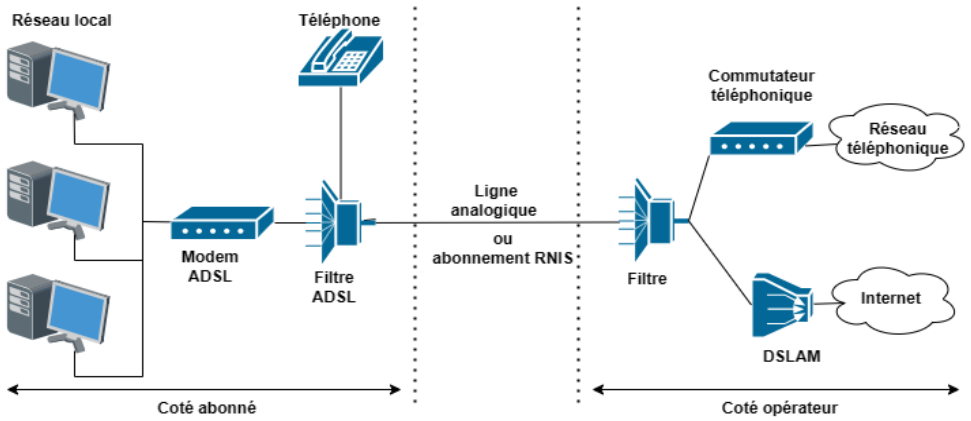

Figure 1-7 : Exemple d'une architecture ADSL

5.1.4 Avantages et inconvénients de la technologie XDSL [26] [27]

Le tableau 1-9 présente les avantages et les inconvénients de la technologie XDSL :

Avantages	Inconvénients
• **Haut débit:** elle offre des vitesses de connexion élevées, ce qui en fait une option idéale. • **Flexibilité:** elle peut être utilisée sur une variété de supports, notamment le câble téléphonique, la fibre optique ou le coaxial, offrant ainsi une grande flexibilité pour les utilisateurs. • **Coût:** elle est généralement moins coûteuse que les autres technologies hautes débit, ce qui est un avantage pour les consommateurs et les entreprises.	• La distance limitée entre le modem et le central téléphonique • La vitesse qui peut être limitée en fonction de la qualité de la ligne téléphonique

Tableau 1- 9 : Avantages et les inconvénients de la technologie xDSL.

La technologie XDSL présente des avantages tels que sa disponibilité étendue, ses vitesses de connexion élevées et son coût relativement abordable. Cependant, ses inconvénients incluent la dépendance à la distance, la fiabilité variable et les limitations de bande passante.

Il est important de prendre en compte ces facteurs lors du choix d'une solution de connexion à Internet.

5.2 Technologie Xpon

Également connue sous le nom de Passive Optical Network (PON), est un système de réseau de communication optique déployé par les fournisseurs de services Internet pour offrir des connexions Internet haut débit à divers clients. Cette technologie permet de partager une unique fibre optique entre plusieurs utilisateurs pour lesquels les signaux optiques sont acheminés via des répartiteurs optiques passifs (PON), ce qui permet de réduire les coûts et d'augmenter la capacité du réseau. [28]

Cette technologie est utilisée dans différents types de réseaux à fibre optique, tels que les réseaux FTTC (Fiber-to-the-cabinet), FTTB (Fiber-to-the-building) et FTTH (Fiber-to-the-home) : [29]

- Avec les technologies FTTC, la fibre optique est déployée jusqu'au sous-répartiteur du réseau local historique ; du sous-répartiteur au domicile de l'abonné, l'opérateur utilise le réseau local cuivre et une technologie VDSL.
- Avec les technologies FTTB, la fibre optique s'arrête au pied de l'immeuble ; les derniers mètres de raccordement sont effectués en utilisant les câbles de cuivre existants.
- Avec la technologie FTTH, la fibre optique est déployé jusqu'au domicile de l'abonné.

Types de technologies Xpon

Il existe plusieurs types de technologies Xpon : [30]

- **GPON (Gigabit Passive Optical Network) :** cette technologie permet de fournir des débits allant jusqu'à 2,5 Gbit/s en descendant et 1,25 Gbit/s en montant.
- **EPON (Ethernet Passive Optical Network) :** c'est une version de la technologie xPON qui utilise la technologie Ethernet pour fournir des services de haut débit.
- **XG-PON (10 Gigabit Passive Optical Network) :** cette technologie permet de fournir des débits allant jusqu'à 10 Gbit/s en descendant et 2,5 Gbit/s en montant.
- **NG-PON2 (Next Generation Passive Optical Network 2) :** c'est la technologie la plus récente de la famille xPON, qui permet de fournir des débits allant jusqu'à 40 Gbit/s en descendant et 10 Gbit/s en montant.

5.2.1 Architectrure X-PON

PON est basée sur des composants opyions tels que : [31]

- **Optical Line Terminal (OLT) :** C'est l'équipement de la tête de réseau de la PON. Il assure la gestion, le contrôle et la distribution des signaux optiques aux récepteurs.
- **Optical Network Unit (ONU) :** C'est l'équipement utilisé par l'utilisateur final pour accéder au réseau. Il reçoit les signaux optiques de l'OLT et les convertit en signaux électriques.
- **Optical Splitter :** Il assure la répartition du signal optique en plusieurs directions, permettant ainsi de connecter plusieurs ONUs à une seule OLT.
- **Optical Fiber :** C'est le support de transmission des signaux optiques. Il est utilisé pour relier l'OLT aux ONUs et autres équipements du réseau.

La figure 1-8 illustre l'architecture de la technologie Xpon :

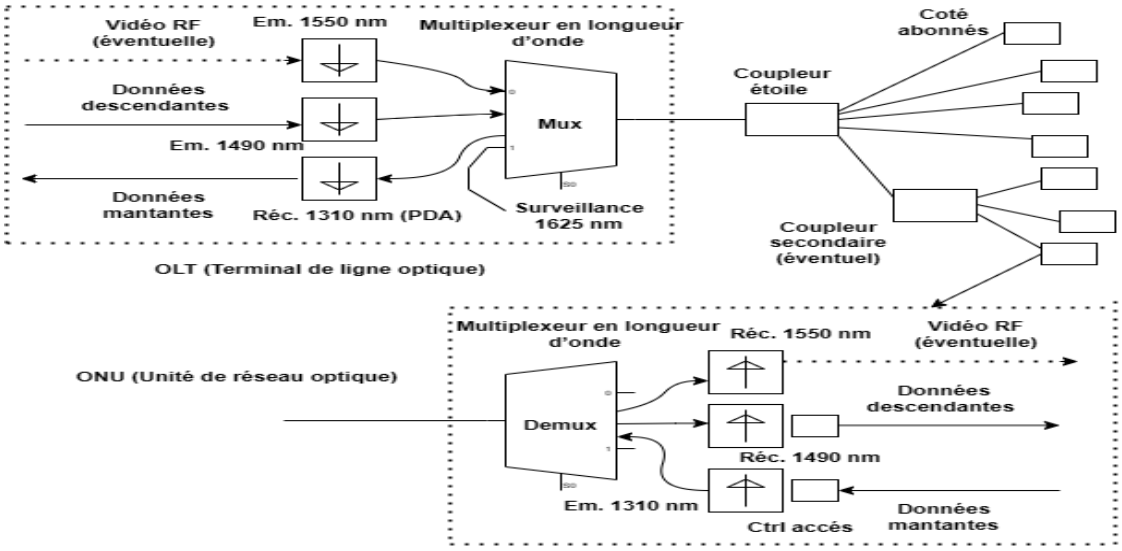

Figure 1-8 : Architecture de la technologie Xpon [32]

5.2.2 Avantages et inconvénients de la technologie Xpon

Le tableau 1-10 présente les avantages et les inconvénients de la technologie Xpon :

Avantages	Inconvénients
• **Haut débit :** Elle offre une bande passante supérieure par rapport à d'autres technologies telles que l'ADSL ou le câble coaxial, permettant d'obtenir des vitesses de téléchargement et de téléversement	• **Coûts élevés :** La technologie Xpon nécessite un investissement important dans l'installation des équipements nécessaires pour la transmission des signaux sur un réseau de fibre optique. • **Dépendance du fournisseur :** Les

plus rapides. • **Fiabilité :** Les réseaux Xpon sont généralement plus sûrs et plus fiables car ils ne sont pas affectés par les interférences électromagnétiques et les perturbations environnementales. • **Économie d'énergie :** Comme les signaux optiques sont transportés sur un câble en fibre optique, l'énergie nécessaire pour transporter les signaux est considérablement réduite, entraînant ainsi une économie d'énergie. • **Distance de transmission :** Les signaux Xpon peuvent être transmis sur une longue distance, jusqu'à 20 kilomètres, sans perte de qualité.	réseaux Xpon sont souvent construits et exploités par des fournisseurs de services Internet (FSI) ou des opérateurs de télécommunications, ce qui signifie que les abonnés dépendent de ces fournisseurs pour l'accès à Internet. • **Infrastructures limitées :** Le déploiement de la fibre optique nécessaire pour les réseaux Xpon est limité géographiquement, ce qui signifie que certains abonnés dans des zones rurales ou éloignées peuvent ne pas y avoir accès.

Tableau 1- 10 : Avantages et les inconvénients de la technologie Xpon. [33]

La technologie X-PON offre des avantages significatifs en termes de haut débit, de grande capacité, de distance de transmission et de fiabilité. Cependant, elle comporte également des inconvénients tels que des coûts élevés, une dépendance à l'alimentation électrique et une complexité de gestion. Il est important d'évaluer attentivement ces aspects en fonction des besoins spécifiques avant de choisir cette technologie pour une mise en œuvre.

5.3 Technologie réseau cellulaire

La technologie de réseau cellulaire est un type de technologie de communication sans fil qui utilise des cellules géographiquement limitées pour offrir une couverture à large bande de données et de voix. Chaque cellule utilise une tour de transmission pour diffuser des signaux radiofréquences à des appareils mobiles tels que les téléphones portables et les tablettes.

Il existe plusieurs types de technologies de réseau cellulaire, notamment :

- **GSM (Global System for Mobile Communications) :** un standard de réseau 2G utilisé pour la voix et les données.

- **CDMA (Code Division Multiple Access) :** une technologie de réseau 2G et 3G utilisée pour la voix et les données.
- **3G (Troisième génération) :** une évolution de la technologie de réseau cellulaire qui permet des débits de données plus rapides.
- **4G (Quatrième génération) :** un réseau cellulaire à haut débit conçu pour une utilisation intensive de la bande passante, y compris la diffusion en continu de vidéos.
- **5G (Cinquième génération) :** une technologie de réseau cellulaire encore plus rapide avec des débits de données gigabit et une latence ultra-basse, destinée à alimenter des technologies émergentes telles que l'Internet des objets et les véhicules autonomes. [34]

5.3.1 Comparaison entre la 4G et la 5G

Il y a plusieurs différences principales entre la 4G et la 5G. La 5G :

- **Vitesse de connexion :** la 5G offre une vitesse de connexion beaucoup plus rapide que la 4G. Les vitesses de téléchargement et de téléversement peuvent être jusqu'à 10 fois plus rapides que la 4G.
- **Latence réduite :** la 5G offre une latence considérablement réduite par rapport à la 4G. Cela signifie que la connexion sera beaucoup plus rapide et plus réactive.
- **Efficacité énergétique :** la 5G est plus efficace en termes d'utilisation de l'énergie que la 4G. Cela se traduira par une meilleure durée de vie de la batterie de votre smartphone.
- **Capacité de traitement accrue :** la 5G permettra de traiter beaucoup plus de données que la 4G. Cela se traduira par une meilleure expérience utilisateur pour les applications qui nécessitent une grande quantité de données.
- **Connectivité massive des objets :** la 5G permettra de connecter un grand nombre d'objets ensemble. Cela signifie que les objets connectés pourront communiquer beaucoup plus rapidement et efficacement. [35]

5.3.2 Avantages et inconvénients de la technologie réseau cellulaire

Le tableau 1-11 présente les avantages et les inconvénients de la technologie réseau cellulaire :

Avantages	Inconvénients
• **La portabilité :** les utilisateurs peuvent accéder au réseau cellulaire depuis n'importe quel endroit dans	• **Les coûts élevés :** les coûts d'utilisation des réseaux cellulaires peuvent être relativement élevés, surtout si l'utilisateur

la zone de couverture du réseau. • **Les communications en temps réel :** grâce à la technologie cellulaire, les utilisateurs peuvent communiquer avec leurs contacts en temps réel, que ce soit pour des appels ou des messages textuels. • **La possibilité de naviguer sur internet :** les réseaux cellulaires permettent également aux utilisateurs de naviguer sur Internet depuis leur téléphone portable ou leur tablette. • **La disponibilité 24h/24 et 7j/7 :** les réseaux cellulaires sont généralement disponibles en permanence, ce qui permet aux utilisateurs d'accéder à leurs services à tout moment.	effectue de nombreuses communications ou utilise fréquemment des services de données. • **La qualité variable du réseau :** la qualité du réseau cellulaire peut varier en fonction de l'endroit où l'utilisateur se trouve, ainsi que de la saturation du réseau. • **Les problèmes de sécurité :** les communications via les réseaux cellulaires peuvent être interceptées par des tiers, ce qui peut poser des problèmes de sécurité pour les utilisateurs.

Tableau 1- 11 : Avantages et les inconvénients de la technologie réseau cellulaire. [36]

Les réseaux cellulaires offrent une connectivité mobile pratique et une large couverture, mais ils peuvent être coûteux et présenter des problèmes de fiabilité et de sécurité. Il est important de peser ces avantages et inconvénients lors de l'évaluation de l'utilisation de cette technologie.

6 Conclusion

En conclusion, les réseaux informatiques sont devenus des outils indispensables pour les entreprises. Les avancées technologiques ont permis de développer des réseaux performants, sécurisés et évolutifs, qui peuvent répondre aux besoins croissants des entreprises en matière de communication et de partage de données.

Le chapitre suivant sera consacré à la présentation de l'organisme d'accueil et l'étude de son réseau.

Chapitre II : Etude de l’architecture existante et proposition de solutions.

1 Introduction

Dans ce chapitre, nous allons présenter l'entreprise pour laquelle nous avons effectué notre stage. Nous allons notamment décrire sa structure, ses services ainsi que ses missions afin d'avoir une meilleure compréhension de sa situation actuelle. Nous aborderons ensuite le réseau informatique de l'entreprise à travers l'identification de ses principales faiblesses et des besoins des utilisateurs pour proposer des solutions adaptées. Enfin, nous discuterons du système CVSS qui permet d'évaluer la gravité des vulnérabilités de l'entreprise et proposer une correction.

2 Présentation de l'organisme d'accueil

2.1 Définition de l'organisme d'accueil

L'Etablissement National de la Navigation Aérienne (ENNA) de Béjaïa est une entité publique algérienne chargée de la gestion de la circulation aérienne dans la région de Béjaïa. L'établissement est chargé d'assurer la sécurité et la régularité des vols dans la région en fournissant des services de navigation aérienne tels que le contrôle de la circulation aérienne, la surveillance radar, la communication et l'information de vol aux équipages des aéronefs.

L'ENNA de Béjaïa assure également la gestion des aéroports de la région et est responsable de l'exploitation, de la maintenance et de la sécurité des équipements et des infrastructures aéroportuaires [37].

L'ENNA de Béjaïa fait partie du réseau national de contrôle de la navigation aérienne et coopère avec d'autres entités similaires pour fournir une coordination et un suivi efficaces du trafic aérien. La figure 2-1 présente l'ENNA de Bejaia :

Figure 2-1 : ENNA de Bejaia

2.2 Historique de l'entreprise ENNA

Depuis l'indépendance, cinq organismes ont été chargés de la gestion, de l'exploitation et du développement de la navigation aérienne en Algérie : OGSA ONAM, ENEMA, ENESA, ENNA.

De 1962 à 1968 c'est l'Organisation de Gestion et de Sécurité Aéronautique (OGSA), organisme Algéro-Français, qui a géré l'ensemble des services d'Exploitation de l'Aviation Civile en Algérie.

Le 1 Janvier 1968, l'OGSA a été remplacé par l'Office de la Navigation Aérienne et de la Météorologie (ONAM). Ce dernier a été remplacé, en 1969, par l'Etablissement National pour l'Exploitation Météorologique et Aéronautique (ENEMA) qui a géré la navigation aérienne jusqu'à 1983.

En 1975, les activités de météorologie ont été transférées à l'Office National de Météorologie créé le 29 Avril 1975, sous forme d'Etablissement Public à caractère administratif.

Le décret N°83.311 du 07/05/1983 a réaménagé les structures de L'ENEMA et modifié sa dénomination pour devenir ENESA « Entreprise Nationale d'Exploitation et de Sécurité Aéronautique » avec statut d'entreprise nationale à caractère économique [37].

Afin de clarifier les attributions de l'ENESA, il a été procédé aux réaménagements de ses statuts ainsi qu'au changement de dénomination en « ENNA » par décret exécutif N° 91-149 du 18 mai 1991. La figure 2-2 illustre le logo de l'entreprise ENNA :

Figure 2-2 : ENNA

2.3 Organisation d'ENNA

2.3.1 Organigramme d'ENNA

L'ENNA, est un Etablissement Public à Caractère Industriel et Commercial (EPIC), sous tutelle du Ministère des Travaux Publics et des Transports, est dirigé par un directeur général et administré par un Conseil d'Administration se basant sur une gradation hiérarchique.

L'établissement assure le service public de sécurité de la navigation aérienne dont fait partie la DSA de Bejaia. La figure 2-3 illustre L'organigramme de l'organisation ENNA [37] :

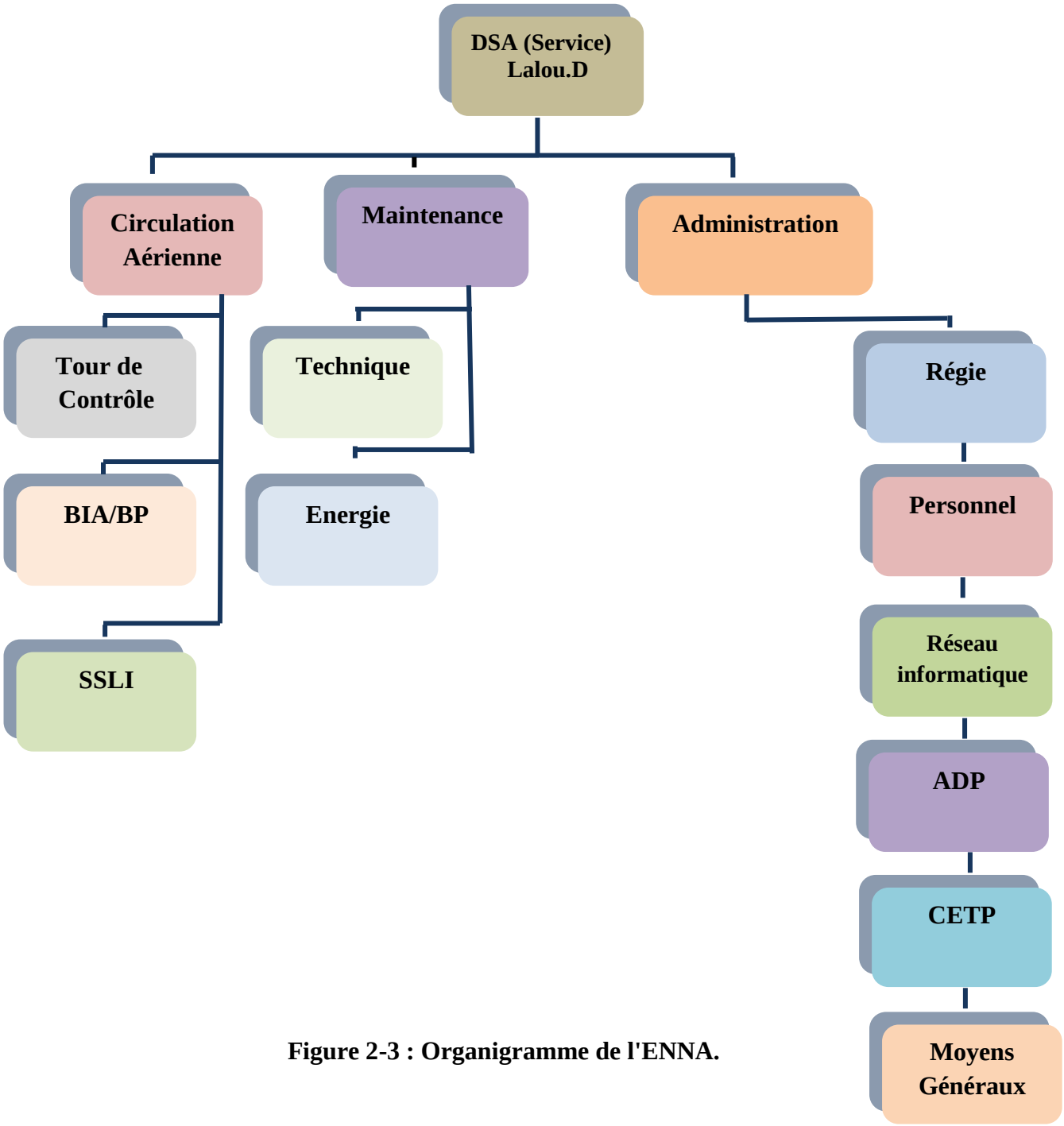

Figure 2-3 : Organigramme de l'ENNA.

2.3.2 Structure de l'entreprise ENNA

L'ENNA, est constitué d'un bloc technique/administratif (tour de contrôle), un bloc SSLI (service de sécurité et lutte contre les incendies), une centrale d'énergie électrique, différentes installations de radionavigation, balisage, pylônes d'éclairages parking, une piste d'atterrissage d'une longueur de 2400m. En effet le transport aérien est vital pour les

communautés éloignées [37].

La direction ENNA /Bejaia est implantée au niveau aérodrome représentée par un directeur de sécurité aéronautique avec des services répartis comme il est monté dans la figure 2-4 [37] :

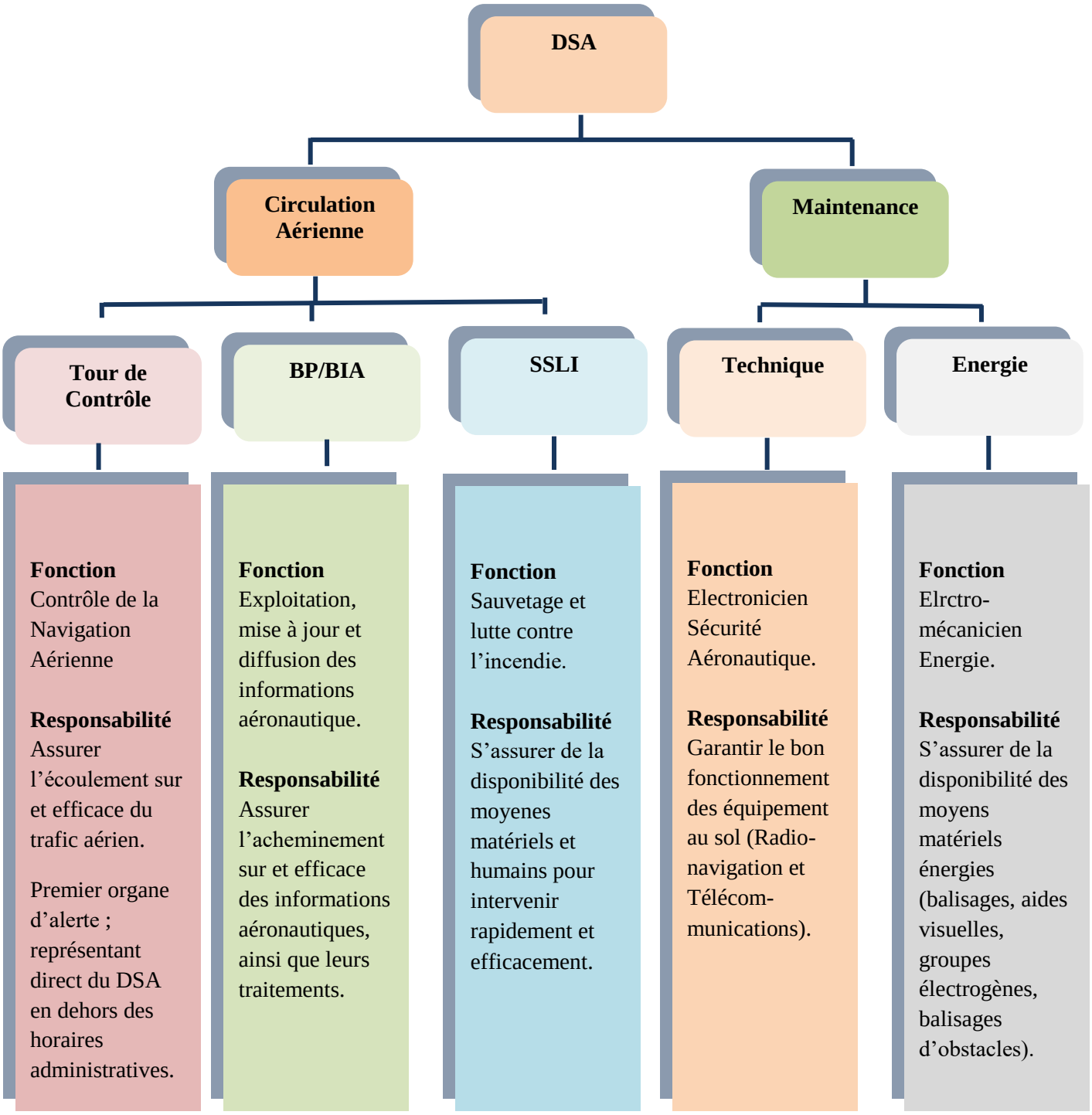

Figure 2-4 : Structure de l'entreprise ENNA

2.3.2.1 Service circulation aérienne

- **Tour de contrôle :** La tour de contrôle est l'organe le plus visible de toute la chaine dédiée au contrôle aérien c'est à partir d'elle que les « contrôleurs du ciel » opèrent pour guider les avions dans les phases du vol liées au survol de l'aéroport :

  - Instruction pour les phases finales d'approche et délivrance de l'autorisation d'atterrir, délivrance de l'autorisation de décollage et instruction pour rejoindre le couloir aérien défini dans le plan de vol de l'avion.

  - La tour de contrôle est placée de manière à pouvoir suivre visuellement les évolutions des avions sur les voies de circulation et sur les pistes, c'est elle qui gère, en fonction des conditions météorologiques, le choix des pistes à utiliser et l'activation de balisage lumineux au sol.

- **Bureau d'information aéronautique :** Le bureau d'information traite les plans de vol, gestion et la publication de l'information aéronautique, la diffusion des messages d'urgence liée à la sécurité aéronautique et le contrôle des documents pour le personnel navigant.

2.3.2.2 Service Sécurité Incendie et Sauvetage

Le service assure la lutte contre les incendies au sein de l'aérodrome, le secours et le sauvetage des passagers en cas d'incendie dans un avion. La figure 2-5 présente le bloc SSLI de l'ENNA :

Figure 2-5 : Bloc SSLI.

2.3.2.3 Service administratif

Le service est assuré par le directeur et l'assistant de direction. Il se charge de la gestion de personnel et des moyens financiers et comptabilité, œuvres sociales, contentieux, projets et redevances aéronautiques sur les différents atterrissages, il rend compte périodiquement de la situation à la direction générale dont le siège se trouve à Alger.

2.3.2.4 Service Technique

Il comprend à son tour deux services à savoir le service radionavigation et le service énergie et balisage.

- **Service radionavigation** : Est assuré par des électroniciens sécurité aérienne, leur mission est l'installation des équipements de radionavigation télécommunications et veiller à leurs bon fonctionnements. La radionavigation est assurée par un équipement spécifique dont :
  - Balise non directionnelle (non Directionnel Bacon) NDB
  - Very High Frequency unidirectional bange (VOR) alignement omnidirectionnel (VHF).
  - Distance measuring équipement (DME) équipement de mesure de distance.
  - instrument landing system (ILS) système d'aide à l'atterrissage aux instruments.
  - Dipôle de champs.
- **Service Energie et Balisage :** Ce service est assuré par des électrotechniciens sécurité aérienne, leur mission est l'installation et la maintenance de tous les équipements d'énergie et balisages lumineux aéroportuaire et ils veillent au bon fonctionnement et à la continuité du service en cas de coupure d'énergie électrique.

2.4 Situation géographique de l'ENNA

L'établissement (ENNA) se situe à l'aérodrome de BEJAIA SOUMMAM ABANE RAMDHANE en bordure de mer et occupe la plaine alluvionnaire de l'embouchure sur la rive droite de l'ouest à 2,6km (notical mille 1nm=1852m) (mille marins) et à 4,8 km au sud-ouest de Bejaia ville. La figure 2-6 présente la Situation géographique de l'aéroport de Bejaia (ENNA) :

Figure 2-6 : Situation géographique de l'aéroport de Bejaia (ENNA).

3 Présentation du réseau de l'entreprise

Le réseau informatique est un outil essentiel pour la DSA Bejaia qui souhaite optimiser son utilisation des nouvelles technologies de l'information et de la communication. Grâce à ce réseau, l'entreprise pourra bénéficier de toutes les améliorations apportées par ces technologies. Ce réseau fait partie du projet plus global de construction du réseau informatique de l'ENNA, qui dispose actuellement d'une topologie en étoile. Le réseau est basé sur la famille des protocoles TCP/IP, ce qui garantit une connectivité universelle et une compatibilité accrue avec les autres équipements informatiques. Actuellement, l'entreprise dispose d'un réseau avec un switch non administrable, non empilable et non évolutif, ce qui limite sa capacité d'adaptation et d'expansion. Il est donc important de mettre à jour le matériel et de réfléchir à de nouvelles configurations pour répondre aux besoins présents et futurs. La figure 2-7 illustre l'architecture du réseau ENNA :

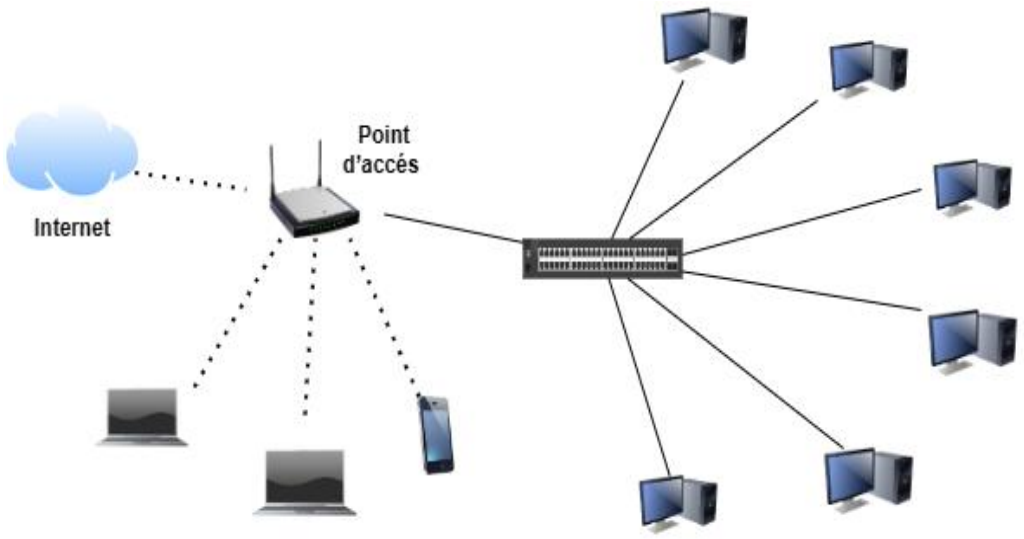

Figure 2-7 : Architecture du réseau ENNA.

3.1 Problématique

De nos jours, la compétitivité des entreprises est un enjeu majeur. Elles cherchent constamment à améliorer leur productivité tout en réduisant leurs coûts, notamment en adoptant de nouvelles technologies matérielles ou logicielles. Dans ce contexte, le réseau de l'ENNA nécessite un système de communication efficace qui soit capable de sécuriser les données de l'entreprise. Cependant, après une étude approfondie, il apparait que le réseau LAN de l'entreprise n'est pas exploité en raison de l'absence de logiciel pour serveur et de matériel réseau adéquats. Notre projet consiste à mettre en place un système adapté aux besoins de l'ENNA qui permettra de sécuriser leurs informations et de limiter l'accès aux données en fonction des différents niveaux d'accessibilité adaptés aux tâches de travail assignées. Ce système permettra également de faciliter le partage d'informations entre les membres de l'entreprise de manière efficace et confidentielle.

3.2 Critiques

L'étude du réseau de l'ENNA, nous a permis de déterminer un nombre important de contraintes pouvant réduire ses performances, voir sa dégradation, on a :

- Le réseau local est installé anarchiquement et non administré et non sécurisé.
- La configuration du switch est basique (switch non empilable, non administrable et non évolutif).
- L'absence d'une segmentation du réseau en vlan ou en sous-réseau favorise l'action des utilisateurs pirates.
- L'absence d'un serveur principal pour héberger les différentes applications partagées sur le réseau.
- L'absence d'un contrôle d'accès aux stations de travails.
- L'absence de control d'accès à certains sites internet qui ralentissent les employés dans leur travail (YouTube, Facebook).
- Les utilisateurs ne possèdent pas des adresses électroniques institutionnels, et cela peut rendre les données de l'entreprise vulnérables aux attaques informatiques. .

Au regard de toutes ces difficultés rencontrées, l'ENNA souhaiterait mettre en place un système de gestion et de suivi plus efficace de son réseau. C'est ainsi qu'il nous a été proposé de réfléchir sur le thème: «Conception et déploiement d'une architecture réseau sécurisée à la direction de la sécurité Aéronautique de Bejaia ».

3.3 Analyse de vulnérabilités

Pour évaluer la gravité des vulnérabilités trouvées dans l'ENNA, une méthode a été utilisée pour estimer leur gravité. Cette méthode s'appelle le système CVSS (Common Vulnerability Scoring System). Nous avons la choisis parce qu'elle est largement utilisée dans le domaine de la cybersécurité Elle fournit une mesure standardisée permettant de quantifier l'impact, l'exploitabilité et la complexité d'une vulnérabilité. Cette méthode permet aux professionnels de la sécurité de hiérarchiser les vulnérabilités et de prendre des décisions éclairées pour les corriger en fonction de leur priorité.

3.3.1 Présentation de système CVSS

Le Common Vulnerability Scoring System (CVSS) est un système d'évaluation standardisé des vulnérabilités dans les logiciels et les systèmes informatiques. Le CVSS permet de mesurer l'impact potentiel d'une vulnérabilité sur la confidentialité, l'intégrité et la disponibilité des données. Il est utilisé pour évaluer la gravité d'une vulnérabilité et prioriser les mesures de sécurité à prendre pour la corriger. [38]

3.3.2 Métriques de CVSS

Le Common Vulnerability Scoring System Est constituée de trois mesures appelées métriques: métrique de base, métrique temporelle et la métrique environnementale.

3.3.2.1 Métrique de base

Cette métrique évalue les caractéristiques intrinsèques d'une vulnérabilité. Elle prend en compte l'impact potentiel et la faisabilité de l'exploitation de la vulnérabilité. Elle se base sur trois critères principaux : la confidentialité (C), l'intégrité (I) et la disponibilité (A). Le score de base du CVSS est calculé à partir de la formule suivante : « Score de Base = 0.6*C + 0.3*I + 0.1*A », Le score de base est compris entre 0 et 10. [39]

- **Métrique d'exploitation**
  - **Vecteur d'accès :** Le vecteur d'accès de CVSS (Common Vulnerability Scoring System) est une chaîne de caractères qui permet d'évaluer la sévérité d'une vulnérabilité informatique. Voici un exemple de vecteur d'accès CVSS : AV:N/ AC:M/ AU:N /C:P /I:P /A:P. [40]
  - **Complexité d'accès :** La complexité d'accès dans CVSS mesure à quel point un attaquant doit s'ingénier pour exploiter une vulnérabilité donnée. Elle est notée de 0.0 (le moins complexe) à 1.0 (le plus complexe). [41]

- **Authentification** : la mesure d'authentification de CVSS mesure l'impact potentiel d'une vulnérabilité sur l'authentification et l'identification des utilisateurs. La métrique d'authentification CVSS évalue la probabilité que l'attaque réussisse en fonction de l'authentification requise pour exploiter la vulnérabilité. Elle prend en compte plusieurs facteurs, tels que la complexité de l'attaque et les privilèges requis, pour calculer un score de gravité. [42]

➢ **Métrique d'impact**

- **Métrique de confidentialité** (Confidentiality Impact) fait partie du système de notation CVSS (Common Vulnerability Scoring System), qui est un standard industriel permettant d'évaluer la gravité des vulnérabilités informatiques. Elle mesure l'impact qu'une vulnérabilité peut avoir sur la confidentialité des données. Plus précisément, la métrique d'impact confidentialité évalue dans quelle mesure la vulnérabilité permet à un attaquant d'accéder à des informations confidentielles, de modifier, de supprimer ou de bloquer l'accès à ces informations. [39]
- **Métrique d'intégrité** est une mesure utilisée pour évaluer le degré d'impact qu'une vulnérabilité peut causer en termes d'intégrité des données. Cette métrique mesure la capacité de l'attaque à modifier ou détruire les données d'une application ou d'un système. [43]
- **Métrique de disponibilité** mesure l'impact qu'une vulnérabilité peut avoir sur la disponibilité d'un système informatique. Elle prend en compte le temps de récupération nécessaire pour rétablir la disponibilité du système et les conséquences liées à l'indisponibilité (pertes financières, atteinte à la réputation, etc.). Cette métrique est notée de 0 à 10, 10 indiquant un impact maximal sur la disponibilité. [43]

3.3.2.2 Métrique temporelle

La métrique temporelle de CVSS (Common Vulnerability Scoring System) est l'un des groupes de métriques utilisées pour attribuer des scores de vulnérabilité aux vulnérabilités informatiques. Elle évalue la probabilité qu'un attaquant exploite une vulnérabilité dans un certain laps de temps après sa découverte. La métrique temporelle de CVSS est divisée en trois sous-métriques [43]:

- Exploitabilité (E) qui mesure la facilité avec laquelle un attaquant pourrait exploiter avec succès une vulnérabilité.

- Remédiation (R) qui mesure le temps nécessaire pour corriger la vulnérabilité une fois qu'elle est découverte.
- Reportabilité (RC) qui mesure la probabilité qu'une vulnérabilité soit signalée à la personne chargée de l'appliquer.

3.3.2.3 Métrique environnementale

La métrique environnementale de système CVSS permet de calculer un score de vulnérabilité qui prend en compte les caractéristiques de l'environnement cible où la vulnérabilité est présente. Ce score est basé sur des facteurs tels que l'impact potentiel sur la confidentialité, l'intégrité et la disponibilité des données et des systèmes. Le score final de vulnérabilité, qui prend en compte la métrique environnementale, peut aider à évaluer la gravité d'une vulnérabilité et à prioriser les actions nécessaires pour la corriger. [40]

3.3.3 Système de notation de gravité

Le système de notation de gravité utilisé inclut quatre niveaux: critique, élevé, modéré et faible. Ces niveaux sont attribués en fonction du score CVSS de chaque vulnérabilité. Cette information est cruciale pour permettre aux utilisateurs de prendre les mesures nécessaires pour protéger leur système contre les vulnérabilités identifiées.

Le tableau 2-1 présente le système de notation de gravité du système CVSS :

Plage de score CVSS v3	Gravité de l'avertissement
9,0 - 10	**Critique**
7,0 - 8,9	**Elevé**
4,0 - 6,9	**Moyen**
0,1 - 3,9	**Bas**

Tableau 2-1 : Système de ntation de gravité.

3.3.4 Evaluation de vulnérabilités détectées

Le tableau 2-2 présente l'évaluation de vulnérabilités que nous avons détectées :

La vulnérabilité	ARP Spoofing	MAC Flooding	DHCP Starvation	DHCP Spoofing	Switch Spoofing	Double Tagging
Le vecteur d'accès	**Réseau**	**Réseau**	**Réseau**	**Réseau**	**Local**	**Local**

La complexité d'accès	**Bas**	**Bas**	**Bas**	**Bas**	**Bas**	**Bas**
L'authentification	**Inexistant**	**Inexistant**	**Inexistant**	**Inexistant**	**Inexistant**	**Inexistant**
L'impact de confidentialité	**Complet**	**Aucun**	**Aucun**	**Partiel**	**Complet**	**Complet**
L'impact d'intégrité	**Complet**	**Aucun**	**Aucun**	**Partiel**	**Complet**	**Complet**
L'impact de disponibilité	**Partiel**	**Complet**	**Complet**	**Complet**	**Complet**	**Complet**
Le score de Base	**Elevé**	**Elevé**	**Elevé**	**Elevé**	**Elevé**	**Elevé**
L'exploitabilité	**Elevé**	**Elevé**	**Elevé**	**Elevé**	**Elevé**	**Elevé**
La remédiation	**Elevé**	**Elevé**	**Moyenne**	**Elevé**	**Elevé**	**Elevé**
La reportabilité	**Moyenne**	**Moyenne**	**Elevé**	**Elevé**	**Elevé**	**Elevé**
Le score temporel	**Moyen**	**Moyen**	**Elevé**	**Elevé**	**Elevé**	**Elevé**
L'exigence de confidentialité	**Elevé**	**Bas**	**Bas**	**Bas**	**Elevé**	**Elevé**
L'exigence d'intégrité	**Elevé**	**Bas**	**Bas**	**Bas**	**Elevé**	**Elevé**
L'exigence de disponibilité	**Elevé**	**Elevé**	**Elevé**	**Elevé**	**Elevé**	**Elevé**
Le score environnemental	**Elevé**	**Elevé**	**Elevé**	**Elevé**	**Elevé**	**Elevé**
Score Final	**Elevé**	**Elevé**	**Elevé**	**Elevé**	**Elevé**	**Elevé**

Tableau 2-2 : Evaluation de vulnérabilités détectées.

3.4 Solutions envisagés

Après avoir étudié le réseau, analysé ses failles, nous mettrons le point sur les objectifs et les étapes à suivre pour mettre en œuvre les solutions proposés. Pour cela nous avons opté pour :

- L'installation d'un switch administrable, empilable et évolutif.
- La création des VLANs afin de segmenter et d'améliorer la sécurité du réseau local.
- L'implémentation d'une nouvelle infrastructure à base d'un active Directory sous Windows server 2016 pour le réseau de l'ENNA.

- La mise en place d'un contrôleur de domaine, les règles d'accès et les différentes stratégies de groupe.
- L'installation et la configuration d'un serveur DNS pour associer les noms d'ordinateur à des adresses IP et un serveur DHCP pour attribuer automatiquement les adresses IP aux machines client.
- La mise en œuvre d'un serveur de fichier et de stockage pour fournir un espace de stockage centralisé pour les données partagées par les utilisateurs d'un réseau, et pour permettre aux utilisateurs d'accéder et de partager des fichiers de manière efficace.
- La mise en œuvre d'un serveur d'impression, afin d'améliorer la sécurité et la gestion de plusieurs imprimantes à partir d'un emplacement centralisé.
- La mise en œuvre d'une plateforme de messagerie Exchange 2016 afin d'assurer un transfert de données confidentielles de manière efficace et sécurisée, en utilisant les adresses électroniques institutionnelles.

Les vulnérabilités identifiées ont un score CVSS v3 élevé, ce qui signifie que l'exploit associé représente un danger important et peut causer des dommages considérables. Il est donc crucial de prendre des mesures proactives pour corriger ces vulnérabilités et réduire les risques de compromission de la sécurité. Par ailleurs, il est recommandé de :

- Sécuriser les ports d'accès,
- Configurer la fonctionnalité « DHCP snooping » sur les VLANs,
- Configurer les ports d'un commutateur connectés aux hôtes comme des ports d'accès.
- Affecter les ports inutilisés à un VLAN dédié et les désactiver,
- Créer un VLAN dédié pour le trafic du VLAN natif séparé du trafic utilisateurs.

3.5 Architecture proposée

Après une étude et une analyse de réseau de l'entreprise ENNA on a constaté que ce dernier a manque de matériel et logiciel (Switch administrable, empilable et évolutif et avec un serveur AD) pour réaliser un réseau performant et sécurisé on a met en fonction un serveur Windows 2016 afin d'améliorer l'organisation interne de l'entreprise en optimisant et centralisé la gestion des données et on a pensé à créer des VLANs qui vont regrouper les ordinateurs et les périphériques en fonction du département, du service ou de la fonction, toute en respectant la politique de sécurité .

La figure 2-8 présente l'architecture de la solution que nous avons proposée :

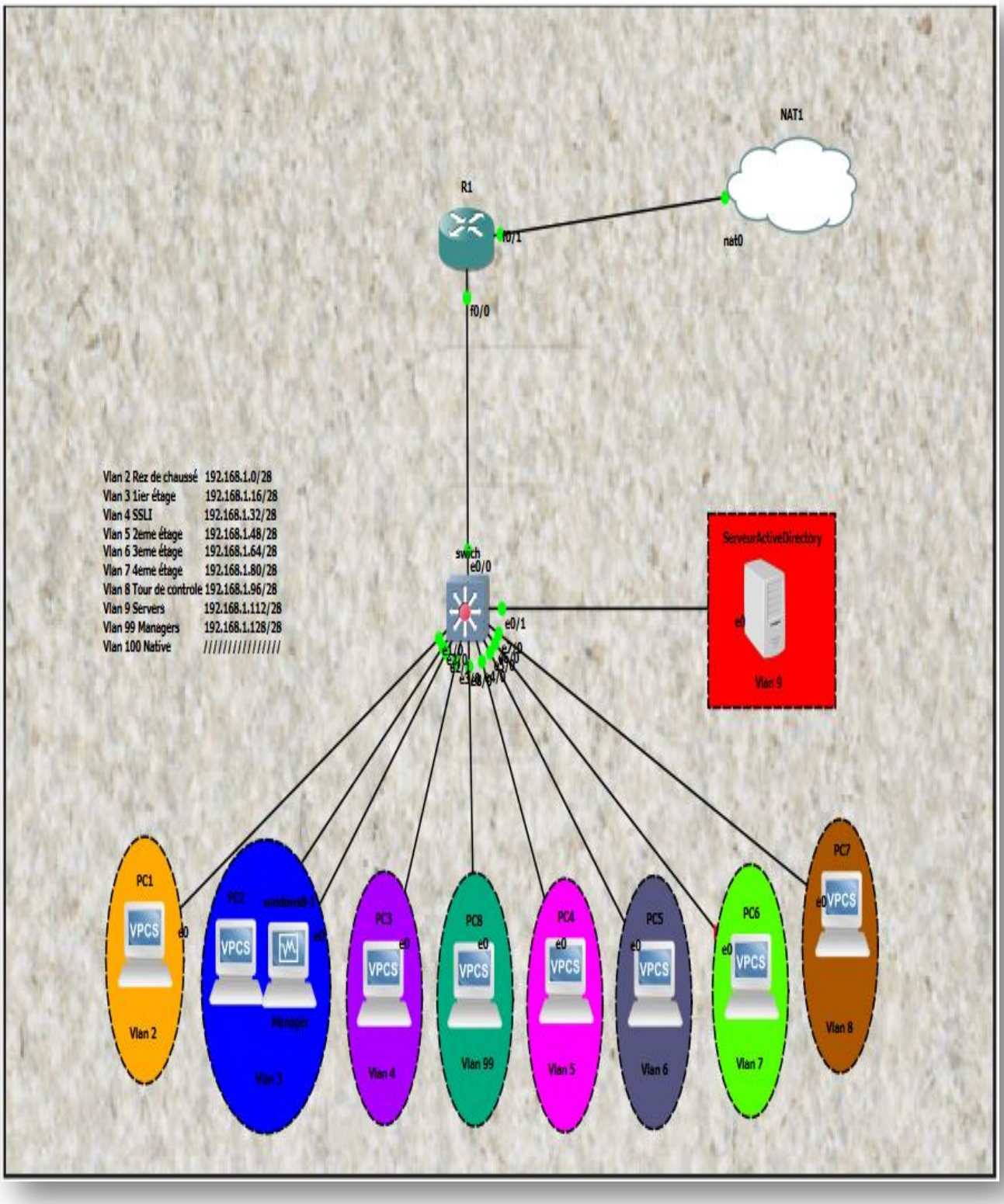

Figure 2-8 : Architecture proposée du réseau de l'ENNA.

4 Conclusion

Ce chapitre a été dédié à une présentation complète de l'entreprise, ainsi qu'à l'analyse de son réseau informatique et à l’évaluation de la sévérité de ses vulnérabilités. Cette étude nous a permis d'identifier les faiblesses de l'entreprise et de proposer des solutions adaptées pour répondre aux besoins des utilisateurs. Nous sommes convaincus que cette analyse approfondie a été bénéfique pour l'entreprise en termes d'amélioration de la sécurité de son réseau et de l'efficacité de ses services.

Le prochain chapitre portera sur la partie pratique de ce thème de mémoire.

Chapitre III : Réalisation.

1 Introduction

Ce chapitre est essentiellement consacré à la mise en œuvre pratique de notre application sur le réseau informatique de l'ENNA, en détaillant les étapes clés de configuration des VLANs de l'installation et de la configuration de notre Active Directory, ainsi que des services de fichiers et de stockage, du serveur d'impression et du serveur de messagerie. Nous terminons en exposant les résultats des tests de vérification, qui confirment le bon fonctionnement de notre application. Cette étape de déploiement est d'une importance cruciale pour la réalisation de notre projet qui nous permettra de réaliser avec succès notre projet et de répondre aux besoins de l'ENNA.

2 Plan d'adressage

2.1 Tableau d'adressage des VLANs

Nous avons créé 10 VLANs qu'on site au tableau ci-dessous : Ce tableau présente le dimensionnement de notre réseau au niveau des VLANs. Le tableau 3-1 présente le plan d'adressage des VLANs :

VLAN ID	Nom du VLAN	Adresse de sous-réseau	Masque de sous-réseau
Vlan 2	Rez de chaussé	192.168.1.0	255.255.255.240
Vlan 3	1ier étage	192.168.1.16	255.255.255.240
Vlan 4	SSLI	192.168.1.32	255.255.255.240
Vlan 5	2ème étage	192.168.1.48	255.255.255.240
Vlan 6	3ème étage	192.168.1.64	255.255.255.240
Vlan 7	4ème étage	192.168.1.80	255.255.255.240
Vlan 8	Tour de contrôle	192.168.1.96	255.255.255.240
Vlan 9	Servers	192.168.1.112	255.255.255.240
Vlan 99	Managers	192.168.1.128	255.255.255.240
Vlan 100	Native	//////////////////////	

Tableau 3-1 : Tableau d'adressage des VLANs.

2.2 Tableau d'adressage des équipements

Le tableau 3-2 présente les adresses IP que nous avons attribuées aux interfaces du routeur et au Windows server 2016 ainsi le vlan du manager du switch :

Nom de l'équipement	L'interface	Adresse IP	Masque de @IP	Passerelle par défaut
Routeur	**F0/1**	**@ fournie par l'internet**		
	F0/0.2	**Encapsulation dot1Q 192.168.1.14**	**255.255.255.240**	**NA**
	F0/0.3	**Encapsulation dot1Q 192.168.1.30**	**255.255.255.240**	**NA**
	F0/0.4	**Encapsulation dot1Q 192.168.1.46**	**255.255.255.240**	**NA**
	F0/0.5	**Encapsulation dot1Q 192.168.1.62**	**255.255.255.240**	**NA**
	F0/0.6	**Encapsulation dot1Q 192.168.1.78**	**255.255.255.240**	**NA**
	F0/0.7	**Encapsulation dot1Q 192.168.1.94**	**255.255.255.240**	**NA**
	F0/0.8	**Encapsulation dot1Q 192.168.1.110**	**255.255.255.240**	**NA**
	F0/0.9	**Encapsulation dot1Q 192.168.1.126**	**255.255.255.240**	**NA**
	F0/0.99	**Encapsulation dot1Q 192.168.1.142**	**255.255.255.240**	**NA**
Switch	**Vlan 99**	**192.168.1.141**	**255.255.255.240**	**192.168.1.142**
Windows Server 2016	**E0**	**192.168.1.125**	**255.255.255.240**	**192.168.1.126**

Tableau 3-2 : Tableau d'adressage des équipements.

Pour les adresses des ordinateurs seront attribuées par le serveur DHCP.

3 Configuration des équipements

3.1 Configuration du routeur

Commençons d'abord par la configuration de base et les outils d'accès à distance :

- Sécurisation de ligne console.
- Sécurisation de l'accès en mode d'exécution privilégié.
- Sécurisation des lignes virtuelles.
- Configuration de l'outil d'accès à distance SSH.

La figure 3-1 illustre la configuration de base du Routeur :

```
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#username cisco password cisco
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#exit
R1(config)#enable secret cisco
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#ip domain-name cisco.com
R1(config)#ip domain-name cisco.com
R1(config)#ip ssh version 2
Please create RSA keys (of atleast 768 bits size) to enable SSH v2.
R1(config)#crypto key generate rsa
The name for the keys will be: R1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar  1 00:07:01.915: %SSH-5-ENABLED: SSH 2.0 has been enabled
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#end
R1#
*Mar  1 00:07:41.691: %SYS-5-CONFIG_I: Configured from console by console
R1#copy run
R1#copy running-config sta
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
R1#
```

Figure 3-1 : La configuration de base du Routeur.

- Nous allons maintenant configurer le routage Inter-VLAN en utilisant des sous-interfaces au niveau du routeur. La figure 3-2 montre les commandes à suivre :

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#no shutd
R1(config-if)#no shutdown
R1(config-if)#
*Mar  1 00:10:03.771: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:10:04.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#interface FastEthernet0/0.2
R1(config-subif)# encapsulation dot1Q 2
R1(config-subif)# ip address 192.168.1.14 255.255.255.240
R1(config-subif)# ip helper-address 192.168.1.125
R1(config-subif)#
*Mar  1 00:10:33.299: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R1(config-subif)#interface FastEthernet0/0.3
R1(config-subif)# encapsulation dot1Q 3
R1(config-subif)# ip address 192.168.1.30 255.255.255.240
R1(config-subif)# ip helper-address 192.168.1.125
R1(config-subif)#interface FastEthernet0/0.4
R1(config-subif)# encapsulation dot1Q 4
R1(config-subif)# ip address 192.168.1.46 255.255.255.240
R1(config-subif)# ip helper-address 192.168.1.125
R1(config-subif)#interface FastEthernet0/0.5
R1(config-subif)# encapsulation dot1Q 5
R1(config-subif)# ip address 192.168.1.62 255.255.255.240
R1(config-subif)# ip helper-address 192.168.1.125
R1(config-subif)#interface FastEthernet0/0.6
R1(config-subif)# encapsulation dot1Q 6
R1(config-subif)# ip address 192.168.1.78 255.255.255.240
R1(config-subif)# ip helper-address 192.168.1.125
R1(config-subif)#interface FastEthernet0/0.7
R1(config-subif)# encapsulation dot1Q 7
R1(config-subif)# ip address 192.168.1.94 255.255.255.240
R1(config-subif)# ip helper-address 192.168.1.125
R1(config-subif)#interface FastEthernet0/0.8
R1(config-subif)# encapsulation dot1Q 8
R1(config-subif)# ip address 192.168.1.110 255.255.255.240
R1(config-subif)# ip helper-address 192.168.1.125
R1(config-subif)#interface FastEthernet0/0.9
R1(config-subif)# encapsulation dot1Q 9
R1(config-subif)# ip address 192.168.1.126 255.255.255.240
R1(config-subif)#interface FastEthernet0/0.99
R1(config-subif)# encapsulation dot1Q 99
R1(config-subif)# ip address 192.168.1.142 255.255.255.240
R1(config-subif)# ip helper-address 192.168.1.125
R1(config-subif)#end
R1#cop
R1#copy
*Mar  1 00:14:10.011: %SYS-5-CONFIG_I: Configured from console by console
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Figure 3-2 : Configuration du routage inter-VLANs.

3.2 Configuration du switch

3.2.1 Création des VLANs

Les VLANs permettent de diviser le réseau physique en plusieurs réseaux logiques. En effet, deux machines qui sont deux VLANs différents ne pourront pas communiquer entre elle. Les VLANs améliorent la gestion du trafic du réseau et renforcent la sécurité en limitant l'accès aux ressources, et réduisent la charge de travail des commutateurs réseau. La figure 3-3 montre les différentes commandes à suivre pour la création des VLANs :

Figure 3-3 : La création des VLANs.

3.2.2 Attribution des ports au VLANs

Les interfaces en mode accès se trouvent au niveau des liens entre le commutateur d'accès et les PC. La figure 3-4 illustre les commandes à suivre :

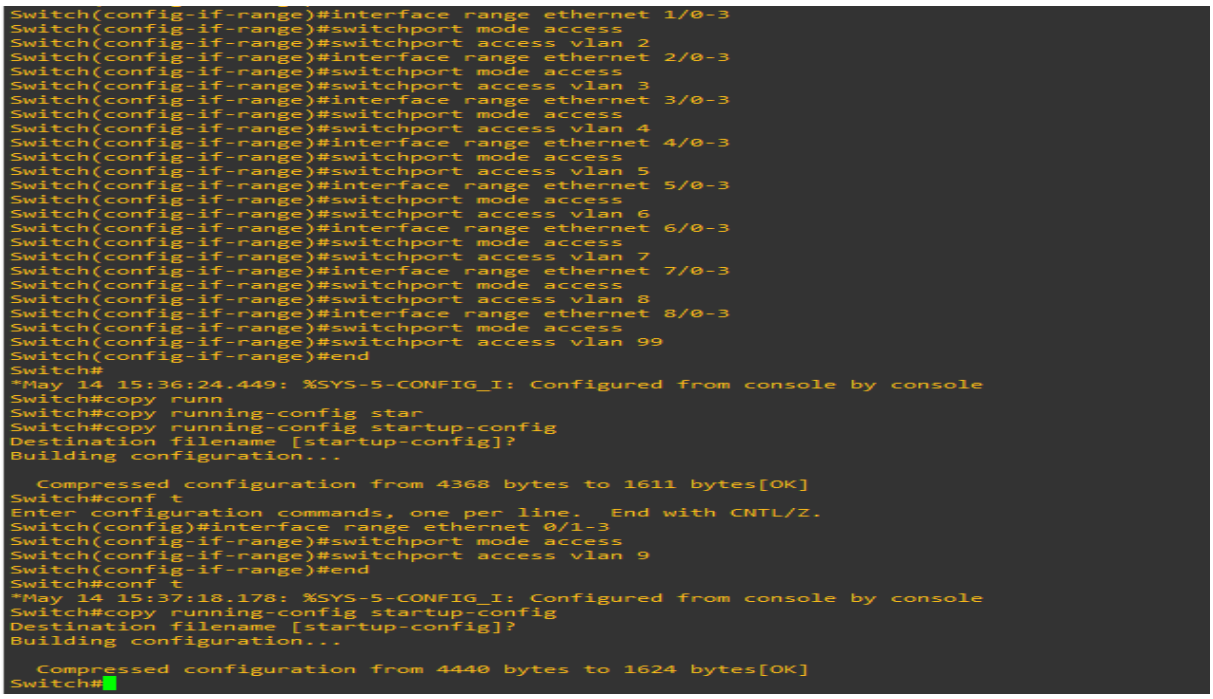

Figure 3-4 : Attribution des ports au VLANs.

3.2.3 Configuration du Vlan managers

Nous allons Attribuer une adresse ip au vlan managers pour pouvoir gérer le switch à distance et activer le mode trunk « **switch port mode trunk** » dans l'interface relier au routeur, La figure 3-5 illustre les configuration à faire :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interfac
Switch(config)#interface eth
Switch(config)#interface ethernet 0/0
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)#
*May 14 15:39:54.976: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
Switch(config-if)#
*May 14 15:39:57.980: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
Switch(config-if)#exit
Switch(config)#interface Vlan99
Switch(config-if)# ip address 192.168.1.141 255.255.255.240
Switch(config-if)#
*May 14 15:40:54.917: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#
*May 14 15:41:52.622: %LINK-3-UPDOWN: Interface Vlan99, changed state to up
*May 14 15:41:53.630: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
Switch(config)#ip default-gateway 192.168.1.142
Switch(config)#exit
Switch#
*May 14 15:41:59.635: %SYS-5-CONFIG_I: Configured from console by console
Switch#copy runn
Switch#copy running-config star
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

  Compressed configuration from 4595 bytes to 1706 bytes[OK]
Switch#
```

Figure 3-5 : Configuration du VLAN managers.

3.2.4 Sécurisation des ports

Une façon d'améliorer la sécurité de réseau consiste à configurer la sécurité des ports qui nous permet de configurer soit un port spécifique ou un groupe d'agrégation de liens, de cette manière nous pouvons limiter ou autoriser l'accès à différentes utilisateurs sur un port ou groupe d'agrégation donné.

Pour commencer il faut d'abord :

- Activer le port de sécurité en encodant une première fois la commande « **switchport port-security** » en configuration d'interface,
- On peut fixer le nombre d'adresse MAC autorisées, ici par exemple 10. Pour ce faire il faut utiliser la commande « **switchport port-security maximum 10** »,

- Les adresses MAC apprise peuvent être inscrites dynamiquement dans la configuration courante avec la commande « **switchport port-security mac-address sticky** ».

- Une violation est une action prise en cas de non-respect d'une règle port-security, dès qu'une violation de sécurité intervient il désactivera automatiquement le port que ne pourra réactiver que par un admin réseau, on utilisant la commande « **switchport port-security violation shutdown ».**

La figure 3-6 montre les différentes commandes de la configuration de la sécurité des ports :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range ethernet 1/0-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 10
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#interface range ethernet 2/0-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 10
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#interface range ethernet 3/0-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 10
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#interface range ethernet 4/0-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 10
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#interface range ethernet 5/0-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 10
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#interface range ethernet 6/0-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 10
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#interface range ethernet 7/0-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 10
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#interface range ethernet 8/0-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 10
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#end
Switch#
*May 14 16:59:55.851: %SYS-5-CONFIG_I: Configured from console by console
Switch#
```

Figure 3-6 : Sécurisation des ports.

3.2.5 Création d'un VLAN et attribuer les ports inutilisés à ce VLAN et les désactiver

Les ports non utilisés sur un switch peuvent constituer un risque pour la sécurité, une méthode simple que de nombreux administrateurs utilisent est de désactiver tous les ports non utilisés.

La commande « **switchport acess vlan 10** » ajoute un niveau de sécurité en plaçant ces interfaces dans un VLAN qui n'est pas utilisé. La figure 3-7 montre les commandes à suivre :

```
Switch(config)#vlan 10
Switch(config-vlan)#name les ports inutilises
Switch(config-vlan)#exit
Switch(config)#interface range ethernet 9/0-3
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#interface range ethernet 10/0-3
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#shutdown
Switch(config-if-range)#shutdown
*May 14 17:29:12.298: %LINK-5-CHANGED: Interface Ethernet10/0, changed state to administratively down
*May 14 17:29:12.302: %LINK-5-CHANGED: Interface Ethernet10/1, changed state to administratively down
*May 14 17:29:12.315: %LINK-5-CHANGED: Interface Ethernet10/2, changed state to administratively down
*May 14 17:29:12.315: %LINK-5-CHANGED: Interface Ethernet10/3, changed state to administratively down
*May 14 17:29:13.298: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet10/0, changed state to down
*May 14 17:29:13.311: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet10/1, changed state to down
Switch(config-if-range)#exit
*May 14 17:29:13.318: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet10/2, changed state to down
*May 14 17:29:13.318: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet10/3, changed state to down
Switch(config-if-range)#exit
Switch(config)#interface range ethernet 11/0-3
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range ethernet 11/0-3
*May 14 17:29:38.075: %LINK-5-CHANGED: Interface Ethernet11/0, changed state to administratively down
*May 14 17:29:38.085: %LINK-5-CHANGED: Interface Ethernet11/1, changed state to administratively down
*May 14 17:29:38.085: %LINK-5-CHANGED: Interface Ethernet11/2, changed state to administratively down
*May 14 17:29:38.086: %LINK-5-CHANGED: Interface Ethernet11/3, changed state to administratively down
*May 14 17:29:39.075: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet11/0, changed state to down
*May 14 17:29:39.085: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet11/1, changed state to down
*May 14 17:29:39.085: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet11/2, changed state to down
*May 14 17:29:39.097: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet11/3, changed state to down
Switch(config-if-range)#exit
Switch(config)#interface range ethernet 12/0-3
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#exit
*May 14 17:30:00.988: %LINK-5-CHANGED: Interface Ethernet12/0, changed state to administratively down
*May 14 17:30:00.999: %LINK-5-CHANGED: Interface Ethernet12/1, changed state to administratively down
*May 14 17:30:01.000: %LINK-5-CHANGED: Interface Ethernet12/2, changed state to administratively down
*May 14 17:30:01.000: %LINK-5-CHANGED: Interface Ethernet12/3, changed state to administratively down
*May 14 17:30:01.994: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet12/0, changed state to down
*May 14 17:30:02.005: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet12/1, changed state to down
*May 14 17:30:02.005: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet12/2, changed state to down
*May 14 17:30:02.005: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet12/3, changed state to down
Switch(config)#interface range ethernet 13/0-3
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#
*May 14 17:30:21.598: %LINK-5-CHANGED: Interface Ethernet13/0, changed state to administratively down
*May 14 17:30:21.598: %LINK-5-CHANGED: Interface Ethernet13/1, changed state to administratively down
*May 14 17:30:21.611: %LINK-5-CHANGED: Interface Ethernet13/2, changed state to administratively down
*May 14 17:30:21.611: %LINK-5-CHANGED: Interface Ethernet13/3, changed state to administratively down
*May 14 17:30:22.604: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet13/0, changed state to down
```

Figure 3-7 : Attribuer les ports inutilisés à un VLAN et les désactiver.

3.2.6 Création du VLAN natif

Le VLAN natif est un VLAN dans lequel seront placées les frames non taguées, donc si un switch reçoit sur une interface trunk une trame ethernet standard, il la placera dans ce VLAN natif, en quelque sorte, un VLAN par défaut (de marquage). La figure 3-8 illustre les commande de la création du VLAN natif :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 100
Switch(config-vlan)#name Native
Switch(config-vlan)#exit
Switch(config)#interface ethernet 0/0
Switch(config-if)#switchport trunk native vlan 100
Switch(config-if)#end
Switch#
```

Figure 3-8 : Création du VLAN natif.

3.2.7 Configuration du DHCP Snooping

Le DHCP Snooping est une technique qui permet de configurer le switch pour écouter le trafic DHCP et arrêter tous les paquets malveillants, qui se ferait passer par un DHCP**.** Pour commencer il faut d'abord :

- Activer en globalité la surveillance du DHCP, avec la commande « **ip dhcp snooping** ».
- Après avoir activé le « **dhcp snooping** », le commutateur ajoute l'option 82 au DHCP discover, dans ce cas-là certains serveurs abandonnent le paquet, donc il faut utiliser la commande « **no ip dhcp snooping information option** ».
- Pour sélectionner les VLANs pour lesquels on souhaite utiliser la surveillance du DHCP on utilise la commande « **ip dhcp snooping vlan + le numéro du vlan** ».
- Il est aussi possible de limiter le nombre de paquets DHCP que l'interface pourra recevoir, pour ce faire, il faut utiliser la commande « **ip dhcp snooping limit rate** ».
- Pour rendre l'interface qui est relié au serveur DHCP fiable, on utilise la commande « **ip dhcp snooping trust** ».

La figure 3-9 illustre la configuration de DHCP Snooping :

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#no ip dhcp snooping information option
Switch(config)#ip dhcp snooping vlan 2-8,99
Switch(config)#interface ethernet 0/0
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
Switch(config)#interface range ethernet 1/0-3
Switch(config-if-range)#ip dhcp snooping limit rate 10
Switch(config-if-range)#interface range ethernet 2/0-3
Switch(config-if-range)#ip dhcp snooping limit rate 10
Switch(config-if-range)#interface range ethernet 3/0-3
Switch(config-if-range)#ip dhcp snooping limit rate 10
Switch(config-if-range)#interface range ethernet 4/0-3
Switch(config-if-range)#ip dhcp snooping limit rate 10
Switch(config-if-range)#interface range ethernet 5/0-3
Switch(config-if-range)#ip dhcp snooping limit rate 10
Switch(config-if-range)#interface range ethernet 6/0-3
Switch(config-if-range)#ip dhcp snooping limit rate 10
Switch(config-if-range)#interface range ethernet 7/0-3
Switch(config-if-range)#ip dhcp snooping limit rate 10
Switch(config-if-range)#interface range ethernet 8/0-3
Switch(config-if-range)#ip dhcp snooping limit rate 10
Switch(config-if-range)#end
Switch#
Switch#
*May 14 17:17:19.732: %SYS-5-CONFIG_I: Configured from console by console
Switch#
```

Figure 3-9 : Configuration de DHCP Snooping.

4 Mise en œuvre de la configuration des serveurs

4.1 Serveur DNS

Le serveur DNS (Domain Name System) est un serveur qui permet de traduire les noms de domaines en adresses IP. Il agit comme une sorte d'annuaire qui permet de connecter les utilisateurs aux sites Web qu'ils souhaitent consulter. Lorsqu'un utilisateur entre un nom de domaine dans son navigateur, le serveur DNS recherche l'adresse IP associée à ce nom de domaine et renvoie cette information au navigateur, permettant ainsi la connexion au site Web. Chaque FAI (fournisseur d'accès à Internet) a ses propres serveurs DNS, mais il est également possible d'utiliser des serveurs DNS tiers.

4.1.1 Installation et configuration DNS

Pour commencer il faut définir l'adresse IP statique du serveur afin de configurer le serveur DNS.

Tout d'abord :

- Nous cliquons sur démarrer.
- Puis sur Panneau de configuration.

Puis suivre les étapes suivantes :

On clique sur "**Réseau et Internet**".

On clique sur "**Centre Réseau et partage**".

On clique sur "**Modifier les paramètres de la carte**".

On clique avec le bouton droit de la souris sur la carte réseaux. Puis Cliquer sur "**Propriétés**".

On double clic sur "**Protocole Internet version 4 (TCP/IPv4)**".

On coche « Utiliser l'adresse IP suivante : ».

Notre DNS préféré **8.8.8.8** (c'est le DNS de Google).

Notre DNS auxiliaire **8.8.4.4** (second DNS de Google).

Pour finir cliquons sur OK.

La figure 3-10 illustre les différentes étapes à suivre :

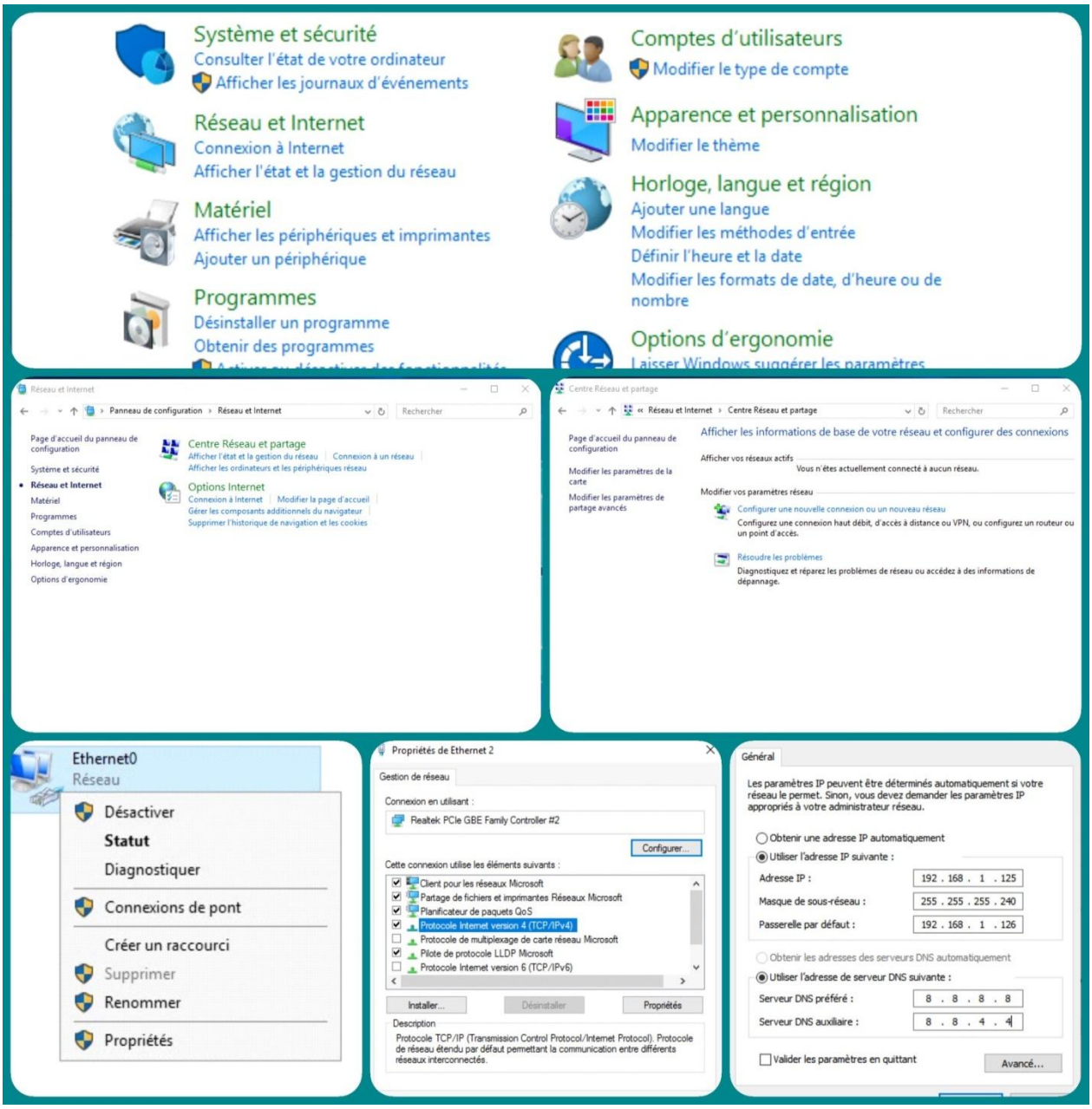

Figure 3-10 : Définir l'adresse IP statique du serveur.

4.1.2 Installation de DNS

Nous allons commencer par installer le DNS sur notre serveur. Nous cliquons sur « Rôle » puis sur « ajouter un rôle ».

Nous cochons ensuite « Serveur DNS » et nous cliquons sur « Suivant »

Une petite remarque apparaitre avant débuter l'installation du rôle DNS serveur, celle qui nous demande de :

- Fixer les adresses IP
- Mot de passe fort
- Les mises à jour

Si la configuration est faite, nous cliquant sur « suivant », puis « installer ».

Patienter pendant l'installation. Apres le chargement d'installation des fonctionnalités on clique sur « Fermer».

Comme nous pouvons le constater que le rôle DNS a bien était ajouter dans la figure 3-11 :

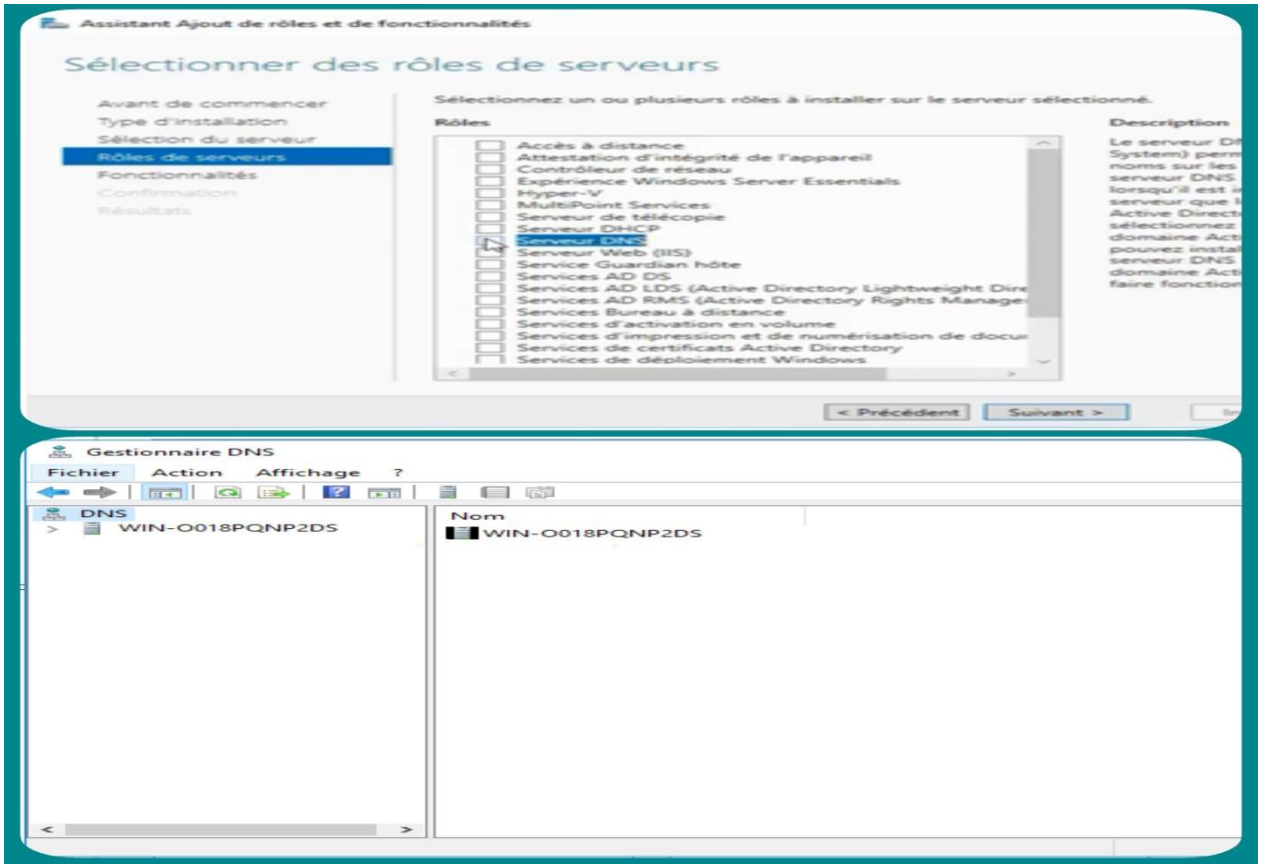

Figure 3-11 : Installation du serveur DNS.

4.1.3 Configuration du serveur DNS

Nous allons maintenant configurer le DNS sur la carte réseaux.

Reprendre « l'étape 1 » et nous mettons en DNS l'adresse IP du serveur.

Dans notre cas l'adresse IP est 192.168.1.125

Puis nous cliquons sur "OK".

Voilà le DNS est configuré sur notre Windows Server. La figure 3-12 présente la configuration du serveur DNS :

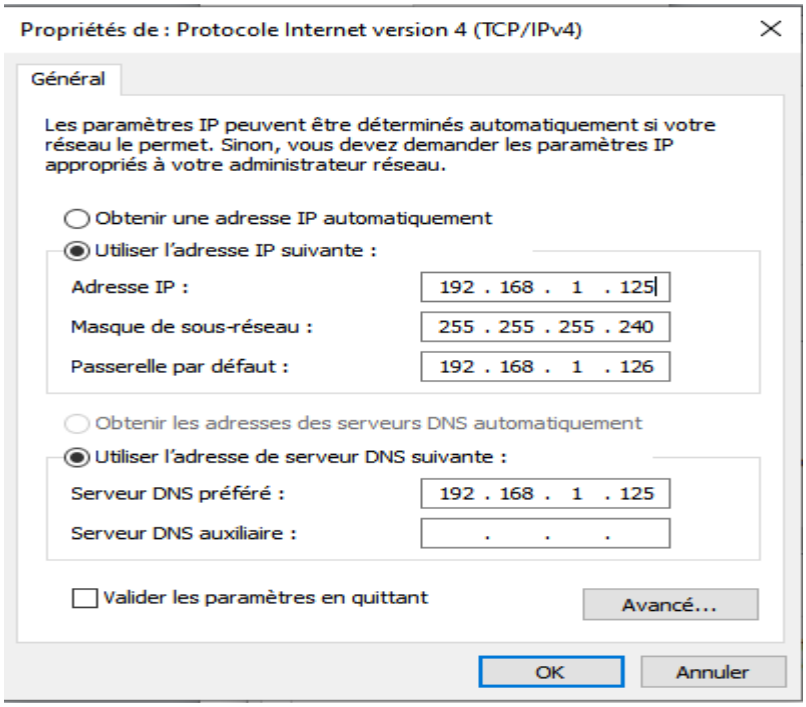

Figure 3-12 : Configuration du serveur DNS.

4.2 ACTIVE DIRECTORY

Active Directory est un service de gestion de répertoires de Microsoft qui permet aux administrateurs informatiques de gérer et de contrôler l'accès aux ressources informatiques de leur organisation. Il est utilisé pour stocker des informations sur les utilisateurs, les groupes, les ordinateurs et les autres ressources réseau, permettant ainsi aux administrateurs de gérer efficacement les autorisations et les stratégies de groupe. Active Directory est principalement utilisé dans les environnements Windows Server, mais il peut également être utilisé avec des systèmes d'exploitation autres que Windows.

4.2.1 Installation d'Active directory

Pour l'ajout du rôle d'Active directory au serveur local, nous allons :

- Lancer le gestionnaire de serveur et cliquer sur : « Ajouter des rôles et des fonctionnalités. »
- Sélectionner le type d'installation « Installation basée sur un rôle ou une fonctionnalité. »
- Sélectionner le serveur sur lequel nous souhaitons installer les services de domaines Active Directory.
- Cocher le rôle « Services AD DS », cliquer sur « suivant ».

La figure 3-13 présente l'ajout du rôle AD DS :

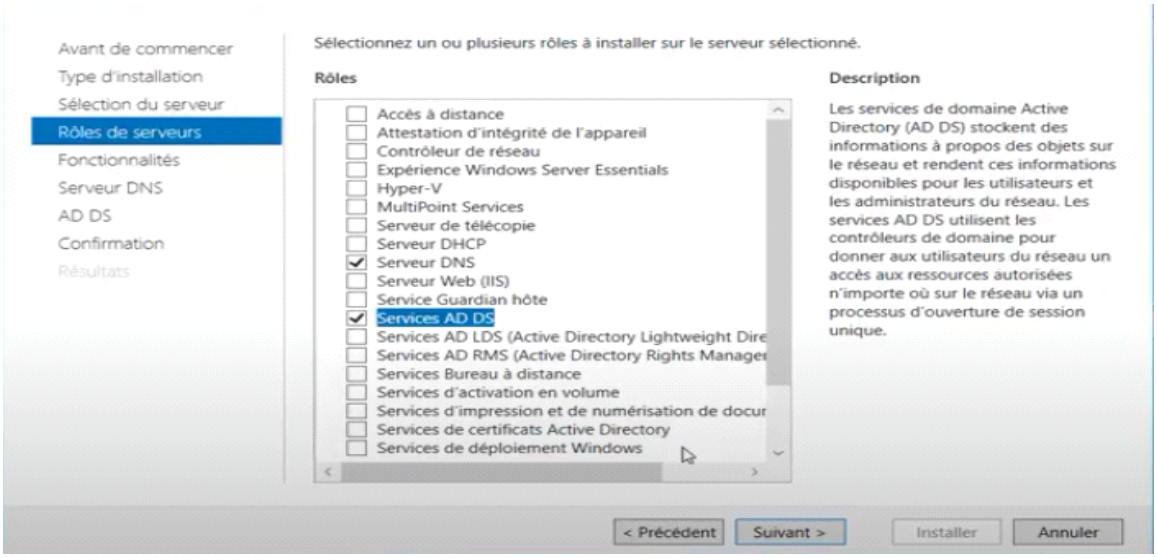

Figure 3-13 : Ajout du rôle AD DS.

Ici l'assistant nous affiche une description des services de domaine Active Directory illustrée dans la figure 3-14, comme indiqué, Microsoft recommande un minimum de 2 contrôleurs de domaines par domaine pour assurer la disponibilité de votre infrastructure Active Directory et ainsi éviter que nos utilisateurs ne puissent plus se connecter en cas de panne de notre contrôleur de domaine.

De plus, les services de domaine Active Directory reposent sur le système DNS et un serveur DNS sera donc automatiquement installé lors de l'installation des services de domaine Active Directory.

Notons que dans ce cas-ci, les zones DNS seront intégrées automatiquement à notre infrastructure Active Directory, ce qui permet notamment bénéficier de la réplication des zones DNS via le système de réplication Active Directory.

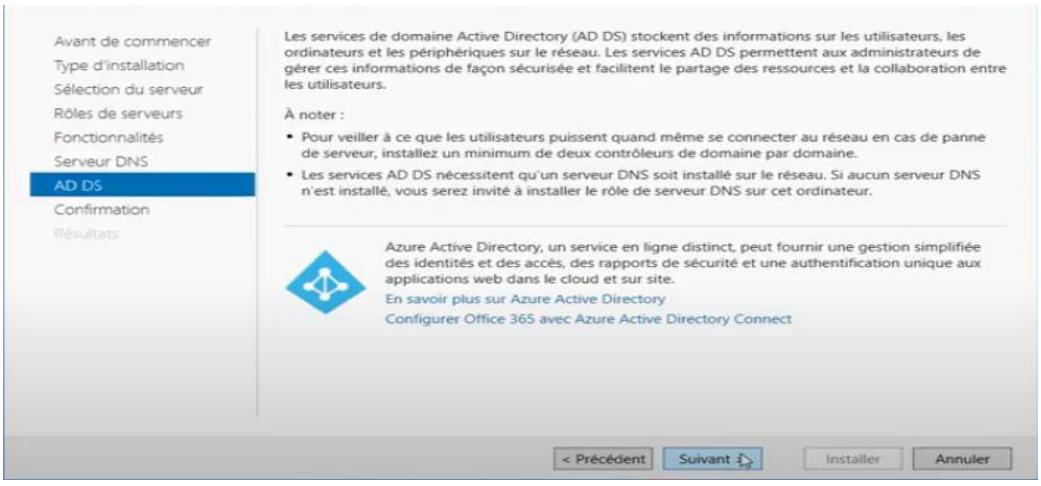

Figure 3-14 : Description des services de domaine Active Directory.

- Cliquer sur « Suivant », puis sur « Installer » pour confirmer les sélections d'installation.
- Patienter pendant l'installation des services AD DS.
- Après l'installation d'Active Directory Domain Service, le système va redémarrer automatiquement.

4.2.2 Création d'un contrôleur de domaine

Une fois les services AD DS installés, nous devons ensuite promouvoir ce serveur en tant que contrôleur de domaine, comme illustré dans la figure 3-15 :

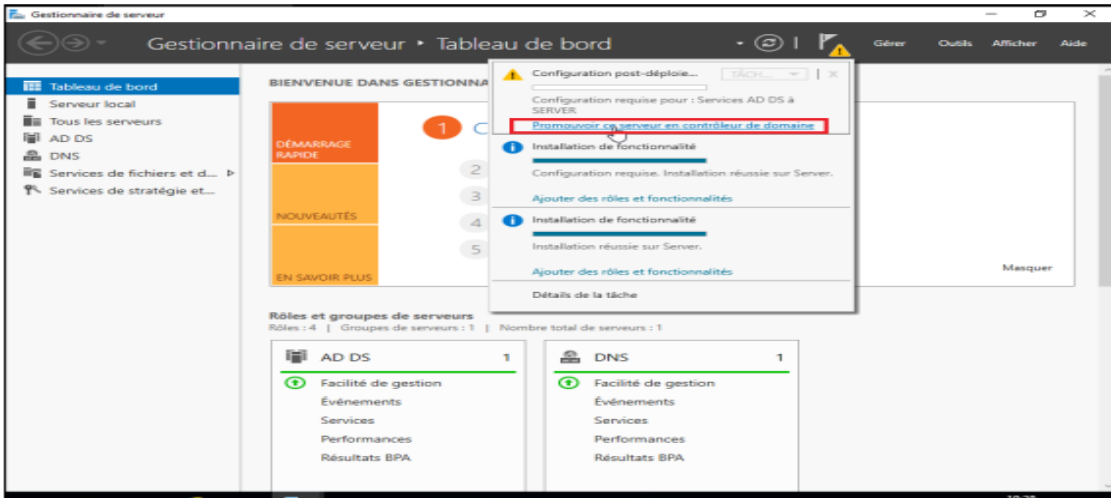

Figure 3-15 : Promouvoir le serveur en contrôleur de domaine.

Etant donné qu'il s'agit de notre 1er contrôleur de domaine, nous devons créer une nouvelle forêt (autrement dit : un nouvel espace de noms).

Pour cela, nous sélectionnons "Ajouter une nouvelle forêt" et indiquer un nom de domaine tel que : Enna.lan comme présente la figure 3-16 :

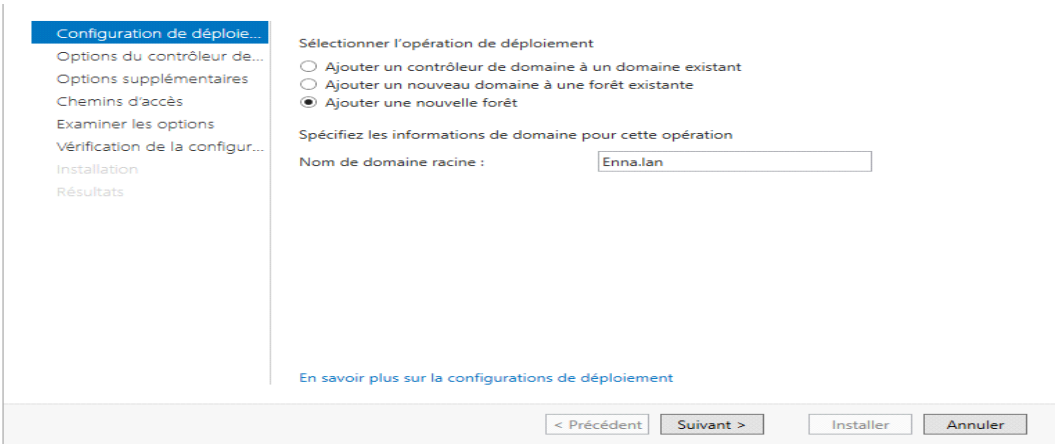

Figure 3-16 : Création du domaine « Enna.lan ».

Lorsque notre domaine sera créé, le niveau fonctionnel de la nouvelle forêt et du domaine racine est sélectionné par défaut. Nous devons saisir un mot de passe pour le mode de restauration des services d'annuaire, comme nous montre la figure 3-17 :

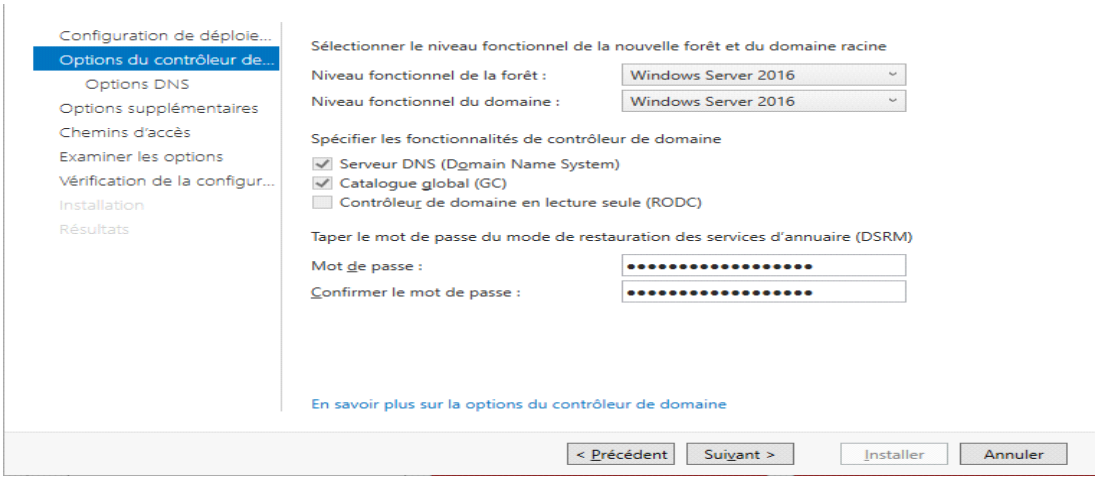

Figure 3-17 : Options du contrôleur de domaine.

Etant donné que la zone DNS parente ".lan" n'existe pas, l'assistant nous indique qu'il n'est pas possible de créer une délégation DNS pour cette zone parent.

Néanmoins, cela n'est pas obligatoire. Donc, on clique sur Suivant.

L'assistant choisira automatiquement un nom de domaine NETBIOS qui est basé sur la partie gauche du domaine spécifié précédemment.

Dans notre cas, ce nom de domaine NETBIOS est donc : ENNA comme illustré dans la figure 3-18 :

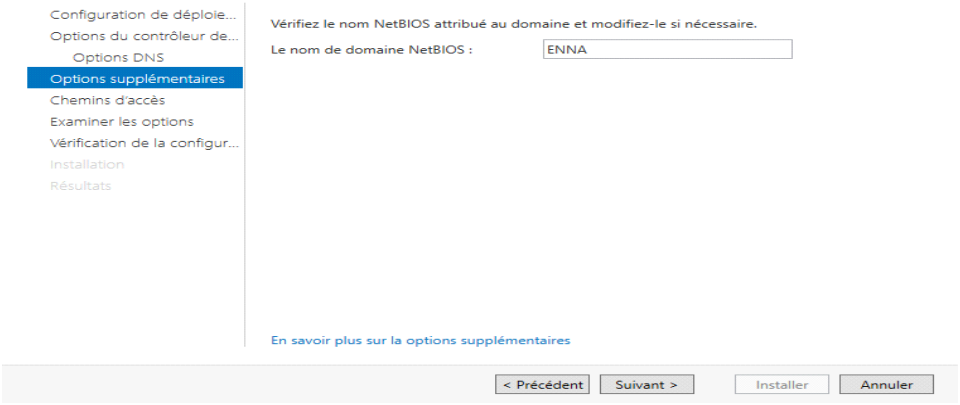

Figure 3-18 : Nom de domaine NetBIOS.

L'assistant nous propose de choisir l'emplacement des dossiers NTDS et SYSVOL qui correspondent à :

- La base de données Active Directory

- Les fichiers journaux d'Active Directory
- Au dossier SYSVOL qui contient notamment les stratégies de groupe (ou GPO en anglais) et les scripts de démarrage et d'arrêt, ...

La figure 3-19 montre l'emplacement des fichiers Active Directory :

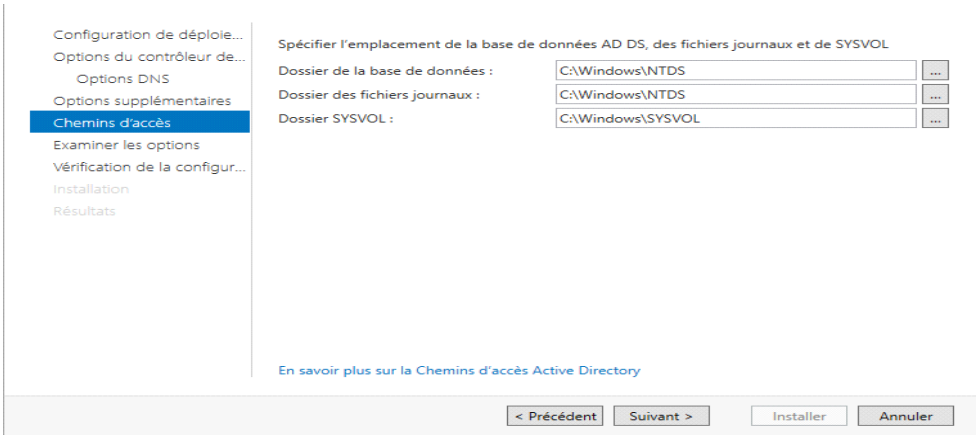

Figure 3-19 : Emplacement des fichiers Active Directory.

L'assistant de promotion Active Directory nous affiche un résumé de la configuration de notre contrôleur de domaine Active Directory.

Noter qu'il est possible d'obtenir très facilement le script PowerShell pour effectuer la même chose en ligne de commandes en cliquant simplement sur le bouton : Afficher le script, comme montre la figure 3-20 :

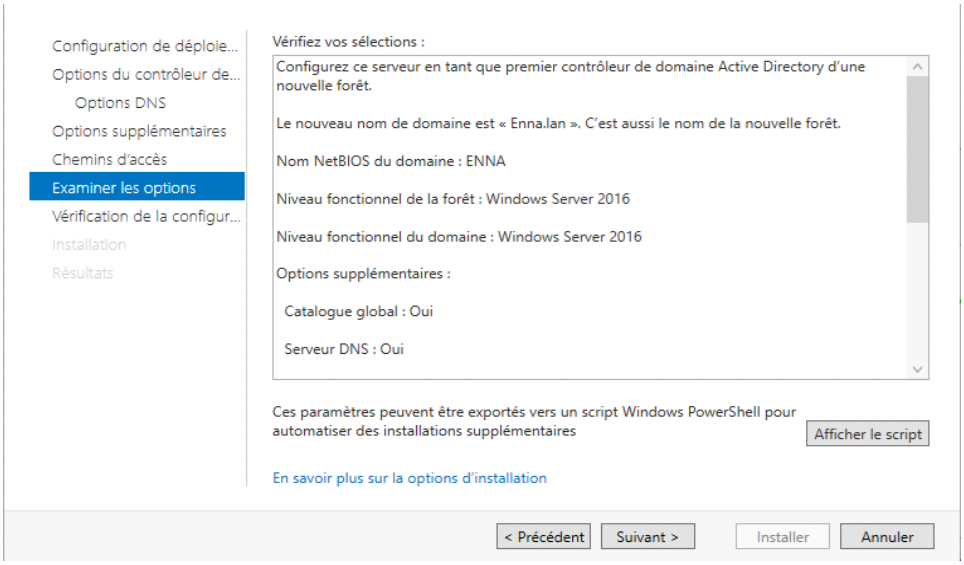

Figure 3-20 : Examiner les options.

L'assistant vérifie la configuration requise pour la promotion de ce contrôleur de domaine :

✓ Le 1er avertissement indique simplement que les contrôleurs de domaine Windows Server 2016 utilisent un paramètre de sécurité qui les empêche de fonctionner avec des

environnements Windows NT 4.0. Néanmoins, si nous n'avons pas de serveurs sous Windows NT 4.0, nous pouvons ignorer cet avertissement.

- ✓ Le 2ème avertissement concerne la délégation DNS qui ne peut pas être créée pour la zone parent pour la raison expliquée précédemment.

Nous pouvons ignorer ceux-ci sans problème et cliquer sur Installer.

Patienter pendant l'installation du serveur DNS et la configuration de notre contrôleur de domaine.

La figure 3-21 illustre l' installation du serveur DNS et la configuration de notre contrôleur de domaine :

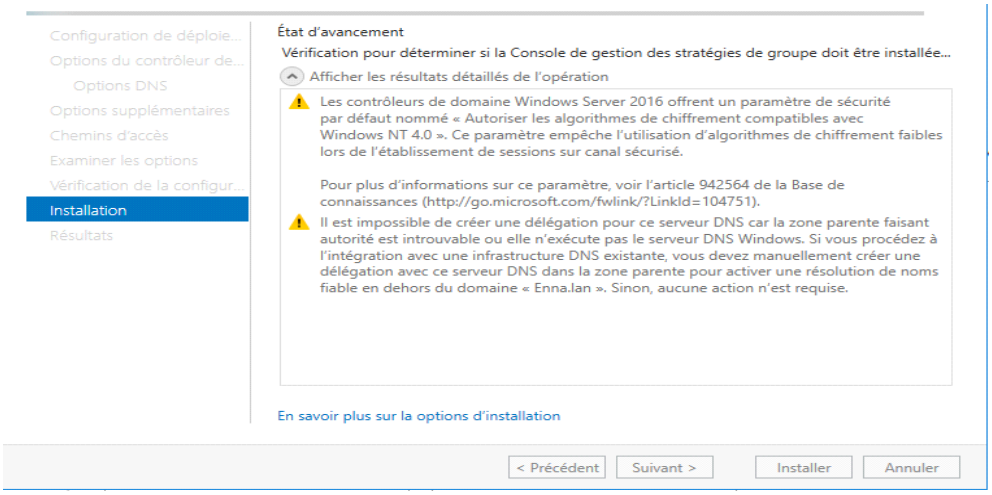

Figure 3-21 : Installation du serveur DNS et la configuration de notre contrôleur de domaine.

Une fois le contrôleur de domaine est installé, un message s'affichera et notre serveur redémarrera quelques secondes plus tard.

Une fois le redémarrage est terminé, nous connectons avec le compte Administrateur du domaine qui correspond à l'administrateur local de ce serveur, comme la figure 2-22 présente :

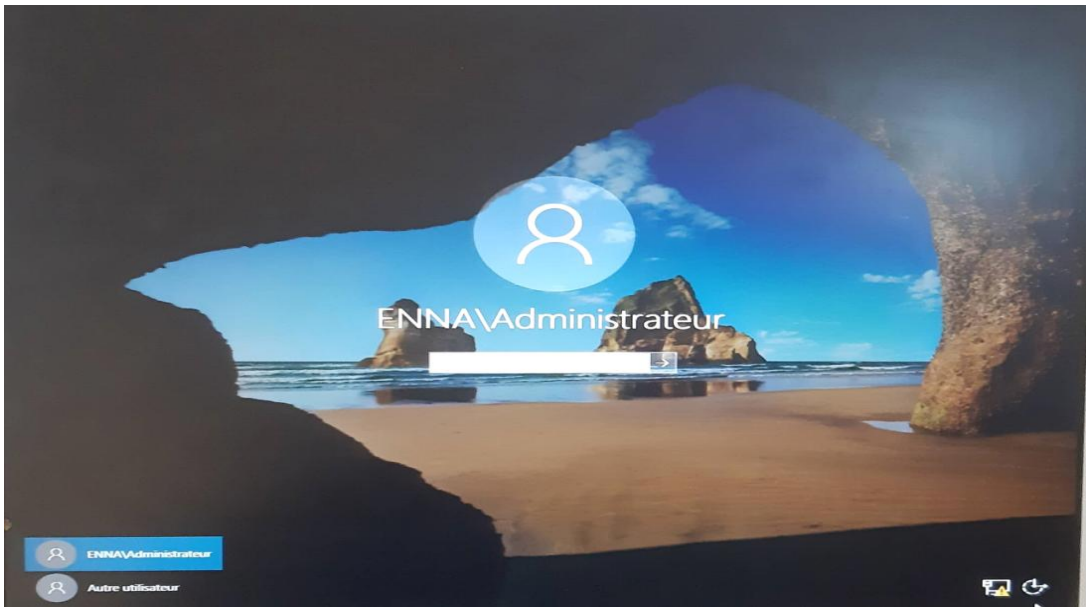

Figure 3-22 : Création réussie de notre contrôleur de domaine.

4.3 Serveur DHCP

Le serveur DHCP (Dynamic Host Configuration Protocol) est un serveur qui permet la distribution automatique des adresses IP et des paramètres de configuration réseau aux périphériques connectés à un réseau. Il attribue de manière dynamique des adresses IP pour éviter les conflits d'adresse, et fournit également des informations telles que les adresses de passerelle, les adresses de serveurs DNS et les options de configuration de réseau supplémentaires. Le serveur DHCP facilite la gestion du réseau en permettant une configuration automatisée des périphériques, ce qui évite les erreurs de configuration manuelle et le temps nécessaire pour le faire.

4.3.1 Installation d'un serveur DHCP

Pour installer un serveur DHCP nous suivons les étapes suivantes :

- Depuis le **Gestionnaire de serveur**, cliquer sur l'étape **Gérer** puis **Ajouter des rôles et fonctionnalités.**
- Sélectionner le type d'installation « **Installation basée sur un rôle ou une fonctionnalité** ».
- Sélectionner le serveur de destination puis cliquer sur **Suivant**.
- Nous sommes maintenant sur la fenêtre de sélection des rôles. Nous allons donc installer le rôle DHCP. Pour cela, nous cochons simplement DHCP dans la fenêtre de sélection des rôles. Enfin, cliquer sur Suivant.
- Des fonctionnalités supplémentaires sont automatiquement sélectionnées pour nous, on

clique sur Ajouter.

- Après avoir ajouté des rôles, nous pouvons ajouter des fonctionnalités supplémentaires. En général, toutes les caractéristiques qui sont nécessaires pour gérer le rôle sont déjà sélectionnées, nous pouvons simplement cliquer sur le bouton « Suivant » pour continuer.
- Nous aurons alors quelques infos sur le rôle que nous sommes en train d'ajouter. Nous cliquons sur « suivant » après en avoir pris connaissance.
- Nous devons confirmer l'ajout du rôle DHCP sur notre serveur. Nous cliquons sur « Installer ».
- Notre serveur est maintenant en cours d'installation, après quelques minutes, l'installation sera terminée. L'installation du rôle DHCP ne nécessite pas de redémarrage du serveur.

La figure 3-23 illustre les différentes étapes pour l'installation du serveur DHCP :

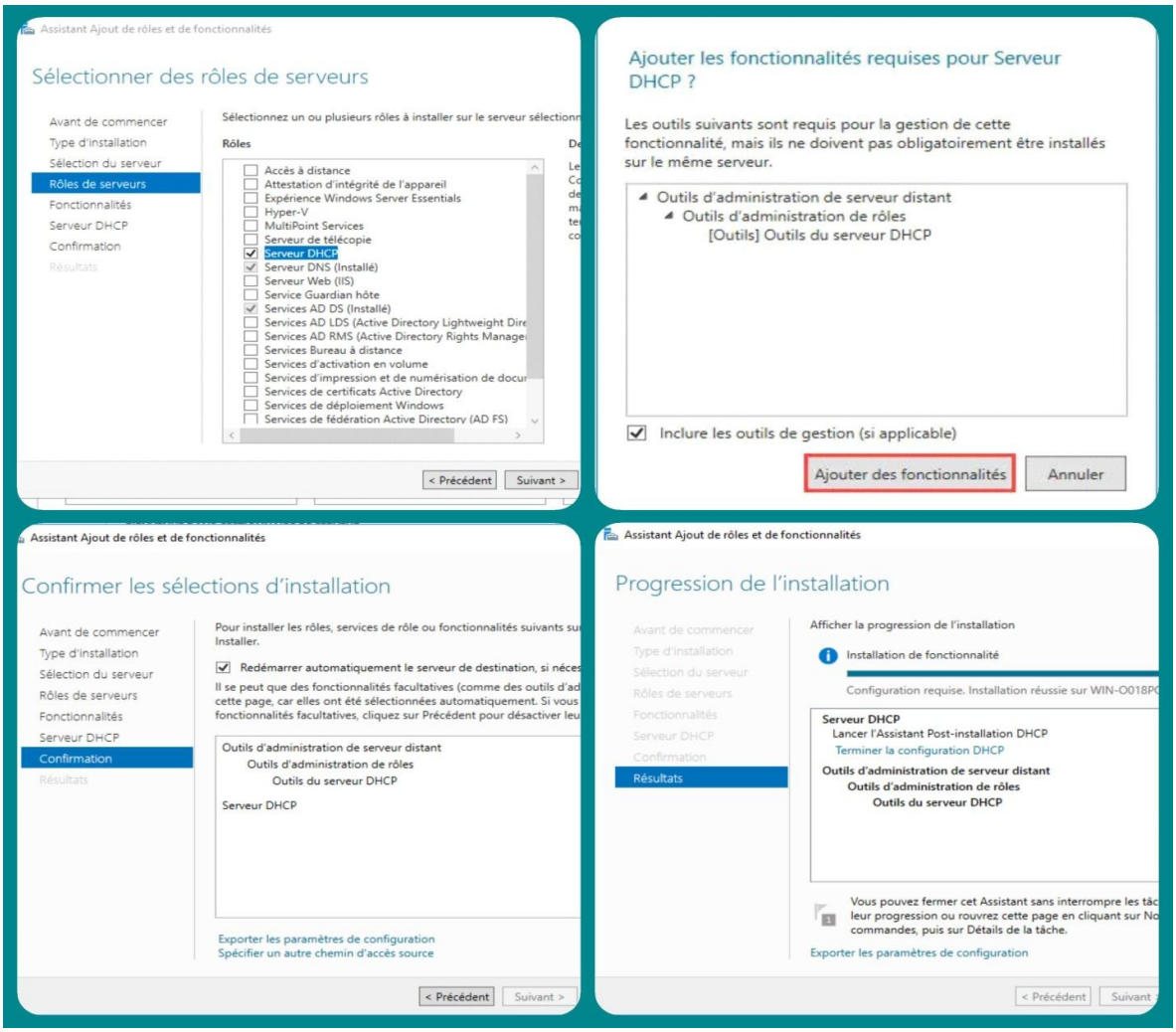

Figure 3-23 : Installation d'un serveur DHCP.

4.3.2 Configuration du rôle DHCP

Une fois notre serveur DHCP est installé, il faut le configurer. Pour cela, depuis le Gestionnaire de serveur, nous devrions avoir une alerte (Configuration post-déploiement), nous cliquons sur « Terminer la configuration DHCP », et on suivre les étapes ci-dessous :

- On va autoriser DHCP dans le domaine, pour cela il nous faudra un compte administrateur du domaine.
- Nous pouvons choisir le compte sur lequel nous sommes actuellement connecté ou bien un autre compte et nous cliquons sur « Valider ».
- L'assistant configuration post-installation DHCP va alors créer des groupes de sécurité dans ADDS et autoriser le serveur DHCP. Nous cliquons sur « Fermer », comme nous montre la figure 3-24 :

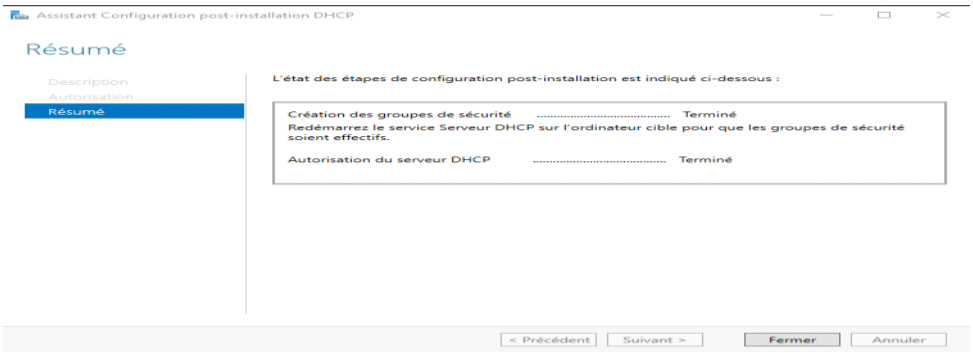

Figure 3-24 : Autorisation du serveur DHCP.

4.3.3 Définition des étendues

Les étendues DHCP désignent la plage d'adresses IP que le service DHCP (Dynamic Host Configuration Protocol) est autorisé à distribuer aux clients sur un réseau. Lorsqu'un client se connecte pour la première fois sur le réseau, il envoie une requête DHCP pour obtenir une adresse IP. Le serveur DHCP répond alors en lui attribuant une adresse IP disponible dans l'étendue DHCP prédéfinie. Les étendues DHCP peuvent être configurées pour inclure des adresses IP statiques ainsi que des adresses IP dynamiques en fonction des besoins spécifiques du réseau.

4.3.3.1 Configuration des étendues

Pour créer nos étendues, nous lançons la console DHCP via notre gestionnaire de serveur. Depuis cette console, nous allons pouvoir créer nos étendues DHCP. Nous allons créer notre première étendue IPv4 pour que les clients puissent obtenir une adresse IP automatiquement :

- Effectuer un clic droit sur « IPv4 », puis sélectionner « Nouvelle étendue… »
- Donner un nom à notre nouvelle étendue.
- Nous pouvons maintenant définir la plage d'adresses IP pour cette étendue ensuite on clique sur « Suivant ».
- Nous pouvons ajouter une ou plusieurs plages d'exclusions. Ce sont les adresses qui ne seront pas distribuées par le serveur DHCP.
- La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de l'étendue que nous sommes en train de créer, par défaut, le bail est limité à 8 jours. Nous pouvons le modifier suivant nos besoins. Par exemple si nous créons un serveur DHCP pour un réseau Wi-Fi public, un bail de 24H est suffisant.
- Lors de la Configuration des paramètres DHCP, nous cliquons sur « Oui, je veux configurer ces options maintenant » puis on clique sur Suivant.
- Lors de la configuration des paramètres DHCP, nous allons pouvoir ajouter la passerelle par défaut, c'est cette passerelle qui sera ajoutée sur tous les clients de l'étendue. Nous pouvons avec une ou plusieurs passerelles.
- Même chose au niveau du serveur DNS, ajouter la ou les adresses des serveurs DNS que nous souhaitons utiliser.
- Si nous voulons utiliser des serveurs WINS, nous pouvons les ajouter dans cette étape. Dans notre cas non donc on clique directement sur « suivant ».
- Enfin nous pouvons activer l'étendue, on clique sur « suivant » puis « terminer ».

La figure 3-25 illustre les différentes étapes à suivre pour la création d'une étendue :

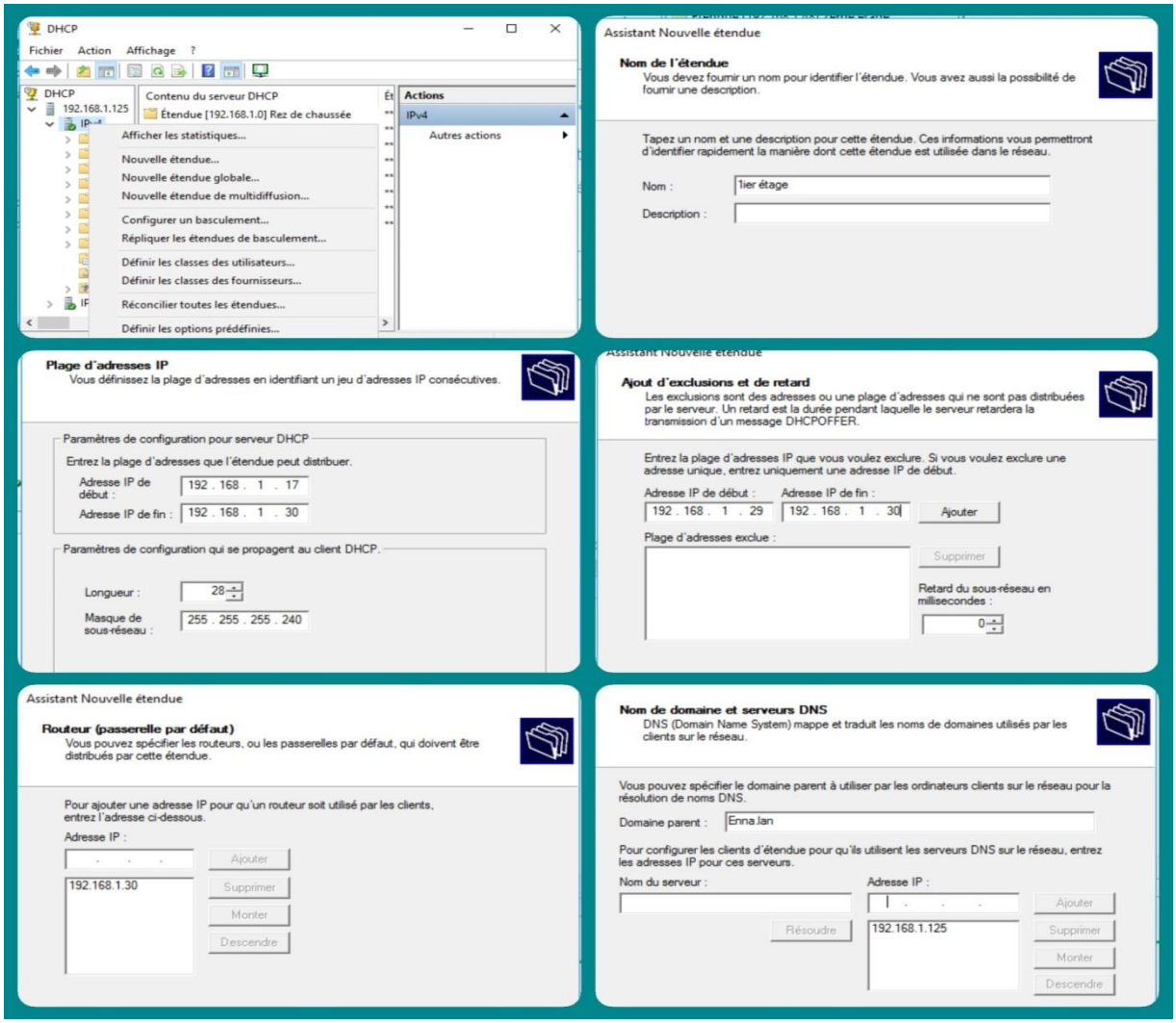

Figure 3-25 : Création d'une étendue.

4.3.3.2 Tableau des étendues

Pour notre établissement ENNA, nous avons créé 8 étendues qu'on site dans le tableau 3-3 :

Nom de l'étendue	Plage d'adresses IP	Plage d'adresses exclue	Passerelle par défaut	Serveurs DNS
Rez de chaussée	192.168.1.1 -192.168.1.14	192.168.1.13 -192.168.1.14	192.168.1.14	192.168.1.125
1ier étage	192.168.1.17 -192.168.1.30	192.168.1.29 -192.168.1.30	192.168.1.30	192.168.1.125

SSLI	192.168.1.33 -192.168.1.46	192.168.1.45 -192.168.1.46	192.168.1.46	192.168.1.125
2ème étage	192.168.1.49 -192.168.1.62	192.168.1.61 -192.168.1.62	192.168.1.62	192.168.1.125
3ème étage	192.168.1.65 -192.168.1.78	192.168.1.77 -192.168.1.78	192.168.1.78	192.168.1.125
4ème étage	192.168.1.81 -192.168.1.94	192.168.1.93 -192.168.1.94	192.168.1.94	192.168.1.125
Tour de controle	192.168.1.97 -192.168.1.110	192.168.1.109 -192.168.1.110	192.168.1.110	192.168.1.125
Managers	192.168.1.29 -192.168.1.142	192.168.1.141 -192.168.1.142	192.168.1.142	192.168.1.125

Tableau 3-3 : Tableau des étendues du serveur DHCP.

4.4 Configuration d'Active directory

Dans notre établissement ENNA, ils existent plusieurs utilisateurs (Administratifs, Techniciens, …), alors pour simplifier et centraliser la gestion de ces derniers, il faut leurs créer des comptes dans le serveur à travers le service AD DS. En premier lieu, nous allons créer des OU (Organisation Unit), pour organiser les utilisateurs et les ordinateurs dans une seule unité afin de pouvoir leurs appliquer des procédures et des stratégies de groupes.

4.4.1 Création d'une Unité d'organisation « OU »

Pour créer une unité d'organisation à l'aide de l'interface de Windows, nous devons :

- Ouvrir Gestionnaire de serveur -> outils -> Utilisateurs et ordinateurs Active Directory.
- Dans l'arborescence de la console, faire un clic droit sur Enna.lan et pointer sur Nouveau puis cliquer sur « Unité d'organisation ».
- Après nous remplions les champs nécessaires. Dans notre cas on a nommé l'Unité Organisation racine : **ENNA.**

La figure 3-26 présente les étapes à suivre pour créer une unité d'organisation :

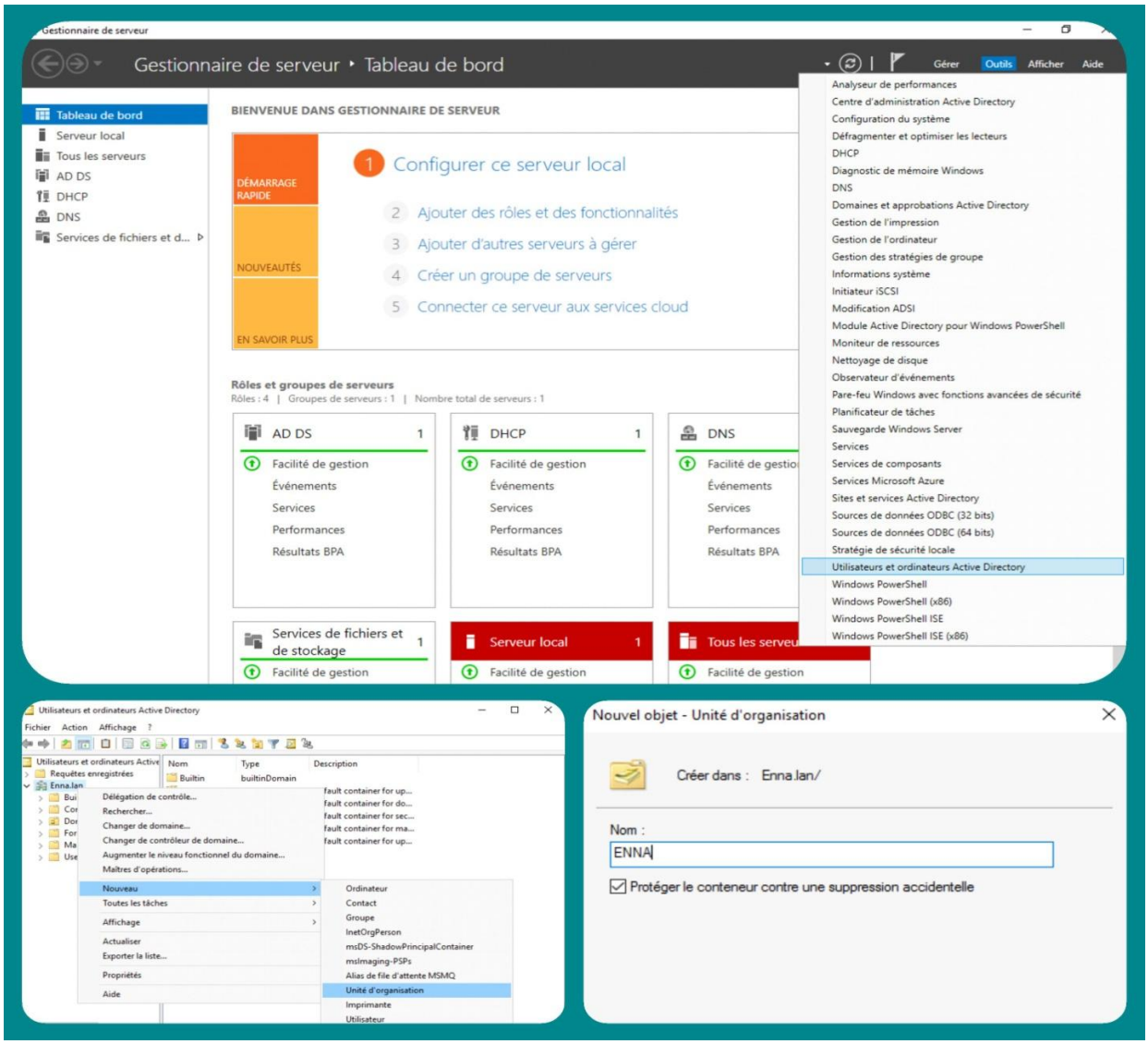

Figure 3-26 : Création d'une unité d'organisation.

4.4.2 Création d'un compte utilisateur dans Active directory

Après la création de l'unité d'organisation, nous passons à la création d'un utilisateur, il suffit suivre les étapes suivantes :

- Ouvrir Gestionnaire de serveur -> outils -> Utilisateurs et ordinateurs Active Directory
- Dans l'arborescence de la console, faisons un clic droit sur l'unité d'organisation et pointons sur « Nouveau » puis cliquons sur « Utilisateur ».
- Ensuite, nous remplissons les champs vides, et on doit introduire le mot de passe, le confirmer et cocher « utilisateur ne peut pas changer de mot de passe ».

Ensuite, cliquons sur « Suivant » pour terminer la création d'utilisateur. Dans ce compte utilisateur, nous pouvons faire plusieurs opérations, comme l'activation, désactivation,

suppression, définition de l'horaire d'accès, l'affichage et le changement des propriétés. La figure 3-27 illustre les étapes à suivre pour créer un compte utilisateur :

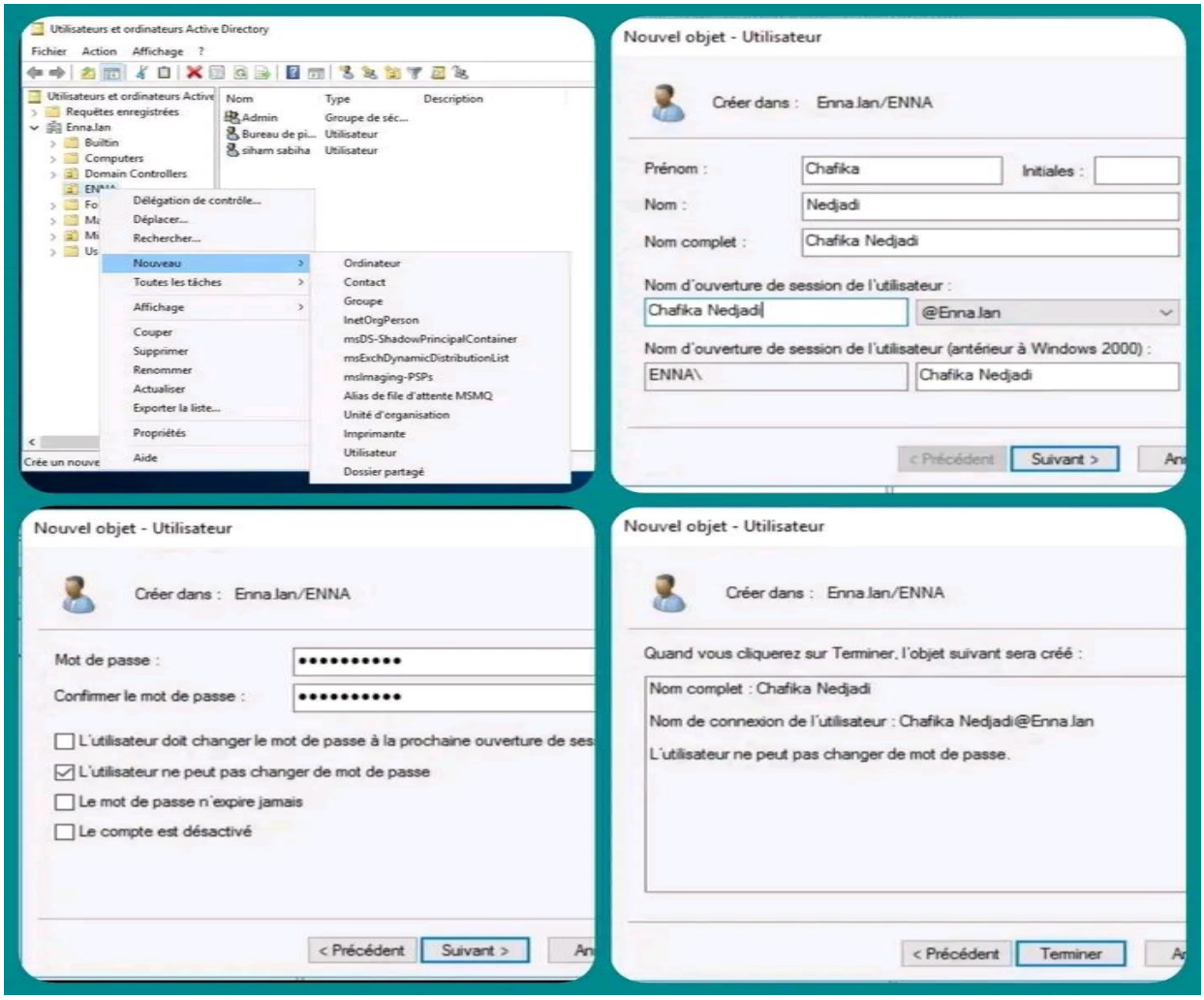

Figure 3-27 : Création d'un utilisateur Active directory.

4.4.3 Création d'un groupe dans Active directory

Pour crée un groupe, il faut suivre les étapes suivantes :

- Sur le Gestionnaire de Serveur cliquons sur Outils, puis sur Utilisateurs et ordinateurs Active Directory.
- Dans l'arborescence de la console, faisons un clic droit sur Enna.lan et pointons sur Nouveau. puis cliquons sur « Groupe ».
- Tapons le nom du nouveau groupe.
- Dans le menu Etendu du groupe sélectionner le type de groupe (Domaine local, Globale ou Universelle). Puis cliquons sur « OK ».

Ces étapes sont illustrées dans la figure 3-28 :

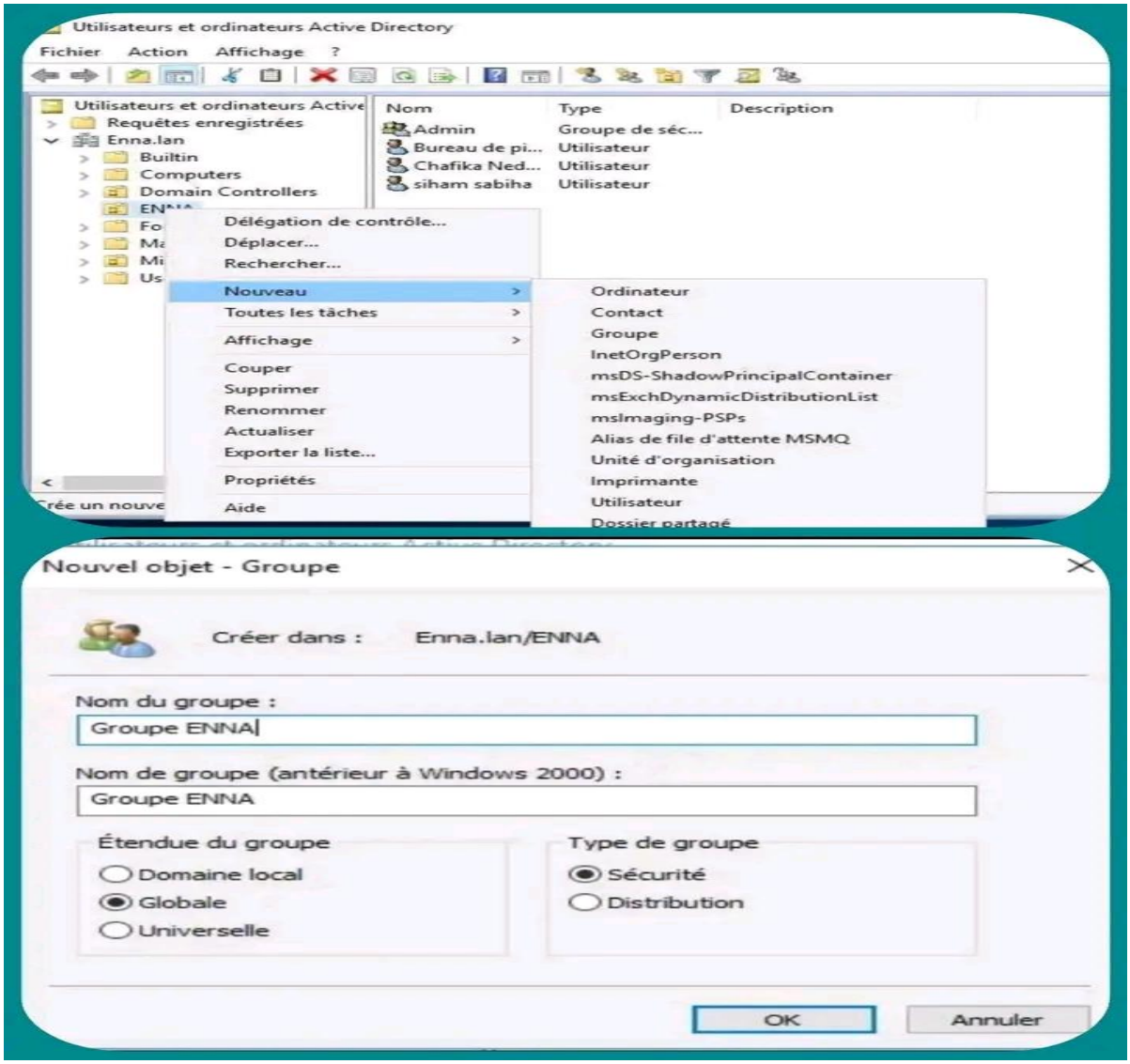

Figure 3-28 : Création d'un groupe Active directory.

4.4.3.1 Addition d'un membre à un groupe

- Restons toujours sur Utilisateurs et Ordinateur Active Directory.
- Cliquons sur le domaine « Enna.lan », et faisons un clic droit sur le groupe, puis choisissons « propriétés ».
- Dans la case Entrez les noms des objets à sélectionner, tapons le nom de l'ordinateur, du groupe ou de l'utilisateur que nous voulons ajouter au groupe, puis cliquons sur OK.

Nous pouvons faire plusieurs opérations sur un groupe, comme le supprimer, renommer, déplacer et modifier son contenu. La figure 3-29 présente l'addition d'un membre à un groupe :

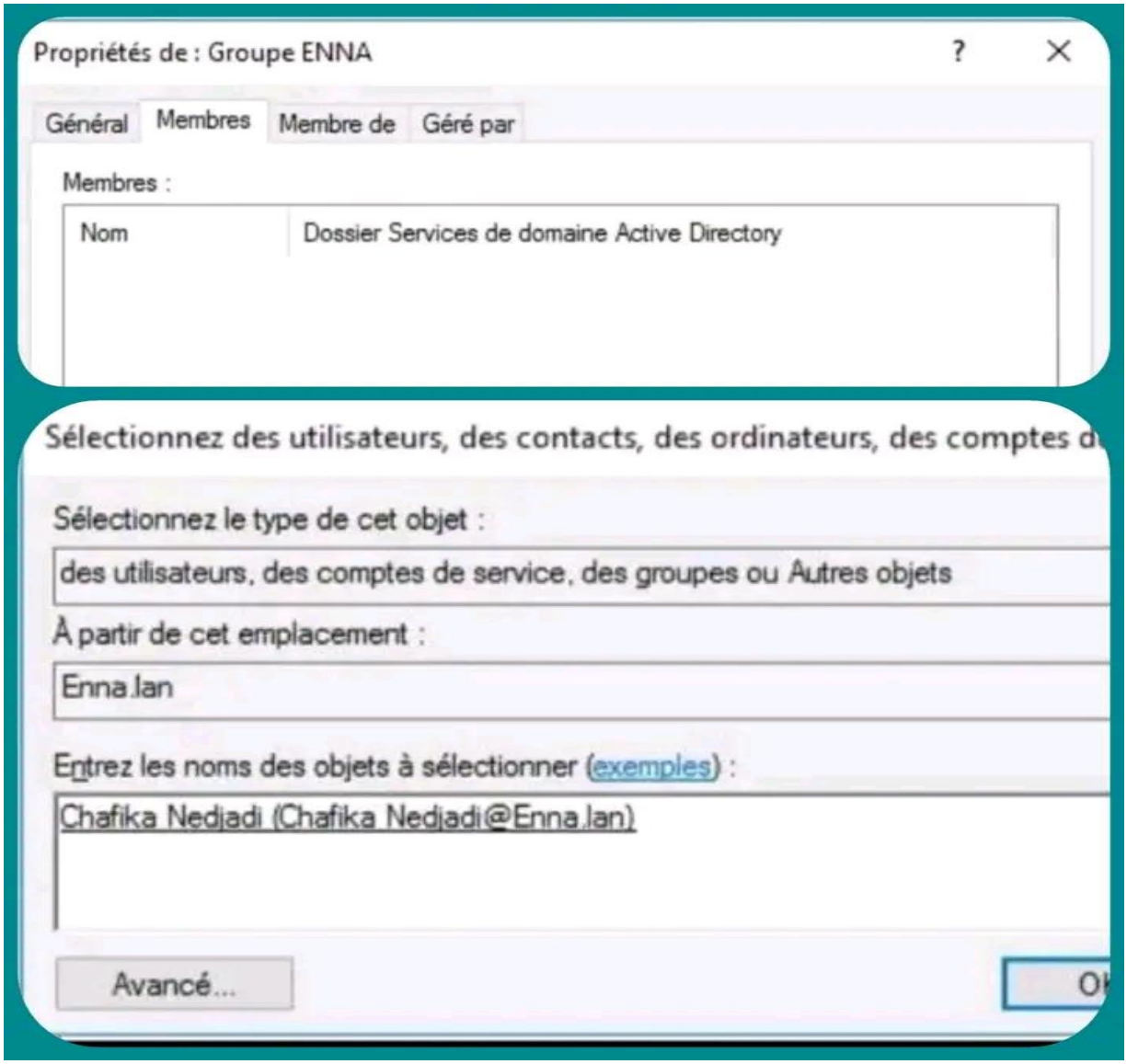

Figure 3-29 : Addition d'un membre à un groupe.

4.4.4 Intégration du client au domaine

- On clique droit sur « Ordinateur » puis « propriétés »
- Puis dans le système on clique sur « modifier les paramètres ».
- On clique « Modifier » dans la fenêtre suivante.
- Ensuite on donne nom de l'ordinateur, membre d'un domaine âpres on va taper « Enna.lan » le nom de domine qu'on a utilisé.
- Une fenêtre va apparaitre pour authentifier le client par le nom d'utilisateur et le mot de passe.
- Message de validation va apparaitre.

La figure 3-30 présente l'étape de l'intégration d'un client au domaine :

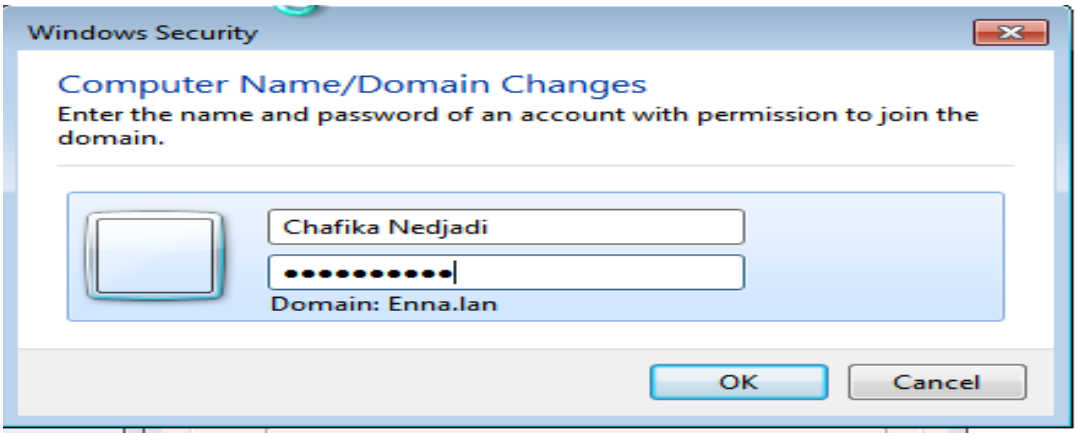

Figure 3-30 : Intégration du client au domaine.

4.4.5 Rendre un utilisateur administrateur du domaine

En faisant de l'utilisateur un administrateur du domaine, il aura un accès illimité aux ressources du système, ce qui facilite la gestion et la maintenance des environnements réseau, la gestion des comptes utilisateur et la configuration de la sécurité sur les ressources sensibles.

Pour rendre un utilisateur administrateur du domaine sur Windows Server, nous suivons les étapes ci-dessous :

- Rechercher l'utilisateur que nous souhaitons rendre administrateur.
- Cliquer avec le bouton droit sur l'utilisateur et sélectionner "Propriétés".
- Dans la fenêtre des propriétés de l'utilisateur, cliquer sur l'onglet "Membre de".
- Cliquer sur le bouton "Ajouter" pour ajouter l'utilisateur à un groupe.
- Dans la fenêtre "Sélectionner les objets", taper "Administrateurs" dans le champ de recherche et cliquer sur "OK".
- Sélectionner le groupe "Administrateurs" dans la liste des résultats de recherche et cliquer sur "OK".
- Cliquer sur "Appliquer" pour enregistrer les modifications et fermer la fenêtre des propriétés de l'utilisateur.

La figure 3-31 présente quelques étapes à suivre pour rendre un utilisateur administrateur du domaine :

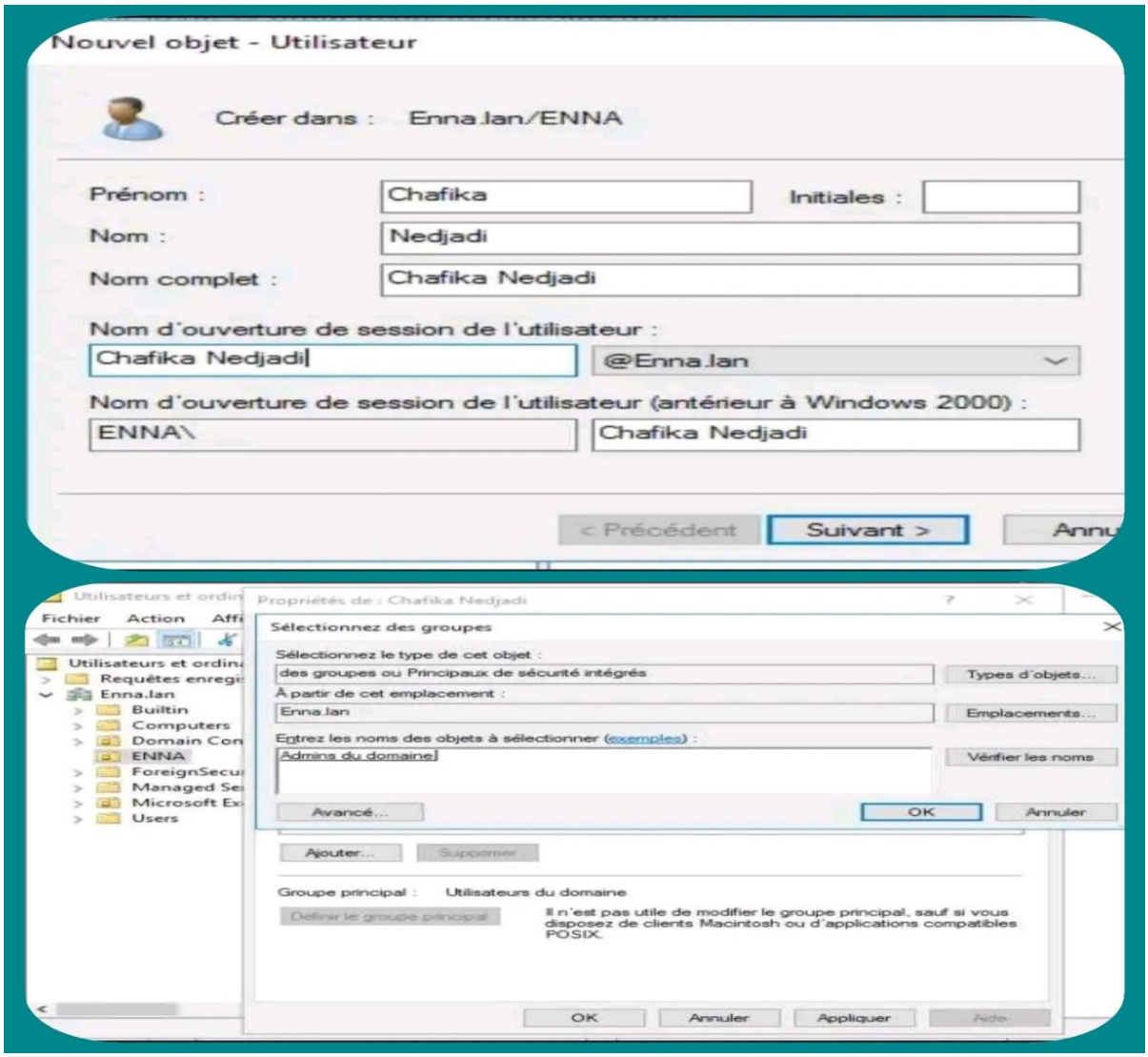

Figure 3-31 : Rendre un utilisateur administrateur du domaine.

Après avoir suivi ces étapes, l'utilisateur sera maintenant membre du groupe "Administrateurs" du domaine et pourra effectuer des actions d'administration sur le serveur.

4.4.6 Configuration de connexion bureau à distance

La configuration de connexion bureau à distance permet à des utilisateurs distants de se connecter en toute sécurité au serveur et d'accéder aux applications et aux données qu'il contient. En autorisant le bureau à distance, nous pouvons faciliter la gestion, la surveillance et la maintenance de notre infrastructure informatique, tout en offrant une expérience utilisateur fluide et sécurisée pour les utilisateurs distants. Il est cependant important de mettre en place des mesures de sécurité appropriées, telles que des mots de passe forts et des protocoles d'authentification multi-facteurs, pour protéger le serveur et les données qu'il contient contre les attaques malveillantes.

Pour la configuration on doit suivre les étapes suivantes :

- Ouvrir le gestionnaire de serveur et cliquer sur le serveur local.
- L'état du Bureau à distance est désactivé, cliquer désactiver pour ouvrir les propriétés système.
- Dans la section bureau à distance, sur l'onglet Utilisation à distance des propriétés système, sélectionner Autoriser les connexions à distance à cet ordinateur
- Activer ou non le NLA puis cliquer sur « Sélectionnez des utilisateurs » pour sélectionner les utilisateurs ou bien le groupe qu'on va l'autoriser l'accès bureau à distance.

Les étapes sont illustrées dans la figure 3-32 :

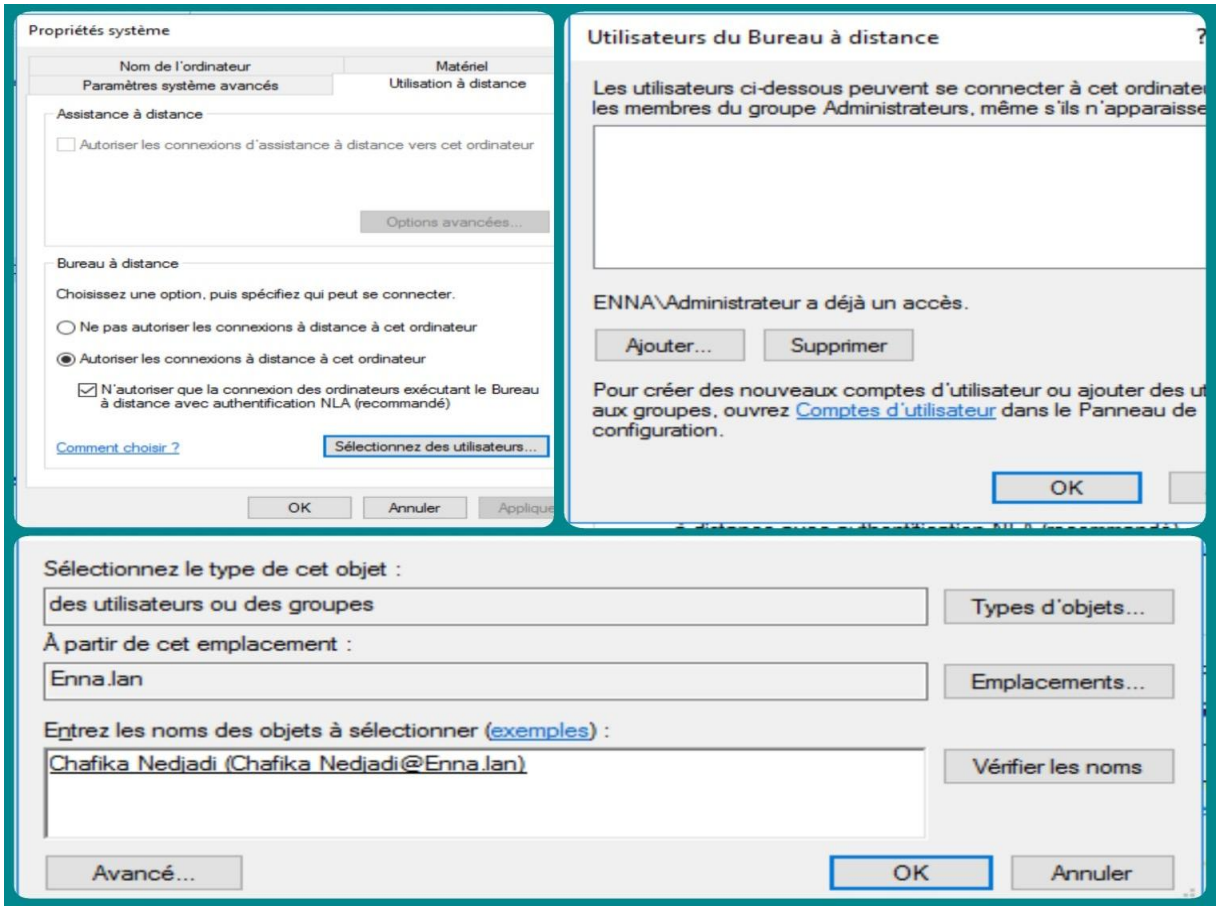

Figure 3-32 : Autoriser l'accès bureau à distance.

- Puis accéder au pare-feu et cliquer sur autoriser les applications à communiquer à travers le pare-feu, et cocher « Bureau à distance », comme montre la figure 3-33 :

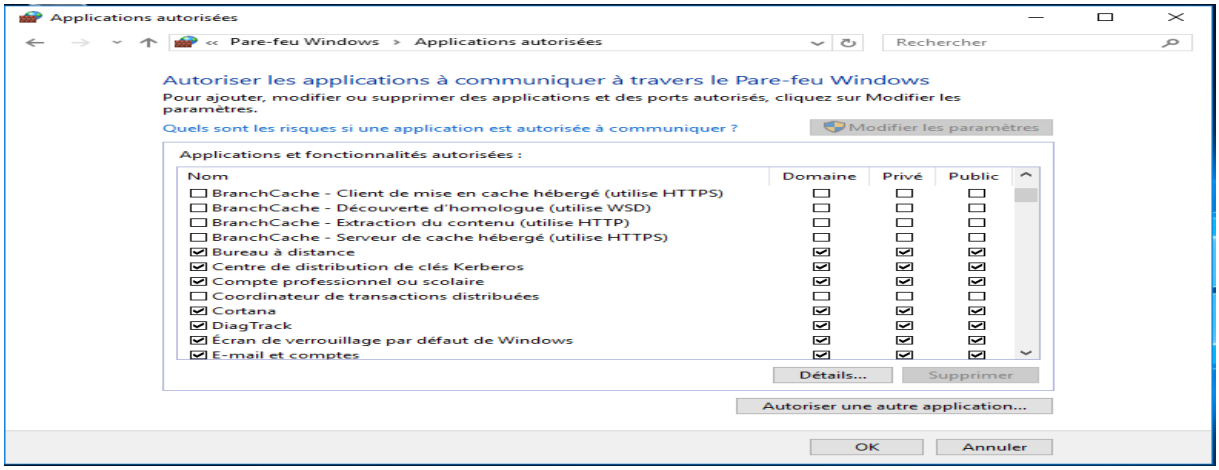

Figure 3-33 : Autoriser bureau à distance à communiquer à travers le pare-feu.

- Accéder à la configuration ordinateur → Stratégies → Paramètres Windows → Paramètres de sécurité → Attribution des droits utilisateur → Autoriser l'ouverture des session par les services bureau à distance pour ajouter le même compte avec lequel nous voulons pouvoir ouvrir une session à distance, la figure 3-34 illustre les étapes à suivre :

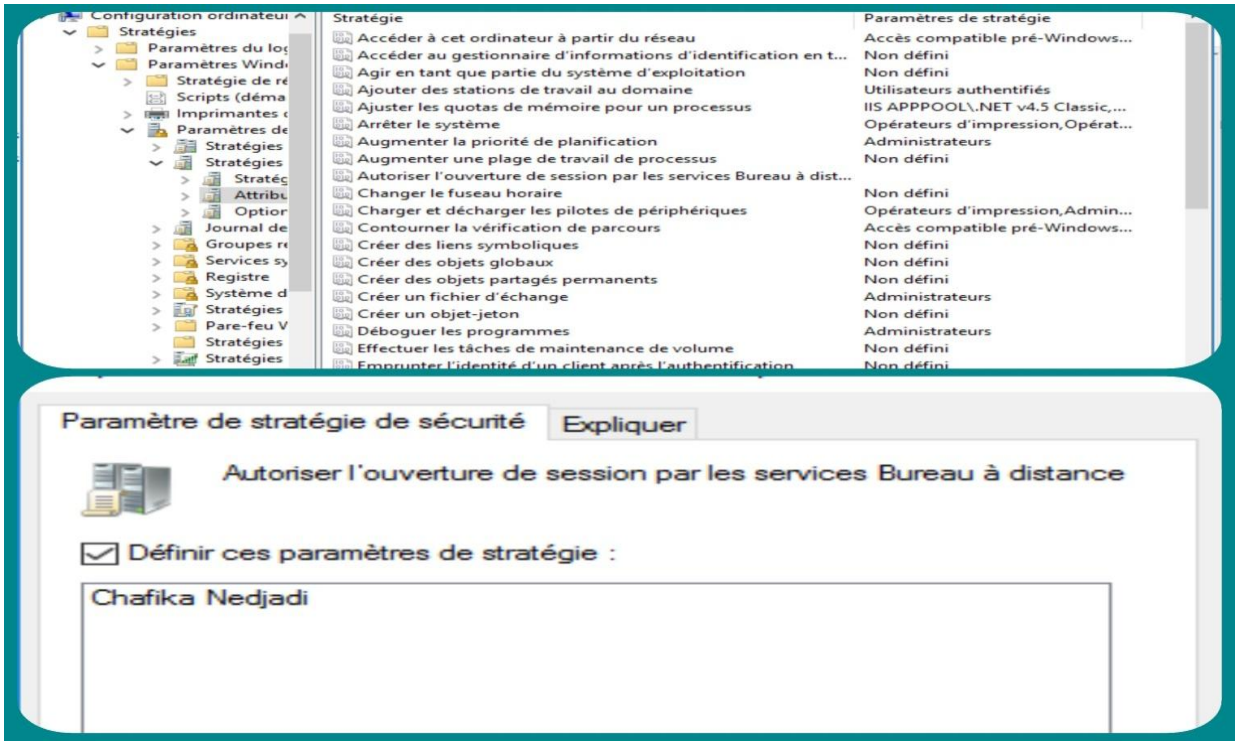

Figure 3-34 : Autoriser l'ouverture de session par les services bureau à distance.

Afin de vérifier l'accès à distance, on essaye d'accéder au serveur d'après la machine cliente de Chafika Nedjadi, comme la figure 3-35 nous montre :

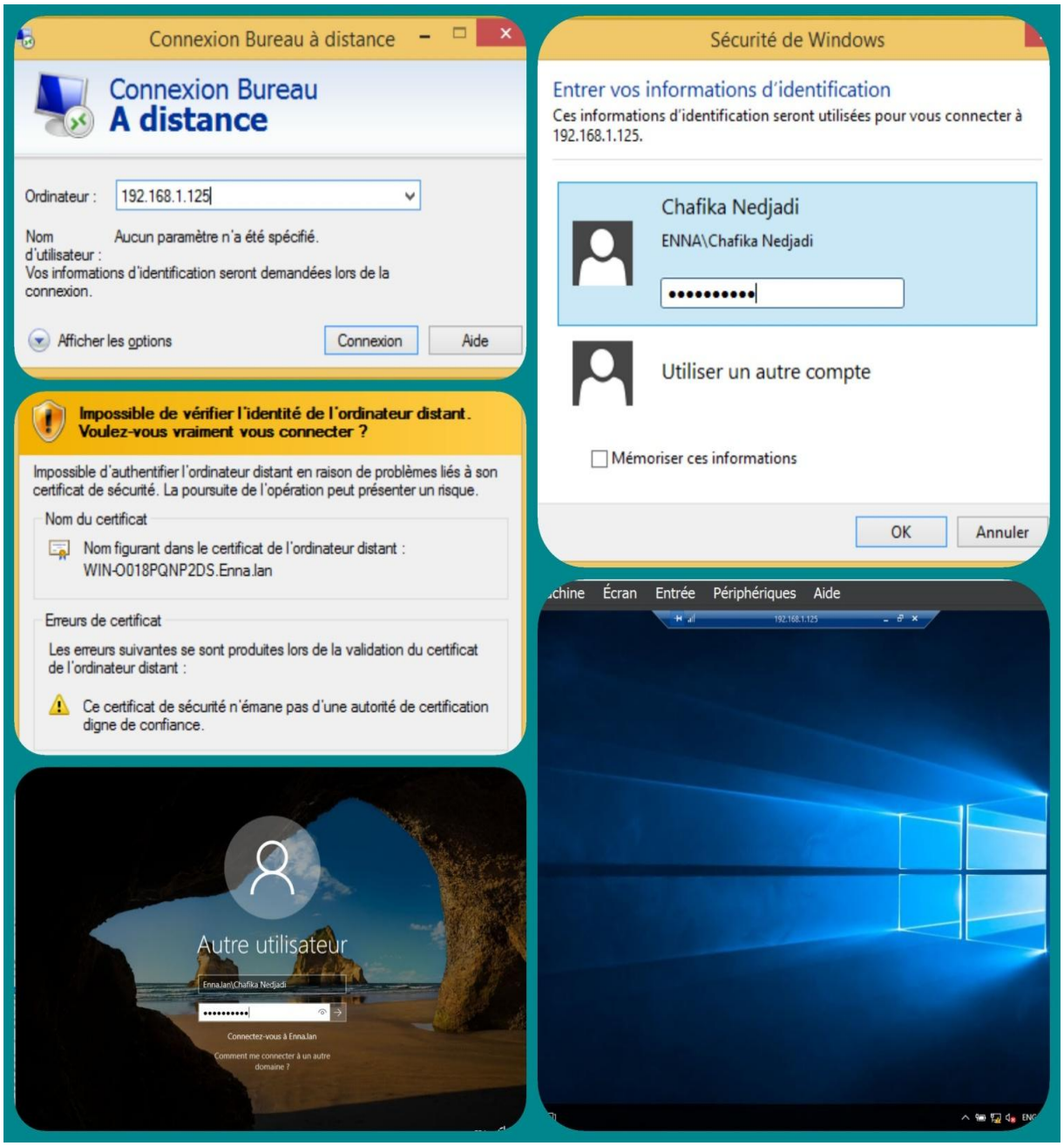

Figure 3-35 : Accéder au serveur à distance.

4.4.7 Spécification d'horaires d'accès au compte utilisateurs

La spécification des horaires d'accès sur Windows Server permet de contrôler quand les utilisateurs sont autorisés à accéder au serveur. Cela peut aider à améliorer la sécurité en limitant l'accès au serveur en dehors des heures de travail ou en autorisant l'accès uniquement aux utilisateurs autorisés pendant certaines heures.

Prenons exemple, pour Chafika Nedjadi, on peut lui programmé l'ouverture de session autorisée est du dimanche au jeudi, de 08 :00 à 16 :00 comme le montre la figure 3-36 :

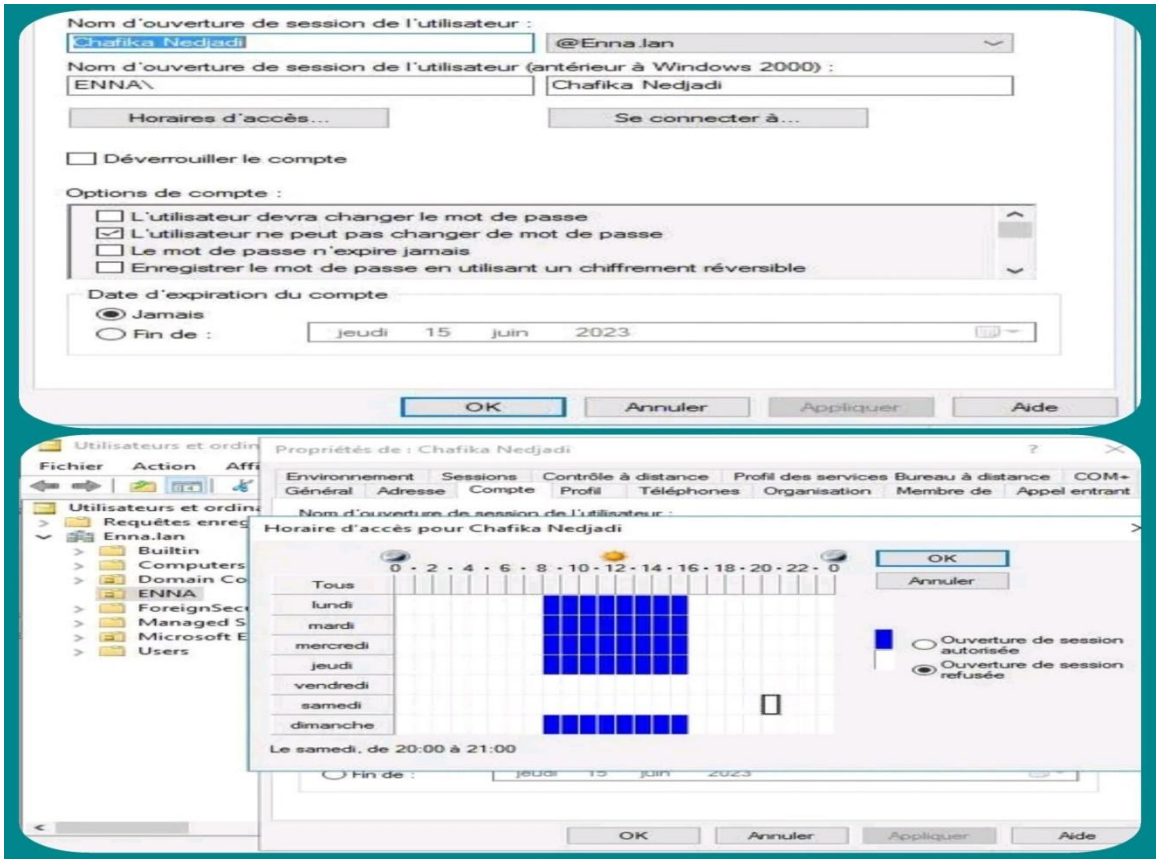

Figure 3-36 : Spécification des horaires d'accès au compte utilisateur.

4.4.8 Créer un profil itinérant pour un utilisateur

Rendre un utilisateur itinérant peut être utile dans plusieurs situations, notamment lorsque l'utilisateur doit accéder à des ressources de l'entreprise ou à des données hors de son lieu de travail habituel. Les utilisateurs itinérants peuvent accéder aux données et aux ressources en utilisant leurs propres appareils ou des appareils fournis par l'entreprise, grâce à des connexions internet sécurisées.

Pour créer un profil itinérant sur Windows Server 2016, suivons ces étapes :

- Créer un répertoire que nous allons partager et qui va stocker les données des profils. Dans notre cas nous avons créé un répertoire nommé « Profils_itinérants » que nous partageons sous le même nom.
- Ensuite cliquer sur « Autorisations **»,** Supprimer « Tout le monde » et préférer à la place « Groupe ENNA ».
- Les utilisateurs auront besoin d'un accès en lecture et écriture à ce dossier, cliquer maintenant sur « appliquer » puis « OK » pour enregistrer les informations.

- Ouvrir la gestion des « utilisateurs et des ordinateurs Active Directory ». Aller à l'unité d'organisation « ENNA » qui contient les utilisateurs pour lesquels nous souhaitons créer des profils itinérants et cliquer avec le bouton droit sur ces utilisateurs.
- Sélectionner « Propriétés » et aller à l'onglet « Profil ».
- Sélectionner l'option « Profil itinérant », dans le champ « Chemin du profil » entrer le chemin du dossier partagé sur le serveur où les profils itinérants seront stockés.
- Cliquer sur « Appliquer » et « OK ».

Ces étapes sont illustrées dans la figure 3-37 :

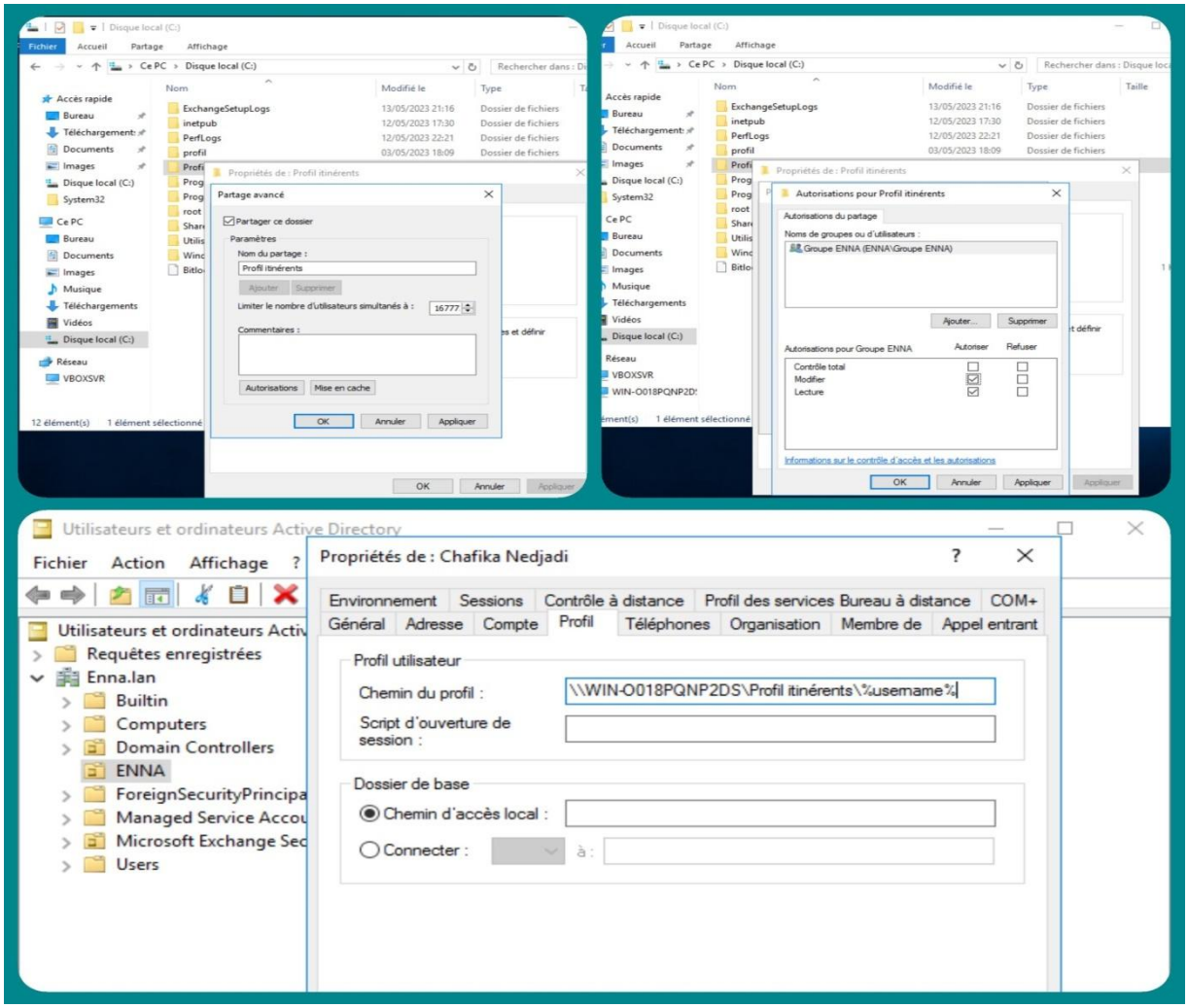

Figure 3-37 : Créer un profil itinérant pour un utilisateur.

Pour vérifier que le profil utilisateur est itinérant, ouvrir le « Panneau de configuration », sélectionner Système et Sécurité**,** Système**,** Paramètres système avancés et Paramètres dans la section Profils utilisateur, puis rechercher Itinérant dans la colonne Type**.**

Comme nous voyons sur la figure 3-38 l'utilisateur « Chafika Nedjadi » est un profil itinérant.

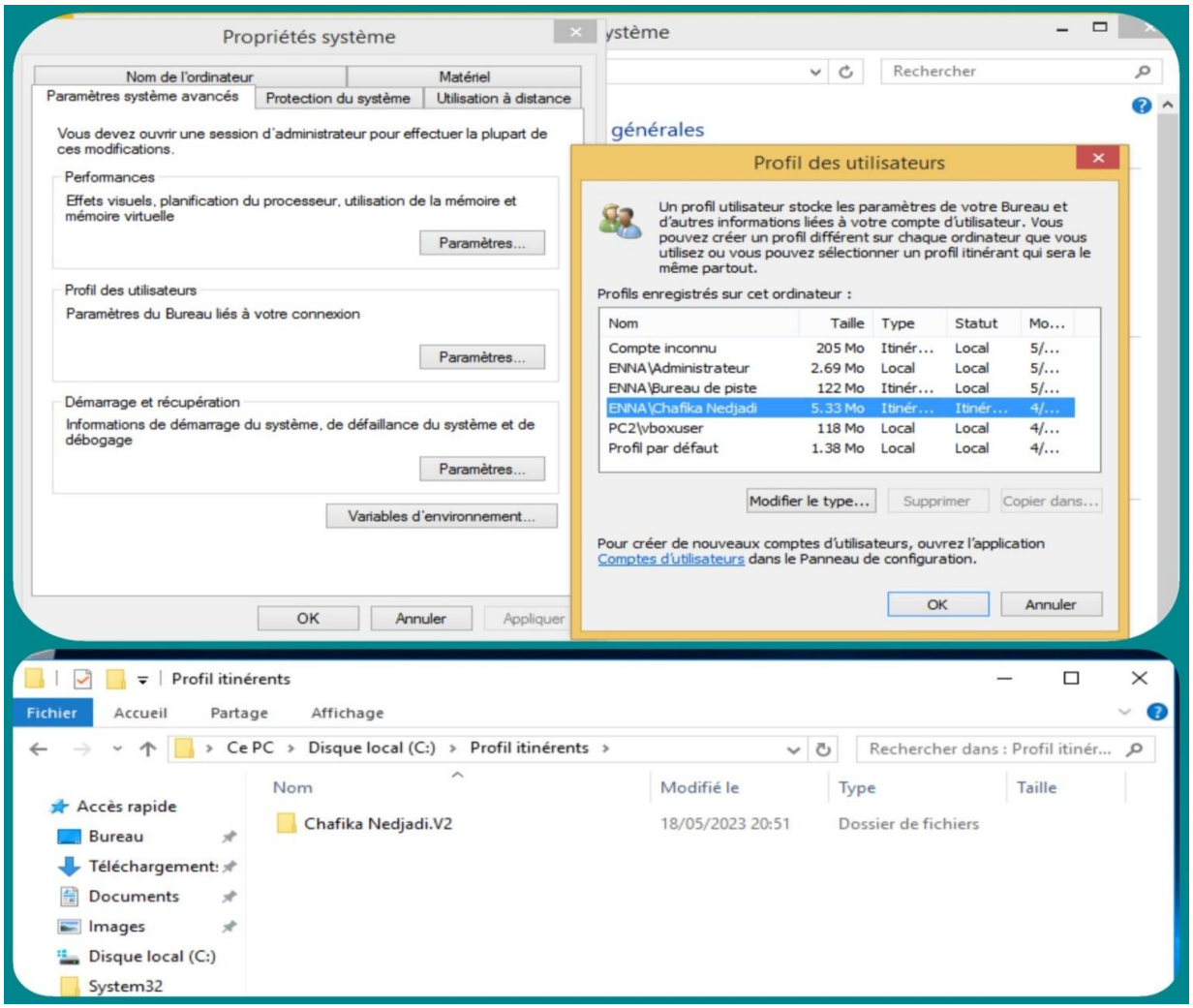

Figure 3-38 : Vérification de la création de profil itinérant.

4.5 Mise en œuvre des stratégies de groupe et des stratégies de sécurité

La stratégie de groupes et de sécurité sont importants pour maintenir la sécurité et l'intégrité des systèmes informatiques d'une organisation. La stratégie de groupe vous permet de définir des règles et des paramètres pour les utilisateurs, les ordinateurs et les groupes d'utilisateurs sur un réseau. Ces règles peuvent inclure des restrictions de sécurité, des stratégies de mot de passe, des autorisations de fichiers, des restrictions logicielles, la configuration d'écran de veille, etc.

Pour crée des GPO, nous devons créer des groupes pour accorder des règles aux même types d'utilisateur, et pour simplifier l'administration des comptes, en nous permettant d'attribuer des autorisations et des droits à des groupes d'utilisateurs au lieu qu'à chaque utilisateur individuel.

4.5.1 Configuration d'une stratégie pour empêcher la lecture d'USB

Le but d'empêcher l'utilisation d'une clé USB est de garantir la sécurité des données transférées. Si une clé USB est branchée sur une machine, cela peut permettre à une personne malencontreuse de copier ou de voler des données sensibles transférées sur le serveur. En outre, l'interdiction des clés USB peut aider à éviter la propagation de virus et de logiciels malveillants. Enfin, cela permet également de s'assurer que les employés travaillant sur le serveur suivent les politiques de sécurité de l'entreprise et ne prennent pas de risques inutiles avec les données de l'entreprise.

Pour configurer cette stratégie suivez les étapes ci-dessous :

- Rendre dans « Gestionnaire de serveur » et cliquer sur « Outils ». Sur la liste qui s'affiche, cliquer sur «Gestion de stratégie de groupe ».
- Aller sur le domaine « ENNA » et faire un clic droit sur l'unité d'organisation « ENNA » afin de créer un objet GPO. On va nommer l'objet « Empêcher la lecture d'USB ».
- Passons sur la configuration des paramètres. Pour ce faire, faites encore un clic droit sur l'objet créé puis cliquer sur « modifier».
- Dans la fenêtre affichée, nous devons aller à la route suivante: « Stratégies » puis Les directives, ensuite « Modèles d'administration » après sur «système ».
- Nous allons double-cliquer dessus et voir que par défaut, il n'est pas configuré. Cocher simplement la case « Activé » pour que la restriction soit effective. Cliquer sur « Appliquer », puis sur « OK» pour enregistrer les modifications.

La configuration de cette stratégie est illustré dans la figure 3-39 :

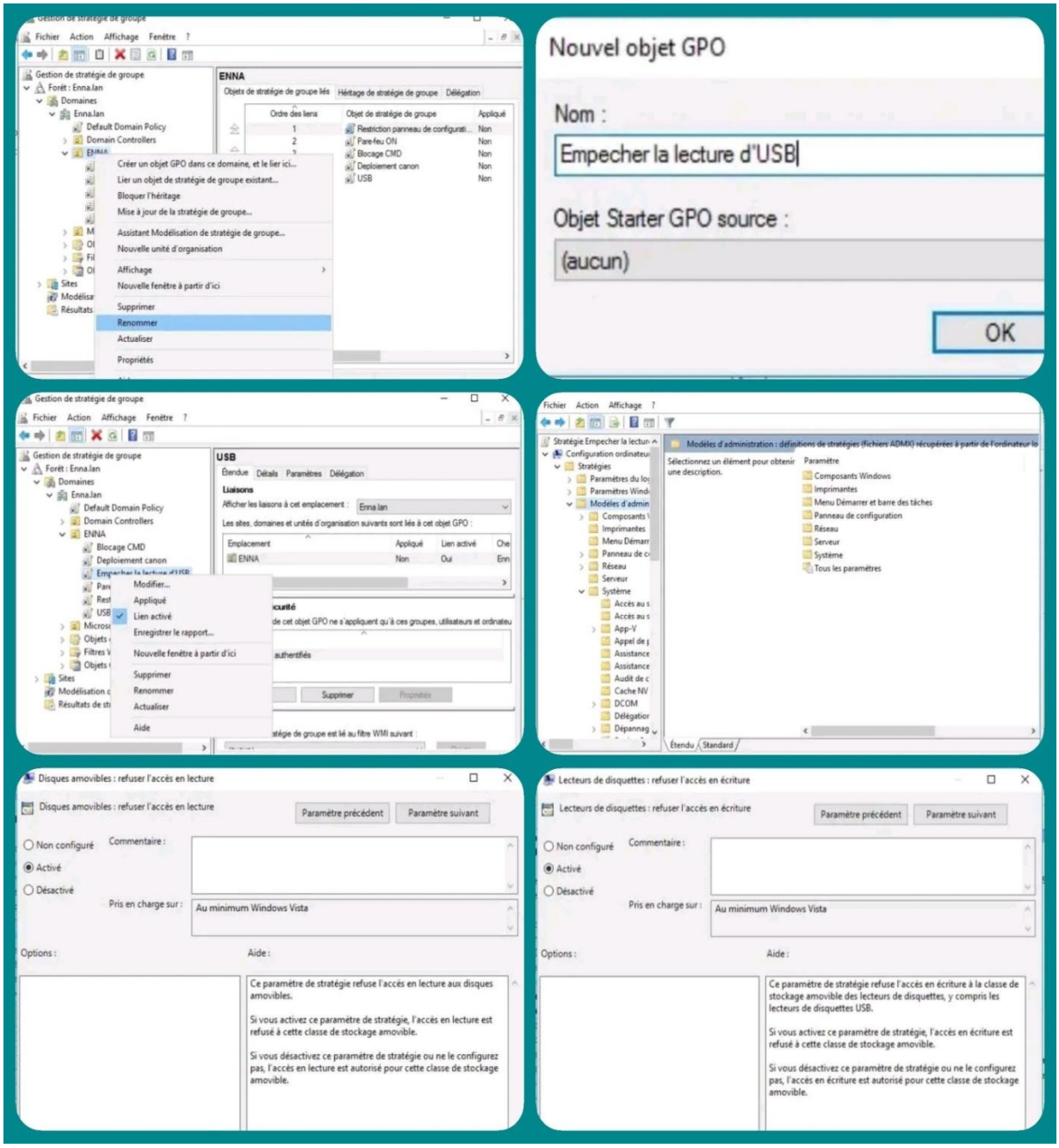

Figure 3- 39 : Configuration d'une stratégie pour empêcher la lecture d'USB.

Afin que le serveur puisse prendre en compte plus rapidement cette stratégie, nous devons lancer la commande « **gpupdate /force** » dans le terminal.

Puis connecter en tant qu'utilisateur afin de tester le fonctionne de la stratégie de groupe.

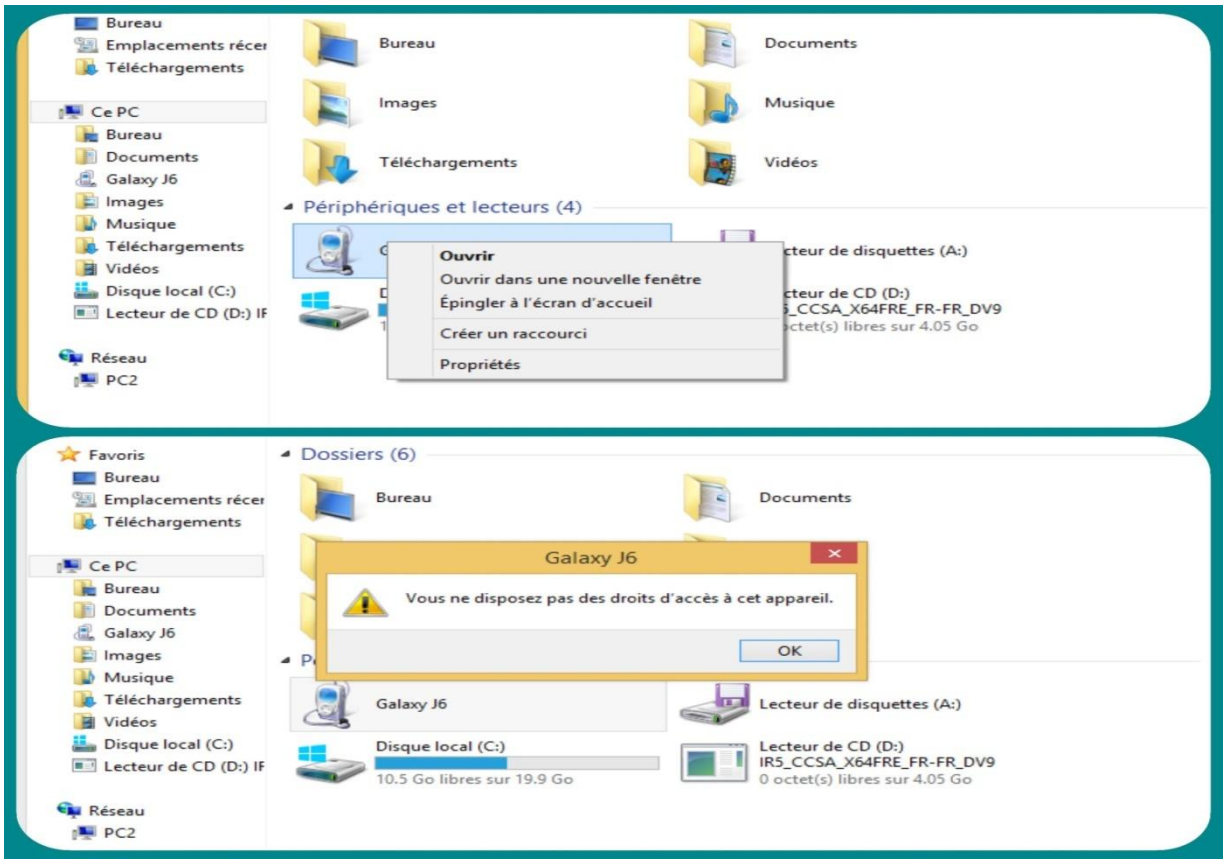

Figure 3-40: Test de la restriction de la lecture d'USB.

Nous voyons sur la figure 3-40 que l'utilisateur ne peut pas lire les données de la clé USB, car il ne dispose pas des droits d'accès à cette clé.

4.5.2 Configuration du pare-feu de domaine

Le rôle de cette GPO est d'activer le pare-feu de domaine sur tous les postes qui y sont rattachés. Nous allons autoriser les flux sortants mais bloquer les autres entrants.

Voici les étapes à suivre pour configurer cette stratégie :

- Cliquer sur la racine « Enna.lan », ensuite une nouvelle GPO **«** Pare-feu **ON »**, puis sélectionner « Modifier ».
- Maintenant suiver le chemin suivant : Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Pare-feu Windows avec paramètres avancés de sécurité.
- Puis clique droit et « Propriété », Puis activer le pare-feu et Bloquer la connexion entrante et Autoriser la connexion sortante.
- Enfin, activer les notifications pour le client en cas de connexion entrante bloquée.

Les étapes sont illustrées dans la figure 3-41 :

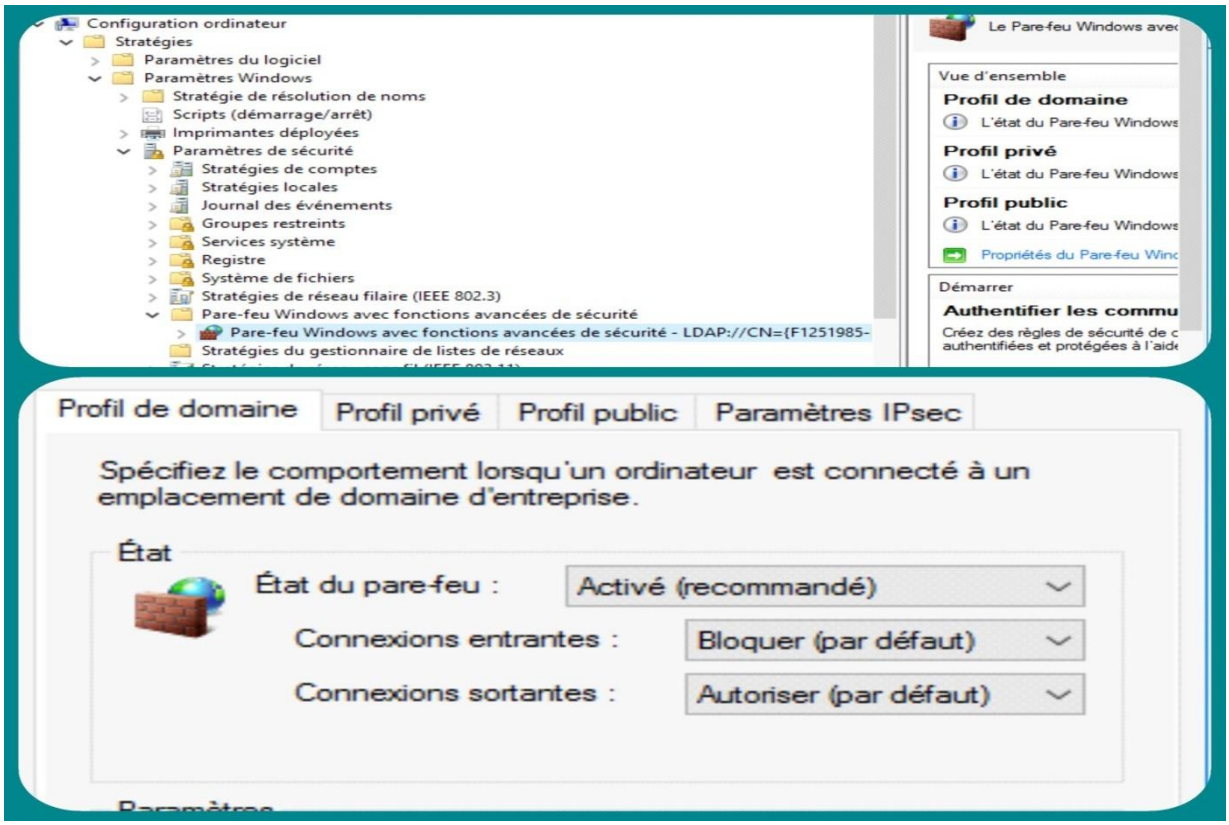

Figure 3-41 : Configuration du pare-feu de domaine.

Afin que le serveur puisse prendre en compte plus rapidement cette stratégie, vous devez lancer la commande « **gpupdate /force** » dans le terminal.

4.5.3 Configuration du blocage du panneau de configuration

C'est une mesure de sécurité pour éviter que des utilisateurs non autorisés ne modifient accidentellement ou délibérément des paramètres critiques du système. En bloquant l'accès au panneau de configuration, on peut réduire le risque que des erreurs de configuration ou des modifications malveillantes se produisent.

Pour configurer cette stratégie suivez les étapes suivantes :

- Sur le « Gestionnaire de Serveur » cliquons sur « Outils », puis sur « Gestion des stratégies de groupe »
- Puis la fenêtre s'ouvrira, cliquez avec le bouton droit de la souris sur la dite « unité d'organisation » et choisissez l'option «Créer un objet de stratégie de groupe dans ce domaine et le lier ici».
- Dans la fenêtre affichée, nous attribuons un nom à cette stratégie « Restriction de

panneau de configuration ».

- Clic droit sur la stratégie et sélectionner l'option « Modifier », Dans la fenêtre affichée, nous devons aller à la route suivante: Paramètres utilisateur > Les directives >Modèles d'administration > Panneau de commande.
- Dans le panneau de droite, vous devez configurer la stratégie avec le nom «Interdire l'accès à la configuration du PC et au panneau de configuration».
- Cochez simplement la case « Activé » pour que la restriction soit effective. Cliquez sur « Appliquer », puis sur « OK ».

La figure 3-41 présente la configuration de blocage de panneau de configuration :

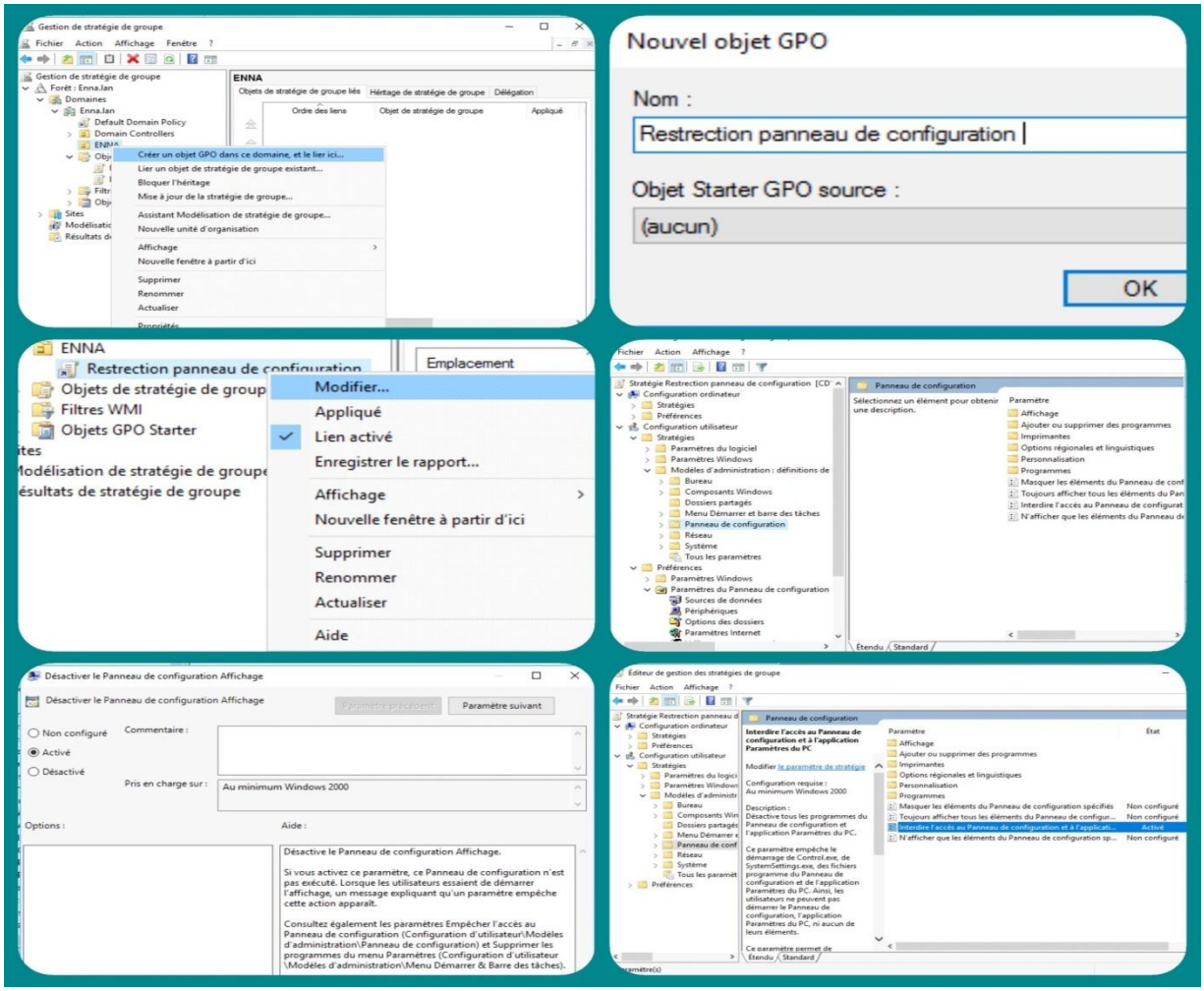

Figure 3-42 : Configuration de blocage de panneau de configuration.

Afin que le serveur puisse prendre en compte plus rapidement cette stratégie, vous devez lancer la commande « **gpupdate /force** » dans le terminal.

Maintenant connecter en tant qu'un utilisateur afin de tester le fonctionne de la stratégie de groupe, si tout est bien configuré, lorsque nous ouvrions le menu démarrer, l'option panneau de configuration sera invisible, comme nous montre la figure 3-43 :

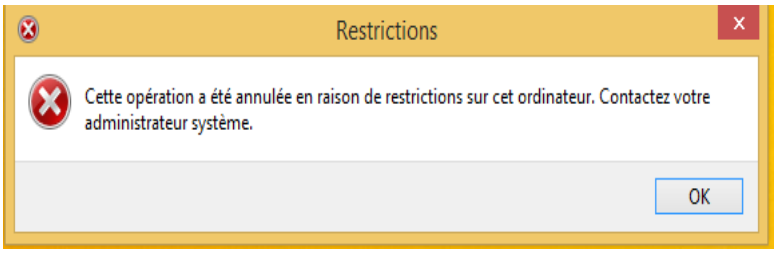

Figure 3-43: Test de restriction de panneau de configuration.

Comme nous le voyons ainsi, nous avons limité l'accès au Panneau de configuration et empêchons par conséquent tout utilisateur inexpérimenté ou non intentionnel d'exécuter des modifications non autorisées de l'équipement.

4.5.4 Configuration du blocage CMD

Il est nécessaire de configurer le blocage de la commande CMD (ou de l'invitation de commandes) pour des raisons de sécurité. L'invitation de commandes CMD peut être utilisée par des pirates informatiques pour exécuter des commandes malveillantes et compromettre la sécurité du système. En désactivant ou en bloquant la commande CMD, on peut limiter l'accès aux commandes système de bas niveau qui peut être utilisé pour causer des dommages au système.

Pour bloquer la commande CMD voici les étapes à suivre :

- Après avoir entré dans la gestion des stratégies de groupe puis « clique droit » sur unité d'organisation puis « créer un objet GPO dans ce domaine et le lier ici » et attribuer un nom de la GPO « blocage CMD »
- Apres avoir créé la GPO « blocage CMD » on clique droit sur la GPO puis « modifier ».
- L'option qui permet de désactiver l'accès à l'invite de commande (CMD) se trouve dans l'arborescence suivante : « configuration > utilisateur > stratégies > modèles d'administration > système ».
- Sur « système » une liste d'option s'affiche sur une colonne à droite. Dans cette liste est présent l'option « désactiver l'accès à l'invite de commandes », puis double clic sur cette option.

- Activer le fait que l'accès de commande soit désactivé, puis « appliquer » et « OK ».

La figure 3-44 présente la configuration de la stratégie de blocage de CMD :

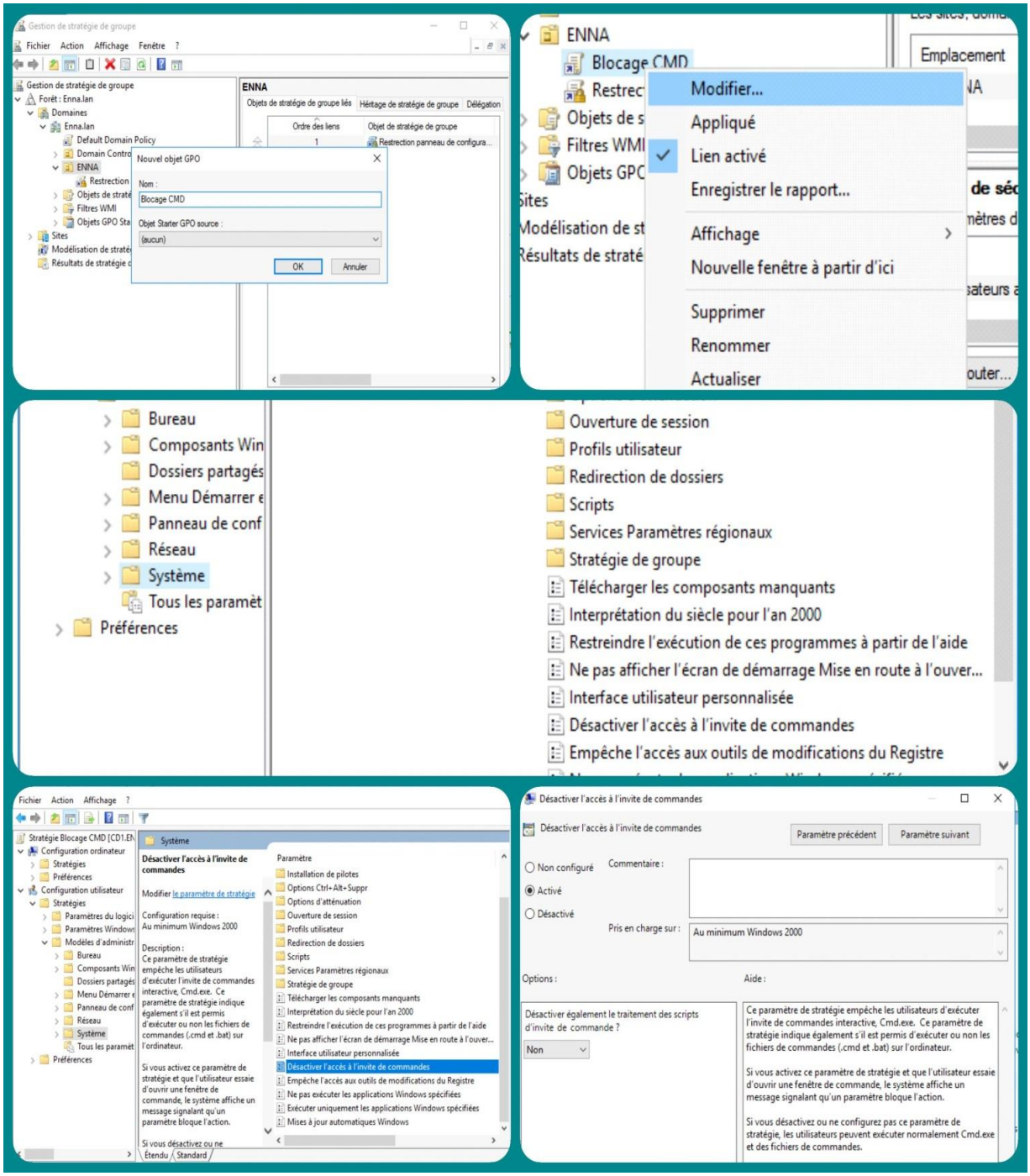

Figure 3-44 : Configuration de blocage CMD.

Afin que le serveur puisse prendre en compte plus rapidement cette stratégie, vous devez lancer la commande « **gpupdate /force** » dans le terminal.

Puis connecter en tant qu'utilisateur afin de tester le fonctionne de la stratégie de groupe.

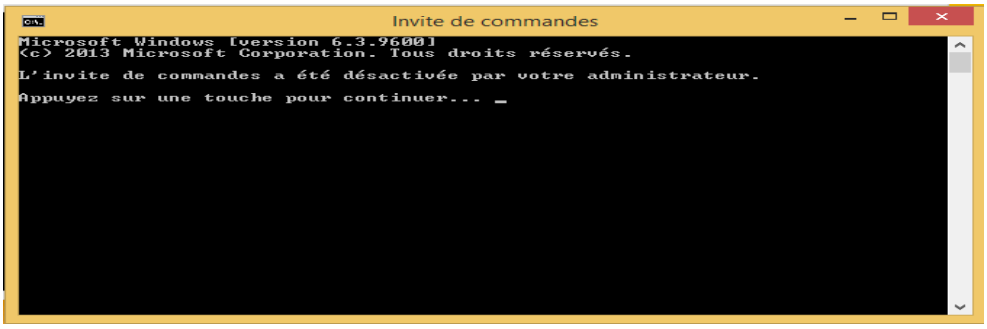

Figure 3-45: Test de restriction de l'invite de commande.

Comme nous pouvons le voir sur la figure 3-45 l'invite de commande est désactivée sur le poste.

4.6 Serveur de fichiers et de stockage

Un serveur de fichier est un type de serveur informatique qui permet à différents utilisateurs de partager des fichiers et des dossiers dans un réseau. En utilisant un serveur de fichier, les utilisateurs peuvent stocker des données sur un emplacement centralisé et y accéder à partir de n'importe quel ordinateur ou dispositif connecté au réseau. Les serveurs de fichiers sont souvent utilisés dans les entreprises pour permettre à différents employés d'accéder et de partager des documents, des présentations, des images et d'autres types de fichiers.

4.6.1 Installation et configuration d'un serveur de fichiers et de stockage

Pour installer un serveur de fichier sous Windows server 2016 voici les étapes à suivre :

- Dans le gestionnaire de serveur, cliquer sur « Services de fichiers et de stockage », puis sélectionner « Partages »
- Sur le menu « Tâches » sélectionner « Nouveau partage ».
- Laisser « Partage SMB - Rapide » coché et Sélectionner le disque que nous allons utiliser pour notre partage.
- Donner un nom à notre partage, le champ « Chemin d'accès distant au partage » indique le chemin que nous pouvons utiliser pour accéder au partage que nous êtes en train de créer.
- Sur la page « Autres paramètres » laisser par défaut et cliquer sur « Suivant ».
- A la fin nous pouvons définir les personnes qui sont autorisées à accéder à ce partage. Par défaut, autorise tout le monde et cliquer sur « Appliquer » et « OK » pour enregistrer les modifications.

La figure 3-46 illustre les étapes de l'installation et de configuration du serveur :

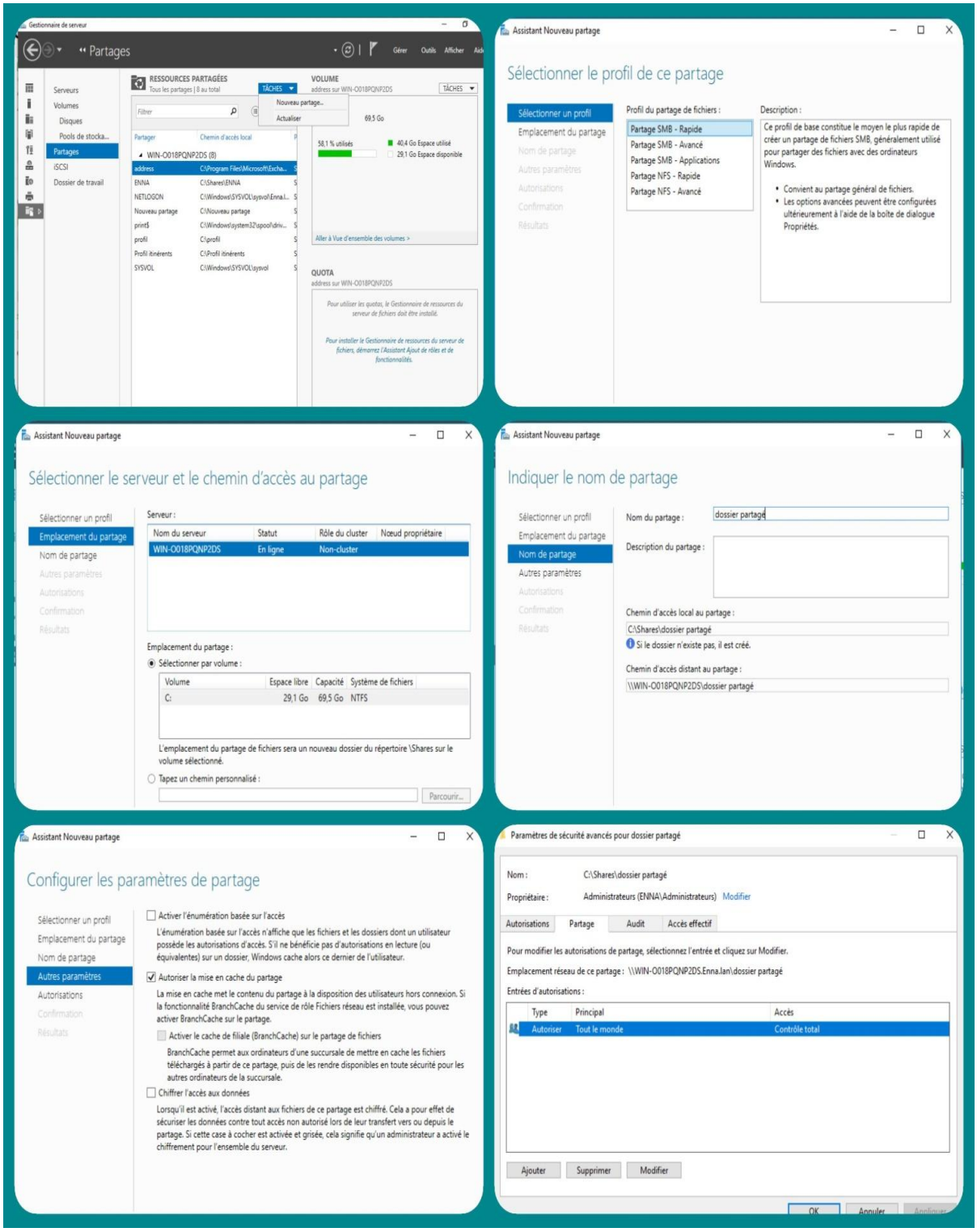

Figure 3- 46 : Installation et configuration d'un serveur de fichiers et de stockage.

Afin de vérifier le dossier partagé, nous connectons en tant qu'un utilisateur et ensuite utilisons le chemin d'accès dans l'explorateur de fichier « \\WIN-O018QNP2DS\\dossier partagé », comme nous montre la figure 3-47 :

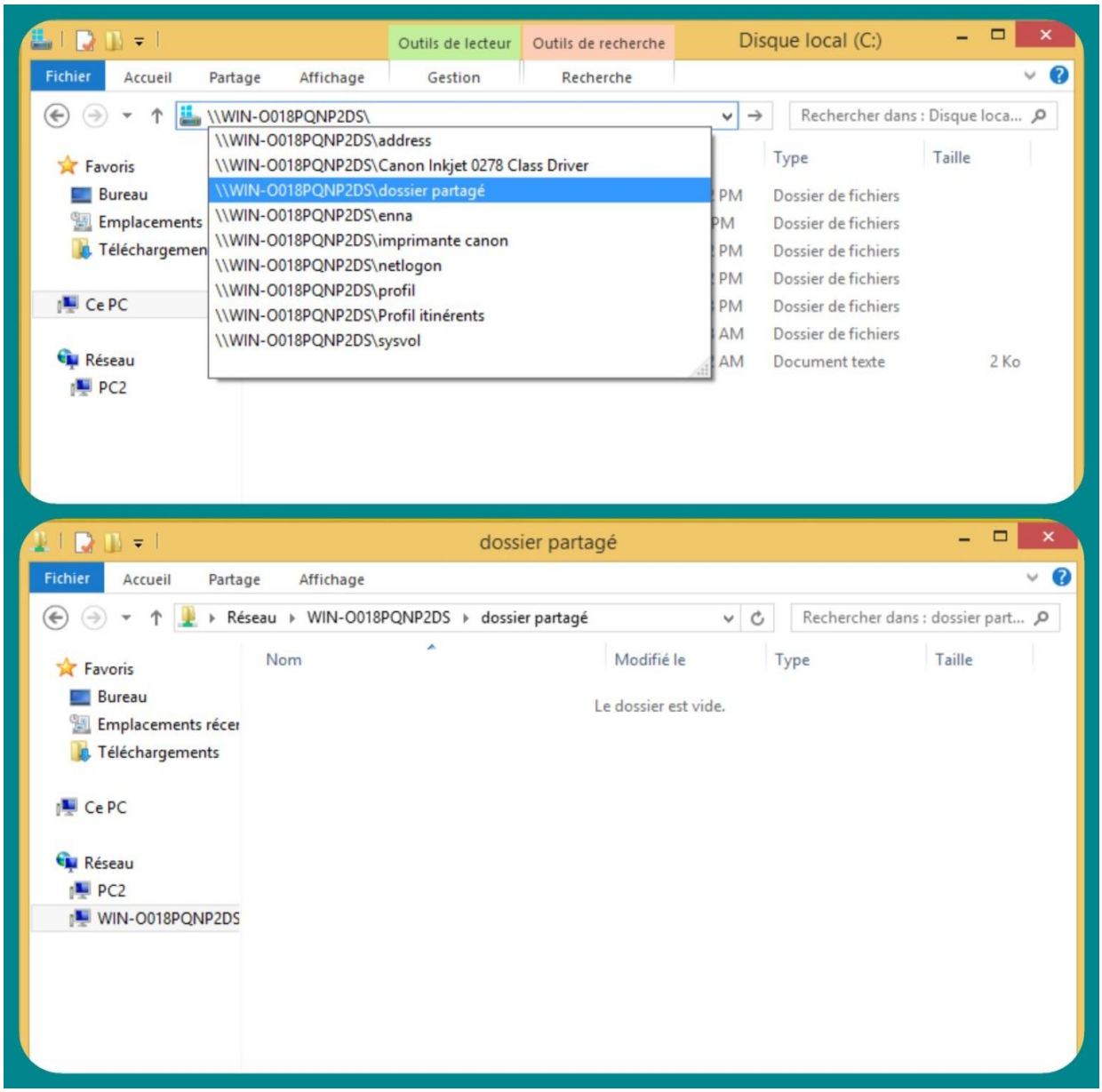

Figure 3-47 : Vérification de dossier partagé.

4.7 Serveur d'impression

Un serveur d'impression est un dispositif qui permet de gérer l'impression de plusieurs utilisateurs sur un réseau commun. L'utilisation d'un serveur d'impression est particulièrement utile dans les environnements professionnels où plusieurs utilisateurs partagent des imprimantes en réseau, car cela permet de réduire les coûts en matériel et en maintenance, ainsi que de faciliter la gestion des impressions.

Le serveur d'impression est un rôle qu'on peut ajouter après l'installation d'Active Directory

4.7.1 Ajout et Partage d'une imprimante sur le réseau

Partager une imprimante sur le réseau permet à plusieurs utilisateurs de se connecter et d'utiliser la même imprimante. Cela permet d'économiser de l'argent car il n'est pas nécessaire d'acheter plusieurs imprimantes. De plus, cela permet aux utilisateurs de travailler plus efficacement car ils peuvent imprimer rapidement sans avoir à transférer des fichiers ou à se déplacer pour se connecter à l'imprimante. L'ajout et le partage d'une imprimante sur le réseau peut également aider à maintenir la sécurité des données car il y a moins de risques de perte ou de vol de fichiers lorsqu'ils sont stockés sur un seul appareil qui peut être surveillé et protégé.

Pour ce faire voici les étapes à suivre :

- Sur le serveur d'impression Windows Serveur, ouvrir la console « Gestion de l'impression » et faire un clic droit sur « Imprimante » et cliquer sur « Ajouter une imprimante » pour lancer l'assistant d'ajout d'une nouvelle imprimante.
- Choisissons ensuite la méthode d'installation.
- Choisissons « TCP/IP » et entrer l'adresse IP de l'imprimante.
- Puis Choisissons le pilote d'impression de l'imprimante.
- Entrer le nom de l'imprimante ainsi que son nom de partage.
- Un résumé de l'imprimante à ajouter s'affiche, confirmer l'installation de l'imprimante sur le serveur d'impression.

Les étapes de l'installation et configuration du serveur sont présentées dans la figure 3-48 :

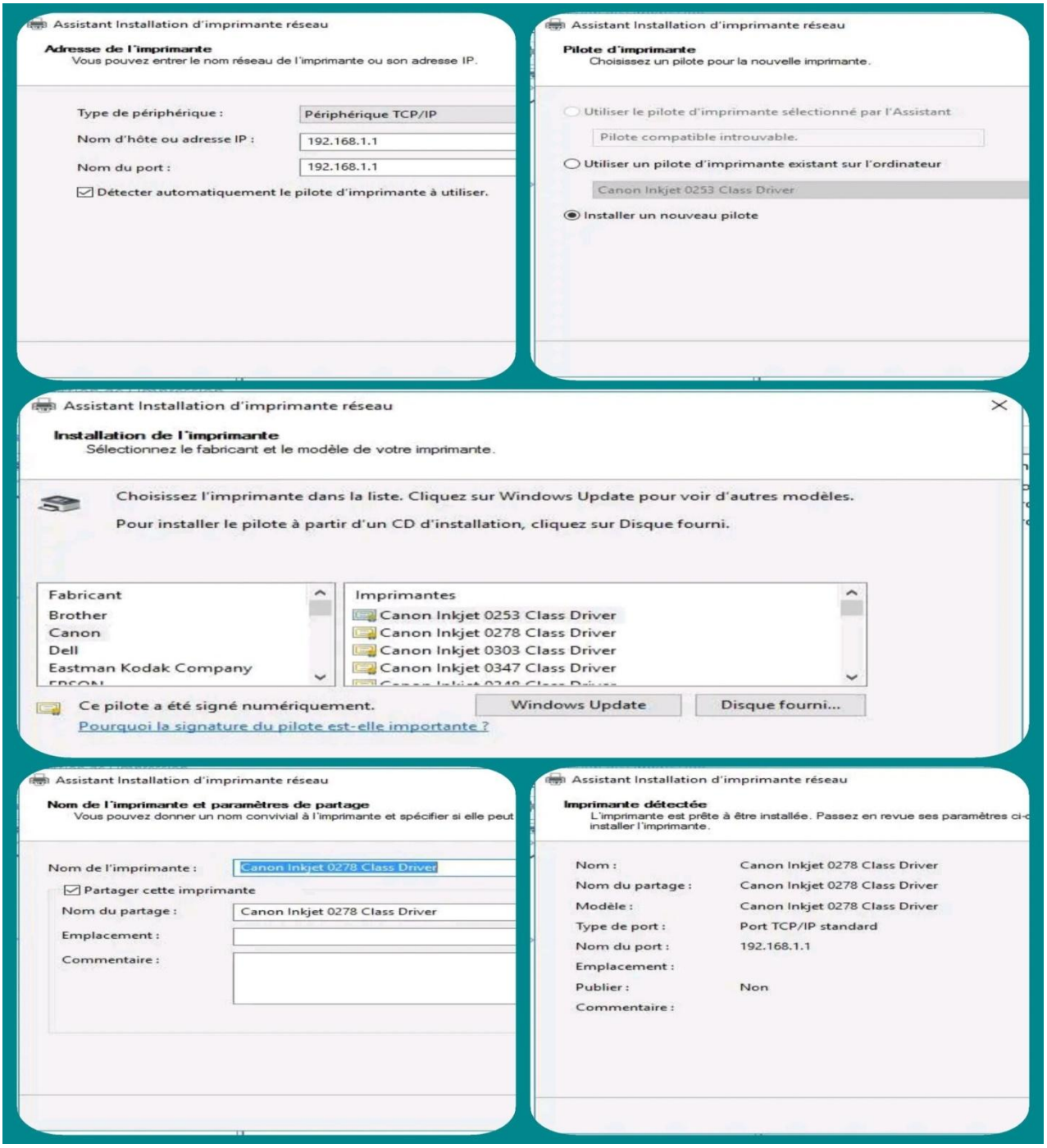

Figure 3-48 : Installation et configuration d'un serveur d'impression.

4.7.2 Connecter une imprimante à un client

Pour que le client puisse imprimer des documents sur l'imprimante ajoutée, faut d'abord l'installer sur le poste client comme montre la figure 3-49 :

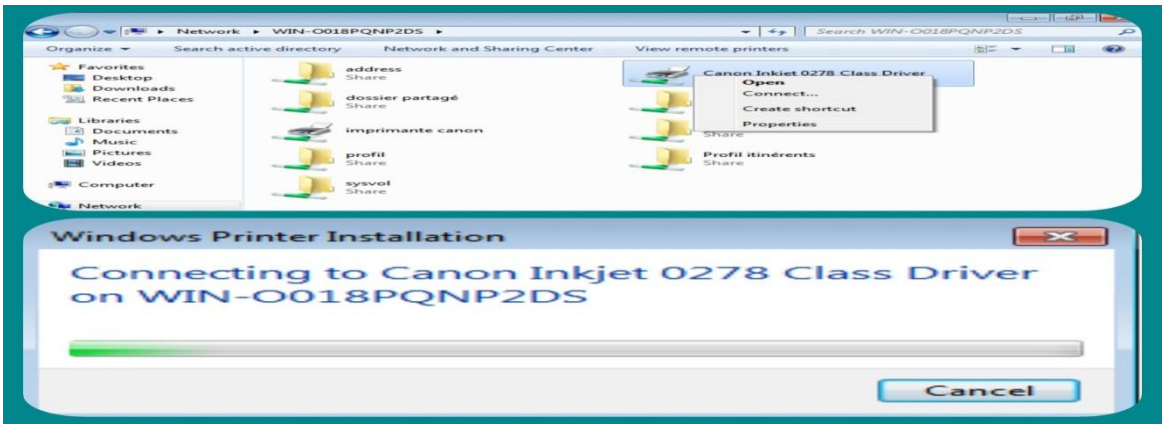

Figure 3-49 : Connecter une imprimante à un client.

4.8 Serveur de messagerie

Le serveur de messagerie permet de mettre en place une infrastructure de courrier électronique pour les utilisateurs d'une entreprise. Cette infrastructure comprend un serveur de messagerie et des clients de messagerie (tels que Microsoft Outlook) pour envoyer et recevoir des messages électroniques. Un serveur de messagerie inclut la possibilité de gérer les comptes de messagerie de l'entreprise, la sécurisation des communications électroniques et la centralisation de la gestion des messages électroniques. Cela permet de faciliter la communication et la collaboration au sein de l'entreprise, et de réduire les coûts liés aux solutions de messagerie tierces.

4.8.1 Installation et configuration d'un serveur de messagerie Exchange 2016

Exchange Server 2016 est une solution de messagerie et de communication d'entreprise de Microsoft. Il permet aux utilisateurs de communiquer via des e-mails, des calendriers et des contacts partagés, ainsi que des fonctionnalités avancées telles que la messagerie unifiée, les règles de transport, la protection contre le spam et la sécurité améliorée.

Pour Installer le serveur Exchange nous suivons les étapes suivantes :

- Installer des composants pré requis : Unified Communications Managed API 4.0 Runtime, et Microsoft NET Framework 4.7.2.
- Installer les fonctionnalités pré requis **:** Ouvrez la ligne de commande PowerShell en tant qu'un administrateur, tapez la commande « Install-WindowsFeature Server-mediafoundation » et « Install-WindowsFeature RSAT-ADDS ».
- Préparer Exchange à l'Active Directory en suivant les commandes suivantes :

« cdC:\Users\Administrateur\Desktop\exchange2016 », « setup/prepareschema » et « setup /prepareschema /IAcceptExchangeServerLicenseTerms ».

- Puis démarrer l'installation d'Exchange avec le setup.exe.

Les étapes de l'instalation d'Exchange 2016 sont illustrées dans la figure 3-50 :

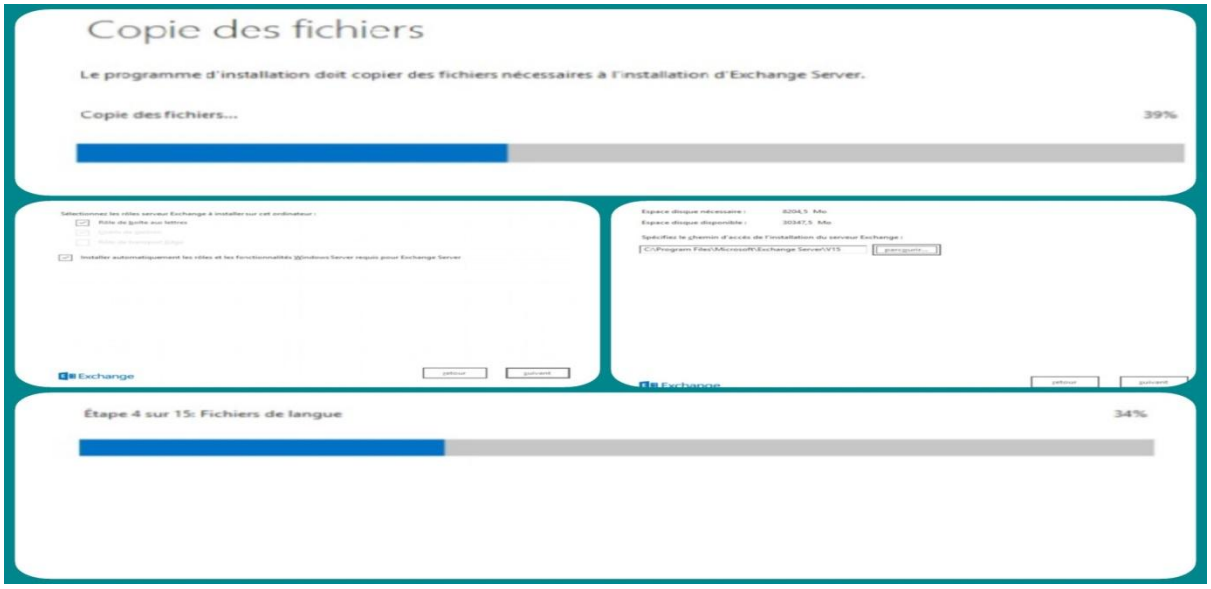

Figure 3-50: Installation d'Exchange 2016.

Après avoir installé Exchange 2016, il ne reste maintenant qu'à configurer le serveur Exchange pour qu'il puisse envoyer et recevoir des emails. La configuration est faite par la console « centre d'administration exchange » présenté dans la figure 3-51 :

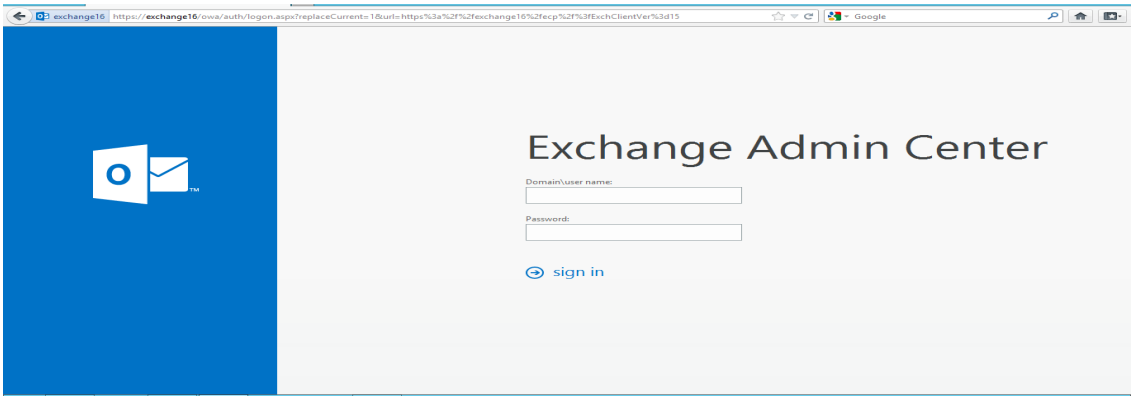

Figure 3-51: Centre d'administration Exchange.

Maintenant on passe à la création des comptes utilisateurs Active Directory suivant les étapes suivants :

- Sur le « gestionnaire de serveur » suiver la route suivante : →Outils → Utilisateurs et ordinateurs Active Directory.
- Faire clic droit sur Users puis sélectionnez Nouveau Utilisateur.

- Ensuite entrer le nom, prénom de l'utilisateur et le nom d'ouverture de session qui doit être unique, puis le mot de passe de la session.

Après avoir créé les utilisateurs on passe maintenant à la liaison des utilisateurs sous exchange et pour ce faire suivez les étapes suivantes :

- Lancer la page web « Centre d'administration d'Exchange », connecter maintenant avec le compte administrateur sans oublier le nom du domaine.
- Ensuite ajouter les boites d'utilisateurs à la boite aux lettres de l'administrateur qui a été créé par défaut, pour cela cliquer sur le logo « + », Puis « boite aux lettres utilisateur », comme montre la figure 3-52 :

Figure 3-52 : Boite aux lettres d'administrateur.

- Sélectionner maintenant les utilisateurs que nous avons déjà créés précédemment.

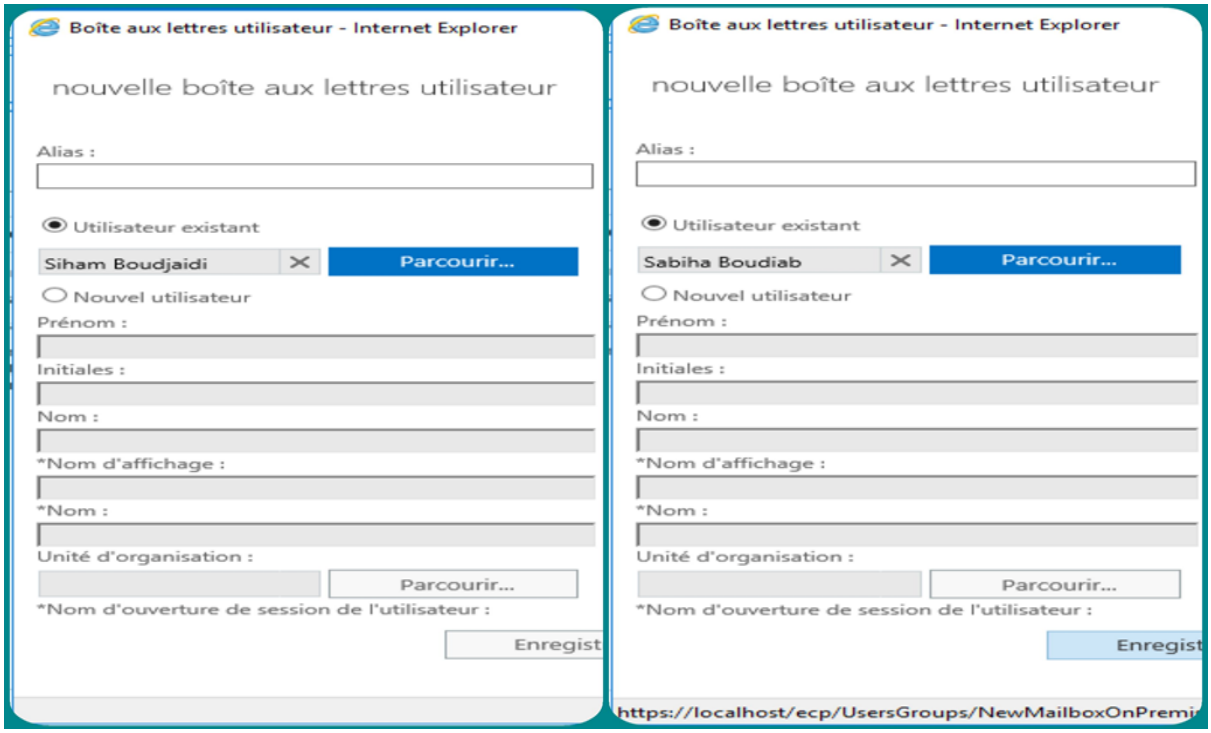

Figure 3- 53: Ajout des boites aux lettres.

Les boites aux lettres sont bien créées comme le montre la figure 3-54 :

Figure 3-54 : Création des boites aux lettres.

4.8.2 Test avec Outlook 2007

La figure 3-55 présente les étapes pour se connecter aux boites aux lettres :

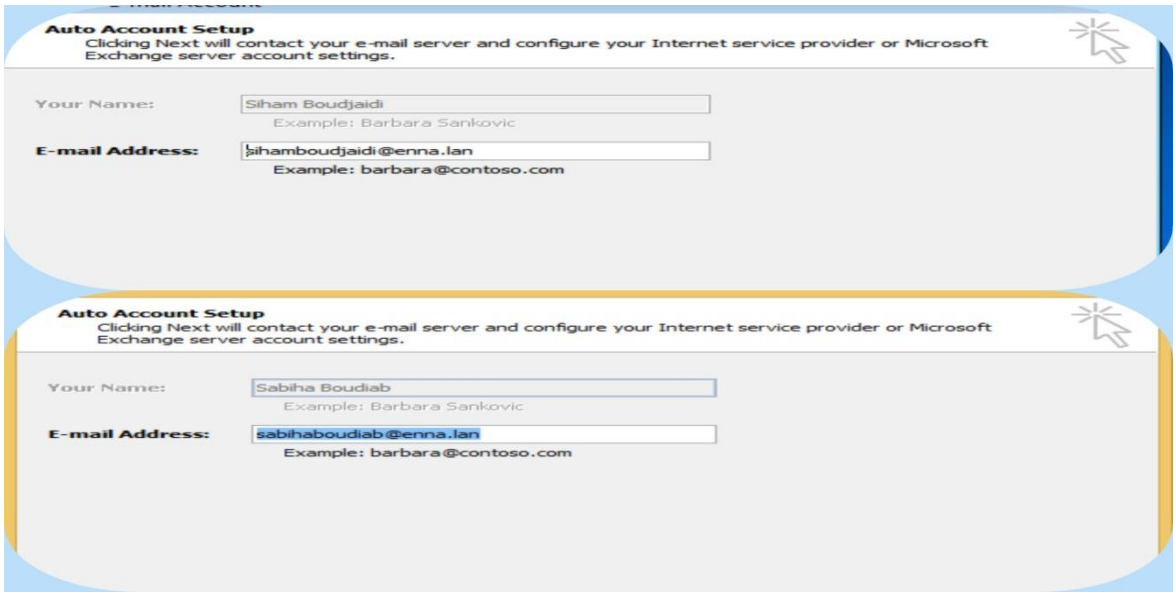

Figure 3-55 : Connexion aux boites aux lettres.

Après que l'utilisateur ait accédé à sa boîte de réception, il aura la possibilité d'envoyer et de recevoir des e-mails.

Pour envoyer des emails, nous allons :

- Cliquer sur « **New** », l'interface de création de nouveau message s'affiche.
- Dans la zone « **To** » sélectionner le destinataire du mail. Puis il faut saisir le corps de l'email et cliquer sur « **Send** ». Il sera enregistré dans le dossier « Sent items».

La figure 3-56 illustre les étapes pour créer et envoyer un émail :

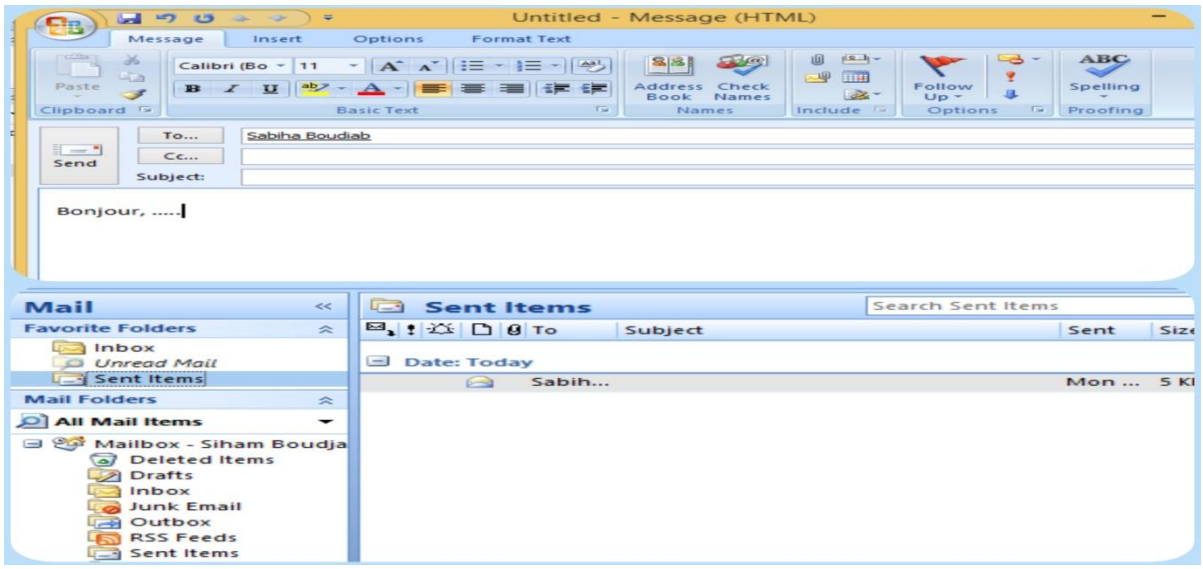

Figure 3-56 : Création et l'envoi d'email.

La figure 3-57 montre que l'email a été bien reçu :

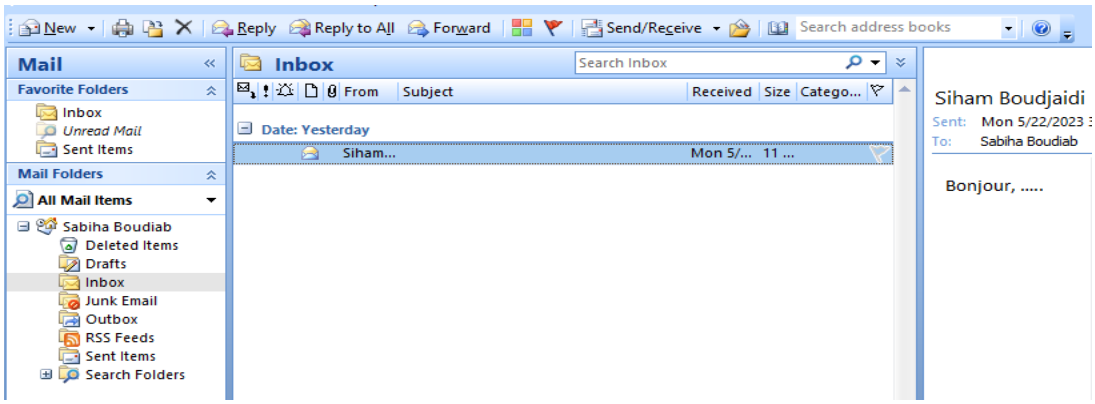

Figure 3-57 : Boite de réception du destinataire.

5 Tests de vérification

Les tests effectués visent à valider les configurations en utilisant les commandes "show". Ces commandes permettent d'afficher les configurations réalisées sur les équipements. Une autre phase de tests consiste à vérifier l'accessibilité et la communication entre les utilisateurs. Cette phase utilise la commande "ping", qui permet de tester la réponse d'un équipement sur le réseau.

5.1 Vérification des configurations

5.1.1 Vérification de la création des VLANs

Pour vérifier que les VLAN ont été créés correctement, il est possible d'exécuter la commande "show vlan brief" sur le commutateur. Cette commande permettra de visualiser un résumé des VLAN configurés sur le commutateur comme le montre la figure 3-58 :

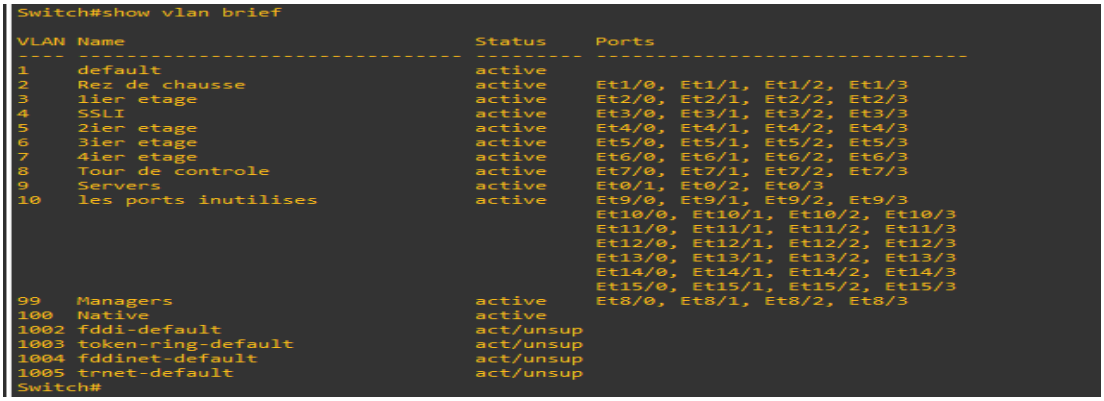

Figure 3-58 : Vérification de la création des VLANs.

5.1.2 Vérification de la configuration des sub-interfaces du routeur

Si l'on souhaite vérifier que les adresses IP des sous-interfaces sont correctement configurées, il suffit de taper la commande "show ip interface brief" sur la console du routeur, comme le montre la figure 3-59

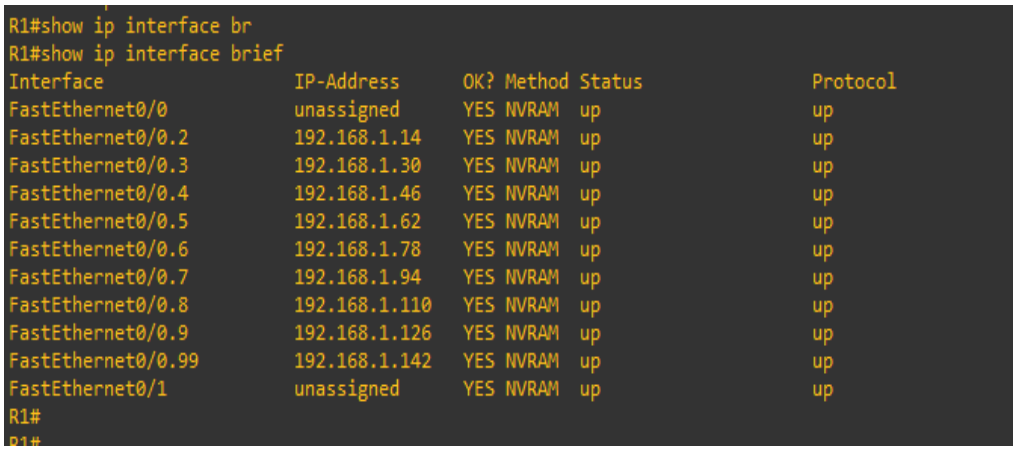

Figure 3-59 : Vérification de la configuration des sub-interfaces du routeur.

5.1.3 Vérification de la configuration du dhcp snooping

Pour vérifier que la sécurité DHCP est configurée correctement et afficher les informations liées à la sécurité du service DHCP sur le réseau, on utilise la commande « **show ip dhcp snooping** », le résultat de la commande est illustré dans la figure 3-60 :

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
2-8,99
DHCP snooping is operational on following VLANs:
2-8,99
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled
   circuit-id default format: vlan-mod-port
   remote-id: aabb.cc00.0100 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
Ethernet0/0                yes        yes             unlimited
  Custom circuit-ids:
Ethernet1/0                no         no              10
  Custom circuit-ids:
Ethernet1/1                no         no              10
  Custom circuit-ids:
Ethernet1/2                no         no              10
  Custom circuit-ids:
Ethernet1/3                no         no              10
  Custom circuit-ids:
```

Figure 3-60 : Vérification de la configuration du dhcp snooping.

5.1.4 Vérification de la sécurité des ports

La commande "show port-security" est utilisée pour afficher des informations sur la sécurité des ports sur un commutateur réseau, comme le montre la figure 3-61 :

```
Switch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
-------------------------------------------------------------------------------
       Et1/0           10            0                  0          Shutdown
       Et1/1           10            0                  0          Shutdown
       Et1/2           10            0                  0          Shutdown
       Et1/3           10            0                  0          Shutdown
       Et2/0           10            0                  0          Shutdown
       Et2/1           10            1                  0          Shutdown
       Et2/2           10            0                  0          Shutdown
       Et2/3           10            0                  0          Shutdown
       Et3/0           10            0                  0          Shutdown
       Et3/1           10            0                  0          Shutdown
       Et3/2           10            0                  0          Shutdown
       Et3/3           10            0                  0          Shutdown
       Et4/0           10            0                  0          Shutdown
       Et4/1           10            0                  0          Shutdown
       Et4/2           10            0                  0          Shutdown
       Et4/3           10            0                  0          Shutdown
       Et5/0           10            0                  0          Shutdown
       Et5/1           10            0                  0          Shutdown
       Et5/2           10            0                  0          Shutdown
       Et5/3           10            0                  0          Shutdown
       Et6/0           10            0                  0          Shutdown
       Et6/1           10            0                  0          Shutdown
       Et6/2           10            0                  0          Shutdown
       Et6/3           10            0                  0          Shutdown
       Et7/0           10            0                  0          Shutdown
       Et7/1           10            0                  0          Shutdown
       Et7/2           10            0                  0          Shutdown
       Et7/3           10            0                  0          Shutdown
       Et8/0           10            1                  0          Shutdown
       Et8/1           10            0                  0          Shutdown
       Et8/2           10            0                  0          Shutdown
       Et8/3           10            0                  0          Shutdown
-------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

Figure 3-61: Vérification de la sécurité des ports.

5.1.5 Vérification la mise en service de DHCP

Après avoir saisi la commande « ipconfig /all » sur l'invite de commande de notre machine cliente, on constate que le DHCP est bien activé « OUI » avec une adresse IPV4 qui a était attribuer par le serveur « 192.168.1.125 ». Les résultats sont illustrés dans la figure 3-62 :

Figure 3-62 : Vérification de ma mise en service de DHCP.

5.2 Tests

Pour vérifier la connectivité entre les différents équipements du réseau, on utilise la commande "ping". Lorsqu'un utilisateur souhaite communiquer avec un autre, il envoie des paquets de données au destinataire à l'aide de la commande "ping". Si ces paquets sont bien reçus par le destinataire, le test de connectivité est réussi. Toutefois, si les paquets ne sont pas reçus, le test a échoué.

5.2.1 Test intra-VLANs

Pour vérifier la connectivité entre des équipements se trouvant dans le même VLAN et le même commutateur, on peut effectuer un test de ping entre le PC2 ayant pour adresse IP "192.168.1.17" et la machine virtuelle "Managers" ayant pour adresse IP "192.168.1.18" comme le montre la figure 3-63 :

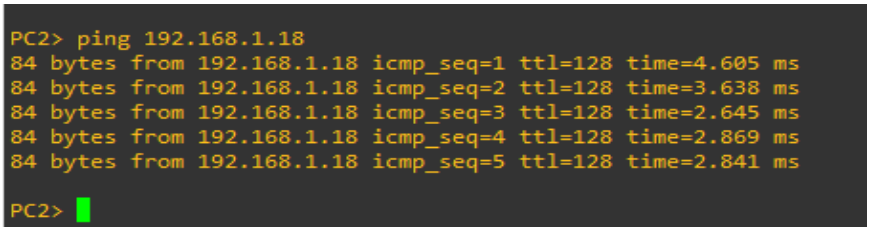

Figure 3-63 : Test intra-VLANs.

5.2.2 Test inter-VLANs

Pour vérifier la connectivité entre des équipements se trouvant dans des VLANs différents, on peut effectuer un test de ping entre la machine virtuelle "Managers" ayant pour adresse IP "192.168.1.18" qui se trouve dans le VLAN 3 et le PC1 ayant adresse « 192.168.1.1 » qui se trouve dans le VLAN 2, comme le montre la figure 3-64

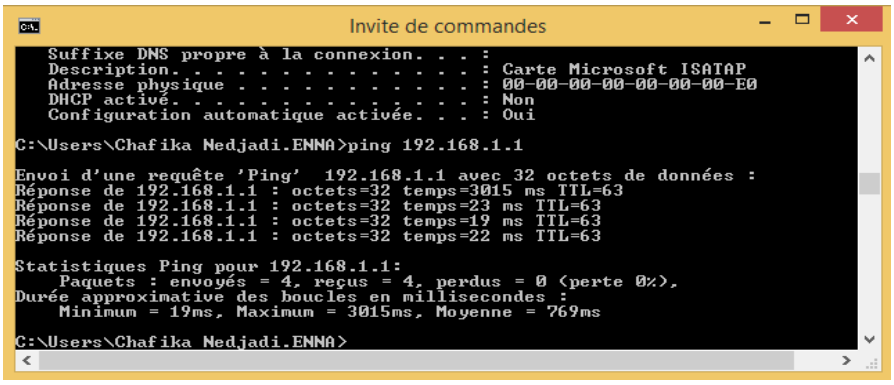

Figure 3-64 : Test inter-VLANs.

5.2.3 Simulation de l'attaque ARP spoofing

- La figure 3-65 présente la simulation dans le VLAN de l'attaquant :

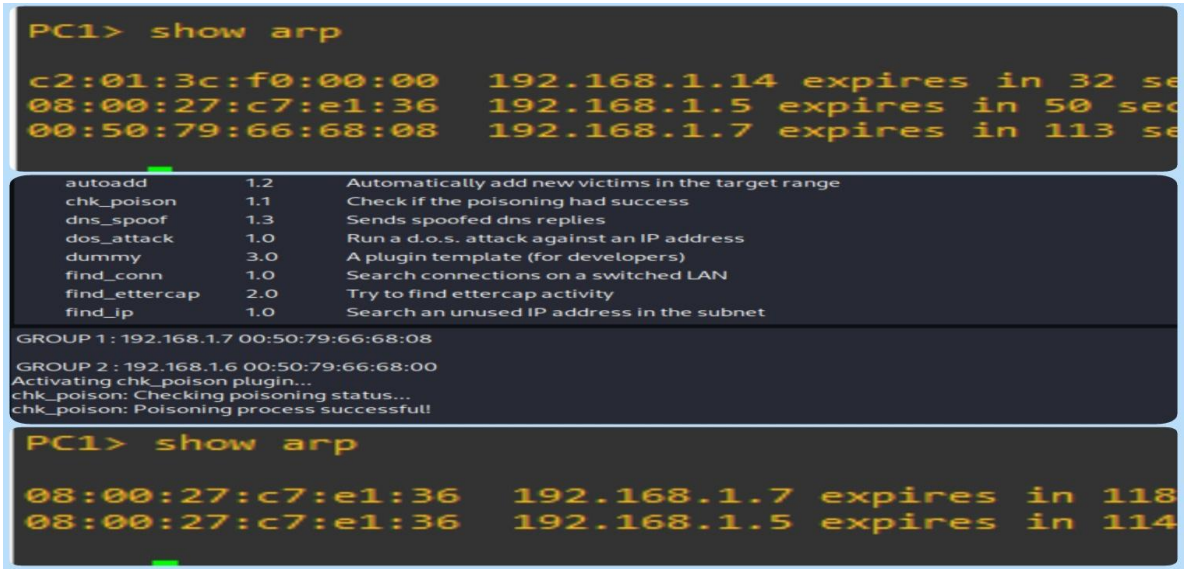

Figure 3-65 : Simulation de l'attaque ARP spoofing dans le VLAN de l'attaquant.

- **La figure 3-66 présente la simulation dans un autre VLAN :**

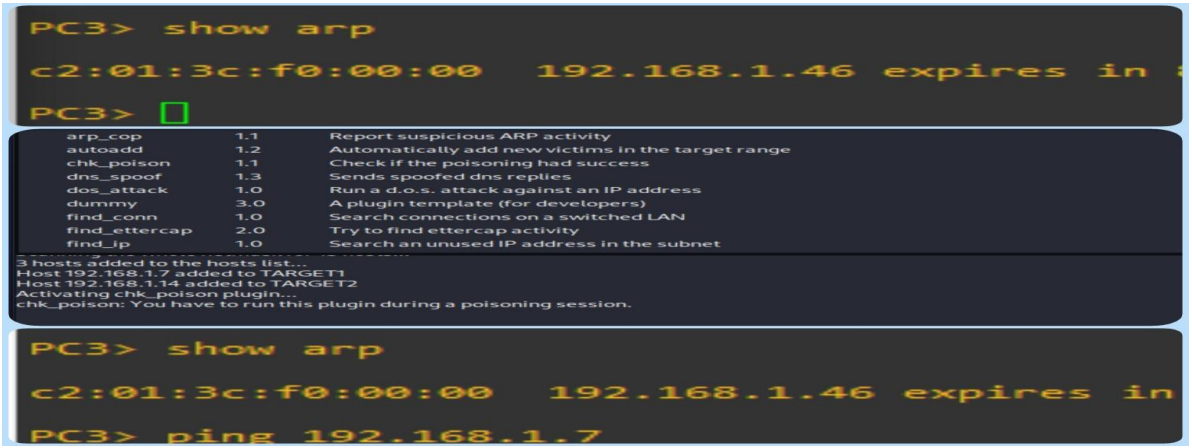

Figure 3-66 : Simulation de l'attaque ARP spoofing dans un autre VLAN.

On constate que cette attaque ne fonctionnera que dans le VLAN où elle a été lancée. Cela est dû au fait que les VLANs sont des réseaux logiques distincts, ce qui signifie que les paquets ARP ne seront transmis que dans le VLAN d'origine.

On peut conclure que l'utilisation de VLANs pour séparer le trafic peut rendre plus difficile pour un attaquant de mener une attaque ARP spoofing ciblant l'ensemble du réseau. Cela permet de limiter les dommages causés par une telle attaque et de rendre plus compliquée la tâche des attaquants qui cherchent à compromettre l'ensemble du réseau.

5.2.4 Simulation de l'attaque MAC flooding

La figure 3-67 montre la simulation de l'attaque mac flooding en utilisant l'outil macof **:**

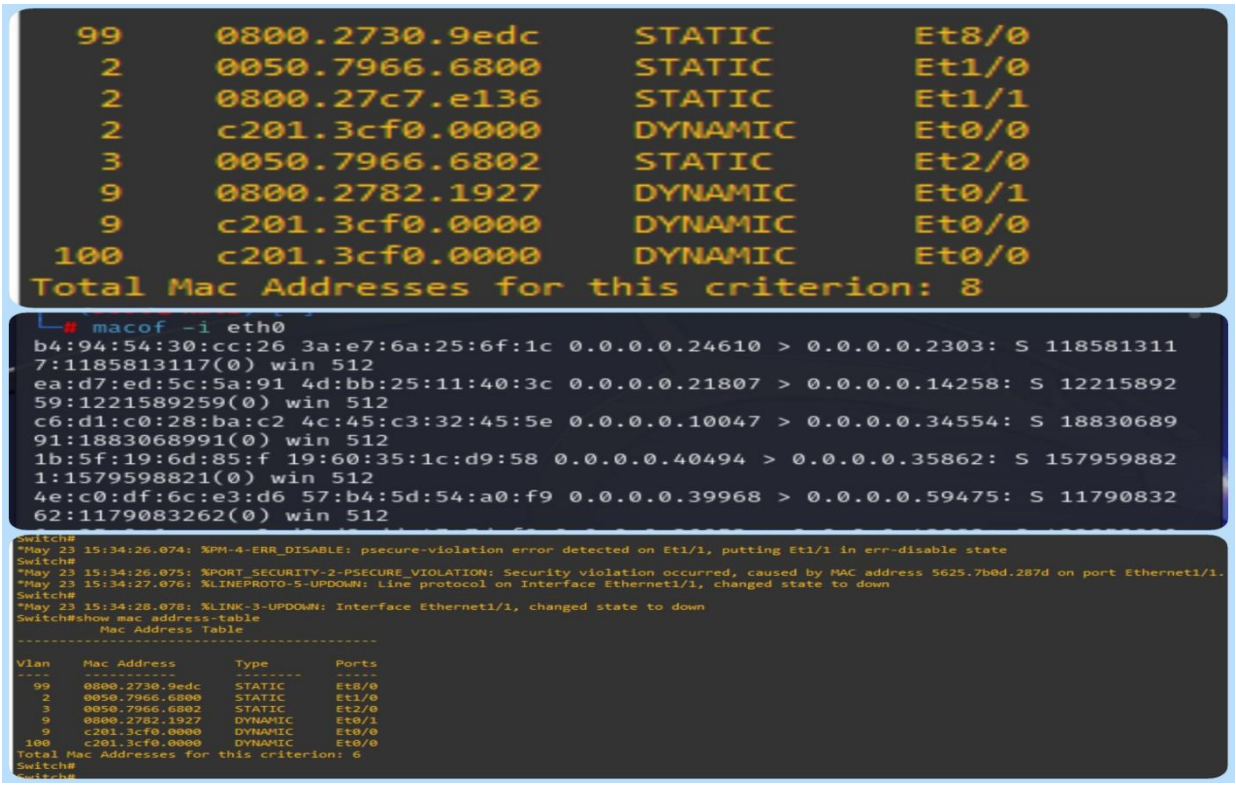

Figure 3-67 : Simulation de l'attaque MAC flooding.

On constate que le commutateur a détecté une erreur sur le port Ethernet1/1 et il a bloqué les adresses MAC illégitimes qui tentent de se connecter au commutateur ce qui conduire des problèmes de connectivité pour les utilisateurs connectés à ce port.

On conclure que la limitation du nombre d'adresses MAC pouvant être connectées à un port de commutateur est une mesure de sécurité qui peut aider à prévenir les attaques MAC flooding. Cette limitation permet de limiter le nombre d'adresses MAC pouvant être connectées à un port et donc réduire la quantité de trafic de broadcast sur le réseau. En cas

d'attaque MAC flooding, la table d'adresses MAC du commutateur arrivera plus rapidement à saturation, limitant ainsi l'impact de l'attaque sur le réseau.

5.2.5 Simulation de l'attaque DHCP Starvation

La figure 3-68 montre la simulation de l'attaque DHCP starvation :

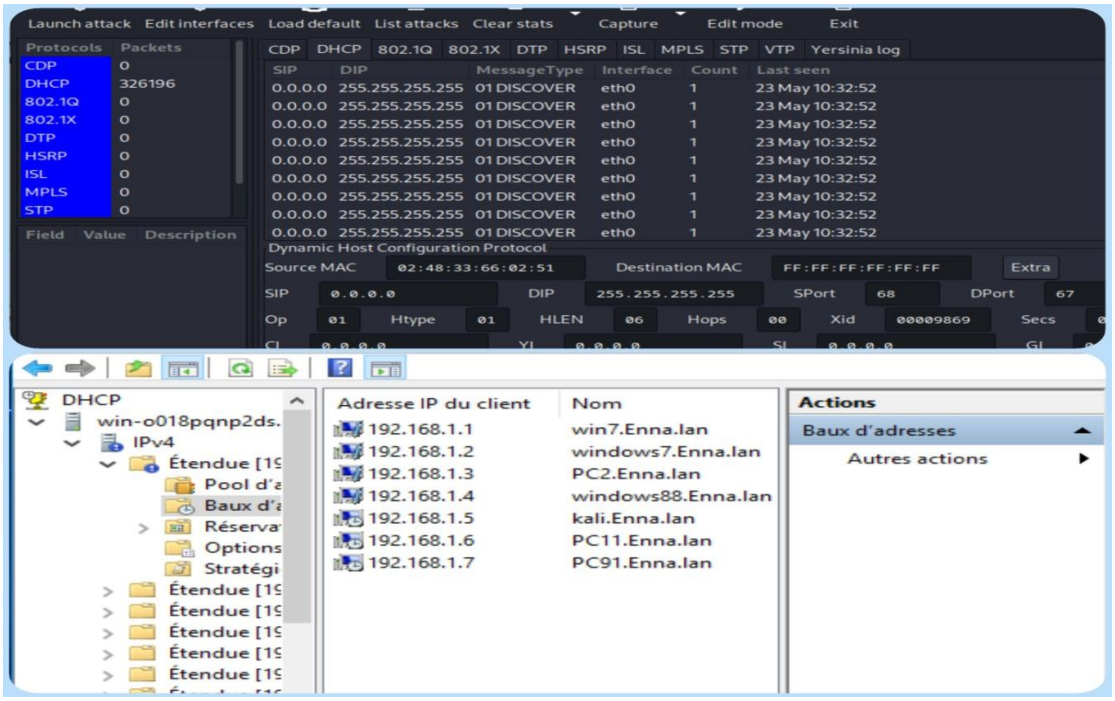

Figure 3-68 : Simulation de l'attaque DHCP Starvation.

On constate que le serveur DHCP ne répondra pas à l'attaque DHCP starvation et que le commutateur a détecté cela et a bloqué les ports sur lequel les demandeurs DHCP illégitimes sont connectés.

On conclure que la configuration de DHCP Snooping est une mesure de sécurité efficace pour empêcher les attaques comme DHCP Starvation sur un réseau et elle permet de bloquer les paquets DHCP provenant de port non autorisés. Ainsi, elle permet de limiter les attaques DHCP starvation en empêchant les clients malveillants d'envoyer des messages DHCP pour obtenir des adresses IP.

Pour l'attaque DHCP Spoofing qui consiste à usurper l'identité du serveur DHCP pour distribuer de fausses adresses IP et ainsi détourner le trafic réseau, elle ne peut pas se lancer si l'attaque DHCP Starvation n'est réussie car les deux attaques sont étroitement liées et souvent utilisées ensemble pour des objectifs malveillants, comme figure 3-69 le montre :

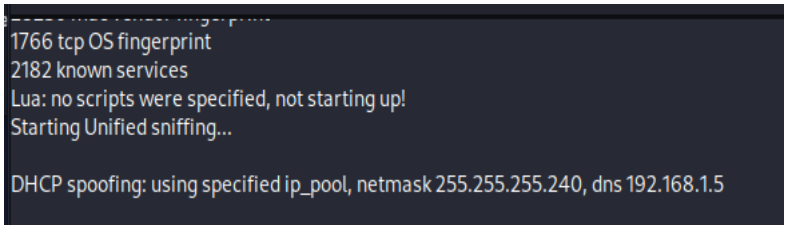

Figure 3-69 : Simulation de l'attaque DHCP Spoofing.

5.2.6 Simulation de l'attaque Switch Spoofing

La simulation de l'attaque Switch Spoofing est présentée dans la figure 3-70 :

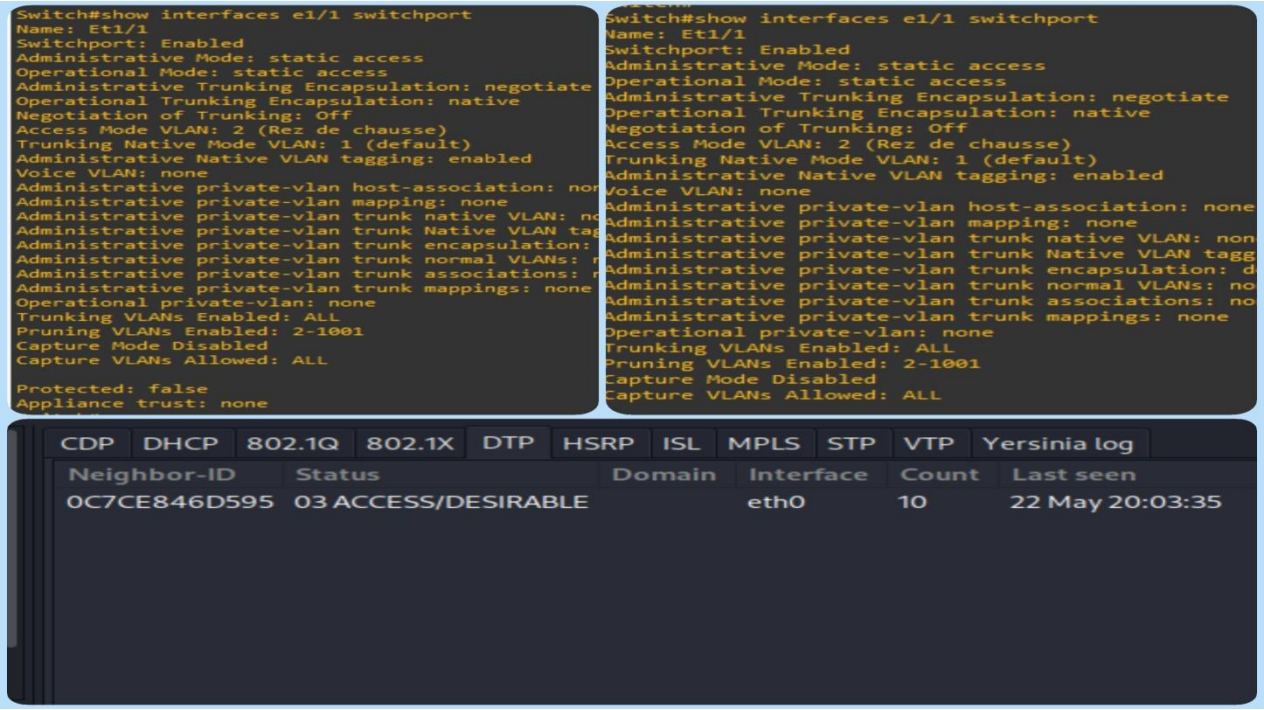

Figure 3-70 : Simulation de l'attaque Switch Spoofing.

En observant le port Ethernet 1/1, on peut constater qu'il était en mode access avant et après l'attaque. Cela permet de conclure que l'attaque de falsification de switch n'a pas réussi à tromper le commutateur auquel il était connecté. Par conséquent, l'attaquant n'a pas pu accéder illégalement au réseau.

5.2.7 Simulation de l'attaque Double tagging

La simulation de l'attaque double tagging est illustrée dans la figure 3-71 :

Figure 3-71 : Simulation de l'attaque Double tagging.

Il a été observé que la table mac du "**pc3**", qui se situe dans le vlan 3, ne contenait aucune information, ce qui indique que ce pc n'a reçu aucune communication provenant du vlan 2 où l'attaquant se trouve. Nous pouvons en déduire que l'attaque double tagging a échoué à transmettre le paquet et par conséquent, n'a pas réussi à induire en erreur le commutateur en lui faisant croire que la trame appartient à un vlan différent de celui auquel elle appartient réellement.

6 Conclusion

En conclusion, ce chapitre est crucial pour la mise en place réussie de notre application sur le réseau informatique de l'ENNA. Il détaille les étapes clés nécessaires à la configuration des différents services et logiciels nécessaires au bon fonctionnement de l'application. Les résultats des tests de vérification exposés à la fin de ce chapitre confirment le bon fonctionnement de l'ensemble du système déployé. Cette étape est donc essentielle pour la réussite de notre projet et son utilisation future. Nous sommes confiants dans le fait que ce chapitre servira de base solide pour le déploiement de notre application et nous permettra de répondre aux besoins de l'ENNA de manière efficace.

Conclusion générale

Il est indéniable que la sécurité informatique totale est difficile à atteindre, car il existe une variété de menaces qui peuvent compromettre la fonctionnalité d'un réseau informatique dans une organisation. C'est pourquoi il est crucial de formuler une politique de sécurité adaptée aux risques réels auxquels un réseau informatique est confronté. Il est également essentiel d'établir des mécanismes appropriés de prévention, de maintenance et de correction, pour garantir une sécurité optimale du réseau informatique de l'entreprise.

Au cours de notre stage au sein de l'entreprise ENNA, nous avons réalisé une analyse approfondie du réseau informatique et identifié diverses lacunes en termes de sécurité. Nous avons ensuite proposé différentes solutions adaptées pour remédier à ces anomalies et renforcer la sécurité du réseau. Nous avons pris en compte les besoins actuels de l'entreprise et veillé à assurer un bon fonctionnement de son réseau informatique. Notre objectif était d'améliorer la sécurité de manière appropriée et efficace, afin de protéger les actifs de l'entreprise et assurer la confidentialité des données sensibles.

Dans la nouvelle infrastructure, nous avons segmenté le réseau en plusieurs VLAN pour améliorer la sécurité et l'efficacité de notre système. Nous avons ajouté avec succès un serveur Windows 2016 basé sur Active Directory pour centraliser la gestion des utilisateurs, des ordinateurs et des groupes, et nous avons mis en place un contrôleur de domaine pour garantir une authentification sécurisée des utilisateurs. De plus, nous avons installé un serveur DNS pour faciliter la résolution de noms et assurer un accès rapide à toutes les ressources du réseau et un serveur DHCP pour faciliter l'attribution d'adresses IP et améliorer la gestion des adresses. Pour le partage de fichiers et le stockage de données, nous avons ajouté un serveur de fichiers et de stockage à notre infrastructure. Nous avons également configuré un serveur d'impression pour permettre l'impression de documents à partir de n'importe quel ordinateur du réseau. Enfin, nous avons implémenté une plateforme de messagerie Exchange 2016 pour faciliter la communication interne et externe de manière confidentielle et sécurisée en utilisant des adresses électroniques institutionnelles.

La réalisation de ce projet a été bénéfique pour nous, car cela nous a permis de contribuer à l'avancement de l'entreprise ENNA, tout en acquérant de nouvelles connaissances et compétences qui seront utiles pour notre avenir professionnel.

Il y a de nombreuses idées qu'on aurait pu intégrer dans ce projet, car il reste encore de travail à accomplir pour le concrétiser dans son ensemble. En prespective nous pouvons envisager quelques améliorations pour rendre ce projet plus performant Parmi ces prespectives, nous citons en particulier :

- L'implémentation d'un serveur NAS qui offre une solution de stockage fiable, rapide à un coût réduit.
- La mise en place d'un firewall qui permet de protéger un réseau contre les intrusions provenant d'un réseau tiers ou externe (internet).

Bibliographie

[2] P.Guy. Initiation-aux-réseaux, Eyrolles 7éme édition, 2011.

[3] A.Born, services et réseaux, Juillet 2016.

[4] A.Pérez , Architecture des réseaux, La Voisier, 2011.

[5] J.Francois, informatique commerciale, Bréal, Rosny-sous-Bois, 2004.

[6] IEEE 802.3 Ethernet Working Group, "IEEE Standard for Ethernet," 2018.

[8] P.Antouly, Installer un réseau chez soi, 2006.

[9] L.Soyer, Mise en place du Wi-Fi : 6 solutions entreprises par la pratique, Avril 2005.

[11] J.Green, Je me perfectionne avec les réseaux : types, normes, technologies, matériels, 2014.

[13] J.Green, je me perfectionne avec les réseaux, 2022.

[14] A.Ould Bamba Med, Développement d'un Outil de planification et Dimensionnement de réseau WiMAX, 2006.

[15] A.Benhamza, Projet de Fin d'Etude pour l'obtention du Diplôme d'ingénieur d'état, Planification d'un réseau WIMAX mobile, Institut National des Télécommunication set des Technologies de l'Information et de la Communication, 2009.

[17] A.Naikwade, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 7, July 2017.

[18] W.Stallings, Réseaux d'entreprise : Théorie et pratique publié par Pearson Education, livre.

[19] J.Berman et A.Wilson, DSL Technologies: Fiber to the x, Digital Subscriber Line, ADSL, VDSL and G.fast, publié par Springer, 2017 .

[21] M.Cohen, Data communications: A beginner's guide to concepts and technology. New York: McGraw-Hill, 2012.

[22] P.Golden, Digital Subscriber Line (DSL) Technologies.

[23] P. Golden, H.Dedieu et S. Jacobsen, Digital Subscriber Line Technology: Fundamentals of xDSL Technology.

[26] DSL (Digital Subscriber Line) Technology, publié par l'International Journal of Advanced Research dans Computer Engineering & Technology (IJARCET).

[27] A. Bouguettaya, Web Services. Springer Science Business Media, 2006.

[28] Municipal Broadband: An Introduction to Passive Optical Networks (PON), Fiber-to-the-Home Council, 2016.

[29] L.Gille, Les dilemmes de l'économie numérique, fyp éditions.

[30] F. Lam, K.Vincent et N. Lau, Passive Optical Networks: Principles and Practice de Cedric.

[31] F. Lam, Passive Optical Networks: Flattening the Last Mile Access de Cedric.

[32] P.Lecoy, Communications sur fibres optiques 4 éditions, Lavoisier, Paris, 2015

[33] G.Kramer, Emerging technologies for broadband access networks, IEEE Communications Magazine, vol. 40, Jan. 2002.

[34] C.Beard, W.Stallings, Wireless Communication Networks and Systems, Pearson Education.

[35] B.Das and S.Roy, 5G for Future Wireless Networks, 2019.

[36] S.Sharma, Advantages and Disadvantages of Cellular Phones, International Journal of Advanced Research in Computer and Communication Engineering,2016.

[38] Y.Diogenes and W.Thomas, Shinder Cybersecurity: Attack and Defense Strategies, Syngress, 2019.

[40] CVSS: Common Vulnerability Scoring System, Metrics, User's Guide, publié par le Forum National de Cybersécurité des Etats-Unis.

[41] F.Golshani et A. Vladimirov, The Standard for Vulnerability Assessment and Ratings.

[42] P .Mell et S.Christey, CVSS: Assessing Vulnerability Severity in Software Systems.

Webographie

[1] https://fr.theastrologypage.com/enterprise-network , consulté le 24/04/2023.

[7] https://www.geeksforgeeks.org/advantages-and-disadvantages-of-ethernet/ , consulté le 26/04/2023.

[10] https://reseau-informatique.prestataires.com/reseau-wifi-avantages-et-inconvenients, consulté le 26/04/2023.

[12]https://ufrsciencestech.ubourgogne.fr/licence3/SystemesEtReseaux2/SupportsCours/ch10.pdf, consulté le 29/04/2023.

[16] http://dictionnaire.sensagent.leparisien.fr/WiMAX/fr-fr/, consulté le 28/04/2023.

[20] Les technologies XDSL (samomoi.com) , consulté le 30/04/2023.

[24] https://www.versatek.com/www.GNS3.COM/what-is-dslam, consulté le 30/04/2023.

[25] https://www.ariase.com/fr/guides/filtre-adsl-xdsl, consulté le 30/04/2023.

[37] https://www.enna.dz/organisation.htm, consulté le 10/03/2023.

[39] https://nvd.nist.gov/vuln-metrics/cvss, consulté le 28/05/2023.

[43] https://www.first.org/cvss/specification-document, consulté le 28/05/2023.

Résumé

Aujourd'hui, la mise en place de réseaux informatiques de qualité est devenue essentielle pour assurer le fonctionnement optimal d'une entreprise. Pour garantir une qualité de service maximale, des administrateurs de réseau compétents doivent veiller à gérer les droits d'accès et les comptes utilisateurs de manière rigoureuse. En outre, la sécurité des données doit être une priorité absolue. Notre projet consiste à améliorer le réseau de l'ENNA en intégrant une solution de contrôle d'accès pour les utilisateurs ainsi qu'une adaptation efficace du partage de ressources. Nous avons donc segmenté le réseau en plusieurs VLAN et centralisé les équipements et les ressources utilisés par les utilisateurs grâce à un annuaire Active Directory. Dans le cadre de cette mise en place, nous avons installé un serveur DNS et un serveur DHCP, ainsi nous avons configuré un serveur de fichiers et de stockage, un serveur d'impression et avons également mis en place une plateforme de messagerie Exchange 2016**.** Nous avons utilisé des technologies avancées telles que GNS3, VirtualBox, VMware et Windows Server 2016 pour mettre en place cette solution de manière efficace.

Mots clés: VLANs, DNS, DHCP, GNS3, VirtualBox, Windows Server 2016.

Abstract

Today, high-quality IT network are essential to the smooth running of a company. To guarantee the highest possible quality of service, comptent network administrators must ensure that access rughts and user accounts are rigotouslymanaged. Data security must also be a top priority. Our project involved improving ENNA’s network by integrating an access control solution for users, as well as efficient adaptation of resource of sharing. We therefore segmented the network into several VLAN’s, and centralized the equipment and resources used by users via an Active Directory. As part of this set-up, we installed a DNS server and a DHCP server, configured a file and storage server, a print server and also set up an Exchange 2016 messaging platform. We used advanced technologies such as GNS3, VirtualBox, VMware and Windows Server 2016 to implement this solution efficiently.

Keywords: VLANs, DNS, DHCP, GNS3, VirtualBox,Windows Server 2016.

ملخص

اليوم، أصبح إنشاء شبكات حاسوبية عالية الجودة أمرًا ضروريًا لضمان عمل مثالي للشركات. لضمان أقصى جودة للخدمة، يجب على مسؤولي الشبكات المؤهلين الاهتمام بإدارة حقوق الوصول وحسابات المستخدمين بشكل صارم. بالإضافة إلى ذلك، يجب أن تكون أمان البيانات أولوية قصوى. يتمثل مشروعنا في تحسين شبكة ENNA من خلال دمج حل لمراقبة الوصول للمستخدمين وتكييف فعال لمشاركة الموارد. لقد قسمنا الشبكة إلى عدة شبكات محلية افتراضية (VNAL) وجمعنا المعدات والموارد التي يستخدمها المستخدمون من خلال الدليل النشط (Directory Active) ضمن إطار هذا النهج، قمنا بتثبيت خادم DSN وخادم DHCP ، وقمنا بتكوين خادم ملفات وتخزين، طباعة، وأنشأنا أيضًا منصة بريد إلكتروني Exchange 2016 لقد استخدمنا تقنيات متقدمة مثل GNS3 و VirtualBox و VMware و Server 2016Windows لتنفيذ هذا الحل بكفاءة.

الكلمات الرئيسية : VLANs، DNS، DHCP، GNS3، VirtualBox، Windows Server2016.