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

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Master professionnel

En

Informatique

Option

Administration et Sécurité des Réseaux

Thème

Etude et amélioration de l'administration réseau et sécurité. Cas d'étude : Université de Béjaia

---

Présenté par : M^{lle} ALLOUACHE Fairouz

Soutenu le 06 Juillet 2023 devant le jury composé de :

Président	**Dr F. BOUCHEBBAH**	**U. A/Mira Béjaia.**
Examinateur	**M. R. OUZEGGANE**	**U. A/Mira Béjaia.**
Rapporteur	**Dr F. CHERIFI**	**U. A/Mira Béjaia.**

Béjaia, Juillet 2023.

Remerciements

Pour commencer, je remercie avant toute chose dieu le tout puissant de nous donner la force, le courage et la patience pour réaliser ce modeste travail.

Un grand merci à mon encadrante académique Dr F. CHERIFI, dont les conseils éclairés, les suggestions précieuses et l'expertise ont grandement contribué à l'amélioration de mon mémoire. Ses orientations ont été d'une grande valeur pour moi et m'ont permis de développer mes compétences et mes connaissances dans le domaine de la recherche.

Je souhaite également exprimer ma reconnaissance envers mon encadrant de stage l'administrateur système et réseau Mr MADAOUI Madjid, qui a généreusement consacré de son temps et de son expertise pour m'accompagner et me guider pendant mon stage. Sa disponibilité et ses conseils précieux ont été d'une aide précieuse pour moi, et j'apprécie sincèrement son soutien tout au long de cette expérience professionnelle.

Je remercie chacun des membres du jury pour l'intérêt porté à ce travail en acceptant de l'examiner et de l'enrichir de leurs propositions.

Enfin, je tiens à remercier toutes les personnes qui m'ont soutenu moralement et pratiquement tout au long de ce parcours. Vos encouragements, vos conseils et votre soutien ont été d'une importance capitale pour moi, et je suis profondément reconnaissante de pouvoir compter sur votre appui.

Dédicace

Je dédie humblement ce travail, symbole de ma détermination et de mon engagement, à la fois à moi-même et à vous, mes parents. Votre amour inconditionnel, vos encouragements constants et votre confiance en moi ont été les piliers de ma réussite.

À moi-même, je rends hommage à ma persévérance, à ma ténacité et à ma capacité à surmonter les obstacles. Que cette dédicace rappelle ma force intérieure et ma capacité à réaliser de grandes choses.

À mes parents, je vous remercie pour vos sacrifices, votre soutien indéfectible et votre amour. Vous avez façonné la personne que je suis aujourd'hui, et je ne saurais jamais assez vous remercier.

Que cette dédicace symbolise notre lien indéfectible, notre complicité et notre fierté mutuelle. Ensemble, nous avons construit un avenir prometteur, et nos réalisations futures refléteront notre amour et notre dévouement.

Avec amour et gratitude,

Fairouz

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AD	Active directory
CAN	Campus Area Network
CSRICTED	Centre des Systèmes et Réseaux d'Information, de Communication de Télé-enseignement et de l'Enseignement à Distance
DMZ	Demilitarized Zone
DoS	Denial of Service
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
FSE	Faculté des Sciences Exactes
FSNV	Faculté des Sciences de la Nature et de la Vie
FT	Faculté de Technologie
FHRP	First Hop Redundancy Protocol
GLBP	Global System for Mobile Communication
GPMC	Group Policy Management Console
GPO	Group Policy object
HSRP	Hot Standby Router Protocol
HCI	Hyper-Converged Infrastructure
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LDAP	Internet Protocol Private Branch eXchange
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
NVRAM	Non-Volatile Random Access Memory
OSI	Open Systems Interconnection
PAgP	Port Aggregation Protocol
PVLAN	PrivateVirtual Local Area Network
SDN	Software-Defined Networking
UFC	Université de Formation Continu
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
VTP	VLAN Trunking Protocol
WAN	Wide Area Network

Introduction générale

Au sein de toute entreprise, la mise en place d'un réseau informatique est essentielle pour faciliter le partage des ressources et des données, ainsi que pour favoriser la collaboration entre les membres de l'organisation. La gestion, la sécurité et la continuité du réseau jouent un rôle crucial dans le développement de l'entreprise [**1**].

Les universités ne font pas exception à cette règle. Elles doivent également assurer la connectivité d'un grand nombre d'utilisateurs et gérer des stratégies de sécurité et d'accès aux ressources numériques, aux données de recherche, etc. L'université de Béjaia fait face à ces défis.

Pendant notre stage au centre des systèmes et réseaux sis au centre de calcul de l'université A. Mira de Bejaia, nous avons eu l'opportunité d'explorer le réseau de l'université et de comprendre son fonctionnement actuel. Dans le cadre de notre travail, notre objectif principal était d'améliorer l'administration et la sécurité de ce réseau afin d'optimiser son fonctionnement global.

Pour atteindre cet objectif, nous avons identifié plusieurs solutions et mesures que nous avons configurées et proposées dans ce mémoire. Tout d'abord, nous avons étudié les configurations des protocoles utilisés sur le réseau de l'université. En analysant attentivement ces configurations, nous avons identifié des opportunités d'optimisation et de renforcement de la sécurité. En mettant en place des paramètres de configuration appropriés, nous avons pu minimiser les risques potentiels liés à des vulnérabilités connues et améliorer la stabilité et la performance du réseau.
Ensuite, nous avons examiné l'utilisation de VLANs (Virtual Local Area Networks) et de private VLANs sur le réseau de l'université. Les VLANs permettent de segmenter le réseau en sous-réseaux logiques, ce qui facilite la gestion et l'administration du réseau. En utilisant les VLANs de manière stratégique, nous avons pu renforcer la sécurité en limitant la propagation des données sensibles et en contrôlant l'accès aux ressources réseau.
Une autre mesure importante que nous avons proposée est la centralisation de la gestion des utilisateurs. En regroupant les informations d'identification et les autorisations des utilisateurs dans un système centralisé, nous avons pu améliorer la sécurité en mettant en place des contrôles d'accès plus robustes et en simplifiant la gestion des comptes utilisateur.

L'implémentation de ces solutions, telles que les configurations des protocoles, l'utilisation de VLANs et de private VLANs, ainsi que la centralisation de la gestion des utilisateurs, a permis d'améliorer significativement la disponibilité, la sécurité et le contrôle du réseau de l'université A. Mira de Bejaia. Ces améliorations contribuent à optimiser l'efficacité des

opérations administratives et à assurer la protection des données et des ressources du réseau contre les menaces potentielles.

Le mémoire est structuré en trois chapitres. Le premier chapitre présente l'organisme d'accueil, le contexte général du projet et expose les critiques concernant le réseau LAN de l'université de Béjaia. La problématique de notre travail est également abordée, ainsi que quelques solutions potentielles.

Le deuxième chapitre se concentre sur la conception hiérarchique du réseau et présente quelques notions théoriques essentielles pour la résolution de notre problématique, telles que HSRP, PVLAN, VTP et Etherchannel.

Le dernier chapitre, intitulé "Configuration et Tests", présente l'environnement de travail, l'architecture proposée, les tableaux d'adressage, ainsi que des captures d'écran illustrant les différentes configurations et tests effectués pour vérifier si les objectifs ont été atteints.

En conclusion, ce mémoire étudie l'administration réseau et la sécurité à l'université A. Mira de Béjaia et présente des solutions visant à optimiser le réseau. Des perspectives d'amélioration sont également discutées.

Chapitre 1

Présentation de l'organisme d'accueil

1.1 Introduction

Afin d'améliorer nos connaissances dans le domaine des réseaux, il est indispensable de développer nos capacités professionnelles. Pour cela, nous avons suivi un stage pratique au centre des Systèmes et Réseaux d'Information, de Communication de Télé-enseignement et de l'Enseignement à Distance (CSRICTED) de l'université de Béjaia que nous allons présenter dans ce chapitre.

Ce chapitre est consacré pour la présentation de l'organisme d'accueil, cette présentation nous permettrons d'effectuer une analyse sur le réseau de l'université, d'étudier les problèmes. Afin de mettre en œuvre une solution, l'étude d'existant sert à connaitre l'état actuel et de porter une connaissance sur ses besoins recommandés.

1.2 Présentation de l'université A. Mira de Béjaia

L'université de Béjaïa, crée en octobre 1983, est un établissement public pluridisciplinaire. Elle compte aujourd'hui plus de 45 700 étudiants,1714 enseignants et 1227 personnels techniques et administratifs, répartis sur huit facultés. L'université de Béjaïa dispose actuellement une trentaine de laboratoires de Recherche, agréés par le Ministère de l'Enseignement

Supérieur et de la Recherche Scientifique portant sur plusieurs domaines : modélisation et Optimisation des systèmes, technologie des matériaux et du génie des procédés, matériaux organiques, ect [**2**].

L'université de Bejaia dispose de troix campus :

1. **Campus Targa Ouzemmour :** le campus de Targa Ouzemmour propose des formations diplômantes d'ingéniorat, et licences LMD assurées par trois facultés :
   • Faculté de technologie.
   • Faculté des sciences exactes.
   • Faculté de la nature et de la vie.
2. **Campus Aboudaou :** Ouvert en 2003, le campus d'Aboudaou situé sur la route de Tichy Béjaia regroupe quatre facultés :
   • Faculté de droit.
   • Faculté des sciences économiques, des sciences de gestion et des sciences commerciales.
   • Faculté des Lettres et des Langues.
   • Faculté des Sciences Humaines et Sociales.
   • Faculté de médecine.
3. **Compus el-kseur :** le campus d'elkseur regroupe les premières années des facultés de Targa Ouzemour.

Les structures de l'université A.Mira de Bejaïa sont illustrées dans Figure 1.1.

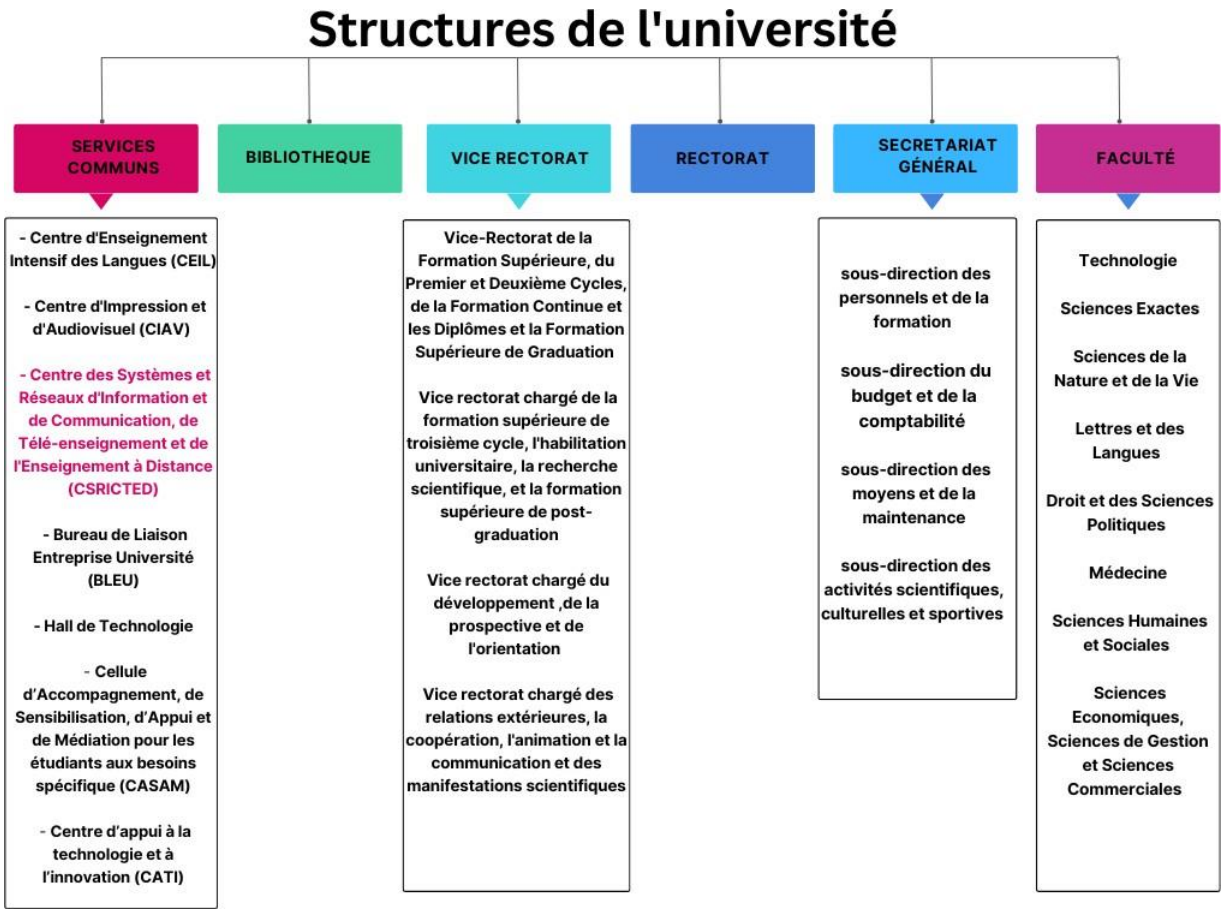

FIGURE 1.1 – Structures de l'université de Béjaia [**2**].

1.3 Présentation du service d'accueil

Le centre des Systèmes et Réseaux d'Information, de Communication de Télé-enseignement et de l'Enseignement à Distance (**CSRICTED**) est l'un des services communs de l'université de Bejaïa, il se charge de la gestion de toutes les ressources informatiques de l'université ainsi que de l'assurance de la continuité des services informatiques et de leurs maintenances, tels que le service pédagogique, la disponibilité de la connexion aux réseaux intranet et internet et l'exploitation des différents services offerts, et enfin la maintenance du parc informatique de l'université [**2**].

1.3.1 Organisation

Le CSRICTED se constitue de quatre sections : la section système d'information, la section réseau, la section e-learning et la section maintenance comme c'est montré dans la Figure 1.2 .

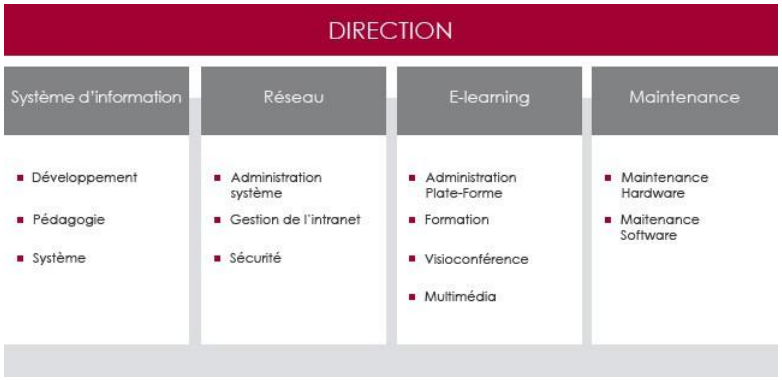

FIGURE 1.2 – Organigramme du CSRICTED [**2**].

1.3.2 Description et rôles de chaque section

1. **Section Système d'Information**

   La Section Système d'Information (S.I), a pour mission de mettre en œuvre la politique des systèmes d'information et des technologies de l'information et de la communication , la gestion d'une manière plus générale à tout ce qui touche au traitement automatique de l'information. La section se compose de trois cellules qui sont : cellule de développement, cellule pédagogique et cellule systéme [**2**].

2. **Section Réseau**

   La section réseau a pour missions de maintenir le fonctionnement normal du réseau intranet de l'université, d'assurer la sécurité des équipements réseaux et des services offerts par le réseau au système d'information et aux applications et enfin de fournir des services de connexion internet, de messagerie électronique, de support utilisateur,

d'étude et de suivi des projets réseau de l'université de Béjaia [**2**].

3. **Section chargée du Télé-enseignement (e-learning)**

   Cette sections a pour mission de prendre en charge toutes les opérations liées au e-learning à l'université de Bejaia. Son champ d'intervention concerne au moins deux domaines : le domaine pédagogique et le domaine technique.

   - Le domaine pédagogique englobe la formation des enseignants, des responsables et du personnel ATS de l'université sur l'usage des technologies de l'information et de la communication [**2**].

   - Le domaine technique englobe la mise en place d'une solution e-learning répondant à la fois aux besoins et aux ambitions de cette université. Il s'agit notamment de l'installation , de l'administration et de la maintenance des plates formes de e-learning. En plus de cela, cette cellule gère une salle de visioconférence [**2**].

4. **Section Maintenance**

   Comme son nom l'indique, cette section assure le maintient en bon état des équipements informatiques des différents services de l'université [**2**].

1.4 Étude de l'existant

Dans cette section nous incluons une analyse approfondie du réseau de l'université de Béjaia. Nous avons eu l'opportunité de réaliser un stage à l'université qui s'est déroulé sous la forme de visites au centre des système et réseau (CSRICTED) précisément dans la section réseau. Ces visites nous ont permis d'interagir avec des professionnels du secteur et de recueillir des informations précieuses pour notre projet.

1.4.1 Présentation du réseau de l'université de Béjaia

Le réseau informatique de l'université de Bejaia, comme l'indique la Figure 1.3, est constitué de quatre zones, sa topologie physique est en étoile étendue, chaque zone a l'architec-

ture d'un arbre, et est connectée au backbone (zone 1).

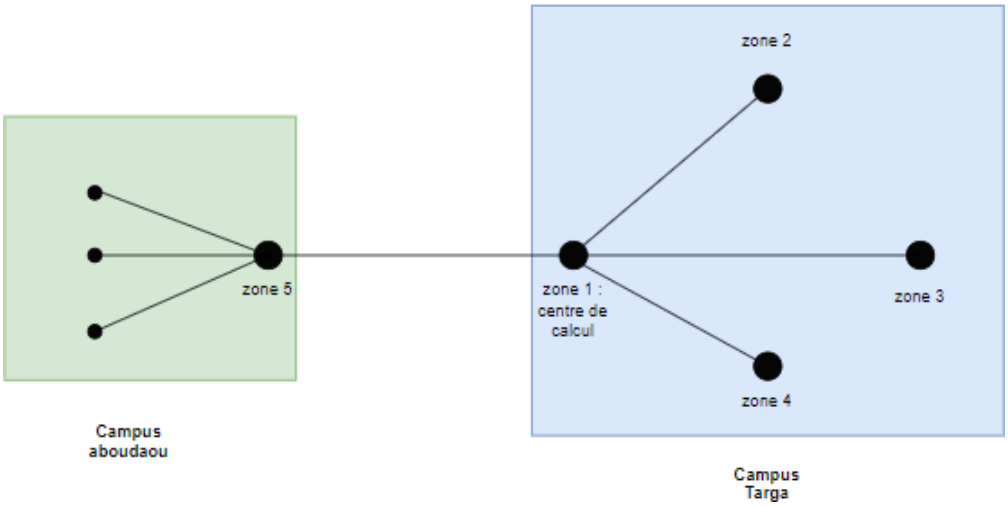

FIGURE 1.3 – Architecture physique du réseau intranet de l'université.

Le choix de la zone 1 comme étant l'épine dorsale (backbone en anglais) est justifié par le fait de la présence du centre de calcul qui héberge la salle des administrateurs (CSRICTED) ainsi que tous les serveurs du réseau local. Tandis que, le campus ABOUDAOU est connecté directement au backbone via une fibre optique.

D'autre part, comme le montre la Figure 1.4, qui représente l'architecture réseau détaillée réalisée d'après les informations obtenues du CSRICTED, le campus el-kseur est connecté au réseau intranet via une connexion VPN, l'université possède une zone démilitarisée (DMZ) qui est connectée au switch fédérateur de la zone 1 et qui héberge l'ensemble des serveurs, et d'un routeur qui connecte le réseau interne à l'internet.

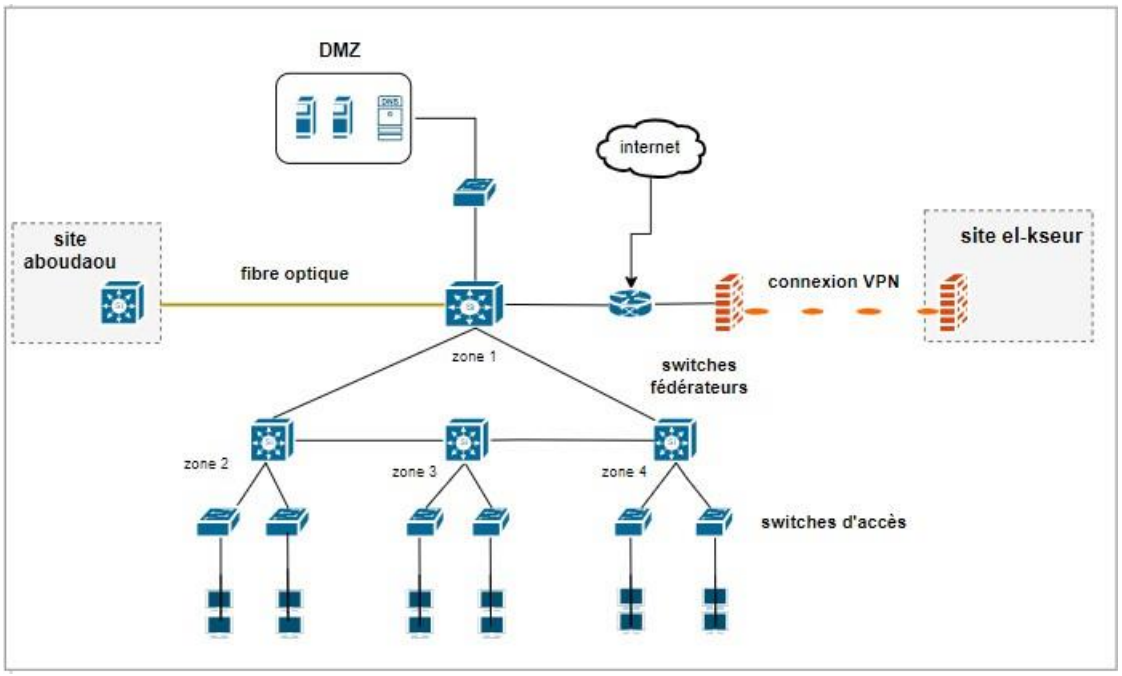

FIGURE 1.4 – Architecture en couches du réseau de l'université A.Mira.

1.4.2 Description d'une zone

Chaque zone du réseau intranet rassemble des blocs physiquement proches les uns des autres, c'est-à-dire composés de blocs contigus.

Chaque zone s'appuie sur un modèle en couches car ce dernier a beaucoup d'avantages tels que :

- La hiérarchisation : le rôle de chaque couche est précis et spécifique.
- L'évolution : les zones sont constituées de blocs, l'évolution est alors plus facile à planifier et à gérer.
- La gestion, car c'est facile de gérer une zone à cause de sa structure en couches.

L'architecture illustrée dans la Figure 1.4 décrit la structure en couches, on y distingue :

- Les Terminaux, qui sont des postes, des stations ou des imprimantes réseau par exemple.
- La couche d'accès, c'est le point d'entrée des postes clients ou des serveurs sur le réseau. C'est dans ce rang qui sont définit tous les services de niveau 2.

- La couche de distribution (Switches fédérateur), c'est à ce niveau que le routage et le filtrage sont accomplis.

1.4.3 Analyse du parc informatique

Dans le cadre de notre étude approfondie, nous entreprenons une analyse complète du parc informatique afin de mieux comprendre sa configuration, son efficacité et ses besoins.

a) **Caractéristiques des équipements de raccordement :** chaque zone du réseau inra-net est constitué de blocs avoisinants. Les tableaux suivants(Tables 1.1, 1.2, 1.3, 1.4) décrivent les switches distribués sur chaque bloc, tout en présentant également l'état actuel du matériel en utilisation ainsi que les recommandations émises par l'équipe chargée de l'évaluation.

	Etat actuel	Recommandations
Salle machines CSRICTED (data center)	3 switchs 2950 24 ports 3 switchs 2960 24ports	3 switchs 9200 48 ports
Salle 12 CSRICTED	4 switchs 2950 24ports 1 switchs 2960 24ports	2 switchs 9200 48ports
Bureau 2 CSRICTED	5 switchs 2950 24ports 1 switch 2960 24ports	3 switchs 9200 48ports
Bloc 1 département ST	1 switchs 9200 48ports 1 switchs 2960 24ports	RAS
Bureau comptable (centrale)	1 switches 2960X 48ports	Ras
Faculté Technologie	1 switches 2960X 48ports 1 switches 2950 24ports	1 switches 9200 24ports
Bloc 11	1 switch 2960S 48ports 1 switch 2950G 24ports	1 switches 9200 24ports
UFC	2 switches 2950 24ports	1 switch 9200 48ports

TABLE 1.1 – Dispositifs matériels (switches) dans la zone 1 : centre de Calcul

	Etat actuel	Recommandations
Génie des Procédés Labo 24	4 switchs 2950 24ports	2 switchs 9200 48ports
Nouvelle bibliotheque	2 switchs 2950 24ports	1 switchs 9200 48ports
Bloc 8	1 switch 2950 24ports	RAS
Moyens generaux	2 switch 2950 24ports	RAS
Bloc des enseignants	10 switch 2960s 48 ports| 1 switch 3560X 24 ports	RAS
Bibliothèque 250 places	1 switch 2960s 24 ports| 1 switch 3560X 24 ports	RAS
Auditorium	1 switch 2960s 24 ports	1 switch 9200 24ports

TABLE 1.2 – Dispositifs matériels dans la zone 2 : génie des procédés

	Etat actuel	Recommandations
Bloc 5 bureau 112	2 switchs 2950 24ports 1 switchs 2960G 24ports	1 switchs 9200 48ports 1 switch 9200 24 ports
Bureau 211	2 switchs 2950 48ports 1 switchs 2950G 24ports	1 switchs 9200 48ports 1 switch 9200 24ports
Centre culturel	1switch 2950G 24 ports	Ras/2960s
Bibliothèque centrale	1 switch 9200 48ports 1 switchs 2950 24ports	1 switch 9200 24ports
Département Architecture	1 switch 9200 24ports | 1 switchs 2950 24ports	1 switch 9200 48ports
Salle hydraulique	2 switch 2960g 24ports 1 switch2950g 24ports	1 switch 9200 48ports 1 switch 9200 24ports
Ex rectorat	1 switch 9200 48ports 1 switch 2960S 24ports	1 switch 9200 24ports
Hall technologie	1 switch 2950G 24ports 1 switch 2950 24ports	1 switch 9200 48port
Centre d'impression	1 switch 2950G 24ports	1 switch 9200 24ports
Traitement des eaux	1 switch 2950G 24ports 1 switch 2950 24ports	1 switch 9200 48port
hydraulique	1 switch 2950g 24ports Ras/2960s	
Parc Auto	1 switch 2950g 24ports	1 switch 9200 24ports
recherche	RAS	RAS
FSE	1 switch 9200 48port 1 switch 2960S 48ports 1 switch 2960S 24ports 2 switchs 2950 24ports	2 switch 9200 48port 1 switch 9200 24ports

TABLE 1.3 – Dispositifs matériels dans la zone 3 : bloc 5

	Etat actuel	Recommandations
Bloc10 salle 10	3 switchs 2950 24ports	1 switchs 9200 48ports 1 switch 9200 24ports
FSNV	2 switchs 2950 48ports	2 switchs 9200 48ports
Animalerie	1 switch 2950G 24 ports 1 switch 2950 12 ports 1 switch 9200 48ports	
Haute Tension	1 switch 2950G 24ports 1 switch 2950 24ports	1 switch 9200 48ports
Bloc 3	1 switch 2950G 24ports 1 switch 2950 24ports	1 switch 9200 48ports
Bloc 6	1 switch 2950G 24ports	Ras/2960s
Bloc 9	3 switch 2950G 24ports	1 switch 9200 48ports|1 switch 9200 24ports
Bloc 12 côté gauche	1switch 2950G 24ports 1 switch 2950 24ports	1 switch 9200 48ports
Bloc 12 coté droit	2 switch 2950G 24ports 1 switch 9200 48ports	

TABLE 1.4 – Dispositifs matériels dans la zone 4 : bloc 10

b) **Description des équipements materiel et logicel**

La table 1.5 décrit les serveurs dont l'université de Béjaia dispose.

Equipement	Nombre d'unité	Série et marque	Année de mise en place
serveur HP	1	HP Proliant DL580G5 -1 To	2010
serveur HP	1	HP Proliant DL580G5-2.5 To	2010
serveur HP	1	HP Proliant DL580G5 -3.5 To	2010
serveur HP	1	HP Proliant DL580G5 -1 To	2010
serveur HP	1	HP Proliant DL580G5 -1 To	2010
serveur HP	1	HP Proliant DL580G5 -1.5 To	2010
serveur IBM	1	HP Proliant DL580G5 -4 To	2010
serveur IBM	1	HP Proliant DL580G5 -4 To	2010
serveur IBM	1	HP Proliant DL580G5 -5 To	2010

TABLE 1.5 – Caractéristiques des serveurs.

1.5 Analyse du réseau de l'université A. Mira de Béjaia

Pendant nos visites au centre CSRICTED, nous avons eu des discussions approfondies avec les professionnels, au cours de l'entretien de suivi où nous avons abordé des points que nous avons soigneusement préparé (l'axe de discussion est inclus dans l'annexe). Cet entretien nous a aidé à structurer nos échanges et à obtenir des réponses pertinentes à nos questions. Les réponses obtenues ont été d'une grande importance pour comprendre l'état actuel du domaine d'étude.

Grâce aux réponses obtenues, nous avons pu examiner les pratiques mise en vigueur dans l'université et comprendre les défis auxquels les professionnels sont confrontés. Ces informations ont été d'une grande importance pour analyser et détecter les points forts et les points faibles du réseau de l'université.

1.5.1 Les points forts du réseau

Le réseau de l'université présente un ensemble de points forts qu'il faut préserver citons à titre d'exemple :

- Présence de pare-feux de nouvelle génération (de type FORTINET 301 E) qui protègent le réseau informatique interne , analysent le trafic et filtrent les données provenant de sources non sécurisées ou suspectes pour prévenir les attaques.
- Disposition de deux pare-feux (Fortigate) qui travaillent en paralléle (actif/ actif) au niveau du campus Targa.
- La mise en place d'une zone démilitarisée (DMZ) dans l'architecture réseau qui vise à renforcer la sécurité en créant une zone intermédiaire entre le réseau interne et le réseau externe.
- Existence d'un système de surveillance des équipements (NAGIOS).
- Solution de virtualisation en phase de déploiement : l'université de Béjaia a opté pour une approche plus souple et plus dynamique (EMC Vx Rail de Dell), l'infrastructure hyperconvergée (HCI ou Hyper-converged infrastructure en aglais) a pour ambition de simplifier l'informatique en combinant les ressources de calcul, de stockage et de virtualisation dans un système unique.

1.5.2 Les points faibles du réseau

Après avoir mis en avant les points forts de notre réseau universitaire, explorons maintenant objectivement les domaines qui demandent une attention particulière. Analysons quelques-uns des points faibles identifiés pour mieux comprendre les défis auxquels nous faisons face.

– Manque de configurations et de gestion sur les VLANs : un manque de gestion appropriée des VLAN peut entraîner une complexité croissante dans la gestion du réseau, tout en augmentant les risques de sécurité.

- Une défaillance d'un des Switch raccordé au Switch fédérateur couperait du réseau à tous les utilisateurs qui sont connectés.
- Saturation de la bande passante diminue fortement les puissances de réseau et de son bon fonctionnement.
- Absence de serveurs en redondance pour assurer la tolérance aux pannes (manque de la haute disponibilité).
- Manque de quelques paramétrages de sécurité ce qui peut entraîner des vulnérabilités dans le réseau, exposant ainsi le système à des risques potentiels..

1.5.3 Problématique

La gestion déficiente des VLANs peut entraîner une complexité croissante, des risques de sécurité accrus, des coupures de réseau en cas de défaillance, une utilisation inefficace de la bande passante et une absence de haute disponibilité. Il est essentiel d'accorder une attention particulière à la configuration, à la gestion et à la sécurisation adéquates des VLANs pour assurer un fonctionnement optimal du réseau.

Une administration et une sécurité adéquates des VLANs permettent d'améliorer la performance, la disponibilité et la sécurité du réseau. Cela peut être réalisé grâce à des pratiques de gestion optimisées, à l'introduction de mécanismes de redondance et de tolérance aux pannes, ainsi qu'à la mise en place de mesures de sécurité appropriées pour protéger les VLANs.

1.5.4 Solution proposée

Afin de résoudre les défis identifiés dans la problématique, nous avons développé un éventail de solutions, chacune d'entre elles étant spécifiquement orientée vers les aspects pertinents. Dans le chapitre 3, nous présenterons un schéma de mise en œuvre détaillé pour la concrétisation de ces solutions.

1. Pour les VLANs
   - Configurations du protocoles VTP : pour faciliter la gestion des VLANs.
   - NATIF VLAN : pour renforcer la sécurité de 802.1Q.
   - Rajouter des VLANs de gestion et de serveurs.
2. Agrégation des liens avec le protocole LACP : vise à augmenter la capacité de bande passante, à améliorer la fiabilité, à équilibrer la charge, à optimiser les performances et à simplifier la gestion du réseau .
3. Configuration de protocole HSRP : pour la redondance et assurer la haute disponibilté.
4. Améliorer la configuration de la DMZ avec les PVLANs.
5. Proposition de quelque rôles pour la centralisation :
   - Active Directory : pour la gestion des comptes et droits d'accés.
   - Centraliser le serveur DHCP.

1.6 Conclusion

Dans ce premier chapitre, consacré à la présentation du cadre du projet et l'organisme d'accueil où nous avons effectués notre stage, nous avons met en avant une analyse du réseau qui nous a permet d'identifier ses points faible ce qui nous a conduit à proposer un ensemble de solutions pour y faire face et améliorer le réseau de l'université de Béjaia.

Chapitre 2

Administration réseau et sécurité

2.1 Introduction

Une bonne conception de réseau, que ce soit un réseau de très grande taille ou de petite taille, ne se fait pas facilement. Il faut prendre en compte la disponibilité, l'extensibilité, la sécurité et la facilité de gestion du réseau. Afin d'assurer ces quatre objectifs d'une bonne conception, nous présentons dans ce chapitre les différents techniques à concevoir pour le bon fonctionnement d'un réseau.

2.2 Réseau de campus

Un réseau peut être classé selon son étendue, parmi ces classes nous pouvons citer : réseau local (LAN, Local Area Network), réseau métropolitain (MAN, Metropolitan Area Network), réseau étendu (WAN, Wide Area Network) et réseau de campus (CAN, Campus Area Network) [**3**].

Un réseau de campus est un réseau informatique qui s'étend sur une zone géographique limitée. C'est un ensemble de réseaux locaux interconnectés servant une entreprise, un organisme gouvernemental, une université ou une organisation similaire. Dans ce contexte, un campus englobe un ensemble de bâtiments à proximité. Les utilisateurs finaux dans un

réseau de campus peuvent être dispersés plus largement que dans un seul réseau local, mais ils ne sont en général pas aussi dispersés qu'ils le seraient dans un réseau étendu WAN [3].

Le réseau de campus évolue pour supporter les nouvelles applications métiers mais aussi les nouvelles applications multimédia et collaboratives nécessaires à l'entreprise. Toutes ces applications reposent sur des fondations bien définies [3].

2.3 Modèle de conception hiérarchique d'un CAN

Afin de mieux répondre aux besoins des entreprises, la conception d'un CAN doit s'effectuer suivant un modèle hiérarchique.

Le modèle de conception hiérarchique, également connu sous le nom de modèle Cisco hierarchial design model, est une approche utilisée pour concevoir et structurer les réseaux informatiques, en particulier les réseaux d'entreprise. Il divise le réseau en plusieurs couches fonctionnelles distinctes, chacune remplissant un rôle spécifique dans le fonctionnement global du réseau. On distingue deux modèles de conception hiérarchique : un modèle à trois couches et un modèle à deux couches[4].

1. **Modèle à trois couches**

   Cisco a développé un modèle à trois couches pour concevoir un réseau de campus. Ce modèle est généralement utilisé dans les réseaux de grandes entreprises, il divise le réseau en trois couches fonctionnelles distinctes qui sont :

   — **La couche d'accès (Access Layer)**

   Cette couche est la plus basse dans la hiérarchie et est responsable de la connectivité des utilisateurs et des périphériques finaux au réseau. Elle se concentre sur la fourniture de ports d'accès physiques, tels que des commutateurs d'accès LAN ou des points d'accès sans fil pour les utilisateurs [5] [6].

   — **La couche de distribution (Distribution Layer)**

   La couche de distribution fournit une connectivité entre les utilisateurs finaux de

la couche d'accès et les autres couches supérieures du réseau. Elle peut inclure des commutateurs de distribution qui agrègent le trafic provenant de plusieurs commutateurs d'accès et le transmettent vers la couche suivante [5] [6].

— **La couche cœur de réseau (Core Layer)**

La couche de cœur est responsable du transport du trafic entre les différentes zones du réseau. Elle est conçue pour offrir une connectivité haute performance et une bande passante élevée [5][6].

La figure 2.1 illustre les trois couches du modèle de conception du réseau de campus de Cisco.

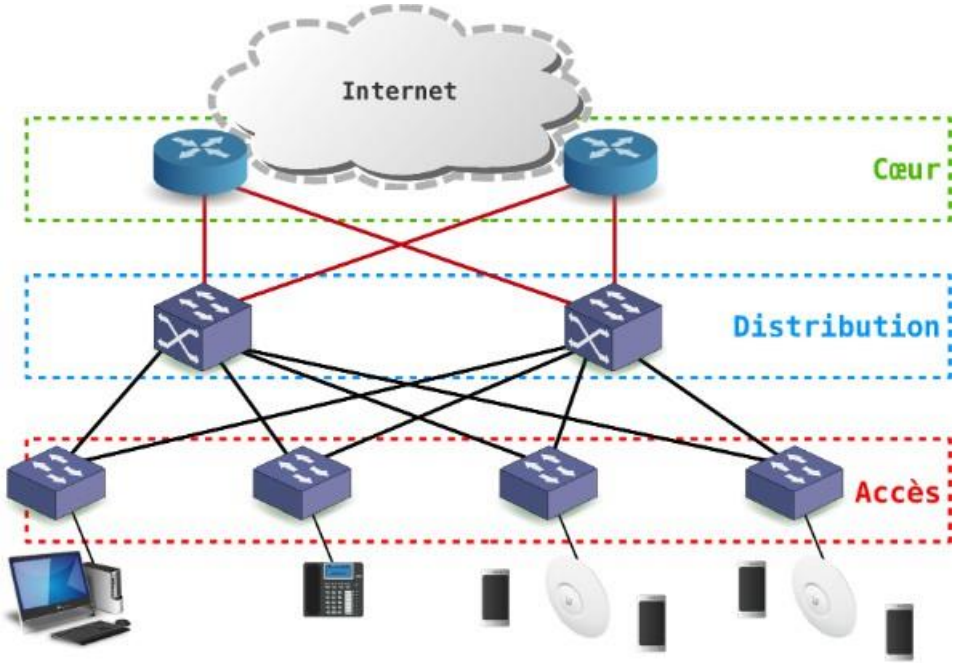

FIGURE 2.1 – Architecture type basée sur le modèle hiérarchique à trois couches[6].

2. **Modéle à deux couches**

Un réseau n'a pas complètement besoin de ces trois couches pour fonctionner. Un modèle à deux couches, n'ayant que les couches de distribution et d'accès, peut être utilisé dans le cas d'un réseau de petite à moyenne taille, idéalement pas plus de trois blocs d'interruption fonctionnelle à interconnecter, où les fonctions de base et de distribu-

tion peuvent être combinées en une seule couche [5].

2.3.1 Avantages d'un réseau hiérarchique

Les réseaux hiérarchiques offrent plusieurs avantages, notamment [4] :

- Evolutif : ces réseaux peuvent s'étendre plus facilement.
- Redondant : la redondance au niveau de la couche cœur de réseau et de la couche de distribution permet d'assurer une continuité de service pour la couche d'accès.
- Performant : la mise en place d'agrégat de liens entre les commutateurs de la couche de distribution et ceux de la couche cœur du réseau permet d'augmenter la vitesse.
- Sécurité : la sécurité du réseau peut être renforcée avec la mise en place de la sécurité des ports au niveau de la couche d'accès et la mise en place des stratégies de sécurité et/ou des listes de contrôle d'accès au niveau de la couche de distribution.
- Cout de gestion diminué : la cohérence de paramétrage entre les différents commutateurs de même couche permet une simplification de la gestion.
- Maintenance : la conception modulaire d'un réseau hiérarchique permet une mise à jour plus aisée.

2.3.2 Principes du modéle d'un réseau hiérarchique

Pour mettre en place correctement un réseau hiérarchique, il faut commencer par étudier la couche d'accès et définir les périphériques finaux. Pour les autres couches, il faut étudier ces éléments [5] :

Les liens agrégés : il faut identifier les ports permettant la liaison entre les commutateurs de chaque couche et surtout estimer les débits nécessaires et disponibles pour mettre en place les liens agrégés permettant d'augmenter la bande passante disponible.

Les liens redondants : en plus des liens agrégés, il faut prévoir des liens redondants permet- tant d'assurer la continuité de service sur la couche de distribution et la couche cœur de réseau en cas de défaillance d'un commutateur sur ces couches.

2.4 Administration réseaux et système

L'administration de réseaux informatique se définit comme étant l'ensemble des moyens mis en œuvre (connaissances, techniques, méthodes, outils, ...) pour superviser, exploiter des réseaux informatiques et planifier leur évolution en respectant les contraintes de coût, de qualité et de matériel. La gestion des réseaux informatiques constitue un problème dont l'enjeu est de garantir au meilleur coût, non seulement la qualité du service rendu aux utilisateurs mais aussi la réactivité dû aux changements et à l'évolution rapide du secteur informatique [7].

2.4.1 Modèle client/serveur

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes contactent un serveur, une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, etc. Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. On parle ainsi de client (client FTP, client de messagerie, etc.) lorsque l'on désigne un programme tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès d'un serveur (dans le cas du client FTP il s'agit de

fichiers, tandis que pour le client de messagerie il s'agit de courrier électronique) [8][9].
Le modèle client/ serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atout sont :

- **Une administration centrale :** Cette structure simplifie l'administration et la maintenance des ressources importantes et sensibles. La position centrale du serveur permet aussi d'effectuer facilement et sûrement les mises à jour avec peu de risques.
- **Les clients se partagent les ressources du serveur :** Le nombre de clients est extensible et plusieurs clients travaillent simultanément avec un serveur. Les clients se partagent les ressources du serveur
- **Contrôle global des droits d'accès :** La centralisation des ressources-clés permet aussi de gérer au plus près les droits d'accès pour une plus grande sécurité.
- **Un réseau évolutif :** grâce à cette architecture il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure [8] [9].

2.4.2 Active Directory (AD)

Active Directory (AD) est le service d'annuaire de la famille Windows Server 2012. C'est un service réseau qui identifie toutes les ressources d'un réseau et met ces informations à la disposition des utilisateurs ainsi que des applications. Les services d'annuaires sont importants, car ils fournissent un moyen cohérent de nommer, décrire, localiser, administrer et sécuriser les informations relatives à ces ressources et d'y accéder. Lorsqu'un utilisateur recherche un dossier partagé sur le réseau, le service d'annuaire identifie la ressource et fournit l'information à l'utilisateur [10].
La gestion d'un réseau Active Directory peut devenir un peu lourde lorsque le nombre de ressources dans le réseau augmente. Il existe une myriade de choses qui doivent être contrôlées, telles que les autorisations de sécurité, l'installation de logiciels, les

paramètres du bureau pour les utilisateurs et les ordinateurs, les privilèges de l'administrateur, et bien d'autres encore. C'est là que les stratégies de groupe et les objets de stratégie de groupe entrent en jeu [**10**].

2.4.2.1 Stratégie de groupe Active Directory

Les stratégies de groupe AD sont des instructions essentielles qu'un administrateur informatique peut configurer dans un environnement AD. Les stratégies de groupe AD déterminent le comportement et les privilèges des utilisateurs et des ordinateurs. Les stratégies de groupe sont avant tout une solution de sécurité pour le réseau AD. Les administrateurs peuvent configurer ces paramètres, puis mettre en œuvre des ensembles de paramètres sur des sites, des domaines contenant des utilisateurs et des ordinateurs [**10**].

2.4.2.2 Objet de stratégie de groupe

Plusieurs paramètres de stratégie de groupe sont regroupés dans un ensemble appelé objet de stratégie de groupe (GPO). Une fois que l'administrateur a configuré les stratégies de groupe dans l'objet de stratégie de groupe, il peut lier l'objet de stratégie de groupe aux objets des conteneurs. Les objets des conteneurs en question agiront alors dans les limites et les règles définies par les politiques du GPO qui leur a été attribué. Les GPO peuvent être créés et gérés à l'aide de la console de gestion des stratégies de groupe (GPMC) [**10**].

2.4.2.3 Protocole Lightweight Directory Access Protocol (LDAP)

Le Lightweight Directory Access Protocol (LDAP) est un protocole logiciel ouvert et multiplateforme utilisé pour l'authentification et la communication dans les services d'annuaire. LDAP fournit le langage que les applications utilisent pour communiquer entre elles dans les services d'annuaire, qui stockent les comptes d'ordinateur, les utilisateurs et les mots de passe et les partagent avec d'autres entités sur les réseaux. Cela permet aux applications et aux utilisateurs de trouver et de vérifier les informations dont ils ont besoin dans l'ensemble de leur organisation [**11**].

2.4.3 Système de nom de domaine (DNS)

DNS, acronyme de Domain Name System, désigne un système utilisé sur Internet pour traduire les noms de domaine en adresses IP. Les ordinateurs communiquent entre eux en utilisant des adresses IP, qui sont des séries de chiffres. Cependant, les êtres humains ont généralement du mal à se souvenir des adresses IP. C'est là qu'intervient le DNS [**12**].
le DNS est un système de dénomination hiérarchique connectés à l'internet ou à un réseau privé. Le DNS attribue des noms de domaine tels que www.canva.com à des adresses IP numériques (78.47.199.152) et vice versa. Le DNS est constitué de milliers de serveurs qui travaillent ensemble. Si un serveur ne parvient pas à résoudre un nom ou une adresse IP, il peut contacter un autre serveur qui peut alors interroger le suivant, et ainsi de suite [**12**].
En résumé, le DNS est un système crucial pour la navigation sur Internet. Il permet de traduire les noms de domaine en adresses IP, facilitant ainsi l'accès aux ressources en ligne .

2.4.4 Protocole de configuration dynamique des hôtes (DHCP)

Le protocole de configuration dynamique des hôtes (DHCP, Dynamic Host Configuration Protocol) attribue dynamiquement des adresses IP et d'autres options de configuration aux appareils d'un réseau. Ainsi, il est très facile d'ajouter de nouveaux ordinateurs, tablettes ou smartphones, les administrateurs ne doivent plus configurer chaque appareil manuellement, puisque le serveur DHCP s'en charge. C'est pourquoi le DHCP est idéal pour les grands réseaux dont les clients changent constamment, comme les universités, les entreprises, etc [**13**].

2.5 Agrégation des liens

L'agrégation de liens vous permet de combiner plusieurs liaisons Ethernet en une seule liaison logique entre deux périphériques en réseau. Il existe deux méthodes d'agrégation des liens : ETHERCHANNEL et IEEE 802.3ad.

1. **ETHERCHANNEL**

   La technologie EtherChannel a initialement été développée par Cisco comme une technique de réseau local entre deux commutateurs permettant d'assembler plusieurs liens physiques Ethernet identiques en un seul lien logique. Cette technologie a pour but d'augmenter la bande passante et d'améliorer la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs [**14**].

2. **IEEE 802.3ad**

   C'est une méthode standard d'agrégation de liens. Conceptuellement, il fonctionne de la même façon que EtherChannel en ce que plusieurs ports Ethernet sont agrégées en un seul adaptateur virtuel, offrant une plus grande bande passante et une protection contre les pannes. Les avantages de l'utilisation de IEEE 802.3ad Link Agrégation à la place d'EtherChannel sont que vous pouvez utiliser des commutateurs qui prennent en charge la norme IEEE 802.3ad mais qui ne prennent pas en charge EtherChannel et qui offrent une protection contre les défaillances de l'adaptateur [**14**] [**15**].

2.5.1 Protocoles d'agrégation

Il existe deux protocoles d'agrégation de lien suivant lesquels que l'on peut configurer un Etherchannel :

— Port Aggregation Protocol (PAgP) : c'est un protocole propriétaire de Cisco, il facilite la création automatique de liaison Etherchannel. Les modes PagP sont : PagP désirable et PagP auto [**14**].

— Link Aggregation Control Protocol (LACP) : il fait partie d'une spécification IEEE qui permet également de regrouper plusieurs ports physiques dans un seul canal logique. Les modes LacP sont : LacP active et LacP passive [**14**].

2.5.2 ETHERCHANNEL VS IEEE 802.3ad

Les protocoles EtherChannel et IEEE 802.3ad sont très semblables et accomplissent le même but. Il y a néanmoins quelques différences entre les deux :

• EtherChannel est un protocole propriétaire de Cisco, alors que 802.3ad est un standard ouvert.

• EtherChannel peut être configuré automatiquement à la fois par LACP et par PAgP, tandis que 802.3ad ne peut l'être que par LACP [**16**].

2.6 Protocoles de redondance à premier saut

Protocoles de redondance à premier saut (FHRP, First Hop Redundancy Protocols) est un acronyme Cisco pour désigner les solutions qui permettent de combler le point unique de rupture que constitue la passerelle par défaut dans les réseaux locaux. Les protocoles qui offrent ce service sont : HSRP, GLBP et VRRP [**17**].

1. **Hot Standby Routing Protocol (HSRP)**

   Le EHSRP est un protocole propriétaire Cisco de la haute disponibilité accrue de la passerelle d'un réseau, implémenté pour la gestion des liens de secours. Il peut être mis en place sur un routeur ou un switch de niveau 3 du modèle OSI. Le but est qu'une éventuelle panne du routeur ne perturbe pas le routage. Il se met en place par la mise en commun du fonctionnement de plusieurs routeurs physiques ou switches multicouche (au minimum 2) qui, de manière automatique assurons la relève entre eux, c'est-à-dire d'un routeur à un autre [**18**].

   Le protocole HSRP permettra aux routeurs situés dans un même groupe de former un

routeur virtuel qui sera l'unique passerelle des hôtes du réseau local, en se cachant derrière ce routeur virtuel aux yeux des hôtes. Les routeurs garantissent en fait qu'il y est toujours un routeur qui assure le travail de l'ensemble du groupe. Un routeur dans ce groupe est donc désigné comme actif et ce sera lui qui fera passer les requêtes d'un réseau à un autre. Pendant que le routeur actif travail, il envoie également des messages aux autres routeurs indiquant qu'il est toujours vivant et opérationnel. Si le routeur principal (élu actif) vient à tomber, Il sera automatiquement remplacé par un routeur qui était alors jusque-là passif et lui aussi membre du groupe HSRP [**19**].

Aux yeux des utilisateurs toutefois, cette réélection et ce changement de passerelle sera totalement invisible car ils auront toujours pour unique passerelle le routeur virtuel que forment les routeurs membres du groupe HSRP. Le routeur virtuel aura donc toujours la même IP et adresse MAC aux yeux des hôtes du réseau même si en réalité il y a un changement du chemin par lequel transitent les paquets [**19**].

2. **Gateway Load Balancing Protocol (GLBP)**

Le GLBP est un protocole propriétaire Cisco qui fournit une redondance ainsi que de la répartition de charge sur plusieurs routeurs utilisant une seule adresse IP virtuelle. Il protège les données de toutes failles d'un routeur ou d'un circuit, à peu près comme le fait le VRRP et le HSRP, tout en permettant le partage de charge de paquets entre plusieurs routeurs redondants. Le GLBP offre un service similaire mais plus que le HSRP et que le VRRP. Les deux derniers protocoles nommés permettent l'utilisation de plusieurs routeurs qui participent à faire un routeur virtuel configuré avec une adresse IP virtuelle. Le souci, quand on utilise HSRP ou VRRP, c'est qu'un seul des routeurs est sélectionné c'est lui qui gère tout le trafic, et les autres routeurs attendent, par conséquence les routeurs inactifs n'utilisent pas la bande passante qui leur est allouée. Tous les groupes de routeur servant à faire un routeur virtuel ne servent qu'à cela [**18**].

Le GLBP permet donc une utilisation complète de la bande passante dédiée à tous les routeurs. Il permet aussi de gérer les différentes pannes sans pour autant arrêter le service pour les utilisateurs [**18**].

3. **Virtual Router Redundancy Protocol (VRRP)**

   Le protocole de redondance pour le routeur virtuel élimine le seul point d'échec inhérent à un environnement routé par défaut et en statique. VRRP spécifie un protocole d'élection qui assigne dynamiquement les responsabilités pour un routeur virtuel à un concentrateur VPN provenant d'un réseau LAN. Le routeur VRRP, qui contrôle les adresses IP associées au routeur virtuel, est appelé maitre, et les transferts de paquets sont redirigés vers ses adresses IP. Quand le maitre est indisponible, un back up concentrateur VPN prend la place du maitre [**18**].

2.7 Sécurité réseau et système

Pour sécuriser l'infrastructure réseau d'une entreprise nous avons besoin de plusieurs systèmes, logiciels et matériels dont on présente l'essentiel dans ce qui suit :

2.7.1 Réseau local virtuel (VLAN)

Un réseau local virtuel (VLAN, Virtual local area network) est une technique qui permet de créer des réseaux locaux logiques au sein d'un réseau physique. Il permet de segmenter un réseau en groupes virtuels, indépendamment de la configuration physique du réseau.
Les VLANs offrent des avantages tels que la sécurité, la flexibilité, les performances améliorées et une gestion simplifiée. Cela est réalisé en utilisant des commutateurs réseau intelligents[**20**].

2.7.1.1 Typologie des VLANs

Il existe cinq types de VLAN de base : VLAN basé sur l'interface, VLAN basé sur l'adresse MAC, VLAN basé sur le sous-réseau IP, VLAN basé sur le protocole et VLAN basé sur la politique [**20**].

1. **VLAN basé sur les ports (interfaces)**

   Le VLAN basé sur le port, également appelé VLAN basé sur l'interface, est une technologie qui permet aux administrateurs réseau d'attribuer manuellement des VLAN à chaque port de commutateur. Elle convient à un réseau de petite taille sans qu'il soit nécessaire de modifier fréquemment l'infrastructure du réseau.

2. **LAN basé sur l'adresse MAC**

   Le VLAN basé sur l'adresse MAC consiste à attribuer des VLAN en fonction de l'adresse MAC source des trames. L'application de cette technologie peut améliorer considérablement la sécurité et la flexibilité du réseau même si les utilisateurs changent fréquemment d'emplacement physique, l'administrateur réseau n'aura pas besoin de reconfigurer les VLANs.

3. **VLAN basé sur le sous-réseau IP** Le VLAN basé sur le sous-réseau IP peut attribuer des VLAN en fonction des sous-réseaux IP des périphériques. Il s'agit d'une solution efficace pour un réseau public dont la demande de mobilité et de gestion simplifiée est élevée et la demande de sécurité faible. Avec cette technologie, les utilisateurs peuvent automatiquement rejoindre un nouveau VLAN ID après que leur IP ait changé.

4. **VLAN basé sur protocole**

   Appliqué à un réseau comportant plusieurs protocoles, le VLAN basé sur protocole permet d'attribuer des VLAN en fonction des types de protocole et des formats d'encapsulation des trames.

5. **VLAN basé sur les politiques**

   Le VLAN basé sur les politiques peut être décrit comme une combinaison des éléments ci-dessus. Il peut attribuer des VLAN en fonction de politiques telles que des combinaisons d'adresses MAC et d'adresses IP. En combinant les politiques pour réaliser le contrôle d'accès inter-VLAN, la sécurité et la flexibilité du réseau seront grandement améliorées.

2.7.1.2 VLAN NATIF (NATIVE VLAN)

Le "VLAN natif" est le VLAN par défaut sur un port ‘ trunk ’ d’un commutateur réseau. C’est le VLAN auquel les paquets non étiquetés sont associés lorsqu’ils sont reçus sur ce port. Le VLAN natif facilite la communication entre les ports trunk configurés de la même manière [21] [22].

2.7.1.3 VLAN privé (PVLAN)

Le VLAN privé (PVLAN, Private VLAN) permet de subdiviser un VLAN en sous-groupes avec des politiques de communication spécifiques, tels que les ports promiscuous, isolés et communautaires. Les PVLANs offrent une isolation renforcée, une utilisation efficace des adresses IP et une gestion simplifiée des politiques de communication au sein d’un VLAN[23].

Au sein d’un réseau VLAN privé, les VLAN sont accessibles sous trois modalités :

- **VLAN primaire :** ce type de VLAN fait référence au VLAN d’origine, qui peut descendre des trames vers tous ses sous-VLAN (VLAN secondaires) à partir des ports promiscuous vers tous les ports connectés à l’hôte [23].
- **VLAN isolé :** en tant que VLAN secondaire, le VLAN isolé ne peut prendre en charge que les ports de commutation (ports isolés) au sein du VLAN isolé qui transmettent des données aux ports promiscuous du VLAN primaire. Même dans un même VLAN isolé, les ports isolés ne peuvent pas communiquer entre eux[23].
- **VLAN communautaire :** Le VLAN communautaire est également un type de VLAN secondaire. Les ports de commutation (ports communautaires) au sein d’un même VLAN communautaire peuvent communiquer entre eux ainsi qu’avec les ports du VLAN primaire. Mais un tel type de VLAN est également incapable de communiquer avec d’autres VLAN secondaires, y compris d’autres VLAN communautaires[23].

Il existe trois types de port VLAN :

• **Port promiscuous :** ce type de port est capable d'envoyer et de recevoir des trames de n'importe quel autre port du VLAN. Il se connecte généralement à un commutateur de couche 3, un routeur ou d'autres dispositifs de passerelle[**23**].

• **Port isolé :** existant dans un sous-VLAN, le port isolé se connecte à un hôte et ne peut communiquer qu'avec des ports promiscuous[**23**].

• **Port communautaire :** le port communautaire réside également dans un sous-VLAN et se connecte à un hôte. Cependant, il ne peut dialoguer qu'avec les ports promiscuous et les autres ports communautaires du même sous-réseau[**23**].

2.7.2 VLAN Trunking Protocol (VTP)

VTP est un protocole propriétaire de CISCO, il est chargé de gérer les VLANs d'une manière centralisée et évite ainsi aux administrateurs du réseau de se connecter autant de fois qu'il y a de commutateurs dans un réseau pour ajouter, modifier ou supprimer la configuration d'un appelé serveur VTP, afin de distribuer ces informations de configuration VLAN d'un bout à l'autre du réseau commuté. Un tel protocole réduit les délais d'administration et de maintenance des réseaux VLAN. À noter que ce protocole s'applique au niveau de la couche liaison de données du modèle OSI [**23**]. Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants :

• **Le mode serveur :**
- L'information est stockée dans la NVRAM.
- Il définit le nom de domaine VTP.
- Il peut ajouter, modifier ou supprimer un VLAN.
- Il stocke la liste des VLANs du domaine VTP.

• **Le mode client :** - Il possède un nom de domaine.
- Il stocke une liste de VLANs non modifiable.

• **Le mode transparent :** - Il ne participe pas aux domaines VTP du réseau.
- Il transmet les paquets VTP via ses liens trunk.
- Il possède sa propre liste de VLANs qu'il est possible de modifier.

Si une des conditions suivantes n'est pas respectée, le domaine de VTP ne sera pas valide et l'information ne se propagera pas :
• Il faut assigner le même nom de domaine de VTP à chaque commutateur.
• L'option trunk pour l'interconnexion des commutateurs doit être activée.

2.7.3 Pare-feu

Le pare-feu est un programme, ou un matériel, chargé de protéger du monde extérieur en contrôlant tout ce qui passe, et surtout tout ce qui ne doit pas passer entre internet et le réseau local. Le pare-feu joue un rôle essentiel dans la sécurisation d'un réseau. Tous les trafics doivent y passer et y être contrôler. Peu importe que ce soit un réseau d'entreprise ou réseau domestique, un pare-feu actif est nécessaire pour se protéger du réseau public. Les menaces sont nombreuses, on ressent actuellement de nombreuses menaces de virus, de vers, d'attaques par déni de Service (DoS, Deny of Service), de hacking, ect [**24**]. Le rôle du pare-feu peut se résumer à :

• Gérer les connexions sortantes à partir du réseau local. (Rôle de contrôle) .
• Protéger le réseau interne des intrusions venant de l'extérieur. (Rôle de sécurité).
• Surveiller et tracer le trafic entre le réseau local et l'internet. (Rôle de vigilance).

2.7.4 Zone démilitarisée

Une zone démilitarisée (ou DMZ, DeMilitarized Zone) est un sous-réseau séparant le réseau local d'un réseau considéré comme moins sécurisé, comme internet et cette séparation est faite par un pare-feu. La DMZ hébèrge des machines du réseau interne qui ont besoins d'être accessibles depuis l'exterieur c'est le cas notamment lorsqu'ils fournissent des services aux utilisateurs sur internet comme par exemple : un serveur wem, serveur de messagerie, ect [**26**].

2.7.5 Network Address Translation (NAT)

Le NAT est une technique qui permet de traduire les adresses IP lors de la communication entre les réseaux internes et externes. Il facilite le partage des adresses IP publiques, la redirection des connexions entrantes et offre une certaine sécurité en masquant les adresses IP internes [**27**].

2.8 Conclusion

À l'issue de ce chapitre, nous avons pu collecter les différentes techniques, logiciels , matériels et méthodes d'administration, gestion et sécurisation des infrastructures réseaux .
Le chapitre suivant sera consacré à la conception de notre travail étudié dans les deux chapitres précédents.

Chapitre 3

Configuration et Tests

3.1 Introduction

Après avoir décrit les différentes solutions proposées aux problèmes identifiés sur le réseau de l'université de Béjaia, nous exproserons dans ce présent chapitre les différentes configurations nécessaires à implémenter sur le LAN avec des tests qui démontreront son bon fonctionnement.

3.2 Environnement du travail

Dans cette section, nous présentons les outils qui ont été utilisés pour la réalisation de notre projet au sein de l'environnement de travail.

1. **VMware Workstation**

VMware Workstation Pro est l'hyperviseur de bureau standard pour l'exécution de machines virtuelles sur des PC Linux ou Windows[**28**].

2. **GNS3**

GNS3 est un outil open source de simulation de réseaux informatiques largement utilisé. Il permet aux professionnels des réseaux de créer des topologies virtuelles et de simuler différents scénarios de réseau sans avoir besoin de matériel physique. Avec GNS3, les utilisateurs peuvent concevoir et configurer des environnements réseaux complexes en émulant des routeurs, des commutateurs et d'autres équipements réseaux. Il prend en charge une large gamme de systèmes d'exploitation et d'équipements réseau, notamment Cisco IOS et bien d'autres [**29**].

3. **Windows server 2022**

Windows Server 2022 est le système d'exploitation orienté serveur de Microsoft. Windows Server 2022 améliore la gestion des serveurs hybrides grâce à une gestion des ma-

chines virtuelles considérablement améliorée, un observateur d'événements optimisé, et bien d'autres fonctionnalités [**30**].

3.3 Architecture proposée

La Figure 3.1 dépeint l'architecture proposée afin de simuler les différentes améliorations discutées dans le chapitre 1 :

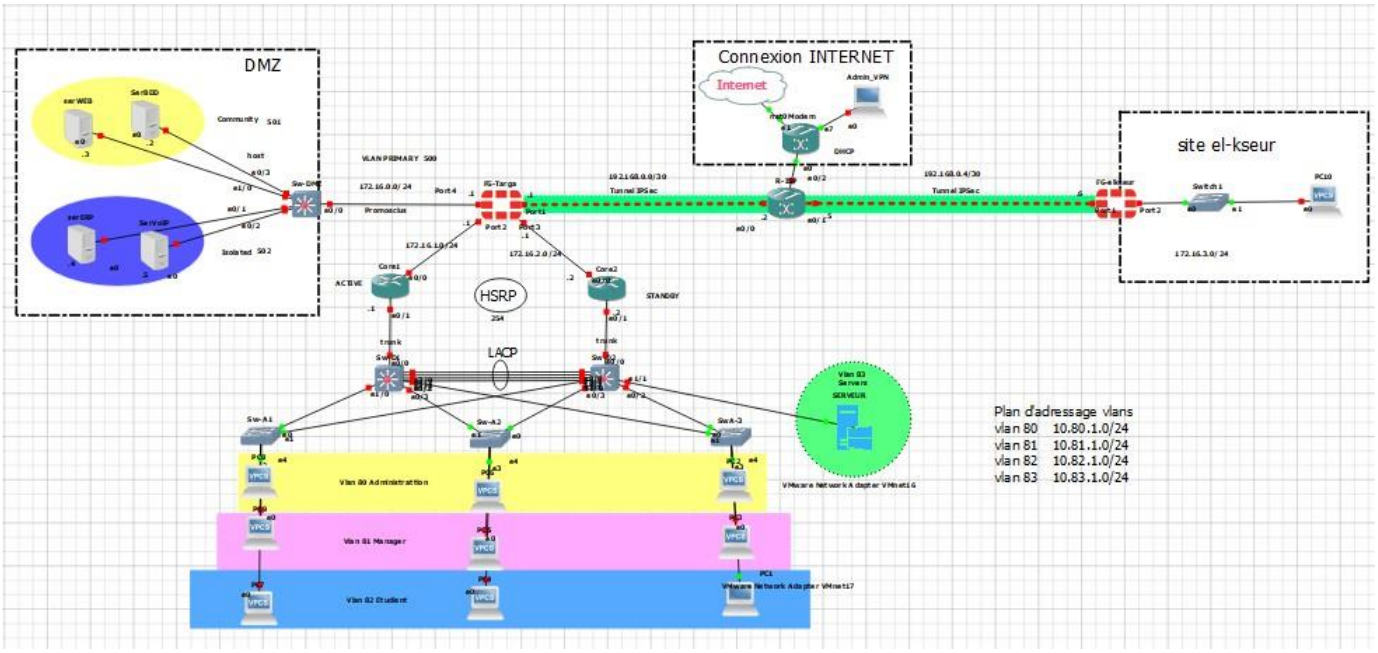

FIGURE 3.1 – Architecture proposée

1. **au niveau de la DMZ**
   L'utilisation des PVLANs (Private VLANs) dans la configuration de la DMZ est une approche efficace pour renforcer la sécurité et la segmentation des réseaux. Les PVLANs permettent de subdiviser une VLAN en plusieurs sous-groupes isolés, ce qui limite les interactions entre les différents serveurs et ressources présents dans la DMZ. Cela contribue à réduire les risques de propagation d'attaques ou d'accès non autorisés entre les différentes machines hébergées dans la DMZ.

2. **Configuration du protocole HSRP au niveau des routeurs**
   En utilisant le protocole HSRP, garantit la tolérance aux pannes et la haute disponibilité des routeurs en établissant une redondance active-passive et en permettant une transition transparente entre les routeurs en cas de défaillance. Cela contribue à assurer une continuité des services réseau et une meilleure résilience globale du réseau.

3. **Agrégation des liens avec le protocole LACP**
   Tout d'abord, cela permet d'augmenter la bande passante disponible entre les deux switeches (Sw-D1 et Sw-D2) en répartissant le trafic sur plusieurs liens physiques. L'agrégation de liens avec LACP offre une redondance et une tolérance aux pannes améliorées. En cas de défaillance d'un lien physique, le trafic est automatiquement redistribué

sur les liens restants entre les deux switches, assurant ainsi une continuité du service sans interruption notable pour les utilisateurs finaux.

4. **Installation d'Active Directory et centralisation**
   Création des comptes utilisateurs et définition des rôles de contrôle d'accès : ce simplifie grandement l'administration du réseau en permettant aux administrateurs de gérer les utilisateurs, les groupes et les autorisations d'accès à partir d'un emplacement centralisé.

   Centralisation du serveur DHCP : en intégrant le service DHCP avec Active Directory, les informations de configuration des clients DHCP peuvent être stockées dans la base de données d'Active Directory. Cela simplifie la gestion du DHCP en offrant une vue centralisée et un contrôle de la configuration DHCP pour l'ensemble du réseau.

3.4 Tableaux d'adressage

Les tableaux ci-dessous représentent l'adressages utilisée pour les différents équipements.

— Le tableau 3.1 représente l'adressage des équipements.

nom-equipement	interface	adresse IP
core1	e 0/1 e 0/0	sous-interfaces des VLANs 172.16.1.1/24
core2	e 0/1 e 0/0	sous-interfaces des VLANs 172.16.1.2/24
FG-Targa	port 1 (WAN) port 2 (LAN 1) port 3 (LAN 2) port 4 (DMZ)	192.168.0.1 172.16.1.1/24 172.16.2.1/24 172.16.0.1/24
Admin-ser(serveur)	e 0/0	10.83.1.100/24

TABLE 3.1 – Tableau d'adressages des équipement : routeur, pare-feu et serveur.

— Le tableau 3.2 est le tableau d'adressage des VLANs.

Nom	ID	adresse sous-réseau	la passerelle
administrateur	80	10.80.1.0/24	10.80.1.1 10.80.1.2
manager	81	10.81.1.0/24	10.81.1.1 10.81.1.2
etudiant	82	10.82.1.0/24	10.82.1.1 10.82.1.2
servers	83	10.83.1.0/24	10.83.1.1 10.83.1.2

TABLE 3.2 – Tableau des VLANs.

— Le tableau 3.3 représente le routage inter-VLANs :

nom du routeur	interface	la passerelle
core 1	e 0/1.80 e 0/1.81 e 0/182. e 0/1.83	10.80.1.1 10.81.1.1 10.82.1.1 10.83.1.1
core 2	e 0/1.80 e 0/1.81 e 0/182. e 0/1.83	10.80.1.2 10.81.1.2 10.82.1.2 10.83.1.2

TABLE 3.3 – Tableau du routage inter-VLANs.

— Le tableau 3.4 d'adressage HSRP :

Nom	état	Priorité	Version	Interface	Adresse virtuelle
core 1	active	150	2	e1/0.80 e 0/1.81 e 0/1.82 e 0/1.83	10.80.1.254 10.81.1.254 10.82.1.254 10.83.1.254
core 2	standby	100	2	e1/0.80 e 0/1.81 e 0/182. e 0/1.83	10.80.1.254 10.81.1.254 10.82.1.254 10.83.1.254

TABLE 3.4 – Tableau HSRP.

— Le tableau 3.5 d'adressage des PVLANs.

nom	ID	interface	mode d'interface	adresse
primary	500	e0/0	promiscuous	/
issolated	502	e0/1 e0/2	host	172.16.0.4 172.16.0.5
community	501	e1/0 0/3	host	172.16.0.3 172.16.0.2

TABLE 3.5 – Tableau des Private VLANs.

3.5 Configurations

Dans cette section nous allons présenter les différentes configurations effectuées.

3.5.1 Configuration des liens trunk

Dans cette section nous allons configurer les liaisons entre les switches de distribution (sw-D1 et sw-D2) et les switches d'accès (sw-A1,sw-A2 et sw-A3) en mode trunk afin que ces derniers communiquent et transmettent entre eux les Vlans configurés.
Les figures 3.2 et 3.3 indiquent les commandes à saisir, sur les switchs de distribution sw-D1 et sw-D2, afin de configurer les différents commutateurs en mode trunk en utilisons la commande **« interface range »** qui permet de regrouper les interfaces en un seul coup.

```
Sw-D1(config)#interface range eth3/0-3, eth0/2-3, eth1/0
Sw-D1(config-if-range)#sz
Sw-D1(config-if-range)#sw
Sw-D1(config-if-range)#switchport t
Sw-D1(config-if-range)#switchport trunk en
Sw-D1(config-if-range)#switchport trunk encapsulation do
Sw-D1(config-if-range)#switchport trunk encapsulation dot1q
Sw-D1(config-if-range)#sw
Sw-D1(config-if-range)#switchport mo
Sw-D1(config-if-range)#switchport mo tr
Sw-D1(config-if-range)#switchport mo trunk
Sw-D1(config-if-range)#
Sw-D1(config-if-range)#end
```

FIGURE 3.2 – Configuration des liens trunk sur sw-D1

```
Sw-D2(config)#interface range ethernet 3/0-3
Sw-D2(config-if-range)#$ange ethernet 3/0-3, ethernet 0/2-3, ethernet 1/0
Sw-D2(config-if-range)#sw
Sw-D2(config-if-range)#switchport tru
Sw-D2(config-if-range)#switchport trunk endo
Sw-D2(config-if-range)#switchport trunk end
Sw-D2(config-if-range)#switchport trunk enc
Sw-D2(config-if-range)#switchport trunk encapsulation do
Sw-D2(config-if-range)#switchport trunk encapsulation dot1q
```

FIGURE 3.3 – Configuration des liens trunk sur sw-D2.

Au niveau des switchs niveau d'accès, la configuration a été faite comme c'est illustré sur la figure 3.4.

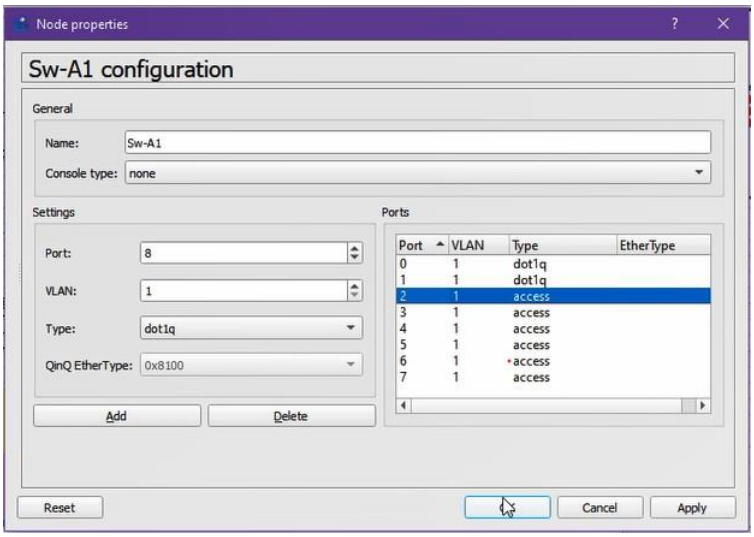

FIGURE 3.4 – Exemple de configuration des liens trunk sur sw-A1.

Afin de vérifier cette configuration, nous avons vérifié l'état des interfaces avec la commande **« show interfaces trunk ».** La figure 3.5, donne un aperçu du résultat du test.

```
Sw-D2#show  interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/2       on               802.1q         trunking      1
Et0/3       on               802.1q         trunking      1
Et1/0       on               802.1q         trunking      1
Et3/0       on               802.1q         trunking      1
Et3/1       on               802.1q         trunking      1
Et3/2       on               802.1q         trunking      1
Et3/3       on               802.1q         trunking      1
```

FIGURE 3.5 – Exemple de vérification des liens trunks sur sw-D2.

3.5.2 Configuration de l'agrégation des liens (etherchannel)

Dans l'architecture proposée, nous avons opté pour une agrégation des liens en utilisant le protocole LACP entre les deux switchs de distribution sw-D1 et sw-D2, on a donc mis les ports Ethernet 3/0-3 dans un groupe en précisant le mode **actif** dans le but d'activer l'emission et la réception avec le protocole LACP, comme le montre la figure 3.6.

```
Sw-D2(config)#interface  range ethernet 3/0-3
Sw-D2(config-if-range)#channel
Sw-D2(config-if-range)#channel-g
Sw-D2(config-if-range)#channel-group 1 mo
Sw-D2(config-if-range)#channel-group 1 mode  ac
Sw-D2(config-if-range)#channel-group 1 mode  active
Creating a port-channel interface Port-channel 1
```

FIGURE 3.6 – Configuration d'agrégation des liens.

On vérifie cette configuration en tapant **« show etherchannel summary »**. Comme le témoigne la figure 3.7, le protocole LACP est bien configuré et le port-channel est actif.

```
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et3/0(P)    Et3/1(P)    Et3/2(P)
                                 Et3/3(P)
```

FIGURE 3.7 – Vérification de la configuration d'etherchannel

Configuration de l'équibrage de charges

La figure 3.8 montre la configuration de l'quilibrage de charges (load balancing).

```
Sw-D2(config)#port-channel load-balance src-dst-mac
Sw-D2(config)#end
```

FIGURE 3.8 – Vérification du load balancing

Configuration du spanning-tree

La figure 3.9 montre la configuration de spanning-tree à fin d'améliorer la qualité de service.

```
Sw-D1(config)#spanning-tree mode  rapid-pvst
Sw-D1(config)#end
```

FIGURE 3.9 – Vérification de spanning-tree

3.5.3 Configuration des VLANs

En explorant la configuration des VLANs, nous détaillerons les étapes clés, allant de la création initiale des VLANs à la gestion experte des ports attribués.

3.5.3.1 Création des VLANs

À présent nous allons créer les différents VLANs de l'université sur le switch de distribution sw-D1 en utilisant la commande **« vlan »** sur le mode configuration et ensuite le nommer avec la commande **« name »** sur le même mode comme illustré dans la figure 3.10 .

```
Sw-D1(config)#vlan 80
Sw-D1(config-vlan)#name administration
Sw-D1(config-vlan)#vlan 81
Sw-D1(config-vlan)#name manager
Sw-D1(config-vlan)#vlan 82
Sw-D1(config-vlan)#name Etudiant
Sw-D1(config-vlan)#end
```

FIGURE 3.10 – Création des VLANs.

Après la création du VLAN nommé servers associé au VLAN 83, nous allons ensuite vérifier leurs créations avec la commande **« show vlan brief »** comme le montre la figure 3.11 .

```
Sw-D1#show  vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et1/1, Et1/2
                                                Et1/3, Et2/0, Et2/1, Et2/2
                                                Et2/3
80   administration                   active
81   manager                          active
82   Etudiant                         active
83   servers                          active
```

FIGURE 3.11 – Vérification de la création des VLANs.

3.5.3.2 Configuration VTP (VLAN tranking protocol)

Afin de profiter des services VTP (création, suppression, modification des Vlans), nous allons configurer le switch de distribution « sw-D1 » en mode Serveur et lui attribué un nom de domaine ainsi qu'un mot de passe, et l'autre switch en mode Client afin que les Vlans se propagent du sw-D1 vers sw-D2. Pour cela nous allons procéder comme suit :

1. Configurer le sw-D1 en VTP serveur :

```
Sw-D1(config)#vtp mode server
Device mode already VTP Server for VLANS.
Sw-D1(config)#vtp pass
Sw-D1(config)#vtp password cisco123
Setting device VTP password to cisco123
Sw-D1(config)#vtp domai
Sw-D1(config)#vtp domain univ_net.vtp
Changing VTP domain name from NULL to univ_net.vtp
Sw-D1(config)#vtp ve
Sw-D1(config)#vtp version 2
Sw-D1(config)#vtp pru
Sw-D1(config)#vtp pruning
Pruning switched on
```

FIGURE 3.12 – Configuration VTP serveur.

Nous allons vérifier cette configuration avec la commande **show vtp status** :

```
Sw-D1#show  vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : univ_net.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0300
Configuration last modified by 0.0.0.0 at 6-14-23 18:04:04
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 9
Configuration Revision            : 6
MD5 digest                        : 0x04 0x62 0x9F 0xF3 0x6A 0x5D 0x1F 0x5C
                                    0xC8 0x50 0x0D 0x65 0xCE 0xF6 0x1C 0x34
```

FIGURE 3.13 – Vérification de configuration VTP serveur.

2. Configurer Sw-D2 en mode VTP client :

```
Sw-D2(config)#vtp mode  client
Setting device to VTP Client mode for VLANS.
Sw-D2(config)#vtp pass
Sw-D2(config)#vtp password cisco123
Setting device VTP password to cisco123
Sw-D2(config)#vtp dom
Sw-D2(config)#vtp domain univ_net.vtp
Changing VTP domain name from NULL to univ_net.vtp
Sw-D2(config)#vtp ve
Sw-D2(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
Sw-D2(config)#end
```

FIGURE 3.14 – configuration de VTP client.

Nous allons aussi vérifier cette configuration avec la commande show vtp status :

```
Sw-D2#show  vtp  status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : univ_net.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0400
Configuration last modified by 0.0.0.0 at 6-14-23 18:04:04

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 9
Configuration Revision            : 6
MD5 digest                        : 0x04 0x62 0x9F 0xF3 0x6A 0x5D 0x1F 0x5C
                                    0xC8 0x50 0x0D 0x65 0xCE 0xF6 0x1C 0x34
```

FIGURE 3.15 – Vérification de configuration VTP client.

3.5.3.3 Attribution des ports aux différents VLANs

Dans cette étape nous allons assigner des ports aux Vlans au niveau des switches d'accès comme on peut le voir sur la figure 3.16.

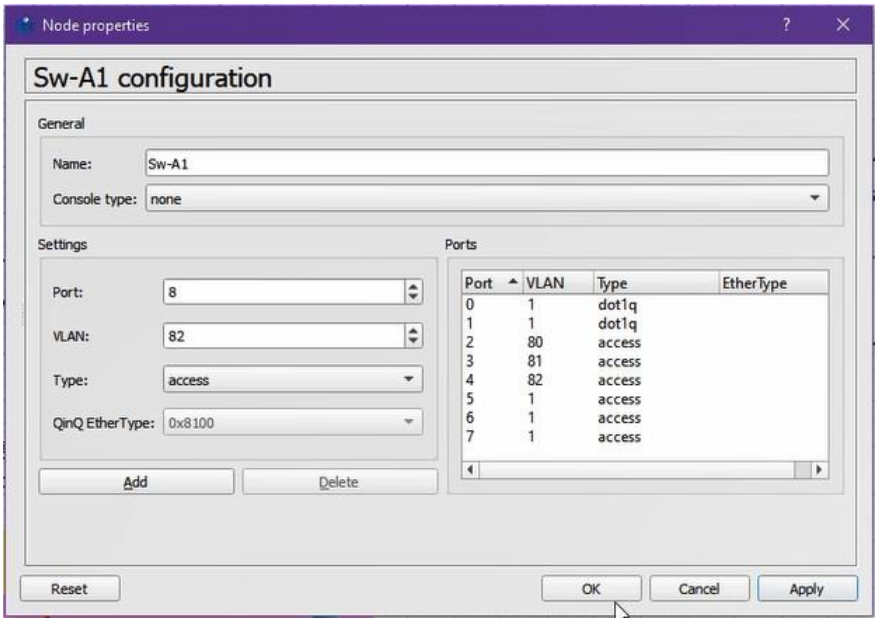

FIGURE 3.16 – Exemple d'attibution de ports aux VLANs au niveau du switch sw-A3

3.5.4 Configuration du routage inter-VLANs

Afin d'assurer le routage inter-VLANs on a créé des sous-interfaces pour chaque VLAN comme le montre les figures 3.17 et 3.18

```
Core1(config)#interface  ethernet 0/1
*Jun 14 18:08:14.846: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Jun 14 18:08:15.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
Core1(config)#interface  ethernet 0/1.80
Core1(config-subif)#en
Core1(config-subif)#encapsulation do
Core1(config-subif)#encapsulation dot1Q 80
Core1(config-subif)#ip add
Core1(config-subif)#ip address 10.80.1.1 255.255.255.0
Core1(config-subif)#exit
Core1(config)#interface  ethernet 0/1.81
Core1(config-subif)#encapsulation dot1Q 81
Core1(config-subif)#ip address 10.81.1.1 255.255.255.0
Core1(config-subif)#exit
Core1(config)#interface  ethernet 0/1.82
Core1(config-subif)#encapsulation dot1Q 82
Core1(config-subif)#ip address 10.82.1.1 255.255.255.0
Core1(config-subif)#exit
Core1(config)#interface  ethernet 0/1.83
Core1(config-subif)#encapsulation dot1Q 83
Core1(config-subif)#ip address 10.83.1.1 255.255.255.0
Core1(config-subif)#end
```

FIGURE 3.17 – Création des sous interfaces des VLAN au niveau du CORE1.

```
Core2(config)#interface ethernet 0/1.80
Core2(config-subif)#en
Core2(config-subif)#encapsulation do
Core2(config-subif)#encapsulation dot1Q 80
Core2(config-subif)#ip add
Core2(config-subif)#ip address 10.80.1.2 255.255.255.0
Core2(config-subif)#exit
Core2(config)#interface ethernet 0/1.81
Core2(config-subif)#encapsulation dot1Q 81
Core2(config-subif)#ip address 10.81.1.2 255.255.255.0
Core2(config-subif)#interface ethernet 0/1.82
Core2(config-subif)#encapsulation dot1Q 82
Core2(config-subif)#ip address 10.82.1.2 255.255.255.0
Core2(config-subif)#interface ethernet 0/1.83
Core2(config-subif)#encapsulation dot1Q 83
Core2(config-subif)#ip address 10.83.1.2 255.255.255.0
Core2(config-subif)#end
```

FIGURE 3.18 – Création des sous interfaces des VLAN au niveau du CORE2.

Le résultat du test de routage inter-VLANs est montré sur la figure 3.19

```
C:\Users\Administrateur>ping 10.80.1.1

Envoi d'une requête 'Ping'  10.80.1.1 avec 32 octets de données :
Réponse de 10.80.1.1 : octets=32 temps=27 ms TTL=255
Réponse de 10.80.1.1 : octets=32 temps=3 ms TTL=255

Statistiques Ping pour 10.80.1.1:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 3ms, Maximum = 27ms, Moyenne = 15ms
Ctrl+C
^C
C:\Users\Administrateur>ping 10.80.1.2

Envoi d'une requête 'Ping'  10.80.1.2 avec 32 octets de données :
Réponse de 10.80.1.2 : octets=32 temps=12 ms TTL=255
Réponse de 10.80.1.2 : octets=32 temps=3 ms TTL=255

Statistiques Ping pour 10.80.1.2:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 3ms, Maximum = 12ms, Moyenne = 7ms
Ctrl+C
^C
C:\Users\Administrateur>
```

FIGURE 3.19 – Test de routage inter-VLANs.

3.5.5 Configuration du protocole HSRP

Maintenant nous allons configurer le protocole HSRP au niveau des deux routeurs core1 et core2, on définit un groupe HSRP, une priorité **« standbay priority »** la plus élevée qui décide le routeur "active", et de la préemption **« standby preempt »**, cette dernière permet au routeur standby (core 2), s'il est éteint, de ne pas perturber le routeur active (core1).
Les figures 3.20 et 3.21 montrent la configuration de HSRP sur les différents routeurs

- Sur core1 pour les Vlans 80, 81, 82 et 83 : avec une priorité égale à 150 pour qu'il devient le routeur actif.

```
Core1(config)#interface  ethernet 0/1.80
Core1(config-subif)#st
Core1(config-subif)#standby ve
Core1(config-subif)#standby version 2
Core1(config-subif)#sta
Core1(config-subif)#standby 80 ip 10.80.1.254
Core1(config-subif)#sta
Core1(config-subif)#standby 80 pri
Core1(config-subif)#standby 80 priority 150
Core1(config-subif)#sta
Core1(config-subif)#standby 80 pree
Core1(config-subif)#standby 80 preempt
Core1(config-subif)#
*Jun 14 18:25:17.771: %HSRP-5-STATECHANGE: Ethernet0/1.80 Grp 80 state Standby -> Active
Core1(config-subif)#exit
```

FIGURE 3.20 – Exemple de configuration HSRP(Vlan 80) mode actif.

- Sur core2 pour les Vlans 80, 81, 82 et 83 : pour qu'il marche en mode standby.

```
Core2(config)#interface ethernet 0/1.80
Core2(config-subif)#st
Core2(config-subif)#standby ve
Core2(config-subif)#standby version 2
Core2(config-subif)#sta
Core2(config-subif)#standby 80 ip 10.80.1.254
Core2(config-subif)#exit
```

FIGURE 3.21 – Exemple de configuration HSRP(Vlan 80) mode standby

Nous allons vérifier cette configuration avec la commande **show standby brief**, comme nous pouvons le voir sur les figures 3.22 et 3.23.

- sur core1 :

```
Core1#show  standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/1.80    80   150 P Active  local           10.80.1.2       10.80.1.254
Et0/1.81    81   150 P Active  local           10.81.1.2       10.81.1.254
Et0/1.82    82   150 P Active  local           10.82.1.2       10.82.1.254
Et0/1.83    83   150 P Active  local           10.83.1.2       10.83.1.254
```

FIGURE 3.22 – Vérification du HSRP sur core1.

- sur core2 :

```
Core2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/1.80    80   100   Standby 10.80.1.1       local           10.80.1.254
Et0/1.81    81   100   Standby 10.81.1.1       local           10.81.1.254
Et0/1.82    82   100   Standby 10.82.1.1       local           10.82.1.254
Et0/1.83    83   100   Standby 10.83.1.1       local           10.83.1.254
```

FIGURE 3.23 – Vérification du HSRP sur core2.

3.5.6 Configuration de l'AD

Dans cette étape, nous avons installé les rôles de l'active directory DHCP et DNS .
Pour terminer l'installation nous avons configuré un domaine racine et un mot de passe d'accés. La figure 3.24 illustre l'interface d'entrés au domaine déja crée aprés l'installation de l'AD.

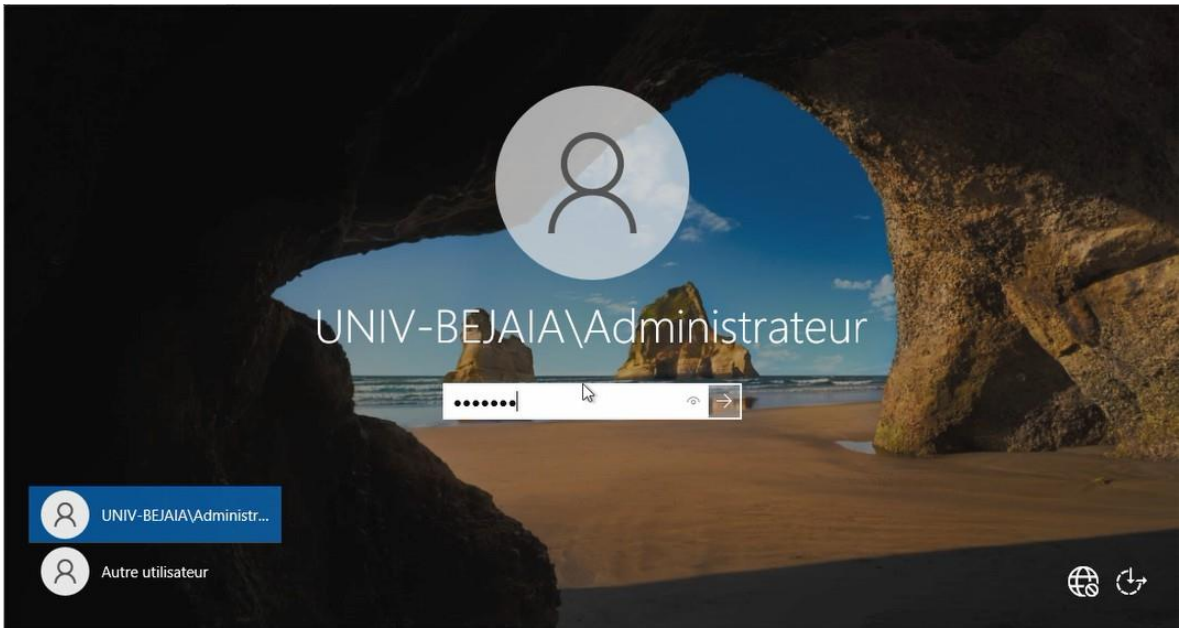

FIGURE 3.24 – Affichage d'entrée à Active directory.

3.5.6.1 Test de l'active directory (AD)

Afin de tester l'active directory, nous avons créé un groupe (Group-etudiants), un utilisateur (fairouz allouache) ainsi que son mot de passe, que nous l'avons rajouter au groupe etudiants comme le montre la figure.
Ensuite nous avons assocoié la session de l'utilisateur(fairouz) à un PC qu'on a connecté aprés au domaine UNIV-Bejaia en tant qu'administrateur.

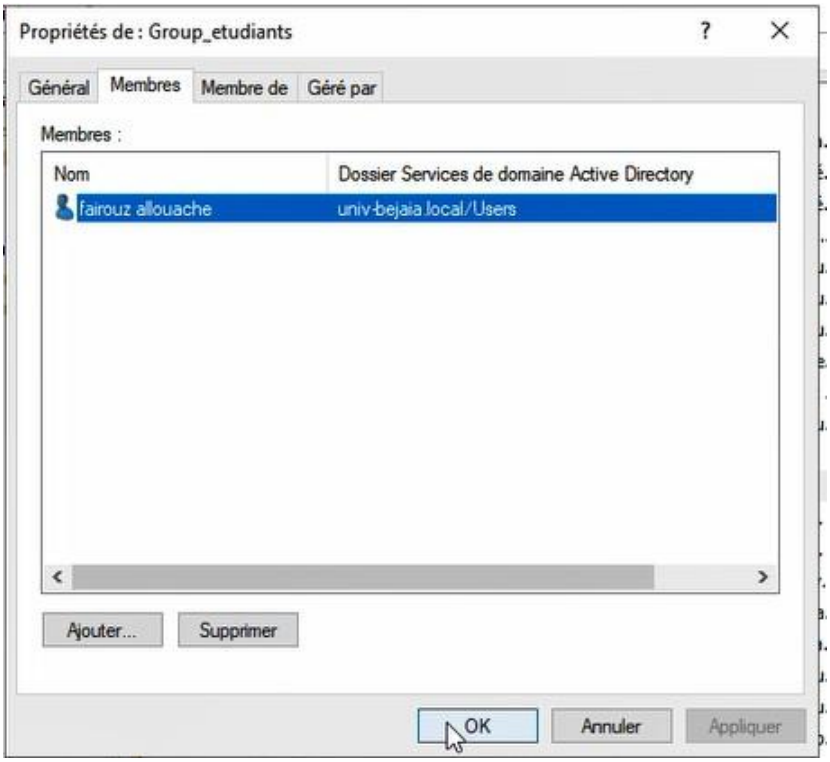

FIGURE 3.25 – Ajout d'un utilisateur au groupe

Création d'une politique de sécurité

Avec l'outil gestion de stratégie de groupe (GPO), on créé une stratégie sous le nom' stratégie-sécurité 1 qui a comme mission de refuser tout les classes de stochage amoviles et d'interdir l'accès au panneau de configuration d'un PC. Les figures ci dessous montrent respectivement les tests qui indiquent que l'accés au panneau de configuration est interdit et refus de lecture d'une clés USB .

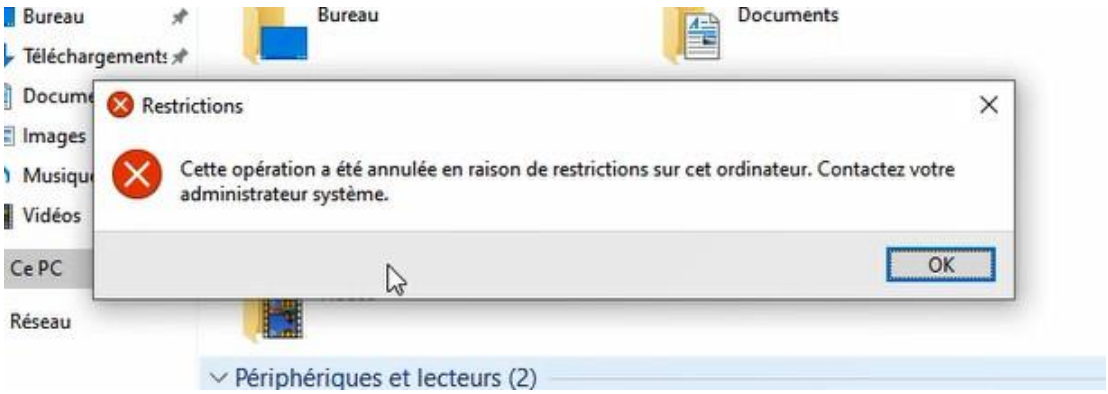

FIGURE 3.26 – exemple 1 de test de stratégie de sécurité1

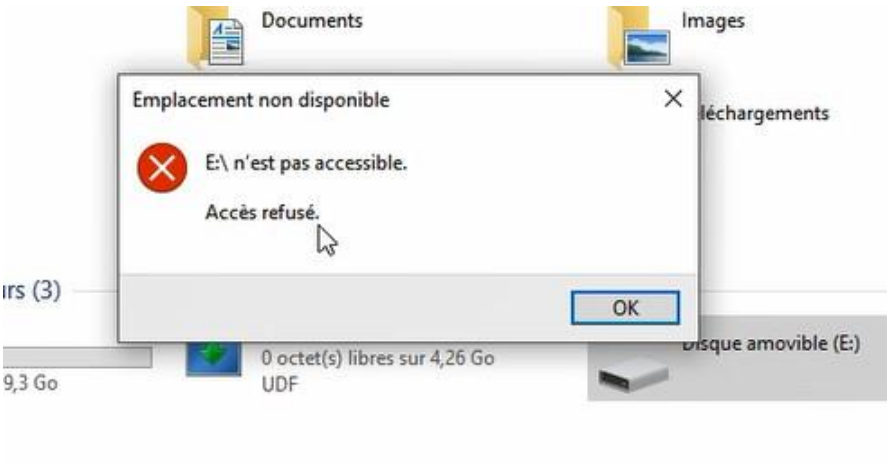

FIGURE 3.27 – exemple 2 de test de stratégie de sécurité1

3.5.6.2 Configuration DHCP

Afin de faciliter la gestion et l'attribution des adresses IP pour chaque hôte du réseau, nous allons utiliser DHCP, ce dernier permet de configurer les paramètres de chaque hôte et le laissera profiter d'un adressage dynamique . La configuration se fera au niveau du serveur DHCP installé dans l'AD.

Les figures qui vont suivre illustrent les étape de configuration du DHCP :
- on a créé une étendue pour chaque VLAN comme le montre la figure suivante.

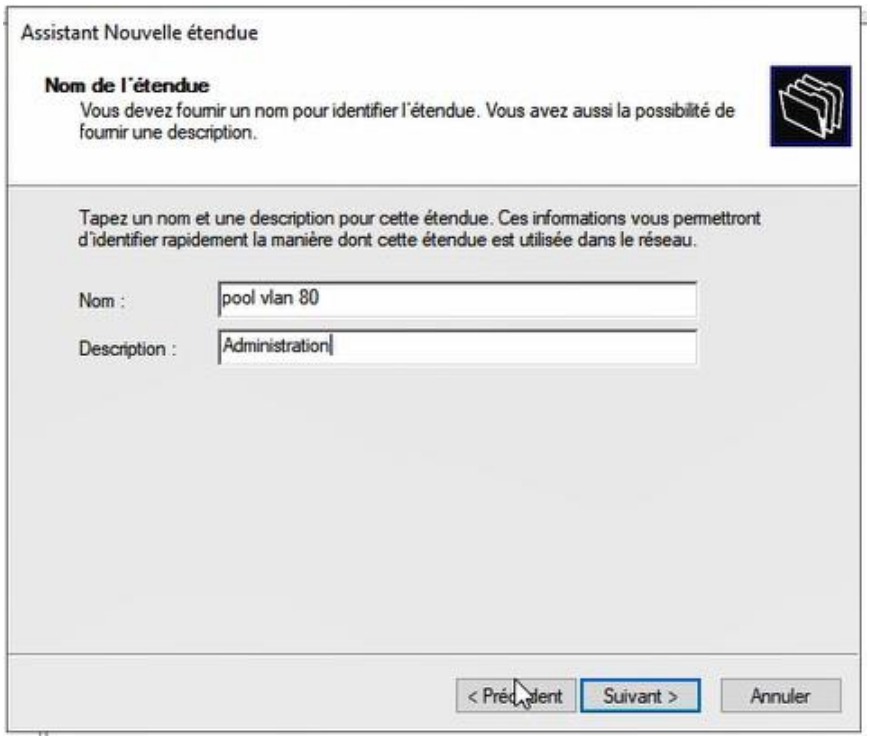

FIGURE 3.28 – Exemple de création de pool DHCP

- Définir une plage d'adresse de début et de fin .

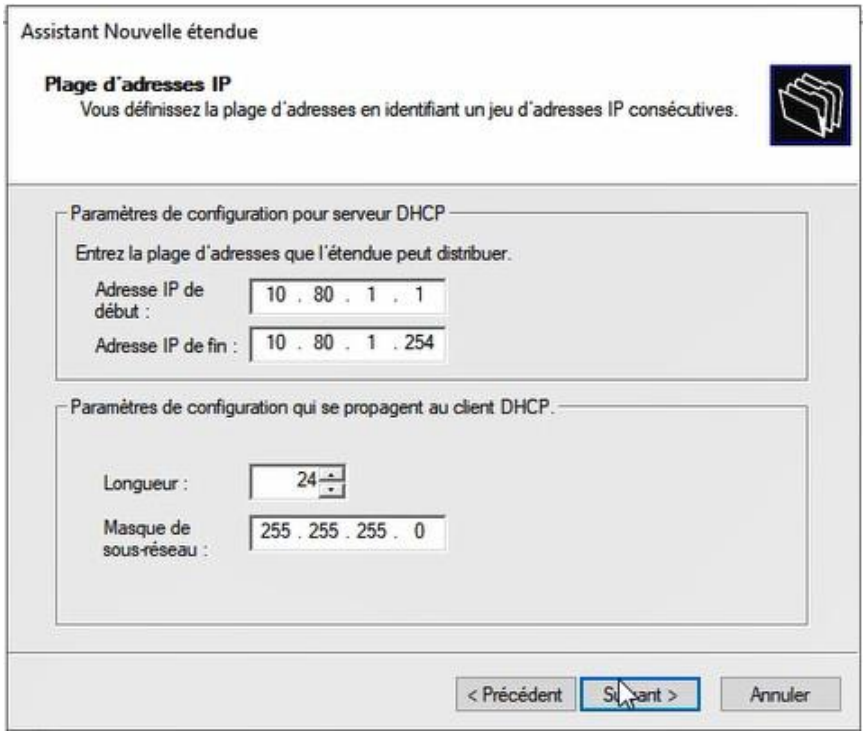

FIGURE 3.29 – Définition de plage d'aressage

- Pour éviter les conflits d'adressage, on a exclus les dix (10) premiéres adresses comme c'est montré dans la figure

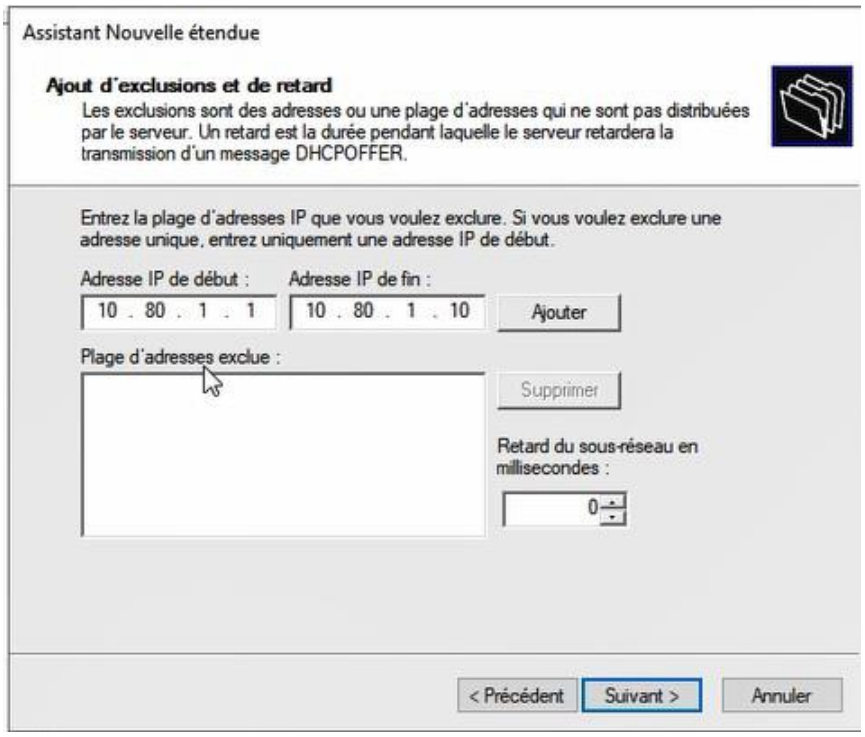

FIGURE 3.30 – Exclusion des adresses non distribuées

- Spécifier la durée d'utilisation d'une adresse IP de cette étendue (durée du bail)

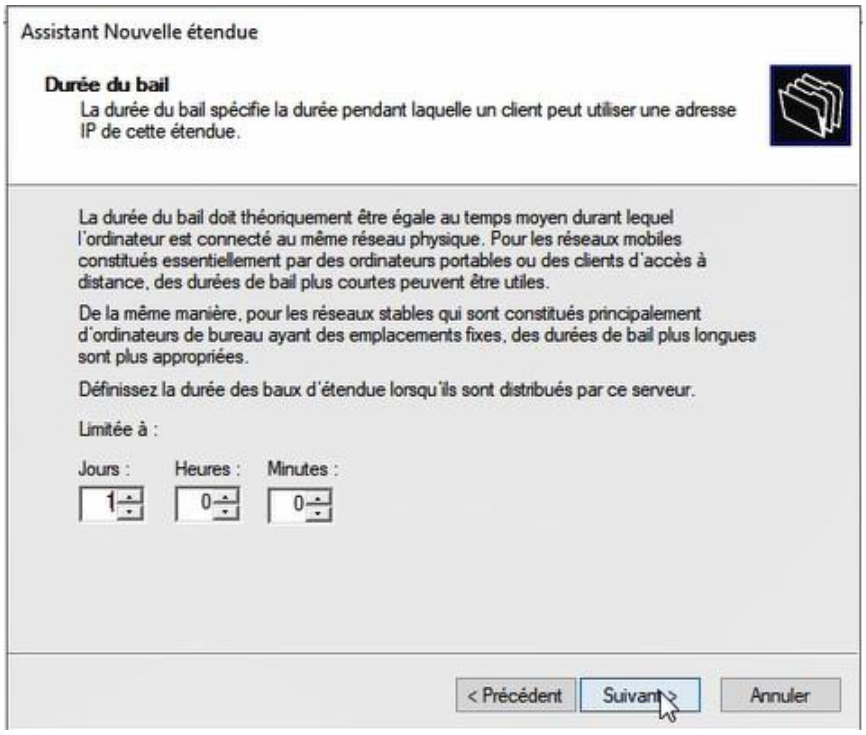

FIGURE 3.31 – Spécification de la durée du bail

- donner la passerelle qui sera utilisée par ce pool.

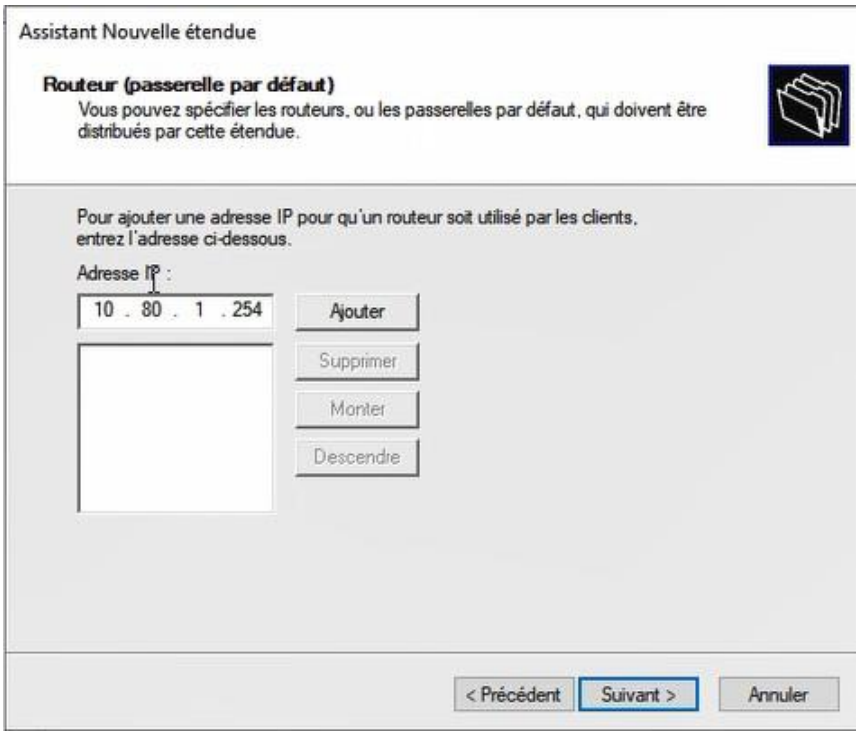

FIGURE 3.32 – La passerelle

- Définir le serveur DNS pour permeter aux hôte de se connecter à internet.

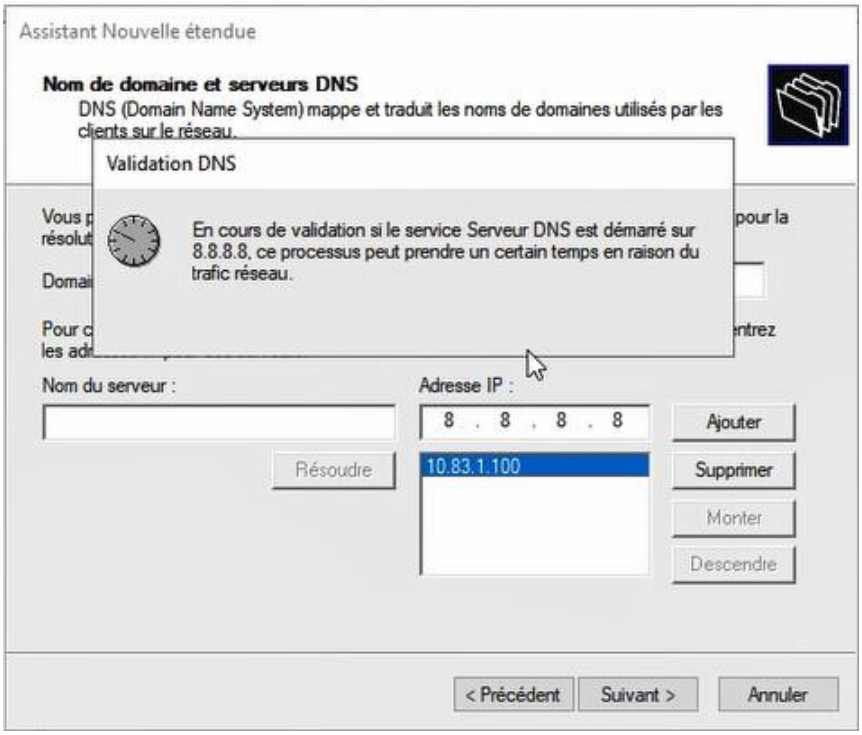

FIGURE 3.33 – Définition de serveur DNS

- Donner une adresse IP au serveur Wins qui va faire la résolution des noms.

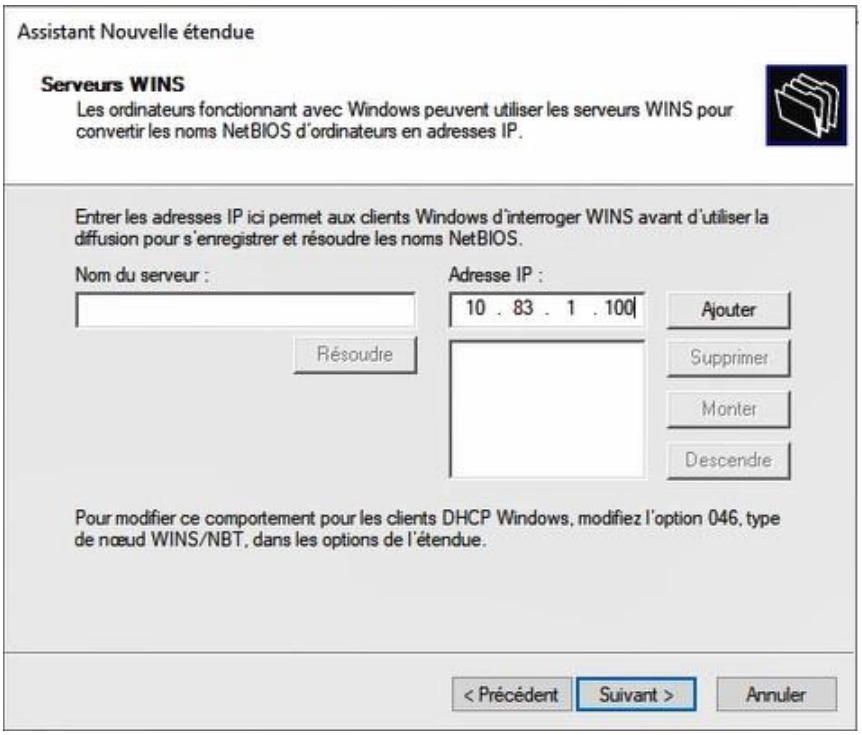

FIGURE 3.34 – attribution d'addresse de serveur WINS

- On procède de la même manière pour les autres VLANs : 81 et 82.

- Afin de réussir ce protocole, et de permettre au serveur DHCP d'attribuer des adresses aux hôtes dans les différents réseaux, on configuré un agent relai pour chaque interface du rou- teur (core1 et core2).
La figure .. montre la configuration de l'agent relai à l'aide de la commande **ip ahelper-address** sur chaque sous-interfaces du routeur core1.

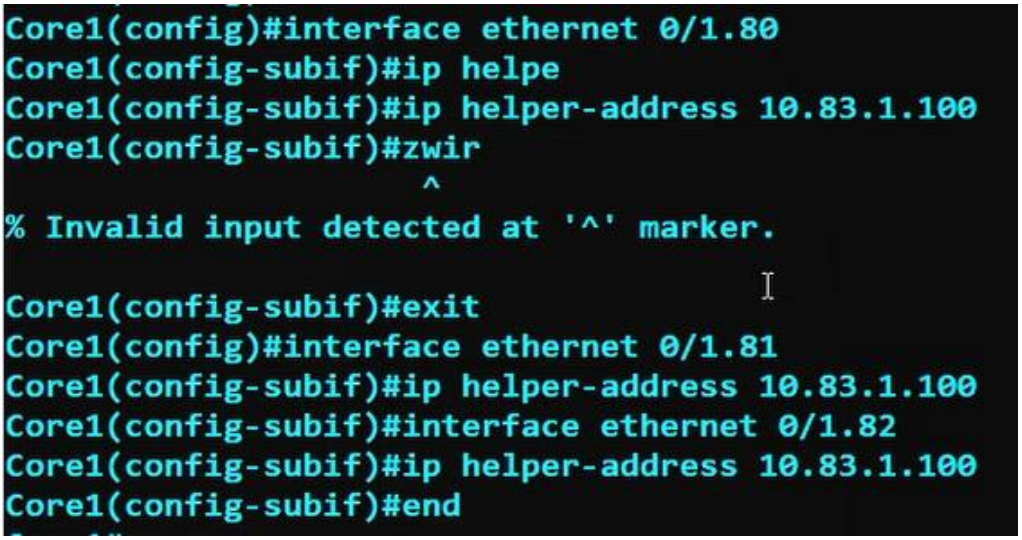

FIGURE 3.35 – Configuration de l'agent relai

-La figure montre l'adressage dynamique d'un PC (PC- test.)

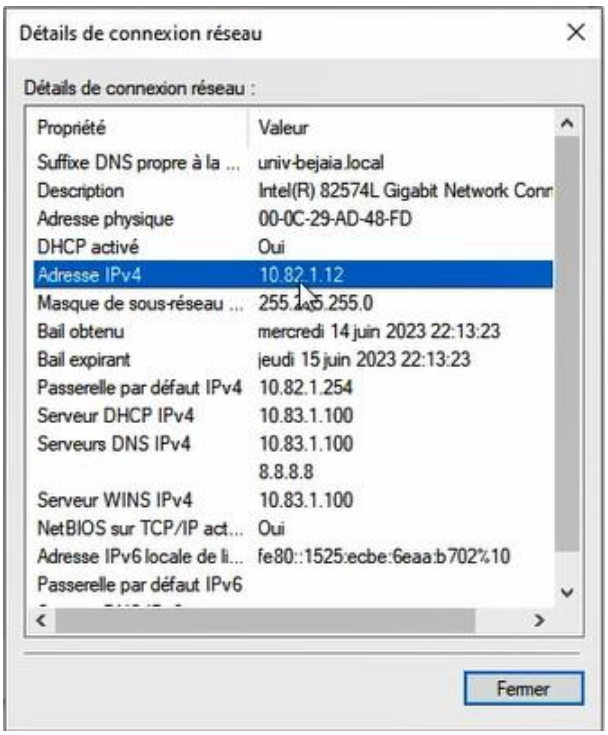

FIGURE 3.36 – Test DHCP

3.5.7 Configuration des Private VLAN

Les PVLAN sont utilisés dans une DMZ dans le but de renforcer la sécurité en empêchant la propagation d'attaques de pirates informatiques à l'intérieur de la DMZ.

1. **Création des PVALN**
   Au niveau du switch Sw-DMZ, on a créé les PVLAN : primary, isolated et community comme le montre la figure 3.37.

```
Sw-DMZ(config)#vlan 500
Sw-DMZ(config-vlan)#proi
Sw-DMZ(config-vlan)#pr
Sw-DMZ(config-vlan)#private-vlan pr
Sw-DMZ(config-vlan)#private-vlan primary
Sw-DMZ(config-vlan)#pri
Sw-DMZ(config-vlan)#private-vlan a
Sw-DMZ(config-vlan)#private-vlan association 501,502
Sw-DMZ(config-vlan)#exit
Sw-DMZ(config)#vlan 501
Sw-DMZ(config-vlan)#pri
Sw-DMZ(config-vlan)#private-vlan co
Sw-DMZ(config-vlan)#private-vlan community
Sw-DMZ(config-vlan)#exit
Sw-DMZ(config)#vlan 502
Sw-DMZ(config-vlan)#private-vlan isolated
Sw-DMZ(config-vlan)#exit
```

FIGURE 3.37 – Création des PVLAN de la DMZ

2. **Association des PVLANs**
   La figure 3.38 montre l'association de PVLAN community avec le PVLAN primary. On procéde de même pour le PVLAN isolated.

```
Sw-DMZ(config)#interface  range ethernet 0/3, ethernet 1/0
Sw-DMZ(config-if-range)#sw
Sw-DMZ(config-if-range)#switchport mo
Sw-DMZ(config-if-range)#switchport mode pri
Sw-DMZ(config-if-range)#switchport mode private-vlan h
Sw-DMZ(config-if-range)#switchport mode private-vlan host
Sw-DMZ(config-if-range)#sw
Sw-DMZ(config-if-range)#switchport p
*Jun 19 16:21:06.532: %LINEPROTO-5-UPDOWN: Line protocol on Interface Et
hernet0/3, changed state to down
*Jun 19 16:21:06.533: %LINEPROTO-5-UPDOWN: Line protocol on Interface Et
hernet1/0, changed state to down
Sw-DMZ(config-if-range)#switchport pri
Sw-DMZ(config-if-range)#switchport private-vlan h
Sw-DMZ(config-if-range)#switchport private-vlan host-association 500 501
Sw-DMZ(config-if-range)#exit
*Jun 19 16:21:31.039: %LINEPROTO-5-UPDOWN: Line protocol on Interface Et
hernet0/3, changed state to up
*Jun 19 16:21:31.039: %LINEPROTO-5-UPDOWN: Line protocol on Interface Et
hernet1/0, changed state to up
Sw-DMZ(config-if-range)#exit
```

FIGURE 3.38 – Association de vlan community avec le vlan primary

3. **Attribution d'adresses aux serveurs de la DMZ**
   Au niveau de la DMZ, on a attribué les adresses ip respectivement la passerelle par défaut selon le plan suivant :

Serveur BDD : 172.16.0.2/24 172.16.0.1
Serveur ERP : 172.16.0.3/24 172.16.0.1172.16.0./24 172.16.0.1
Serveur WEB : 172.16.0.4/24 172.16.0.1
Serveur VoIP : 172.16.0.5/24 172.16.0.1

4. **Test de la configuration des PVLAN dans la DMZ**
   Les PVALN qui sont dans le même groupe peuvent se communiquer hors que c'est le contraire dans le PVLAN isolated.

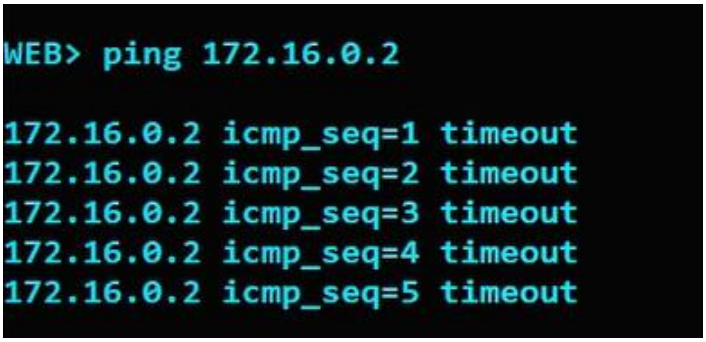

FIGURE 3.39 – Test de ping (ping ne marche pas)

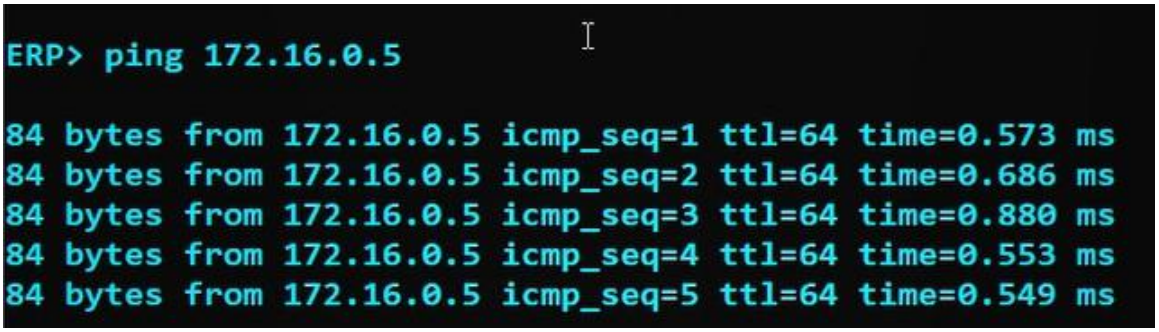

FIGURE 3.40 – Test du ping (ping réussi)

3.6 Conclusion

Au cours de cette étude, nous avons identifié des lacunes et des vulnérabilités potentielles dans les pratiques actuelles d'administration réseau et de sécurité de l'université de Béjaia. Nous avons proposé des améliorations pratiques pour renforcer la robustesse, la disponibilité et la résilience des réseaux, tout en garantissant la confidentialité et l'intégrité des données.

Conclusion générale

De nos jours l'administration et la sécurité des réseaux est primordiale. Afin d'améliorer la sécurité du réseau de l'université de Béjaia, à travers un stage au sein de centre des Systèmes et Réseaux d'Information, de Communication de Télé-enseignement et de l'Enseignement à Distance (CSRICTED) de l'universit, nous avons commencé tout d'abord par bien comprendre le rôle d'un administrateur et la valeur d'une bonne gestion dans le domaine, ainsi que l'importance de bien exploiter les outils d'administration et sécurité, afin d'arriver à définir les méthodes et les outils de cette gestion. Durant cette période nous avons pu cerner les différents points faibles et problèmes du réseau de l'université. Nous avons proposé des solutions afin d'améliorer l'infrastructure réseau opérationnelle et idéal, en s'appuyant sur la redondance des matériels et des liaisons tout en assurant la continuité du service.

Afin de mettre en œuvre ce projet, nous avons commencé par les configurations niveau 2 tous en configurant les liens trunks, les VLANs, le VTP et l'agrégation des liens. Par la suite nous avons approfondi les fonctionnalités des routeurs tels que HSRP. D'autre part, nous avons renforcer la sécurité dans la DMZ par la proposition des Private VLAN , nous avons également proposé quelques rôles pour la centralisation et la gestion des droits d'accès. Afin d'atteindre le résultat escompté, nous avons choisi de simuler notre réseau physique virtuel en utilisant GNS3 et VMware workstation pour les divers avantages qu'il présentent notamment la simplicité de la configuration des équipements et protocoles dont on a besoin.

Dans le cadre de notre projet de fin d'étude, nous avons également pu découvrir l'importance de la planification et de l'organisation dans l'administration réseau et la sécurité. Nous avons appris à élaborer des stratégies efficaces pour la gestion des ressources, la surveillance des activités du réseau et la résolution des problèmes potentiels. Nous avons réalisé l'importance d'établir des protocoles clairs et des procédures bien définies pour assurer la continuité des opérations et minimiser les risques de sécurité. De plus, nous avons eu l'occasion d'explorer différentes technologies et outils utilisés dans le domaine de l'administration réseau, tels que les pare-feux, les systèmes de détection d'intrusion et les dispositifs de sécurité avancés. Cette expérience nous a permis d'acquérir une vision plus large de l'administration réseau et de la sécurité, et de comprendre l'importance d'une approche proactive pour anticiper les problèmes potentiels et garantir la fiabilité et la sécurité du réseau.

Comme perspective future, il est envisageable de passer à l'automatisation de son administration réseau en utilisant les technologies de réseau défini par logiciel (SDN).

Bibliographie

[1] https ://www.lemagit.fr/conseil/Les-5-aspects-de-la-gestion-du-reseau [Consulté le 30 Juin 2023].

[2] http ://www.univ-bejaia.dz [consulté le 15 Avril 2023].

[3] Romain LEGRAND , André VAUCAMPS. Décembre 2014. CISCO :Notions de bases sur les réseaux. Paris : Editions ENI. ISBN 978-2-7460-9213-6.

[4] https://www.edrawsoft.com/fr/hierarchical-network-design.html [Consulté le 15 Avril 2023].

[5] HAGGAR.S, 2009. Conception de réseaux de campus [cours Master2 Pro STIC-Info]. France : Université Reims Champagne-Ardenne.

[6] https://www.inetdoc.net/articles/lan-segmentation/lan-segmentation.modele-hierarchique.html [consulté le 16 Vril 2023].

[7] YENDE R.G, 2019. Cours d'administration des réseaux informatique[support du cour].France : Institut supérieur du Bassin du Nill.

[8] https://www.ionos.fr/digitalguide/serveur/know-how/modele-client-serveur/[Consulté le 26 Avril 2023].

[9] https ://www.geeksforgeeks.org/client-server-model/[consulté le 26 Avril 2023].

[10] https://www.windows-active-directory.com/create-enable-disable-gpo.html [consulté le 29 Mai 2023].

[11] https ://www.fortinet.com/resources/cyberglossary/ldap-authentication [Consulté le 3 Mai 2023].

[12] https ://www.univention.com/blog-en/2019/03/brief-introduction-dhcp-dns/What-is-DNS [consulté le 20 Mai 2023].

[13] HOUHA.A, 2022.Technologie internet[support de cours]Béjaia.Université A.Mira.

[14] https://fr.slideshare.net/lechocokado/prsentation-etherchannel?next-slideshow=50249799 [consulté le 19 Mai 2023].

[15] https ://www.ibm.com/docs/fr/aix/7.3 ?topic=teaming-ieee-8023ad-link-aggregation-configuration [consulté le 19 Mai 2023].

[16] https://cisco.goffinet.org/ccna/redondance-de-liens/cisco-etherchannel-configuration-verification-depannage/[consulté le 19 Mai 2023].

[17] https://cisco.goffinet.org/ccna/disponibilite-lan/redondance-de-passerelle-host-standby-router-protocol-hsrp [consulté le 2 Mai 2023].

[18] https://www.cisco.com/c/fr-ca/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html [consulté le 2 Mai 2023].

[19] https://www.it-connect.fr/mise-en-place-du-protocole-hsrp/II-Etude-du-protocole [consulté le 4 Mai 2023].

[20] https://community.fs.com/fr/blog/understanding-virtual-lan-vlan-technology.html [consulté le 4 Mai 2023].

[21] https://forum.huawei.com/enterprise/fr/qu-est-ce-qu-un-vlan-natif/thread/667491274355261440-667481000260808704 [consulté le 6 Mai 2023].

[22] https ://www.ciscomadesimple.be/2014/03/20/trunk-dot1q-et-vlan-natif/[consulté le 6 Mai 2023].

[23] https://community.fs.com/fr/blog/what-is-private-vlan-and-how-it-works.html [consulté le 10 Mai 2023].

[24] https://www.cisco.com/c/fr-ca/support/docs/lan-switching/vtp/10558-21.pdf [consulté le 12 Mai 2023].

[25] https ://www.avast.com/fr-fr/c-what-is-a-firewall [consulté le 1 Mai 2023].

[26] Vincent REMAZEILLES, Février 2009. La sécurité des réseaux avec CISCO. Paris : Editions ENI. ISBN 978-2-7460-4714-3.

[27] https ://docs.oracle.com/cd/E19957-01/820-3154/nat-11/index.html [consulté le 25 Mai 2023].

[28] VMware, 2022. VMware worksation pro 17.0 [logiciel]. In : VMware[en ligne]. 17 Novembre 2022. [Consulté le 2 Avril 2023] Disponible sur l'adresse : https ://www.vmware.com/

[29] GNS3 Technologies INC, 2022 .GNS3 2.2.32[logiciel]. In : GNS3[en ligne]. 27Avril 2022. [Consulté le 2 avril 2023]. Disponible à l'adresse : https ://gns3.com/

[30] https ://www.microsoft.com [consulté le 02 Mai 2023]

Annexe

Les points suivants ont été abordés dans le cadre de l'étude et de l'analyse approfondie du réseau. L'objectif principal de cette étude et de cette analyse est d'identifier les problèmes, les lacunes et les opportunités d'amélioration du réseau, afin de proposer des solutions adaptées pour optimiser la performance, la sécurité et la gestion globale du réseau.

1) Quels sont les types de topologie physique utilisés?
2) Y a-t-il de la segmentation réseau VLAN? Combien de VLAN? Comment sont-ils utilisés?
3) Quels sont les types d'appareils connectés sur le réseau?
4) Quel est le nombre d'utilisateurs connectés sur le réseau? Quel est le modèle du trafic de réseau actuel?
5) Le réseau est t-il connecté sur internet ou pas?
6) Quelle est la politique de sécurité utiliser, soft et hard?
7) Y a-t-il des réseaux sans fil ? Quelles sont les méthodes d'authentification utilisées?
8) Quels sont les mécanismes d'administration réseau utilisés.
9) Quels sont les protocoles utilisés?
10) Est-ce les utilisateurs sont sensibilisés sur la cyber Security? Quels sont les antivirus utilisés?
11) Quels sont les types de supports de communication utilisés?
12) Quelles sont les stratégies adoptées pour la redondance et l'agrégation des liens?
13) Quelle est la stratégie adoptée pour la gestion d'accès?
14) Y a-il un sytème de détection et de prévention d'intrusion?
15) Les serveurs sont-ils accessibles via une connexion VPN? Est-ce qu'elle est chiffrée?
16) Quelles sont vos mesures de sécurité?
17) Disposez-vous d'une charte informatique?
18) Quelle est la stratégie adoptée en cas de crises?
19) Quelle est la stratégie des mots de passe adoptée?
20) Comment gérez-vous les pannes?

RÉSUMÉ

Dans ce mémoire, nous avons entrepris une étude approfondie de la gestion du réseau de l'université A. Mira de Béjaia, en nous basant sur une expérience pratique acquise lors d'un stage. Notre objectif était de critiquer la gestion actuelle du réseau et de proposer des solutions visant à améliorer son administration et sa sécurité. Pour ce faire, nous avons configuré des protocoles tels que HSRP, VTP et LACP, afin d'assurer une disponibilité maximale du réseau. De plus, nous avons renforcé la sécurité en utilisant des VLANs et des private VLANs, permettant ainsi un contrôle précis des accès au système et au réseau. La centralisation de la gestion des utilisateurs et la définition des droits d'accès ont également été mises en place pour assurer un contrôle total du système. Nous avons réalisé des tests et des simulations de ces solutions en utilisant des outils tels que GNS3 et VMware. Ces tests ont permis de valider l'efficacité et la fiabilité des solutions proposées.

Mots clés : Administration réseau, Université A.Mira de Béjaia, sécurité, HSRP, LACP, haute disponibilité, private VLAN.

ABSTRACT

In this thesis, we conducted a comprehensive study of the network management at A. Mira University of Bejaia. After completing a practical internship, we critically analyzed the existing network management and proposed solutions aimed at enhancing the administration and security of the network. We configured protocols such as HSRP, VTP, and LACP to ensure high availability. Furthermore, we strengthened security by implementing VLANs and private VLANs, enabling precise control over system and network access. Centralizing user management and defining access rights were also key steps to achieve complete control over the system. To validate the effectiveness and reliability of our solutions, we conducted extensive testing and simulations using tools such as GNS3 and VMware.

Key words Network administration, A. Mira University of Bejaia, security, HSRP, LACP, high availability, private VLAN.