République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
Université Abderrahmane Mira
Faculté de Technologie

Département d'Automatique, Télécommunications et d'Électronique

Projet de Fin d'Études

Pour l'obtention du diplôme de Master

Filière : Télécommunication.
Spécialité : Réseaux et télécommunications.

Thème

Mise en place d'un réseau LAN sécurisé et redondant au sein de l'entreprise Cevital.

Préparé par :

- M[lle] Thiziri ABID
- M Abderraouf ZENATI

Dirigé par :

M[me] K. MAMMERI

M[me] H. ZAREB

M S. MENNAD

Examiné par :

M[me] S. Zenadji

M[me] M. Gherbi

Année universitaire : **2023/2024**

Remerciements

En tout premier lieu, on remercie Allah de nous avoir offert l'opportunité d'acquérir des connaissances, de nous accorder la force, la guidance et la persévérance de développer nos compétences et de nous épanouir intellectuellement dans la poursuite de nos études supérieures.

Cher [M SLIMANI.M, M^{me} MAMMERI.K et M^{me} ZAREB.N],

Nous souhaitons exprimer notre profonde gratitude pour votre soutien inestimable et votre contribution précieuse tout au long de la réalisation de notre mémoire de fin d'études. Votre expertise, votre bienveillance et votre disponibilité ont joué un rôle déterminant dans la réussite de ce projet.

Cher Membre du Jury,

On est honorés d'avoir eu l'opportunité de présenter notre travail devant un panel d'experts tels que vous. On tient à vous remercier pour le temps que vous avez consacré à lire, analyser et évaluer attentivement notre mémoire.

Nous adressons nos sincères remerciements à tous les professeurs, intervenants et toutes les personnes qui, par leurs paroles, leurs écrits, leurs conseils et leurs critiques, ont guidé nos réflexions dans ce travail.

Nous aimerions également exprimer notre reconnaissance envers nos proches, nos familles et nos amis, pour leur soutien indéfectible, leurs encouragements constants et leur compréhension durant cette période exigeante. Leur présence et leurs encouragements nous ont permis de persévérer et de repousser nos limites.

Enfin, nous aimerions adresser nos remerciements les plus sincères à toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de notre mémoire. Votre appui moral, vos conseils avisés et votre confiance en notre travail ont été d'une importance capitale.

Nous vous sommes profondément reconnaissants pour votre soutien inestimable tout au long de ce processus académique. Votre contribution a grandement contribué à notre réussite.

Veuillez accepter nos plus sincères remerciements.

Cordialement,

ABID, ZENATI

Dédicaces

À mes chers parents,

Qui ont été ma source constante de soutien, d'encouragement et d'amour inconditionnel tout au long de mon parcours académique. Votre confiance en moi et votre soutien indéfectible ont été les piliers de ma réussite. Ce mémoire est dédié à vous, en reconnaissance de tout ce que vous avez fait pour moi.

À mes frères

Nassim et Mayas, ainsi qu'à ma sœur Maïssa, qui ont toujours été là pour me soutenir et m'encourager. Votre présence et vos encouragements constants ont été une source de motivation pour moi. Je vous dédie ce mémoire en témoignage de mon amour et de ma gratitude.

À ma cousine et meilleure amie

Dehia, qui a été à mes côtés dans les hauts et les bas de ce parcours. Ta présence, tes encouragements et ton soutien inconditionnel ont été d'une importance capitale pour moi. Cette dédicace test adressée avec gratitude et reconnaissance pour notre amitié précieuse.

À mes formidables amis, qui ont été à mes côtés tout au long de cette aventure académique. Votre présence, vos encouragements et votre soutien indéfectible ont été un réconfort précieux.

À mes professeurs et encadrants,

Qui ont partagé leur expertise, leur temps et leur passion pour l'apprentissage. Votre guidance, vos conseils avisés et votre engagement envers mon développement académique ont été d'une importance capitale. Je vous dédie ce mémoire en témoignage de ma reconnaissance et de mon respect.

Enfin, à moi-même,

Je tiens à exprimer ma satisfaction pour ma ténacité, ma résolution et mon ambition à atteindre le succès. Ce mémoire est le résultat de mes ardeurs, de mes longues heures de labeur et des renoncements consentis. Je ressens une profonde fierté vis-à-vis de mes réalisations et je m'engage fermement à poursuivre mon apprentissage et mon épanouissement dans ma carrière professionnelle.

Cette dédicace symbolise ma gratitude envers tous ceux qui ont contribué de près ou de loin à mon parcours d'études. Votre soutien, votre inspiration et votre influence ont été essentiels dans la réalisation de ce mémoire de fin d'études.

Thiziri Abid

Dédicaces

À mes chers parents,

Votre amour, votre soutien et votre sacrifice ont été inestimables tout au long de mon parcours d'études. Je vous dédie ce mémoire en témoignage de ma gratitude éternelle. Votre confiance en moi m'a donné la force de persévérer et d'atteindre mes objectifs.

À mes formidables amis,

Votre présence, vos encouragements et vos sourires ont illuminé mes journées d'études.

Merci d'avoir partagé cette aventure avec moi, de m'avoir soutenu et encouragé à donner le meilleur de moi-même. Ce mémoire est dédié à vous, en témoignage de notre amitié indéfectible.

À mes professeurs et encadrants,

Votre expertise, votre passion pour l'et votre dévouement m'ont inspiré tout au long de mon parcours académique. Je vous remercie pour vos précieux enseignements, vos conseils avisés et votre soutien constant. Cette dédicace vous est adressée en signe de reconnaissance et de respect.

Enfin, à moi-même,

Je tiens à me féliciter pour ma persévérance, ma détermination et ma volonté de réussir. Ce mémoire est le fruit de mes efforts, de mes heures de travail acharné et de mes sacrifices. Je suis fier de ce que j'accompli et je m'engage à continuer à apprendre et à grandir dans ma vie professionnelle.

Cette dédicace représente l'expression de ma gratitude envers tous ceux qui ont contribué à mon parcours d'études. Votre soutien, votre encouragement et votre présence ont été d'une importance capitale dans ma réussite.

Raouf Zenati

Table des matières

Liste des figures

Liste des tableaux

Liste d'abréviations

Abréviations	Significations
ACL	Access Control List.
ARP	Address Resolution Protocol.
BPDU	Bridge Protocol Data Units.
CAM	Content Addressable Memory.
CLI	Commande Langage Interface.
CSMA/CD	Carrier Sense Multiple Access with Collision Direct.
DHCP	Dynamique Host Configuration Protocol.
DMZ	Demilitarized Zone.
DNS	Domain Name System.
FDDI	Fiber Distributed Data Interface.
FTP	File Transfer Protocol.
HSRP	Hot Standby Router Protocol.
HTTP	Hyper Texte Transfer Protocole.
ID	Identificateur.
IOS	Internetwork Operating System.
IEEE	Institute of Electrical and Electronics Engineers.
IETF	Internet Engineering Task Force.
IP	Internet Protocol.
ISO	International Standardization Organization.
LAN	Local Area Network.
LSA	Link State Advertisement.
MAC	Media Access Control (Contrôle d’accès au support).
MAN	Metropolitan Area Network.
MAU	Multistation Access Unit.
OSI	Open System Interconnection.
OSPF	Open Shortest Path First.
PAN	Personal Area Network.
PC	Personal Computer.
PPP	Point-to-Point Protocol
PVST	Per Vlan Spanning Tree.
RJ45	Registered jack 45.
R-PVST	Rapid Per Vlan Spanning Tree.
RSA	Rivest-Shamir-Adleman.
SOCKS v5	SOCK et Secure Version 5
SSh	Secure Shell.
STP	Spanning Tree Protocol.
TCP/IP	Transmission Control Protocol/ Internet Protocol.

UDP	User Datagram Protocol.
VLAN	Virtual Local Area Network.
VPN	Virtual Private Network.
VSAT	Very Small Aperture Terminal.
VTP	Virtual Trunking Protocol.
WAN	Wide Area Network.
WI-FI	Wireless Fidelity.

Introduction générale

La sécurisation et la redondance d'un réseau local (LAN) revêtent une importance cruciale pour garantir la continuité des opérations et la sécurité des données au sein d'une organisation. Dans le cadre de ce projet, nous nous penchons sur l'entreprise Cevital, un acteur majeur de l'économie algérienne, et son initiative visant à moderniser son infrastructure réseau. Face aux défis rencontrés, tels qu'une architecture réseau mal adaptée et des performances suboptimales, l'entreprise a entrepris de revoir et d'améliorer sa configuration réseau.

Ce mémoire explore en profondeur l'architecture actuelle du réseau informatique de Cevital, en mettant en lumière les équipements utilisés, les topologies employées, ainsi que les protocoles critiques comme le Spanning-Tree Protocol (STP), le Hot Standby Router Protocol (HSRP), et l'Open Shortest Path First (OSPF). Nous proposons une nouvelle architecture réseau hiérarchique qui intègre des éléments de redondance pour assurer une disponibilité continue des services réseau et renforcer la sécurité des communications.

Chaque chapitre de ce rapport est conçu pour fournir une analyse détaillée de l'état actuel du réseau, des défis identifiés, et des solutions proposées. À travers des simulations et des tests approfondis, nous démontrons l'efficacité de notre approche dans la résolution des problèmes existants et dans la mise en place d'un réseau LAN sécurisé et redondant au sein de l'entreprise Cevital.

Afin de bien mettre en lumière la réalisation de notre projet, nous avons structuré notre mémoire en trois chapitres, comme suit :

- Le premier chapitre présente l'entreprise Cevital Bejaia, en détaillant les nombreux départements qui constituent son infrastructure. Nous y abordons également la problématique du réseau Cevital EL-KSEUR, qui est au cœur de notre projet.
- Le deuxième chapitre est consacré à la revue de quelques notions de base en réseaux informatiques, afin de faciliter la compréhension des concepts abordés dans le reste du mémoire.
- Le troisième chapitre propose une nouvelle configuration destinée à améliorer et à corriger les faiblesses du réseau existant en introduisant des protocoles tels que le STP, HSRP et OSPF.

Enfin, notre mémoire se conclut par une conclusion générale, résumant les connaissances acquises au cours de la réalisation de notre projet de fin d'études.

Chapitre 1 : Présentation de l’organisme d’accueil

1 Introduction

Dans ce chapitre, nous explorons l'infrastructure réseau de l'entreprise Cevital, en présentant son architecture actuelle et les défis rencontrés. Nous débutons par une vue d'ensemble de l'entreprise et de son réseau. Nous examinons ensuite les logiciels utilisés et mettons en œuvre les configurations établies. Enfin, nous évaluons les points forts, les faiblesses et les problématiques du réseau, posant ainsi les bases de notre projet.

2 Présentation de l’entreprise

Cevital, une entreprise pionnière fondée par ISSAD Rebrab en 1998, se distingue comme un leader de l'industrie agroalimentaire en Algérie. Dotée d'installations ultramodernes, elle opère dans divers secteurs, incluant la production de sucre, de corps gras, d'eau minérale, de boissons et de sauces. Grâce à ses efforts, l'Algérie est passée d'un statut d'importateur à celui d'exportateur dans des domaines tels que les huiles, les margarines et le sucre. Les produits de Cevital sont largement distribués à l'international, couvrant des marchés tels que l'Europe, le Maghreb, le Moyen-Orient et l'Afrique de l'Ouest.

Située à l'extrême-est du port de Bejaia, l'entreprise a considérablement élargi son empreinte au fil des années, avec plusieurs unités de production équipées de technologies de pointe. Son engagement envers l'innovation se manifeste dans ses projets de développement en cours. Au cours des cinq dernières années, elle a connu une croissance significative, devenant un important pourvoyeur d'emplois et de richesse pour la région.

Cette expansion se traduit par une augmentation remarquable de son effectif, passant de 500 employés en 1999 à 3996 en 2008, illustrant ainsi son engagement envers le développement économique et social de l'Algérie [1].

3 Infrastructure de l’entreprise Cevital

L'infrastructure industrielle de Cevital reflète son engagement et son expertise dans différents secteurs clés de l'industrie. Ses principales installations sont :

- 2 raffineries de sucre avec des capacités respectives de 3000 et 3500 tonnes.
- 1 unité de production de sucre liquide et une autre pour le sucre roux.

- 2 unités de conditionnement de sucre.
- 1 raffinerie d'huile.
- 1 unité de conditionnement d'huile.
- 1 margarinerie.
- 1 unité de production d'eau minérale et d'eau gazéifiée.
- 1 unité de fabrication et de conditionnement de boissons fruitées, ainsi que de production de conserves et de confitures.
- 1 unité de production des sauces.
- 1 unité de fabrication de chaux calcinée et de CO2.

Cevital est désormais le principal terminal de déchargement portuaire en Méditerranée grâce à sa possession de plusieurs silos portuaires et d'un terminal de déchargement ayant une capacité de 2000 tonnes par jour. [1]

4 Organigramme général de Cevital

L'organigramme global de la structure administrative de l'entreprise Cevital est représenté dans la **figure 1.1** :

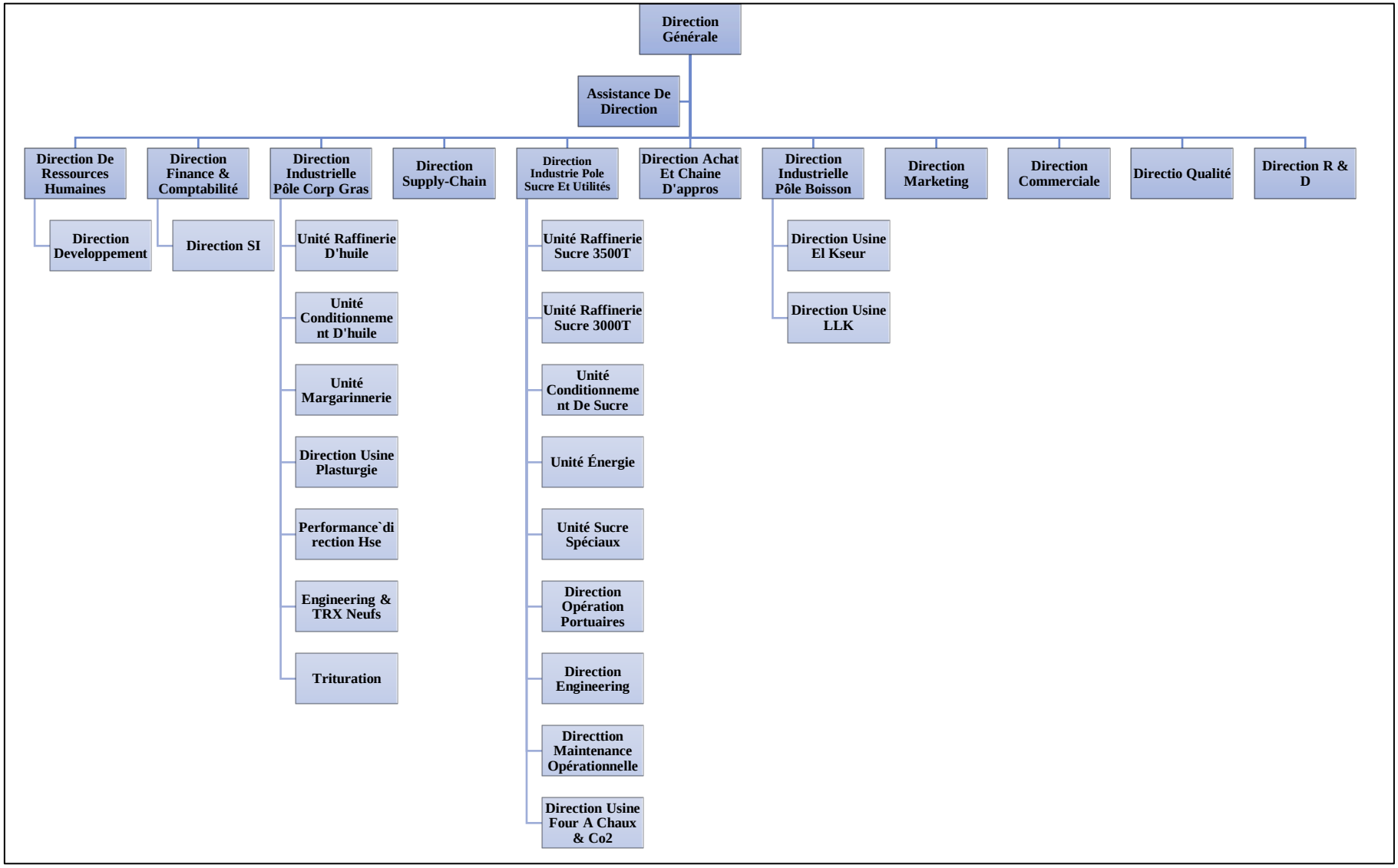


Figure 1.1 : Organigramme Général de CEVITAL [1].

5 Architecture du réseau informatique de CEVITAL

L'entreprise étudiée, Cevital, est dotée d'une infrastructure réseau complexe interconnectant plusieurs sites, dont nous examinerons ici la liaison entre deux sites spécifiques de Cevital, à savoir EL KSEUR et Béjaia. Cette connexion est cruciale pour assurer la communication sécurisée et efficace entre le réseau local du site EL KSEUR et la DMZ située au site de Béjaia. Ce réseau interne couvre différents secteurs de l'entreprise, de la production à la direction, en passant par les annexes. Il est composé de plusieurs éléments clés. Tout d'abord, un backbone, suivi d'un pare-feu et d'une zone démilitarisée (DMZ) pour la sécurité. L'infrastructure inclut également des points d'accès WIFI, des routeurs et un Datacenter hébergeant les serveurs de l'entreprise. Ces composants, majoritairement de marque Cisco comme les switchs, Catalysts et routeurs, sont interconnectés par des liaisons à fibre optique ou en cuivre, garantissant ainsi la robustesse et la fiabilité du réseau.

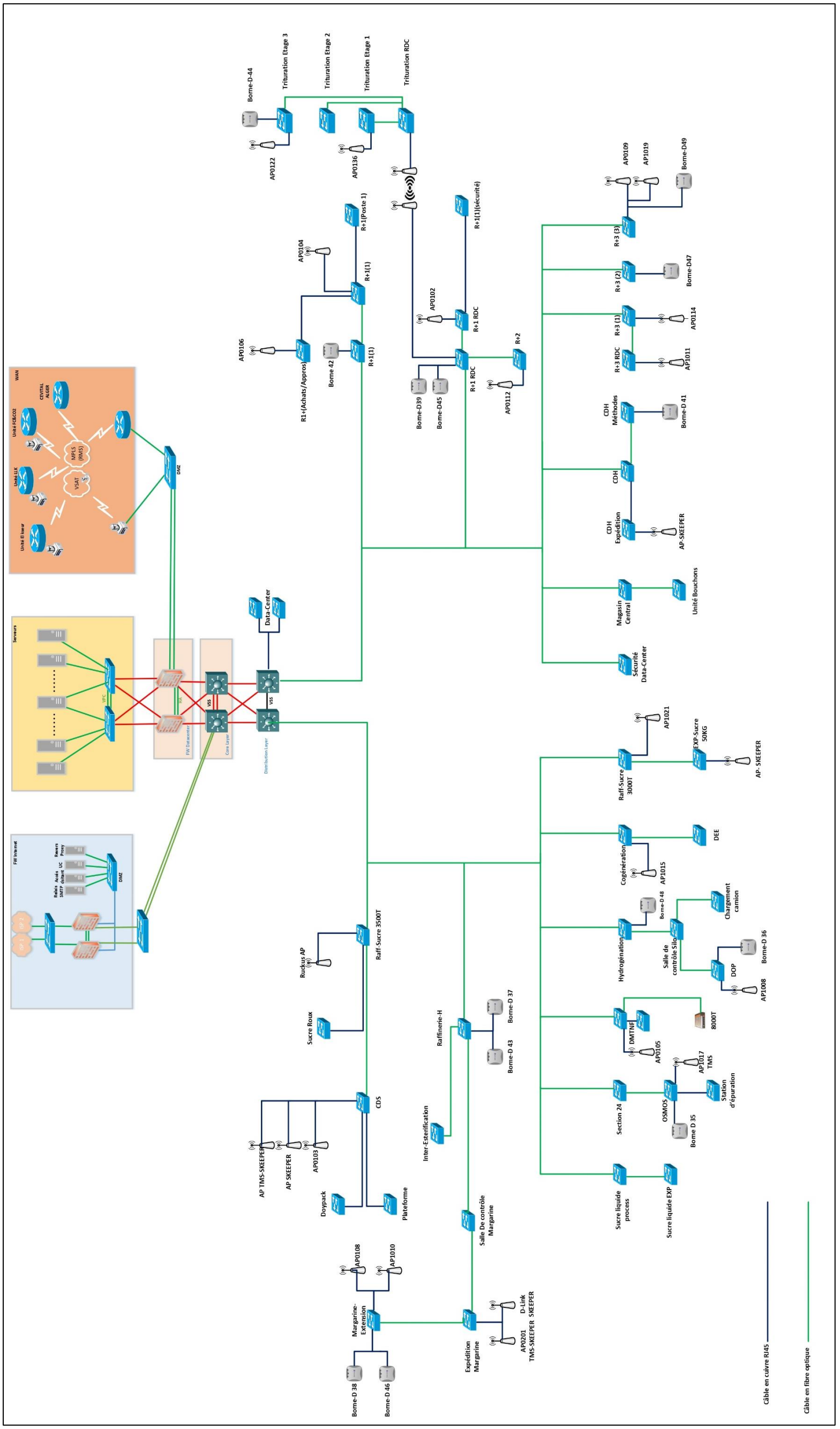


Figure 1.2 : Schéma du réseau informatique LAN & WAN de CEVITAL [1].

6 Architecture du réseau informatique de CEVITAL EL-KSEUR

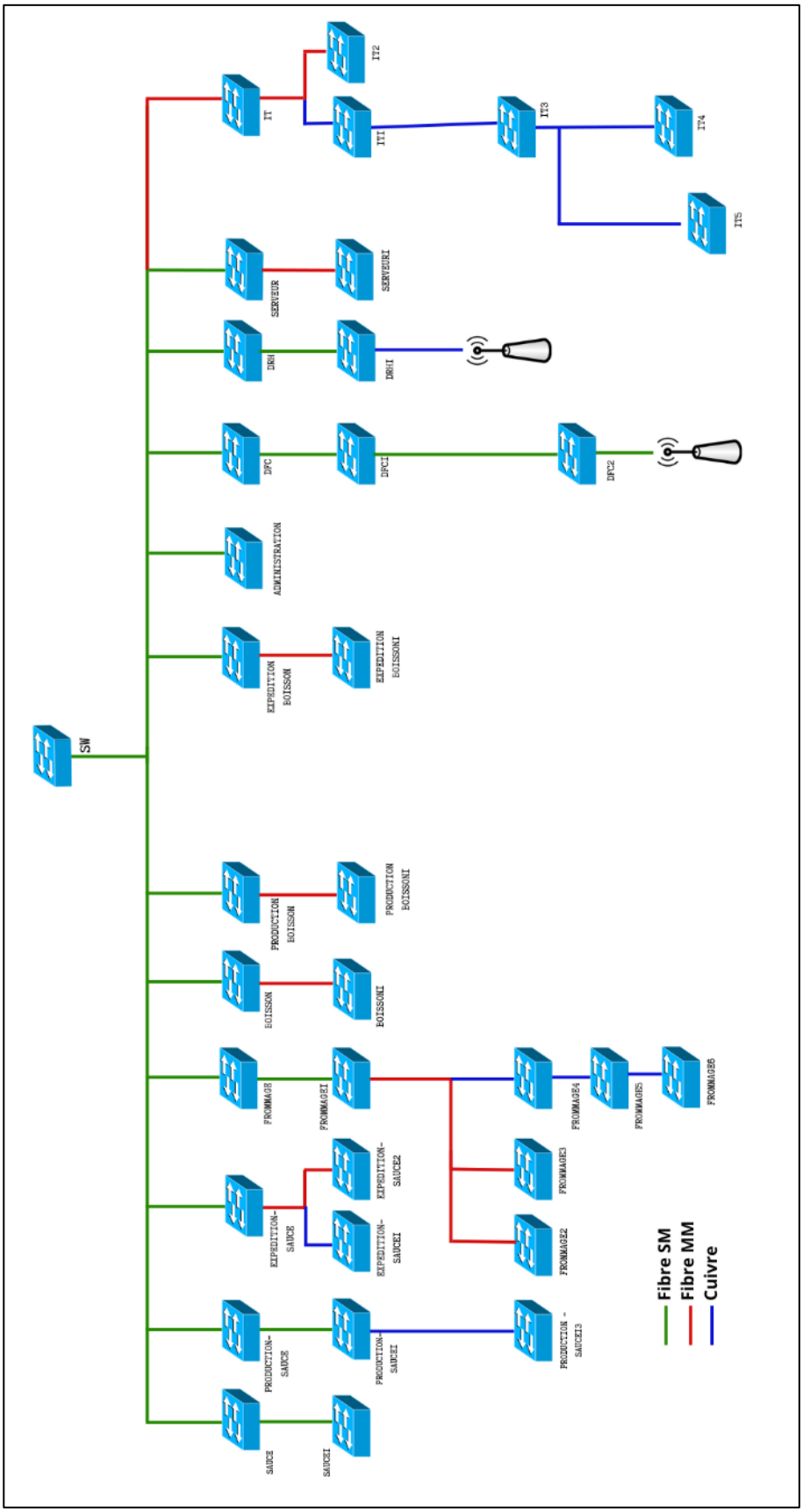


Figure 1.3 : Architecture du réseau informatique de Cevital EL-KSEUR [1]

7 Equipements utilisés dans l'architecture CEVITAL

Nous allons définir les différents équipements utilisés dans le réseau de l'entreprise Cevital **:**

Équipement	**Description**	**Utilisation**
Distributeur (backbone)	**Cisco Catalyst 4507R** - Le cœur du réseau, gérant le trafic de données intense, connectant les commutateurs d'accès, les pare-feu, les serveurs et les routeurs. Il assure le routage inter-VLAN et contrôle l'accès à Internet via un pare-feu, souvent associé à un serveur DHCP.	Gestion du trafic de données, routage inter-VLAN, contrôle d'accès à Internet.
Switch d'accès	**Cisco Catalyst 2960 et 2950** - Déployés dans divers bâtiments, connectés directement au distributeur via des câbles RJ-45, offrant chacun 24 ports.	Connexion des utilisateurs au réseau dans différents bâtiments.
Switch en cascade	**Cisco Catalyst 2950 et 2960** - Interconnectés en cascade pour former une couche, offrant aux utilisateurs un accès au réseau. VLANs configurés pour diviser le réseau en sous-réseaux adaptés aux différents services de l'entreprise.	Interconnexion des utilisateurs, segmentation du réseau en VLAN.
Routeur	**Cisco 2900** - Assurent le transfert efficace des données entre divers réseaux informatiques, agissant comme des passerelles. Dotés de fonctionnalités de sécurité avancées, gérant le trafic réseau et prenant en charge divers protocoles tels que IPv4, IPv6, OSPF, IGRP, et BGP. Modèles avec 2 ou 3 ports GE et un port SFP.	Transfert de données, sécurisation des communications, gestion du trafic réseau.
Point d'accès WIFI	Déploient une couverture réseau sans fil dans des zones spécifiques du site.	Fourniture de réseau sans fil aux utilisateurs dans des zones spécifiques.

Pare-feu	Assure la protection complète du trafic réseau en identifiant et en bloquant les flux indésirables. Utilisation de deux pare-feu en redondance pour isoler certaines parties du réseau et sécuriser l'accès à Internet. Débit global de 2 Gbits/s, capacité de prévention des menaces de 1 Gbits/s, débit VPN de 500 Mbits/s.	Sécurisation du réseau, filtrage de paquets, prévention des intrusions, gestion des communications via VPN.
Datacenter	Zone sécurisée avec accès limité, équipée de climatisation, alimentation redondante, contenant les serveurs, switch central, pare-feu, routeurs et système téléphonique standard.	Hébergement des serveurs, switch central, pare-feu, routeurs, et système téléphonique.

Tableau 1.1 : Equipements utilisés dans le réseau de l'entreprise Cevital.

8 La zone démilitarisé DMZ

La zone démilitarisée (DMZ) dans le contexte de l'infrastructure réseau de Cevital joue un rôle crucial en tant que couche intermédiaire de sécurité entre le réseau interne de l'entreprise et l'Internet. Elle est conçue pour héberger les services accessibles depuis l'extérieur, tout en minimisant les risques pour le réseau interne. Elle permet de publier des services vers l'extérieur, tels que les serveurs web, les serveurs de messagerie, et d'autres services accessibles par les utilisateurs externes et les partenaires de l'entreprise, sans exposer directement le réseau interne aux menaces potentielles.

9 Les liaisons inter-sites

Dans le cadre de la mise en place de la connectivité inter-sites visant à faciliter le partage des ressources et la communication interne au sein de l'organisation, CEVITAL a déployé des infrastructures de communication pour relier de manière efficace le site de Bejaïa à ses différentes annexes. Ces infrastructures comprennent :

- Une liaison point à point utilisant la technologie de fibre optique entre les sites de Bejaïa et Alger.
- Des connexions par satellite (VSAT) établies entre le site de Bejaïa et les sites d'EL Kser (Cojek), du site de Tizi-Ouzou (Lala Khadija) et d'El Khroub.

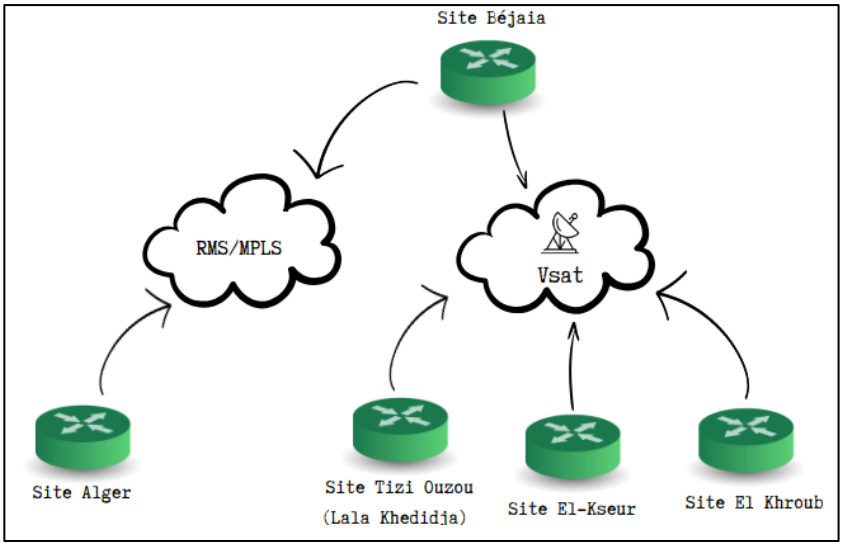


Figure 1.4 : Connexion inter-sites du site CEVITAL Bejaia.

10 Problématique

La gestion des réseaux informatiques au sein des grandes entreprises revêt une importance capitale pour garantir la disponibilité continue des services de collecte, de stockage, de traitement et de communication des données entre les collaborateurs. Cependant, cette gestion se trouve confrontée au défi de la dispersion géographique des effectifs, ce qui peut entraîner des ralentissements ou des interruptions dans les opérations, impactant directement l'efficacité et la productivité des équipes.

Dans le contexte spécifique de Cevital, qui vise à mettre en place un réseau LAN sécurisé et redondant, la question de la sécurité revêt une importance cruciale. Outre la continuité des opérations, il est essentiel de garantir la confidentialité, l'intégrité et la disponibilité des données sensibles de l'entreprise. Ainsi, la conception d'une infrastructure réseau adéquate devient cruciale pour maintenir la continuité des opérations au sein de Cevital. La question centrale réside dans la détermination de la topologie réseau optimale permettant de garantir une communication fluide malgré les pannes éventuelles des équipements, tout en assurant la connectivité des collaborateurs même à partir de sites distants.

11 Solution proposée

Suite à une analyse approfondie du réseau existant du site El Kseur, des solutions professionnelles et robustes ont été proposées pour optimiser son infrastructure. L'approche stratégique comprend :

- L'adoption d'une architecture réseau basée sur 5 switchs de niveau 3, renforcée avec un protocole de routage OSPF (Open Shortest Path First) pour une connectivité performante et redondante.

- Le déploiement du protocole de haute disponibilité HSRP (Hot Standby Router Protocol) au niveau de la couche core pour assurer une continuité opérationnelle en cas de défaillance.
- L'établissement d'une connexion directe des switchs aux backbones de distribution pour réduire les risques de pannes liés à une interconnexion en cascade.
- L'intégration d'un pare-feu pour renforcer la sécurité du réseau en filtrant le trafic entrant et sortant.
- La mise en place de connexions vers les routeurs Algérie Télécom pour établir des liaisons de fibre optique point à point entre Bejaïa et le site distant d'EL Kser (Cojek), améliorant ainsi la connectivité sécurisée.

Ces solutions garantiront :

- ✓ Une connectivité réseau robuste et redondante.
- ✓ La sécurité des données de Cevital.
- ✓ Une évolutivité adaptée aux besoins futurs.

12 Conclusion

Cette section a permis d'appréhender l'ensemble du réseau informatique de Cevital et d'identifier des problématiques majeures ayant mené à une solution proposée. Celle-ci se concentre essentiellement sur une refonte architecturale du réseau, l'intégration de mécanismes de haute disponibilité et de sécurité, ainsi que l'établissement de connexions inter-sites pour une meilleure connectivité et une résilience accrue du système.

Chapitre 2 : État de l’art sur les réseaux informatiques

1 Introduction

Ce chapitre se concentre sur l'état de l'art des réseaux informatiques. Nous commencerons par une définition précise du concept de réseau, suivi d'une exploration approfondie des modèles OSI et TCP/IP qui forment la base des communications réseau modernes. Nous examinerons également les équipements fondamentaux nécessaires au bon fonctionnement d'un réseau informatique et nous plongerons dans les détails des protocoles des réseaux informatiques.

2 Définition d’un réseau informatique

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site centrale puis des ordinateurs entre eux et enfin des machines terminales, telles que stations de travail ou serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd’hui, l’intégration de la parole téléphonique et de la vidéo est généralisée dans les réseaux informatiques [2].

3 Intérêt d’un réseau

Un réseau informatique peut servir plusieurs buts distincts [3] :

- Le partage de ressources (fichiers, applications ou matériels).
- La communication entre personnes (courrier électronique, discussion en direct, etc.).
- La communication entre processus (entre des machines industrielles par exemple).
- La garantie de l’unicité de l’information (bases de données).
- Le jeu vidéo multijoueur.

4 Classification des réseaux informatiques

On distingue généralement quatre catégories de réseaux informatiques, différenciées par la distance maximale séparant les points les plus éloignés du réseau [2] :

- Les réseaux personnels, ou PAN (Personal Area Network), interconnectent sur quelques mètres des équipements personnels tels que terminaux GSM, portables, organiseurs, et autres dispositifs personnels d'un même utilisateur.
- Les réseaux locaux, ou LAN (Local Area Network), correspondent par leur taille aux réseaux intra-entreprise. Ils servent au transport de toutes les informations numériques de l’entreprise. En règle générale, les bâtiments à câbler s’étendent sur

plusieurs centaines de mètres. Les débits de ces réseaux vont aujourd'hui de quelques mégabits à plusieurs centaines de mégabits par seconde

- Les réseaux métropolitains, ou MAN (Metropolitan Area Network), permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole. Ils doivent être capables d'interconnecter les réseaux locaux des différentes entreprises pour leur donner la possibilité de dialoguer avec l'extérieur
- Les réseaux étendus, ou WAN (Wide Area Network), sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et il utilise en ce cas des infrastructures au niveau du sol, essentiellement de grands réseaux de fibre optique, soit hertzien, comme les réseaux satellite.

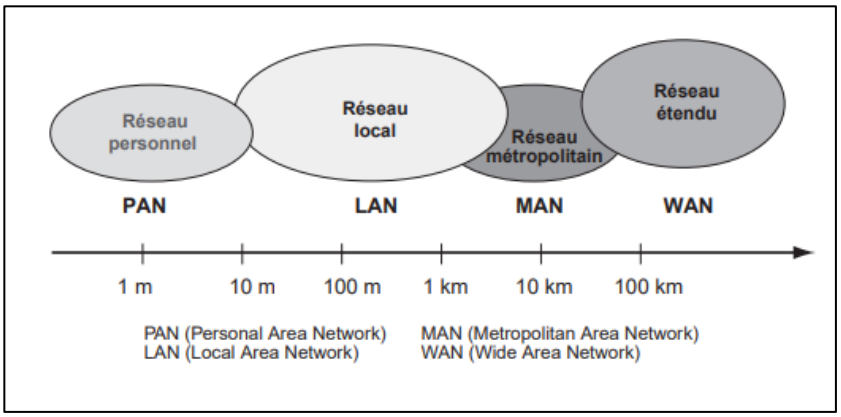


Figure 2.1 : Les grandes catégories de réseaux informatiques

5 Architectures réseau

En élargissant le contexte de la définition du réseau aux services qu'il apporte, il est possible de distinguer deux modes de fonctionnement [3] :

- **L'architecture de type client-serveur**, où un ordinateur (serveur) fournit des services réseau aux ordinateurs clients.
- **L'architecture d'égal à égal** (peer to peer, parfois appelée « poste à poste »), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur joue un rôle similaire,

6 Les topologies des réseaux informatiques

À partir des trois topologies de base : le bus, l'anneau et l'étoile, de nombreuses versions sont possibles. Il faut distinguer la topologie physique de la topologie logique. La première caractérise la manière dont est réalisé le câblage du réseau local (la structure des chemins de câbles, le type de raccordement…) ; la seconde décrit comment on attribue le droit à la parole

entre toutes les stations. La topologie logique définit la méthode d'accès au support (ou niveau MAC) utilisée [4].

6.1 Les topologies physiques

On distingue généralement les topologies suivantes :

6.1.1 Topologie en bus

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câbles, généralement de type coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau. Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté [3].

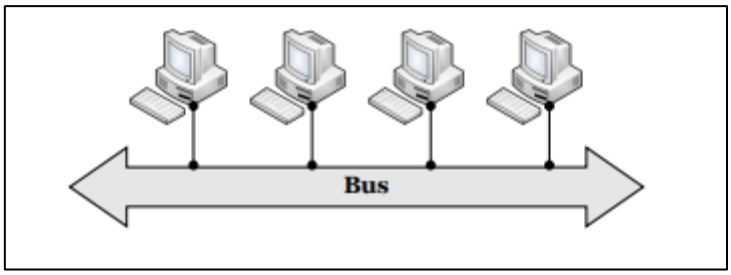


Figure 2.2 : Topologie en bus [5].

6.1.2 Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (hub, littéralement moyeu de roue). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs. Le concentrateur a pour rôle d'assurer la communication entre les différentes jonctions. Comparativement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.

En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le concentrateur) [3].

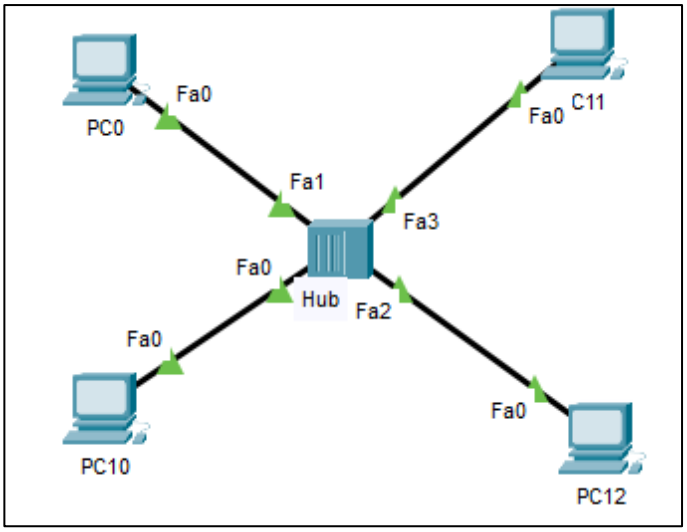


Figure 2.3 : Exemple de topologie en étoile.

6.1.3 Topologie en anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont théoriquement situés sur une boucle et communiquent chacun à leur tour.

Ils sont en réalité reliés à un répartiteur (MAU, Multistation Access Unit) qui va gérer la communication entre eux en impartissant à chacun un « temps de parole » [3].

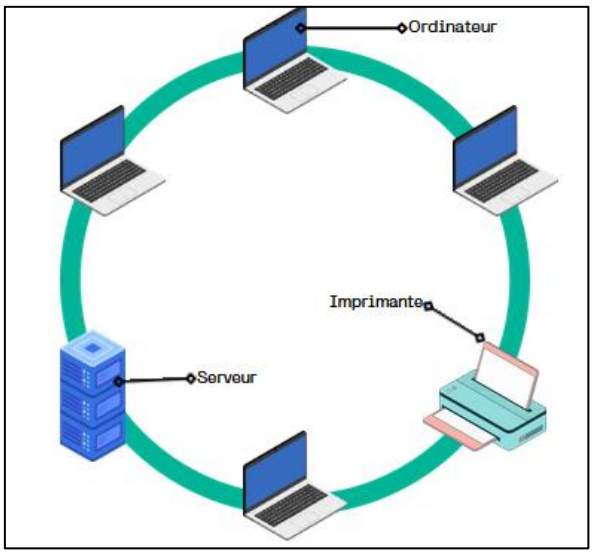


Figure 2.4 : Topologie en anneau.

6.1.4 Topologie en maille

Un réseau maillé est une topologie où chaque hôte est connecté en pair-à-pair sans qu'il y ait de hiérarchie centrale, formant ainsi une structure de type réseau. Dans ce type de configuration, chaque nœud est capable de recevoir, envoyer et relayer des données, ce qui évite les points uniques de défaillance qui pourraient isoler des parties du réseau en cas de panne.

En cas de défaillance d'un hôte, les données peuvent être reroutées à travers d'autres chemins disponibles dans le réseau maillé, assurant ainsi la continuité de la transmission des données.

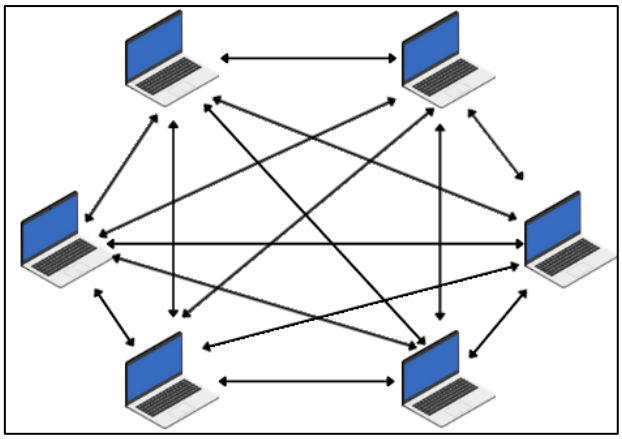


Figure 2.5 : Topologie complétement maillé.

6.2 Les topologies logiques

La topologie logique, par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI (Fiber Distributed Data Interface) [3].

7 Caractéristiques des réseaux

7.1 Supports de transmissions

Les réseaux locaux utilisent tous les types de support : les câbles cuivre (coaxial, paires torsadées), les supports optiques (fibre optique) et les supports hertziens (réseaux sans fil). Le câble coaxial a longtemps été utilisé (réseaux de type Ethernet), mais il est aujourd'hui remplacé par la paire torsadée moins chère et plus facile à installer. La fibre optique est essentiellement réservée aux réseaux haut débit et à l'interconnexion de réseaux [5].

Le tableau 2.1 résume les différents supports de transmission utilisés pour établir une ligne de transmission entre deux machines, chacun ayant ses propres caractéristiques et utilisations spécifiques.

Type de câble	Immunité électromagnétique	Débit courant	Utilisation
Coaxial	Bonne	10 Mbit/s	Ethernet, en milieu perturbé ou confidentiel.

Paires torsadées UTP	Faible	10 à 100 Mbit/s	Ethernet sur paires torsadées
Paires torsadées FTP	Moyenne	10 à 100 Mbit/s	Ethernet sur paires torsadées, Token Ring
Fibre optique	Excellente	100 à 155 Mbit/s	FDDI

Tableau 2.1 : Les différents support de transmissions et leurs caractéristiques [5].

7.2 Les équipements de base d'un réseau informatiques

On appelle ainsi les matériels connectés au réseau, mais qui ne sont pas des hôtes. Ils portent une appellation différente selon leur niveau d'intelligence ou le rôle qu'ils jouent, qui sont [6] :

Équipement	Description
Carte réseau	Interface physique entre l'ordinateur et le support de communication. Nécessaire pour qu'un ordinateur soit connecté au réseau [6].
Concentrateur (Hub)	Dispositif qui reçoit un signal sur une entrée et le diffuse vers tous les ports de sortie. Utilisé pour interconnecter des réseaux locaux et longue distance.
Répéteur	Amplifie et répète les trames pour étendre la portée du réseau au-delà des limitations physiques du câblage [2].
Pont (Bridge)	Connecte les réseaux en redirigeant les trames via des algorithmes ou des tables de routage, créant des réseaux virtuels et filtrant les trames inutiles [2].
Commutateur (Switch)	Boîtier de niveau 2 avec plusieurs prises RJ45, utilise l'adresse MAC pour aiguiller une trame vers la bonne machine en se basant sur la table CAM (Content Addressable Memory) [7].
Routeur	Composant de niveau 3 qui connecte plusieurs réseaux en guidant les paquets entre eux via différentes interfaces, acceptant de transmettre des paquets non destinés [7].

Passerelle (Gateway)	Relie des réseaux totalement différents, assurant une compatibilité au niveau des protocoles de couches hautes entre réseaux hétérogènes [4].

Tableau 2.2 : Les équipements de Base d'un Réseau Informatique.

8 Les modèles de réseaux OSI - TCP/IP

8.1 Le modèle OSI

L'ISO (International Standardization Organization) a normalisé sa propre architecture sous le nom d'OSI (Open Systems Interconnection) [2].

Celui-ci définit un modèle en 7 couches réseau, présentes sur chaque station qui désire transmettre. Chaque couche dispose de fonctionnalités qui lui sont propres et fournit des services aux couches immédiatement adjacentes [8].

Les rôles des différentes couches sont d´écrits comme suit [9] :

- **La Couche Physique** d´définit la façon dont les données sont physiquement converties en signaux numériques sur le média de communication (impulsions électriques, modulation de la lumière, etc.).
- **La Couche Liaison de** Données d´définit l'interface avec la carte réseau et le partage du média de transmission.
- **La Couche Réseau** permet de gérer l'adressage et le routage des données, c'est-à-dire leur acheminement via le réseau.
- **La Couche Transport** est chargée du transport des données, de leur découpage en segments et de la gestion des ´éventuelles erreurs de transmission. – La Couche Session d´définit l'ouverture et la fermeture des sessions de communication entre les machines du réseau.
- **La Couche présentation** d´définit le format des données manipulées par le niveau applicatif (leur représentation, ´éventuellement leur compression et leur chiffrement) indépendamment du système.
- **La Couche Application** assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, gère directement par les logiciels.

8.2 Le modèle TCP/IP

Le protocole TCP/IP, développé à l'origine par le ministère de la Défense américaine en 1981, représente une évolution du concept préalablement utilisé partiellement pour le réseau historique ARPANET en 1972. Il est largement utilisé dans les réseaux Internet. Outre son

contexte historique, le succès du protocole TCP/IP découle également de son autonomie vis-à-vis de tout fabricant informatique [10].

Les deux principaux protocoles qui définissent l'architecture du TCP/IP sont les suivants [10] :

- IP (Internet Protocol), au niveau réseau, offre un service sans connexion, assurant le routage des données à travers le réseau.
- TCP (Transmission Control Protocol), au niveau transport, fournit un service fiable avec connexion, garantissant la livraison ordonnée et sans erreur des données entre les applications sur des machines distantes.

Tout comme le modèle OSI, l'architecture TCP/IP utilise également un modèle en couches pour organiser les opérations réseau. Cependant, elle simplifie ce modèle en regroupant certaines fonctionnalités, ce qui aboutit généralement à quatre couches principales :

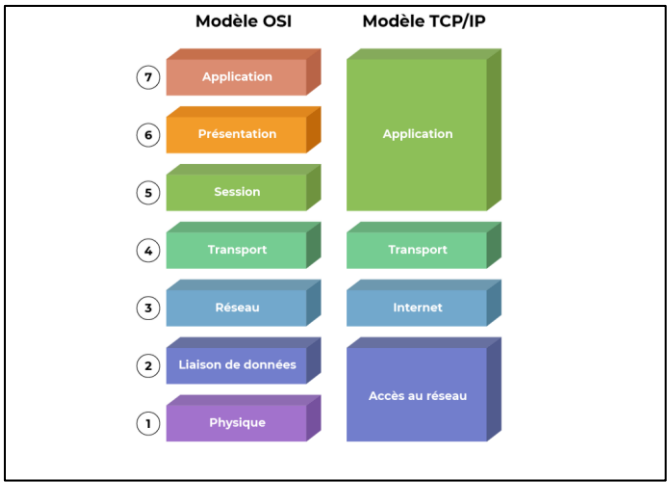


Figure 2.6 : Comparaison des modèles OSI et TCP/IP [W2].

Le modèle OSI présente une organisation structurée en sept couches distinctes, fournissant ainsi une vue détaillée des opérations réseau. En revanche, TCP/IP simplifie cette organisation en fusionnant certaines couches afin d'améliorer les performances globales du système. Malgré cette simplification, TCP/IP est capable de distinguer ces couches dans des situations spécifiques afin de répondre de manière précise aux exigences particulières du réseau.

9 Réseaux locaux virtuels (VLAN)

Un VLAN est un réseau local regroupant un ensemble de machines de façon logique et non physique. En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLAN), il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes

d'adressage...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.) [3].

9.1 Typologie de VLANs

Plusieurs types de VLAN sont définis par les normes IEEE 802.1, selon le critère de commutation et le niveau auquel il s'effectue [3] :

- **Un VLAN de niveau 1** (aussi appelé VLAN par port ou Port Based VLAN) définit un réseau virtuel en fonction des ports de raccordement sur le commutateur.
- **Un VLAN de niveau 2** (également appelé VLAN MAC, VLAN par adresse MAC Address-Based VLAN) définit un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.
- **Un VLAN de niveau 3** on distingue plusieurs types de VLAN de niveau 3 :
  - Le VLAN par sous-réseau (Network Address-Based VLAN) associe des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
  - Le VLAN par protocole (Protocol-Based VLAN) permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk...), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

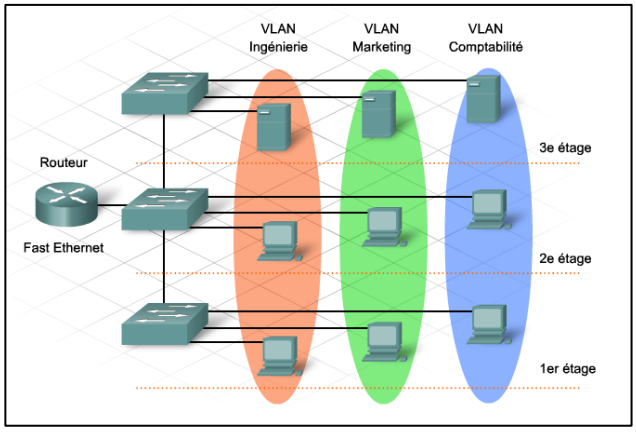


Figure 2.7 : Les réseaux locaux virtuels [W3].

9.2 Les avantages du VLAN

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants [3] :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs.
- Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.
- Réduction de la diffusion du trafic sur le réseau.

10 Les protocoles réseaux

10.1 Le protocole VTP (Vlan Trunking Protocol)

Ce protocole permet en effet aux switchs de diffuser les informations relatives aux VLANs pour les ports trunk à l'ensemble du réseau. Il permet ainsi de simplifier l'administration des VLANs en assurant une configuration centralisée des VLANs à travers le réseau. Il fonctionne avec une architecture client-serveur [11].

10.1.1 Mode de fonctionnement

Le protocole VTP (VLAN Trunking Protocol) est utilisé pour administrer les VLANs sur un réseau en permettant leur diffusion sur l'ensemble des ports trunk des switchs. Il est propriétaire de la marque CISCO et suit une architecture client-serveur. Le serveur maintient une table des VLANs déclarés, qui est diffusée aux clients appartenant au même domaine VTP. Toute modification apportée à la table est répercutée sur l'ensemble des clients, ce qui permet à tous les VLANs définis sur le serveur de circuler sur les ports trunk des switchs clients (sauf si des configurations spécifiques ont été appliquées sur les interfaces). Les matériels peuvent être en mode :

- **Server** Il est associé à un domaine VTP. La déclaration des VLANs s'effectue sur le serveur.

  Il tient à jour la liste des VLANs déclarés et la diffuse à l'ensemble des clients.
- **Client** Il est associé à un domaine VTP. Il reçoit la liste des VLANs, il la propage aux autres clients auxquels il est connecté et met à jour sa propre liste.
- **Transparent** Il est associé à aucun domaine VTP. Sa liste de VLAN est locale et n'est pas mis à jour lorsqu'il reçoit une trame VTP. Cependant il propage les listes de VLAN qu'il reçoit.

10.2 Le protocole DHCP (Dynamic Host Control Protocol)

Ce protocole permet aux administrateurs de réseaux TCP/IP de configurer les postes clients de façon automatique. Il a été utilisé par les fournisseurs d'accès à l'Internet par le câble, mais a été abandonné au profit d'une connexion point à point type PPP, comme pour l'ADSL.

DHCP reste cependant un protocole de configuration de clients extrêmement pratique sur un réseau local Ethernet. DHCP offre les avantages suivants [12].

10.2.1 Configuration d'adresse IP fiable

DHCP réduit les erreurs de configuration causées par la configuration manuelle des adresses IP, telles que les erreurs typographiques ou les conflits d'adresses provoqués par l'affectation d'une adresse IP à plusieurs ordinateurs en même temps.

10.2.2 Administration réseau réduite

DHCP inclut les fonctionnalités suivantes pour réduire l'administration réseau :

- ✓ Configuration TCP/IP centralisée et automatisée.
- ✓ Possibilité de définir des configurations TCP/IP à partir d'un emplacement central.
- ✓ Possibilité d'affecter une plage complète de valeurs de configuration TCP/IP supplémentaires au moyen d'options DHCP.
- ✓ Gestion efficace des modifications d'adresses IP pour les clients qui doivent être mis à jour fréquemment, comme ceux des appareils portables qui se déplacent vers différents emplacements sur un réseau sans fil.
- ✓ Le transfert des messages DHCP initiaux à l'aide d'un agent de relais DHCP, ce qui élimine la nécessité d'un serveur DHCP sur chaque sous-réseau

10.3 Le protocole STP (Spanning Tree Protocol)

La redondance améliore la disponibilité de la topologie du réseau en supprimant le risque de points de défaillance uniques dans un réseau, par exemple, une panne d'un commutateur ou d'un câble du réseau. Lorsqu'une architecture redondante est introduite dans une conception de couche 2, des boucles et des trames en double peuvent apparaître, les conséquences peuvent être dramatiques pour le réseau. Le protocole STP a été conçu afin de résoudre ces problèmes [9].

Le STP (Spanning Tree Protocol) est un protocole de couche 2 (liaison de données) conçu pour les commutateurs. Le standard STP est défini dans le document 802.1d. Il permet de créer un chemin sans boucle dans un environnement commuté et physiquement redondant. STP détecte et désactive ces boucles et fournit un mécanisme de liens de sauvegarde [9].

Dans un réseau commuté on procède à une élection machinale d'un switch maître (root bridge) par le STP. L'élection de ce root bridge sera faite en fonction des numéros de priorité configurés.

Dans le cas de priorité égale on se tournera vers l'adresse MAC la plus basse. Après ça sera au tour de la désignation des ports racine (root port), qui se trouvent être le port avec la «

distance » la plus courte vers le commutateur racine. Chaque commutateur possède un seul root port qui est choisi d'après le coût du trajet vers le root bridge. Pour finir il y'aura ce qu'on appelle la détermination des ports désignés, ça consiste à designer le port relié au segment qui mène le plus directement à la racine. Les ports restants seront bloqués.

Les BPDU (Bridge Protocol Data Unit) sont les diffuseurs de toutes informations du protocole STP, ils servent à conserver une empreinte des changements sur le réseau dans le but d'activer ou de désactiver les ports voulus et déterminer la topologie du réseau [13].

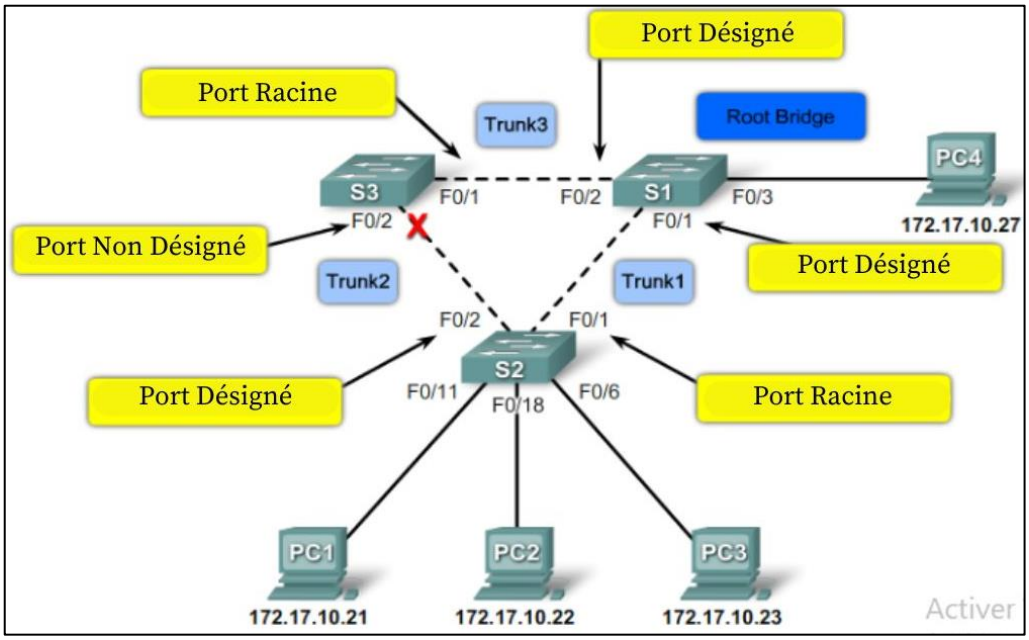


Figure 2.8 : Exemple pour le STP.

10.3.1 États des ports

Les états opérationnels des ports participant à un réseau local sont différents d'un commutateur classique. Des états supplémentaires sont nécessaires pour éviter une boucle et pour limiter l'installation lors du processus de vote ou de changement de topologie. Il existe cinq états [14] :

- ✓ **Désactivé (Disabled)** Le port est complètement non fonctionnel, ce qui signifie qu'il ne peut ni recevoir ni transmettre de trame.
- ✓ **Blocage (Blocking)** Le port n'est ni un port désigné ni un port racine, mais il est reconnu comme un port alternatif par rapport à la racine. Il n'apprend pas les adresses, ne transmet pas les trames ni les BPDUs, mais il peut écouter les BPDUs envoyés car il pourrait être activé un jour.
- ✓ **Écoute (Listening)** Ce port est en cours de préparation pour l'activité en sortant de l'état de blocage. Il n'apprend ni ne transmet les adresses, mais envoie et reçoit des BPDUs. Il participe au vote, mais il pourrait ne pas y participer lors de la sélection.

- ✓ **Apprentissage (Learning)** Ce port sera actif pour la transmission de trames mais doit attendre que le délai de transfert (généralement 15 secondes) expire. Cela permet au port d'ajouter des entrées dans sa table de filtrage pour ne pas inonder les ports lorsqu'il passe à l'état de transfert.
- ✓ **Transfert (Forwarding)** Ce port fonctionne comme n'importe quel autre port de commutation en apprenant et en transférant les trames.

10.3.2 PVST (Per-VLAN Spanning Tree)

Le PVST (Per-VLAN Spanning Tree) est un mode fonctionnement mis en place par Cisco. Il permet au STP dans un réseau qui contient plusieurs VLAN d'agir de manière indépendante sur chacun des VLAN séparément. Il est capable d'effectuer un équilibrage de charge de couche 2 en transférant une partie du trafic VLAN sur une liaison d'assemblage et un autre trafic VLAN sur une autre liaison d'assemblage [13].

10.3.3 Rapid PVST (Rapid Per VLAN Spanning Tree)

R-PVST est une technologie de commutation réseau développée par Cisco qui combine les avantages du Rapid Spanning Tree Protocol (RSTP) avec ceux du Per VLAN Spanning Tree Protocol (PVST). Rapid PVST crée un arbre de recouvrement distinct pour chaque VLAN, permettant une gestion indépendante et efficace du trafic réseau pour chaque VLAN. Il utilise les mécanismes de convergence rapide de RSTP pour minimiser les temps de rétablissement en cas de changement de topologie, assurant ainsi une connectivité rapide et fiable au sein du réseau.

10.4 Le protocole OSPF (Open Shortest Path First)

L'algorithme SPF (Shortest Path First) calcule le plus court chemin vers toutes les destinations de la zone ou du système autonome, en partant du routeur où s'effectue le calcul (à partir de sa base de données topologiques). Il utilise un algorithme conçu par Dijkstra et calcule le plus court chemin, selon un critère de coût où interviennent de multiples paramètres : l'état des liens, l'encombrement du réseau et des mémoires des routeurs intermédiaires [4].

10.4.1 Principe de fonctionnement

Le calcul du plus court chemin est effectué de manière indépendante par tous les routeurs internes d'un système autonome SA. Grâce à cet algorithme, un routeur peut connaître le prochain routeur qui transmettra le message : il trouve les plus courts chemins (en termes de coût) d'un point à un autre, pour que le message arrive de manière optimale à son destinataire, puis il effectue la mise à jour de sa table de routage. Chaque mise à jour de la base de données

entraîne celle de la table de routage. Il y a, comme précédemment, communication entre les routeurs. Celle-ci est régie par le protocole OSPF.

Ce protocole définit les règles et les formats de messages entre routeurs OSPF internes à un système autonome. Il a la particularité de s'appuyer directement sur IP non sur UDP. C'est une nette amélioration, car le routage devient un traitement interne à la couche réseau et n'est plus considéré comme une application [4].

10.4.2 Messages du protocole OSPF

On distingue cinq messages OSPF : hello, description de base de données, requête d'état de lien, mise à jour d'état de lien, acquittement d'état de lien. Ils transportent des informations sur l'état des liaisons du SA et servent à déterminer une fonction de coût plus efficace que dans RIP.

Un routeur OSPF émet des messages hello à intervalles réguliers (environ toutes les dix secondes), sur chacune de ses interfaces. Ces messages établissent les relations d'adjacence avec les routeurs directement liés à l'émetteur de ces messages. Les routeurs qui les ont reçus vérifient que les chemins restent disponibles.

Sur un réseau possédant au moins deux routeurs, on élit un routeur désigné, c'est-à-dire le responsable qui échange avec les routeurs des réseaux voisins. Il s'occupe de la distribution des messages de mise à jour d'état de lien. Son choix se fait sur la base de la plus petite adresse IP parmi les routeurs susceptibles d'assumer ce rôle. Deux routeurs R1 et R2 établissent une relation d'adjacence si et seulement s'ils sont reliés par un lien direct ou si l'un d'entre eux est routeur désigné. Lorsqu'une nouvelle adjacence s'établit entre deux routeurs, ils synchronisent leurs bases de données d'état des liens par le message description de base de données.

OSPF est aujourd'hui le protocole interne le plus utilisé dans Internet. La qualité des informations transportées et la sécurité associée sont ses principaux atouts. Le fait que le routage reste interne à la couche réseau est un élément d'efficacité supplémentaire [4].

10.5 Le protocole HSRP (Hot Strandby Router Protocol)

Le protocole HSRP ou Hot Standby Routing Protocol, est un protocole propriétaire Cisco. Il permet de gérer la redondance de routeur pour que lorsqu'un routeur tombe en panne un routeur de secours prenne le relais. HSRP permet d'augmenter la tolérance de panne sur un réseau en créant un routeur virtuel à partir de 2 routeurs physiques (ou plus), une élection déterminera le routeur actif et les autres routeurs seront en "attente" (standby). L'élection du routeur actif est réalisée grâce à la priorité configurée sur chaque routeur [15].

10.5.1 Principe de fonctionnement

En pratique, HSRP permet qu'un routeur de secours (ou Spare) prenne immédiatement, de façon transparente, le relais dès qu'un problème physique apparaît.

En partageant une seule et même adresse IP et MAC, plusieurs routeurs peuvent être considérés comme un seul routeur "Virtuel".

Un routeur physique peut donc être "responsable" du routage et un autre en redondance. Si le routeur, que nous appellerons primaire, a un problème, le routeur secondaire prendra sa place automatiquement. Les paquets continueront de transiter de façon transparente car les 2 routeurs partagent les mêmes adresses IP et MAC !

Le groupe HSRP comprend un routeur primaire (Active) et un routeur secondaire (Standby) qui sont choisis par priorité pour gérer les paquets vers le routeur virtuel. En cas de panne du routeur primaire.

Pendant la mise en place des liens, le processus d'élection désigne le routeur primaire (Active) qui envoie des messages HSRP multicast en UDP aux autres routeurs pour limiter le trafic. Si le routeur secondaire (Standby) cesse de recevoir ces messages, il assume le rôle d'Actif car le primaire est probablement défaillant.

L'élection du routeur primaire dans HSRP est similaire à celle de Spanning Tree, basée sur une priorité allant de 1 à 255 (255 étant le plus prioritaire), associée à l'adresse IP de l'interface pour déterminer le routeur principal.

En cas de priorités statiques égales, le routeur avec la plus haute adresse IP sera élu comme routeur principal dans HSRP. Il est possible d'avoir plusieurs groupes HSRP sur un même routeur sans conflit (à partir de l'IOS 10.3). Seuls les routeurs du même groupe échangent des messages HSRP [15] .

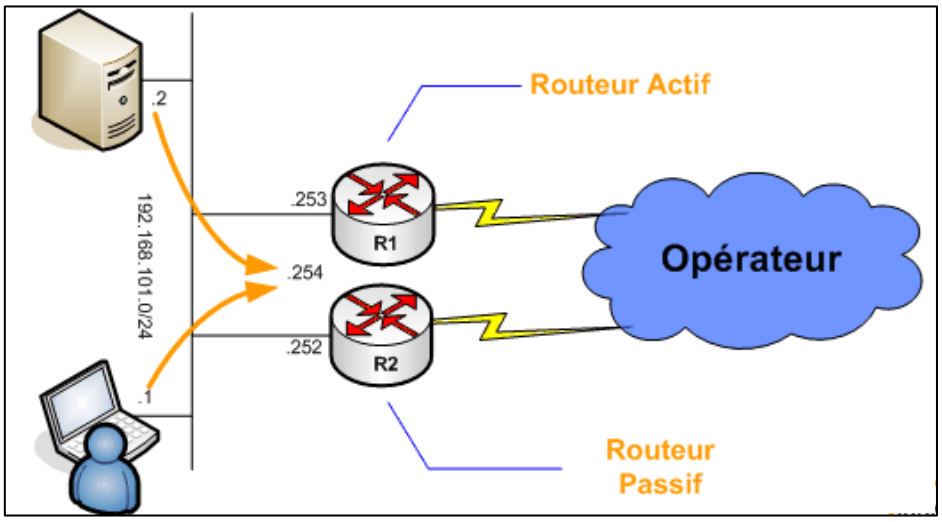


Figure 2.9 : Le protocole HSRP [W4].

10.6 Le protocole ssh (Secure Shell)

Le protocole SSH pour Secure Shell est largement utilisé de nos jours visant à garantir l'authenticité, la confidentialité et l'intégrité des données. En utilisant SSH, la transmission des informations au sein d'un réseau est chiffrée et ne peut donc, en théorie, être que difficilement compromise. SSH se décline en deux versions. La version 1 a été développée en 1995 par le finlandais Tatu Ylönen dans le but de sécuriser les connexions distantes. Aujourd'hui, la version la plus récente du protocole est la version 2, normalisée par l'Internet Engineering Task Force (IETF) en janvier 2006, apportant quelques corrections au niveau de la sécurité par rapport à SSH-1 (notamment au niveau des algorithmes utilisés). SSH est à la fois un protocole et un ensemble de programmes [16].

Il possède plusieurs fonctionnalités [16] :

- ✓ Il permet par exemple d'établir des sessions sécurisées sur un ordinateur distant,
- ✓ De transférer des fichiers sécurisés ou d'établir des tunnels sécurisés.

Pour ce qui concerne l'établissement de communications sécurisées, SSH se base sur le protocole SOCKS v5 intégré dans la plupart des équipements réseau. SSH apporte donc une amélioration indéniable aux protocoles non sécurisés tels que Telnet, Rlogin, FTP.

10.7 Les ACL (Access Control List)

Une ACL (liste de contrôle d'accès) est un ensemble séquentiel d'instructions d'autorisation ou de refus qui s'appliquent aux adresses ou aux protocoles de couche supérieure. Les listes de contrôle d'accès permettent de contrôler le trafic entrant ou sortant d'un réseau. Des listes de contrôle d'accès peuvent être configurées pour tous les protocoles réseau routés [17].

Les ACL peuvent être implémentées dans deux directions [17] :

- **Les ACLs entrantes** les paquets entrants sont traités avant d'être routés vers l'interface de sortie. Les listes de contrôle d'accès entrantes sont idéales pour filtrer les paquets lorsque le réseau relié à une interface d'entrée est la seule source des paquets devant être inspectés.
- **Les ACLs sortantes** les paquets entrants sont acheminés vers l'interface de sortie, puis traités par le biais de la liste de contrôle d'accès sortante. Les listes de contrôle d'accès sortantes sont particulièrement efficaces lorsqu'un même filtre est appliqué aux paquets provenant de plusieurs interfaces d'entrée avant de quitter la même interface de sortie.

10.7.1 Les ACL IPv4

Les routeurs prennent en charge deux types d'ACLIPv4 [17] :

- **Les ACL Standard**
  - ✓ Filtre les paquets IP en se basant uniquement sur l'adresse IPsource.
  - ✓ Peuvent être numérotées ou nommées.
  - ✓ Les plages de nombres valides comprennent 1 – 99 et 1300 –1999.
- **Les ACL Etendues**
  - ✓ Filtre les paquets IP se basant sur les adresses IP source et destination, les ports UDP et TCP source et destination, et les types de messages ICMP,etc.
  - ✓ Peuvent être numérotées ou nommées.
  - ✓ Les plages de nombre valides comprennent 100 – 199 et 2000 –2699.

10.7.2 Recommandation sur les ACL

Il est important de prendre en compte les points suivants lors de l'implémentation des ACL [17] :

- ✓ Les instructions dans une ACL sont traitées dans un ordre séquentiel, il est important de prendre en compte l'ordre de leur positionnement.
- ✓ Les instructions les plus spécifiques doivent être placées dans les premières lignes dans une ACL.
- ✓ Les nouvelles instructions dans une ACL existant sont ajoutées par défaut aux dernières lignes.
- ✓ Il faut s'assurer que la dernière instruction est un refus de tous autres trafics non spécifiés.
- ✓ Une seule ACL est autorisée par interface, par protocole ou par direction.
- ✓ Les paquets générés par le routeur ne sont pas traité par les ACL sortantes.
- ✓ Les ACL standards doivent être placées le plus près possible de la destination.
- ✓ Les ACL étendues doivent être placées le plus près possible de la source.

11 Conclusion

Ce chapitre couvre les fondamentaux des réseaux informatiques, de leur définition à leur classification, en passant par les architectures, topologies, supports de transmission et équipements de base. La redondance, essentielle pour la disponibilité et la résilience des réseaux, est mise en avant. Les modèles OSI, TCP/IP et les protocoles LAN sont explorés pour expliquer la connectivité et la sécurité des réseaux modernes.

Chapitre 3 : Conception et réalisation

1 Introduction

Dans ce chapitre, nous allons d'abord revisiter le réseau préexistant du site EL-KSEUR de Cevital pour mettre en avant les configurations et protocoles actuellement mis en place et expliquer leurs utilisations, puis nous proposerons une nouvelle configuration visant à améliorer et à corriger les faiblesses du réseau existant.

2 Présentation du réseau existant

2.1 Présentation des VLANs existants

La liste des VLANs du réseau existant sont représentés dans **le tableau 3.1** :

VLAN ID	Nom de VLANs	Description
2	SAUCE	/
3	PRODUCTION-SAUCE	/
4	EXPEDITION-SAUCE	/
5	FROMMAGE	/
6	BOISSON	/
7	PRODUCTION-BOISSON	/
8	EXPEDITION-BOISSON	/
9	ADMINISTRATION	/
10	DFC	Direction finance et comptabilité
11	DRH	Direction des Ressources Humaines
12	IT	Technologie de l'information
13	IMPRIMANTE	/
14	SERVEUR	/

Tableau 3.1 : Liste des noms des VLANs du réseau et leur plan d'adressage.

2.2 Architecture du réseau existant du site EL-KSEUR

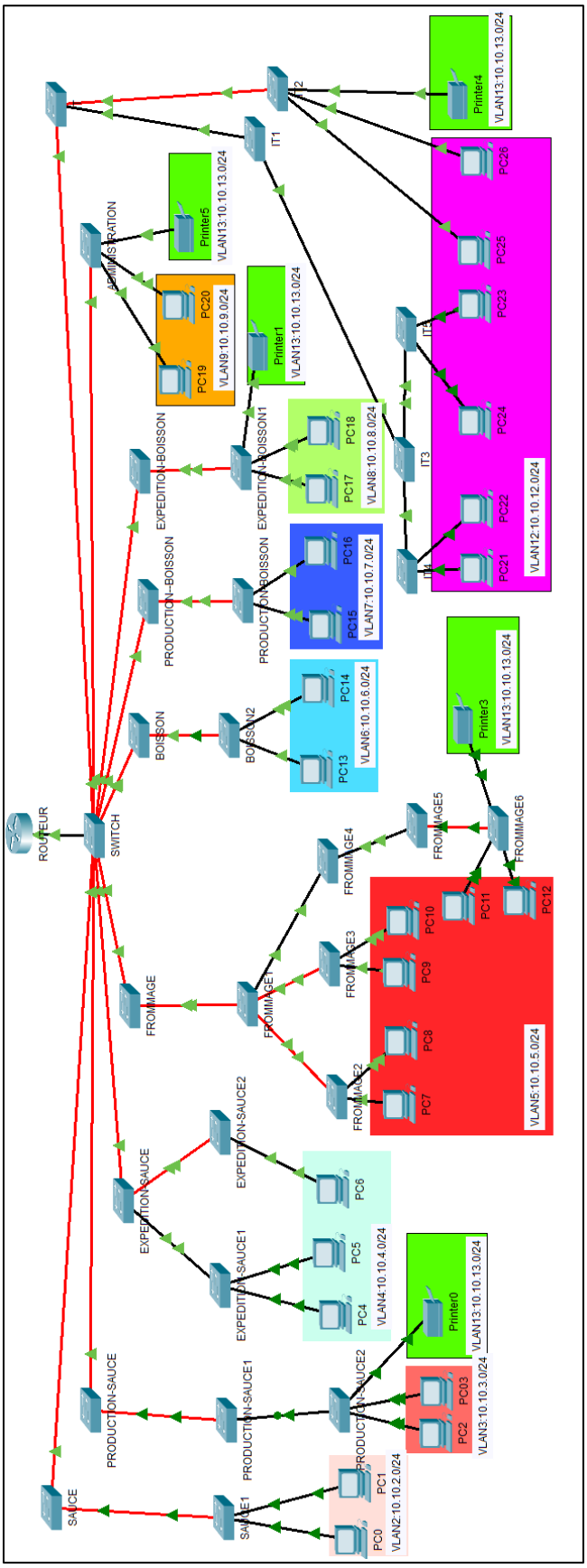


Figure 3.1 : Architecture du réseau local existant de CEVITAL EL-KSEUR.

2.3 Configuration du réseau existant

Les différentes configurations du réseau existant de Cevital EL-KSEUR que nous avons réalisé sont présentées en Annexe.

2.4 Critique de l'existant

Malgré les avantages qu'offre cette architecture en termes de connectivité intra et extra-VLAN, elle présente des limitations majeures en matière de connexion avec des sites distants. Dans une configuration réseau impliquant des switchs de niveau 2 interconnectés en cascade et un routeur, il est essentiel de noter que cette structure peut présenter des limitations en matière de redondance et de connectivité avec des sites distants. Les switchs de niveau 2 offrent des fonctionnalités limitées en termes de gestion avancée du trafic et de tolérance aux pannes. Ainsi, pour assurer la fiabilité, la sécurité et les performances du réseau nous proposerons une nouvelle architecture du réseau de manière à résoudre toutes les problématiques identifiées dans le réseau actuel.

3 Architecture proposée

Nous avons constaté que le réseau de l'unité d'El-Kseur est exposé à un grand risque de pannes. Pour remédier à ce problème, nous allons proposer quelques améliorations pour rendre ce réseau plus fiable. Lors de la conception de l'architecture du réseau, nous devons tenir compte du principe d'un modèle de réseau hiérarchique et de la redondance ainsi que la sécurité.

Notre architecture proposée est représentée dans **la figure 3.2**

3.1 Modèle de réseau hiérarchique

Consiste à diviser le réseau en couches distinctes, Chaque couche ou niveau de la hiérarchie offre des fonctions spécifiques qui définissent son rôle dans le réseau.

Une conception de réseau hiérarchique comprend les trois couches suivantes :

Couche d'accès permet aux groupes de travail et aux utilisateurs d'accéder au réseau.

Couche de distribution fournit la connectivité basée sur les stratégies et contrôle la limite entre les couches d'accès et cœur.

Couche cœur de réseau assure le transport rapide entre commutateurs de distribution dans le campus d'entreprise.

Nous avons établi un réseau hiérarchisé pour l'entreprise Cevital à El Kseur, avec :

- **Couche Cœur** Deux switchs de niveau 3 agissant comme cœur du réseau, assurant le routage efficace du trafic entre les différents sous-réseaux et sites. Ils jouent un rôle crucial

dans la transmission des données à haut débit et la gestion des flux de trafic à grande échelle.

- **Couche Distribution** Trois switchs de niveau 3 gérant la répartition du trafic provenant des switchs cœur vers les différents segments ou départements du réseau. Ils permettent de segmenter et d'optimiser le trafic en fonction des besoins spécifiques de chaque zone du réseau, assurant ainsi une performance optimale.
- **Couche d'Accès** Huit switchs de niveau 2 fournissant une connectivité locale sécurisée et performante aux utilisateurs finaux (PCs, imprimantes, etc.) et aux périphériques. Ils opèrent au niveau le plus bas de la hiérarchie, offrant un accès direct aux appareils du réseau local et permettant la gestion des VLANs pour isoler et sécuriser les flux de données.

3.2 Redondance au niveau de la couche cœur

La redondance est cruciale pour la continuité des affaires et la gestion des risques, assurant le fonctionnement des opérations critiques même en cas de défaillance. Dans notre architecture réseau, nous avons utilisé des liens et des switchs redondants entre la couche cœur et la couche distribution du modèle hiérarchique. Au niveau de la couche cœur, deux switchs de niveau 3 sont interconnectés pour garantir la redondance. À la couche distribution, trois switchs de niveau 3 sont chacun reliés aux switchs cœurs par des liens redondants. Enfin, à la couche d'accès, huit switchs sont répartis et reliés aux switchs de distribution, avec trois switchs connectés à un switch de distribution, deux à un autre, et les trois restants à un troisième switch de distribution. Cette configuration assure une continuité et une fiabilité optimales du réseau.

3.3 Sécurité du réseau proposé

Pour assurer une interconnexion sécurisée et fiable entre le site d'El Kseur et la DM Z qui se trouve au site central de Béjaïa, nous avons mis en place une infrastructure réseau supplémentaire qui comprend :

- ✓ Quatre routeurs pour acheminer le trafic entre les sites, assurant ainsi une connectivité stable et rapide, deux appartiennent à Algérie Télécom, garantissant une connectivité robuste et une gestion efficace des données entre les sites distants et le réseau principal de l'entreprise, un appartient au site EL-KSEUR et l'autre au site central de Béjaia.
- ✓ Deux pare-feu déployés pour renforcer la sécurité des communications et protéger les données sensibles.
- ✓ Configuration d'accès a distance par SSh et la sécurité des ports.

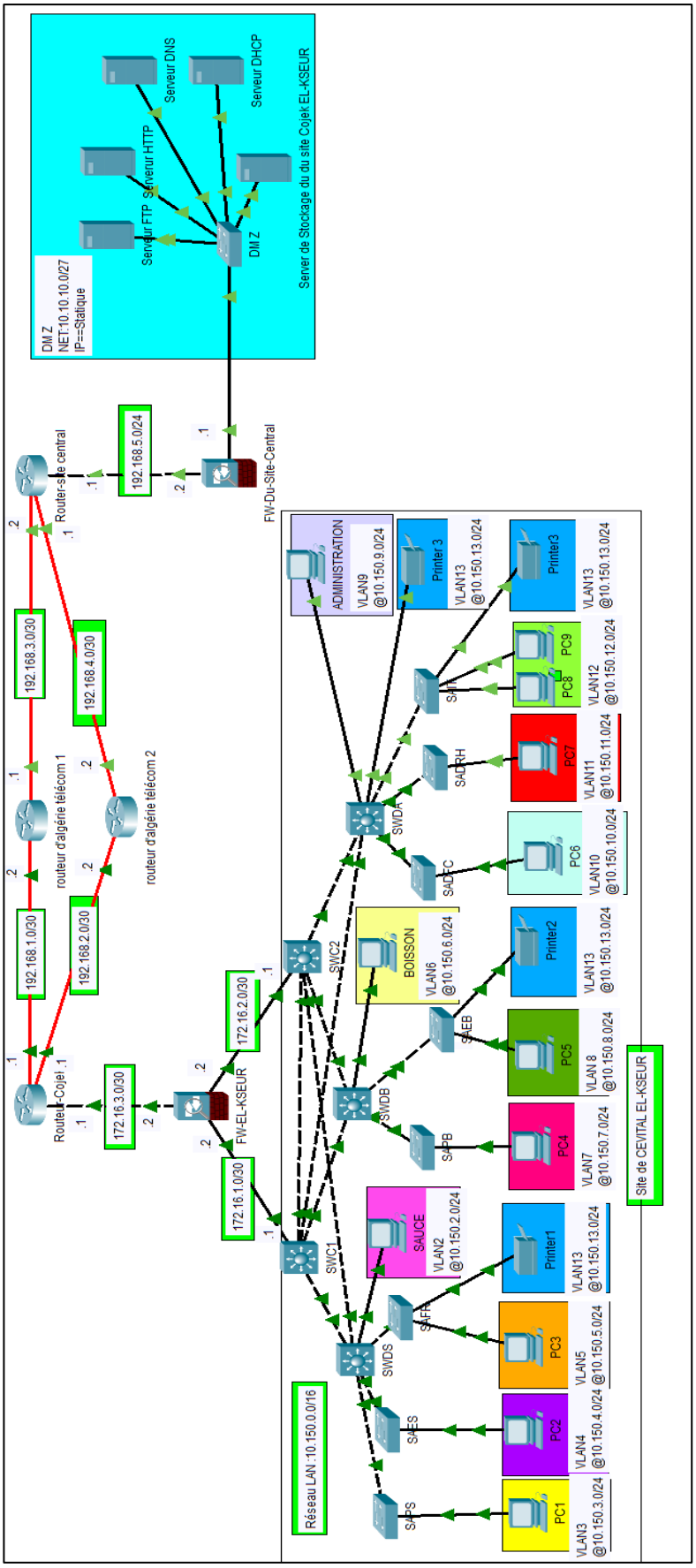


Figure 3.2 : La nouvelle architecture proposée au réseau CEVITAL EL-KSEUR.

3.4 Planification du déploiement

3.4.1 Nomination des équipements et désignations des interfaces

Les interfaces sur les équipements seront comme indique **le tableau 3.2** :

Equipement / Couche	Hostname	Description	Interface
Cœur	SWC1	Switch Cœur 1	Gig1/0/1 Gig1/0/2 Gig1/0/3 Gig1/0/4 Gig1/0/5
	SWC2	Switch Cœur 2	Gig1/0/1 Gig1/0/2 Gig1/0/3 Gig1/0/4 Gig1/0 /5
Distribution	SWDS	Switch de Distribution Sauce	Gig1/0/1 Gig1/0/2 Gig1/0/3 Gig1/0/4 Gig1/0/5 Gig1/0/6
	SWDB	Switch de Distribution Boisson	Gig1/0/1 Gig1/0/2 Gig1/0/3 Gig1/0/4
	SWDA	Switch de Distribution Administration	Gig1/0/1 Gig1/0/2 Gig1/0/3 Gig1/0/4 Gig1/0/5 Gig1/0/6 Gig1/0/7
Accès	SAPS	Switch d'Accès Production Sauce	Gig8/1 Gig9/1
	SAES	Switch d'Accès Expédition sauce	Gig8/1 Gig9/1
	SAFR	Switch d'Accès Fromage	Gig0/1 Gig1/1 Gig8/1
	SAPB	Switch d'Accès Production Boisson	Gig0/1 Gig1/1
	SAEB	Switch d'Accès Expédition Boisson	Gig0/1 Gig1/1

			Gig2/1
	SADFC	Switch d'Accès Direction finance et comptabilité	Gig0/1 Gig1/1
	SADRH	Switch d'Accès Direction de Ressources Humaines	Gig0/1 Gig1/1
	SAIT	Switch d'Accès Technologie de l'Information	Gig0/1 Gig1/1 Gig2/1 Gig3/1

Tableau 3.2 : Nomination des switchs et désignation des interfaces.

3.4.2 Adressage des interfaces des périphériques (routeurs, switchs, pare-feu, serveurs, PCs et imprimantes)

Pour assurer une configuration réseau optimale, la majorité des périphériques de notre réseau utilisent des adresses IP attribuées dynamiquement par le serveur DHCP. Cependant, quelques exceptions notables existent pour des raisons spécifiques de gestion et de sécurité **le tableau 3.3** résume l'adressage des Interfaces des Périphériques :

	Hostname	Interface	Adresses ip / Masque de sous réseau	Adresse ip de passerelle
Routeurs	Routeur-Cojek	Gig4/0	172.16.3.1/30	/
		Gig5/0	192.168.1.1/30	/
		Gig6/0	192.168.2.1/30	/
	Routeur d'algérie télécom 1	Gig5/0	192.168.1.2/30	/
		Gig6/0	192.168.3.1/30	/
	Routeur d'algérie télécom 2	Gig5/0	192.168.2.2/30	/
		Gig6/0	192.168.4.2/30	/
	Routeur-Site-central	Gig5/0	192.168.4.1/30	/
		Gig6/0	192.168.3.2/30	/
		Gig4/0	192.168.5.1/24	/
Switchs	SWC1	Gig1/0/5	172.16.1.1/30	/
	SWC2	Gig1/0/5	172.16.2.1/30	/
Pare-feu (firewall)	FW-EL-KSEUR	Gig1/1	172.16.3.2/30	/
		Gig1/2	172.16.1.2/30	/

		Gig1/3	172.16.2.2/30	/
	FW-Du-Site-Central	Gig1/1	192.168.5.2/24	/
		Gig1/2	192.168.5.1/24	/
PCs	SAUCE	Gig0	10.150.2.1/24	10.150.2.254
	PC1	Gig0	10.150.3.1/24	10.150.3.254
	PC2	Gig0	10.150.4.1/24	10.150.4.254
	PC3	Gig0	10.150.5.1/24	10.150.5.254
	BOISSON	Gig0	10.150.6.1/24	10.150.6.254
	PC4	Gig0	10.150.7.1/24	10.150.7.254
	PC5	Gig0	10.150.8.128/24	10.150.8.254
	ADMINISTRATION	Gig0	10.150.9.1/24	10.150.9.254
	PC6	Gig0	10.150.10.1/24	10.150.10.254
	PC7	Gig0	10.150.11.1/24	10.150.11.254
	PC8	Gig0	10.150.12.127/24 (adress ip static)	10.150.12.254
	PC9	Gig0	10.150.12.128/24	10.150.12.254
Imprimantes	Printer1	Gig0	10.150.13.4/24	10.150.13.254
	Printer2	Gig0	10.150.13.127/24	10.150.13.254
	Printer 3	Gig0	10.150.13.2/24	10.150.13.254
	Printer3	Gig0	10.150.13.3/24	10.150.13.254
Serveurs	Server de Stockage du du site Cojek EL-KSEUR	Gig1	10.10.10.2/27 (Adresse ip static)	10.10.10.1

Tableau 3.3 : Adressage des Interfaces des Périphériques.

3.4.3 Adressage des VLANs

Le tableau 3.4 représente le plan d'adressage et les interfaces des différents VLANs du réseau pour le site EL-KSEUR :

VLAN ID	Nom de VLANs	Adresse réseau / Masque de sous réseau	Périphérique local / Interface		Périphérique distant/ Interface
2	SAUCE	10.150.2.0/24	SWDS : Gig1/0/6		SAUCE : Gig0
3	PRODUCTION-SAUCE	10.150. 3.0/24	SAPS : Gig8/1		PC1 : Gig0
4	EXPEDITION-SAUCE	10.150.4.0/24	SAES : Gig8/1		PC2 : Gig0
5	FROMMAGE	10.150.5.0/24	SAFR : Gig8/1		PC3 : Gig0
6	BOISSON	10.150.6.0/24	SWDB : Gig1/0/6		BOISSON : Gig0
7	PRODUCTION-BOISSON	10.150.7.0/24	SAPB : Gig1/1		PC4 : Gig0
8	EXPEDITION-BOISSON	10.150.8.0/24	SAEB : Gig1/1		PC5 : Gig0
9	ADMINISTRATION	10.150.9.0/24	SWDA : Gig1/0/6		ADMINISTRATION : Gig0
10	DFC	10.150.10.0/24	SADFC : Gig1/1		PC6 : Gig0
11	DRH	10.150.11.0/24	SADRH : Gig1/1		PC7 : Gig0
12	IT	10.150.12.0/24	SAIT	Gig1/1	PC8 : Gig0
				Gig3/1	PC9 : Gig0
13	IMPRIMANTE	10.150.13.0/24	SAFR : Gig1/1		Printer1 : Gig0
			SAEB : Gig2/1		Printer2 : Gig0
			SWDA : Gig1/0/7		Printer 3 : Gig0
			SAIT : Gig2/1		Printer3 : Gig0
14	SERVEUR	10.150.14.0/24	/		/

Tableau 3.4 : Interfaces et plans d'adressage des VLANs.

Le tableau 3.5 suivant présente les configurations VTP des différents commutateurs dans notre infrastructure, incluant le nom de domaine VTP et le mode de fonctionnement de chaque commutateur :

VTP	Nom de domaine	Mode
SWC1	Cevital.com	Serveur
SWC2	Cevital.com	Client
Tous les autres switchs	Cevital.com	Client

Tableau 3.5 : VTP.

4 Mise en œuvre

4.1 Présentation du simulateur

Cisco Packet Tracer est un programme complet d'enseignement et de formation sur les technologies réseaux. Il offre une combinaison unique de simulations et de visualisations réalistes, d'évaluations, de fonctions pour la création d'activités et de possibilités de collaboration et de compétition multi-utilisateur. Les fonctionnalités innovantes de Packet Tracer aident les apprenants et les enseignants à collaborer, à résoudre des problèmes et à apprendre des concets dans un environnement social dynamique et stimulant [W1].

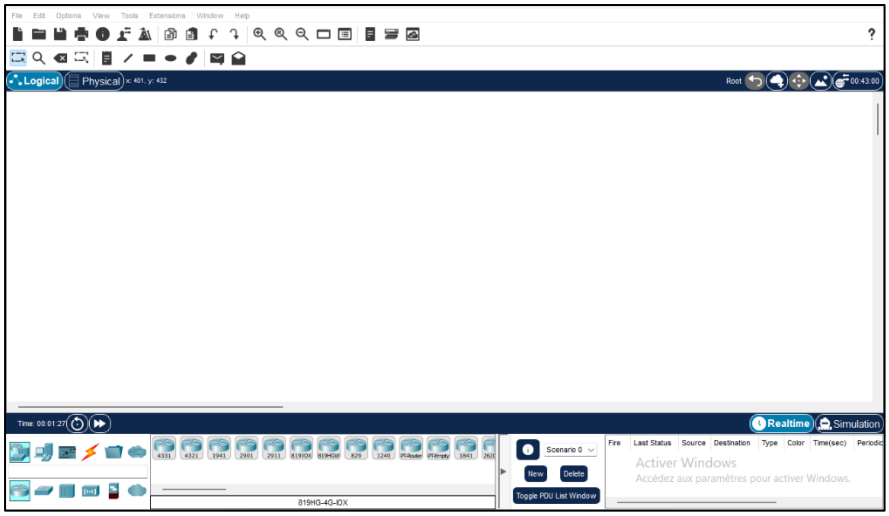


Figure 3.3 : Interface du simulateur Cisco Packet tracer 8.2.2.

4.2 Configuration des équipements du réseau proposé

4.2.1 Configuration de base des équipements réseau

Comme dans la configuration du réseau existant (voire l'annexe) nous avons renommés et sécurisé les équipements du réseau, **la figure 3.4** représente un exemple de configuration des deux switchs Core, que nous avons renommé SWC1 et SWC2 respectivement.

```
Switch>
Switch>en
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SWC1
SWC1(config)#
```

```
Switch#
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SWC2
SWC2(config)#
SWC2(config)#
```

Figure 3.4 : Configuration des noms d'hôtes.

Les équipements ont été sécurisés de manière rigoureuse. Tout d'abord, le mode "enable" et les sessions Console et VTY, garantissant un accès restreint aux utilisateurs autorisés, qu'ils se connectent localement ou à distance. De plus, tous les mots de passe ont été chiffrés à l'aide de la commande « **service password-encryption** » pour assurer la confidentialité des informations d'authentification, **la figure 3.5** montre les étapes de configuration :

```
SWC1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWC1(config)#
SWC1(config)#enable secret cevital
SWC1(config)#line cons 0
SWC1(config-line)#passw cevital
SWC1(config-line)#login
SWC1(config-line)#exi
SWC1(config)#line vty 0 15
SWC1(config-line)#passw cevital
SWC1(config-line)#login
SWC1(config-line)#exit
SWC1(config)#
SWC1(config)#
SWC1(config)#
SWC1(config)#service password-encryption
```

Figure 3.5 : Configuration des lignes sur le switch SWC1.

4.2.2 Configuration d'accès à distance

Pour configurer l'accès à distance par SSH sur un switch Cisco, on suit les étapes décrites sur **la figure 3.6** du switch SWC1 :

```
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SWC1(config)#ip domain-name cevital.com
SWC1(config)#crypto key generate rsa
The name for the keys will be: SWC1.cevital.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

SWC1(config)#ip ssh version 2
*Mar 1 6:22:49.495: %SSH-5-ENABLED: SSH 1.99 has been enabled
SWC1(config)#line vty 0 15
SWC1(config-line)#transport input ssh
SWC1(config-line)#transport output ssh
SWC1(config-line)#login local
SWC1(config-line)#exit
SWC1(config)#username admin password cevital
```

Figure 3.6 : Configuration de l'accès à distance au niveau du switch SWC1.

Résumé des Étapes

1. **ip domain-name cevital.com :** Définir le nom de domaine pour la génération des clés RSA.
2. **crypto key generate rsa :** Générer une paire de clés RSA pour SSH.
3. **1024 :** Spécifier la taille de la clé RSA.
4. **ip ssh version 2 :** Configurer l'appareil pour utiliser SSH version 2.
5. **line vty 0 15 :** Entrer en mode de configuration des lignes VTY.
6. **transport input ssh / transport output ssh :** Restreindre les connexions aux protocoles SSH.
7. **login local :** Utiliser l'authentification locale pour les connexions SSH.
8. **exit :** Quitter le mode de configuration des lignes VTY.
9. **username admin password cevital :** Créer un utilisateur local pour SSH

- Nous appliquons les mêmes étapes pour les autres switchs.

4.2.3 Configuration des ACL

La configuration des ACL implique de définir des règles pour permettre ou refuser le trafic basé sur des critères tels que l'adresse IP source ou destination. Les ACL sont appliquées à des interfaces spécifiques pour contrôler le flux de trafic entrant ou sortant. Cela permet de renforcer la sécurité en limitant l'accès aux ressources réseau.

```
SWC2(config)#access-list 1 permit 10.150.12.127
SWC2(config)#line vty 0 4
SWC2(config-line)#access-class 1 in
SWC2(config-line)#access-class 1 out
SWC2(config-line)#exit
```

Figure 3.7 : Configuration de ACL au niveau du SWC2.

Dans notre cas on a sécurisé l'accès au switch SWC2 via les lignes VTY et restreindre l'accès uniquement aux administrateurs du VLAN 12, nous avons configuré une ACL

standard. La règle « **access-list 1 permit 10.150.12.127 »** permet uniquement l'adresse IP 10.150.12.127, qui appartient au VLAN 12 dédié à la technologie de l'information. Ensuite, nous avons appliqué cette ACL à la ligne VTY **« line vty 0 4 »** pour contrôler le trafic entrant et sortant à l'aide des commandes « **access-class 1 in »** et « **access-class 1 out »**, garantissant que seuls les administrateurs de ce VLAN spécifique peuvent accéder à distance au switch.

- Pour vérifier la configuration des ACL sur un routeur ou un commutateur Cisco, on utilise la commande « **show access-lists** »

```
SWC2#sh access-lists
Standard IP access list 1
    10 permit host 10.150.12.127 (2 match(es))
```

Figure 3.8 : Vérification de la configuration de l'ACL au niveau du SWC2.

4.2.4 Configuration du protocole VTP

La configuration du protocole VTP en mode serveur a été mise en place sur le switch SWC1. Les autres switchs ont été configurés en mode client pour recevoir les informations des VLANs distribués par le switch en mode serveur.

- **Mode serveur**

```
SWC1(config)#vtp mode server
Device mode already VTP SERVER.
SWC1(config)#vtp domain cevital.com
Changing VTP domain name from NULL to cevital.com
SWC1(config)#vtp pass cevital
Setting device VLAN database password to cevital
SWC1(config)#
```

Figure 3.9 : Configuration du protocole VTP en mode serveur.

- **Mode client**

```
SWC2(config)#vtp mode client
Device mode already VTP CLIENT.
SWC2(config)#vtp domain cevital.com
Domain name already set to cevital.com.
SWC2(config)#vtp pass cevital
Password already set to cevital
SWC2(config)#
```

Figure 3.10 : Configuration du protocole VTP en mode Client

- La commande qui permet de vérifier le protocole VTP sur les switchs Cisco est « **show vtp status** ». Cette commande affiche des informations détaillées sur la configuration VTP actuelle du switch, y compris le mode VTP (serveur, client ou transparent), le domaine VTP, **Les figures 3.11** et **3.12** illustrent les résultats.

```
SWC1#sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0001.643E.3100
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
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        : 5
Configuration Revision          : 0
MD5 digest                      : 0x8D 0xBA 0x0E 0x7E 0xB7 0x12 0x88 0x5C
                                  0xB8 0x2F 0xB3 0x15 0xB1 0x72 0x82 0x34
SWC1#
```

Figure 3.11 : Vérification de la configuration du VTP server au niveau du SWC1.

```
SWC2#sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0005.5E14.C500
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN :
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
Configuration Revision          : 0
MD5 digest                      : 0x8D 0xBA 0x0E 0x7E 0xB7 0x12 0x88 0x5C
                                  0xB8 0x2F 0xB3 0x15 0xB1 0x72 0x82 0x34
```

Figure 3.12 : Vérification de la configuration de VTP client au niveau du SWC2.

4.2.5 Création des VLANs

En configurant le switch SWC1 en tant que VTP Server et en créant les VLANs sur ce switch, on assure une gestion centralisée et une propagation automatique des VLANs à tous les switchs VTP Clients. Cette approche simplifie la gestion du réseau et assure une cohérence des VLANs à travers toute l'infrastructure réseau, **la figure 3.13** montre la création des VLANs allant de 2 à 5 au niveau du switch SWC1.

```
SWC1(config)#vlan 2
SWC1(config-vlan)#Name SAUCE
SWC1(config-vlan)#vlan 3
SWC1(config-vlan)#NAME PRODUCTION-SAUCE
SWC1(config-vlan)#vlan 4
SWC1(config-vlan)#NAME EXPEDITION-SAUCE
SWC1(config-vlan)#vlan 5
SWC1(config-vlan)#NAME FROMMAGE
```

Figure 3.13 : Création des VLANs au niveau du SWC1.

- Les VLANs 6 à 14 sont configurés de la même manière en utilisant la syntaxe appropriée pour chaque VLAN.

4.2.6 Configuration des ports en mode trunk et access

On répète la procédure décrite dans l'annexe pour configurer les liens trunks entre les switchs et les liens access entre les PCs, **les figure 3.14** et **3.15** montrent la méthode de configuration :

```
SWC1(config)#int gigabitEthernet 1/0/2
SWC1(config-if)#switchport mode trunk
SWC1(config-if)#ex
SWC1(config)#
```

Figure 3.14 : La configuration des liens trunk.

```
SAPS(config)#interface GigabitEthernet8/1
SAPS(config-if)#switchport mode access
SAPS(config-if)#
```

Figure 3.15 : La configuration des liens access.

- La configuration des autre liens trunk et access se fait de la même manière que SWC1 et SAPS.

4.2.7 Configuration des interfaces VLANs

La configuration des interfaces VLAN implique l'attribution d'une adresse IP à chaque interface, une opération réalisée principalement sur les switchs de niveau 3, souvent appelés switchs Core ou switchs de distribution. Ces switchs gèrent le routage inter-VLAN.

Sur les switchs Core (SWC1 et SWC2), les adresses IP des interfaces VLANs sont attribuées de manière systématique et cohérente :

Nous avons activé ce routage avec la commande « **IP routing », les figures 3.16** et **3.17**

```
SWC1(config)#Interface Vlan 2
SWC1(config-if)#ip add 10.150.2.252 255.255.255.0
SWC1(config-if)#Interface Vlan 3
SWC1(config-if)#ip add 10.150.3.252 255.255.255.0
```

Figure 3.16 : Configuration de l'interface du VLAN 2 et 3 sur le SWC1.

```
SWC2(config)#Interface Vlan 2
SWC2(config-if)#ip add 10.150.2.253 255.255.255.0
SWC2(config-if)#Interface Vlan 3
SWC2(config-if)#ip add 10.150.3.253 255.255.255.0
```

Figure 3.17 : Configuration de l'interface du VLAN 2 et 3 sur le SWC2.

montre la configuration de l'interface du VLAN 2 et 3 sur les switchs coeur 1 et 2.

- L'attribution des adresses ip aux autres interfaces VLANs sur les deux switch SWC1 et SWC2 se fait de la même manière.

➢ Pour visualiser les interfaces VLAN et leurs adresses IP configurées sur le switch SWC1, nous utilisons la commande « **show ip interface brief | exclude unassigned** ». **La figure 3.18** montre la sortie de Cette commande :

```
SWC1# show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1/0/5   172.16.1.1      YES manual up                    up
Vlan2                  10.150.2.252    YES manual up                    up
Vlan3                  10.150.3.252    YES manual up                    up
Vlan4                  10.150.4.252    YES manual up                    up
Vlan5                  10.150.5.252    YES manual up                    up
Vlan6                  10.150.6.252    YES manual up                    up
Vlan7                  10.150.7.252    YES manual up                    up
Vlan8                  10.150.8.252    YES manual up                    up
Vlan9                  10.150.9.252    YES manual up                    up
Vlan10                 10.150.10.252   YES manual up                    up
Vlan11                 10.150.11.252   YES manual up                    up
Vlan12                 10.150.12.252   YES manual up                    up
Vlan13                 10.150.13.252   YES manual up                    up
Vlan14                 10.150.14.252   YES manual up                    up
```

Figure 3.18 : Vérification des interfaces VLANs sur le SWC1.

4.2.8 Attribution des ports des commutateurs aux VLANs

Comme on a vu précédemment chaque port sur un commutateur est assigné à un VLAN spécifique. Cela permet de contrôler quelles données peuvent passer à travers chaque port en fonction du VLAN auquel il est assigné.

```
SAPS(config)#int gig 8/1
SAPS(config-if)#switchport mode access
SAPS(config-if)#switchport access VLAN 3
SAPS(config-if)#ex
SAPS(config)#
```

Figure 3.19 : Assignation des ports aux VLANs.

- On attribue les ports des commutateurs au VLANs spécifique de la même manière que SAPS.

4.2.9 Configuration du DHCP

Nous avons créé un pool d'adresses pour chaque VLAN. Cette opération a été réalisée au niveau des switchs Cœur, où nous avons également défini la passerelle par défaut pour chaque sous-réseau.

```
SWC1(config)#
SWC1(config)#Ip dhcp pool 2
SWC1(dhcp-config)#Network 10.150.2.0 255.255.255.0
SWC1(dhcp-config)#Default-router 10.150.2.254
SWC1(dhcp-config)#Exit
SWC1(config)#Ip dhcp pool 3
SWC1(dhcp-config)#Network 10.150.3.0 255.255.255.0
SWC1(dhcp-config)#Default-router 10.150.3.254
SWC1(dhcp-config)#Exit
```

Figure 3.20 : Configuration du protocole DHCP au niveau du SWC1.

```
SWC2(config)#
SWC2(config)#Ip dhcp pool 2
SWC2(dhcp-config)#Network 10.150.2.0 255.255.255.0
SWC2(dhcp-config)#Default-router 10.150.2.254
SWC2(dhcp-config)#Exit
SWC2(config)#Ip dhcp pool 3
SWC2(dhcp-config)#Network 10.150.3.0 255.255.255.0
SWC2(dhcp-config)#Default-router 10.150.3.254
SWC2(dhcp-config)#Exit
```

Figure 3.21 : Configuration du protocole DHCP au niveau du switch SWC2.

- La configuration des autres pools d'adresses se fait de la même manière que SWC1 et SWC2.

➢ Pour afficher les pools DHCP configurés sur un switch ou un routeur Cisco, on utilise la commande « **show ip dhcp pool** » en mode privilégié, **la figure 3.22** montre le résultat :

```
SWC1#sh ip dhcp pool

Pool 2 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 10.150.2.1           10.150.2.1      - 10.150.2.254      0    / 0     / 254
```

Figure 3.22 : Vérification de la configuration du DHCP pool pour le VLAN 2.

Nous avons configuré l'exclusion des adresses IP de 127 à 251 sur SWC1, permettant ainsi à SWC1 d'attribuer dynamiquement les adresses de 1 à 126. Inversement, sur SWC2, nous avons exclu les adresses de 1 à 126, ce qui permet à SWC2 d'attribuer dynamiquement les adresses de 127 à 251. Cette stratégie vise à éviter les conflits d'adressage lors de l'attribution des adresses IP, assurant ainsi une distribution cohérente et sans chevauchement des adresses IP au sein du réseau.

```
SWC1(config)#ip dhcp excluded-address 10.150.2.127 10.150.2.251
SWC1(config)#ip dhcp excluded-address 10.150.3.127 10.150.3.251
SWC1(config)#ip dhcp excluded-address 10.150.4.127 10.150.4.251
SWC1(config)#ip dhcp excluded-address 10.150.5.127 10.150.5.251
SWC1(config)#ip dhcp excluded-address 10.150.6.127 10.150.6.251
SWC1(config)#ip dhcp excluded-address 10.150.7.127 10.150.7.251
SWC1(config)#ip dhcp excluded-address 10.150.8.127 10.150.8.251
SWC1(config)#ip dhcp excluded-address 10.150.9.127 10.150.9.251
SWC1(config)#ip dhcp excluded-address 10.150.10.127 10.150.10.251
SWC1(config)#ip dhcp excluded-address 10.150.11.127 10.150.11.251
SWC1(config)#ip dhcp excluded-address 10.150.12.127 10.150.12.251
SWC1(config)#ip dhcp excluded-address 10.150.13.127 10.150.13.251
SWC1(config)#ip dhcp excluded-address 10.150.14.127 10.150.14.251
```

Figure 3.23 : Exclusion des adresses sur le SWC1.

```
SWC2(config)#ip dhcp excluded-address 10.150.2.1 10.150.2.126
SWC2(config)#ip dhcp excluded-address 10.150.3.1 10.150.3.126
SWC2(config)#ip dhcp excluded-address 10.150.4.1 10.150.4.126
SWC2(config)#ip dhcp excluded-address 10.150.5.1 10.150.5.126
SWC2(config)#ip dhcp excluded-address 10.150.6.1 10.150.6.126
SWC2(config)#ip dhcp excluded-address 10.150.7.1 10.150.7.126
SWC2(config)#ip dhcp excluded-address 10.150.8.1 10.150.8.126
SWC2(config)#ip dhcp excluded-address 10.150.9.1 10.150.9.126
SWC2(config)#ip dhcp excluded-address 10.150.10.1 10.150.10.126
SWC2(config)#ip dhcp excluded-address 10.150.11.1 10.150.11.126
SWC2(config)#ip dhcp excluded-address 10.150.12.1 10.150.12.126
SWC2(config)#ip dhcp excluded-address 10.150.13.1 10.150.13.126
SWC2(config)#ip dhcp excluded-address 10.150.14.1 10.150.14.126
```

Figure 3.24 : Exclusion des adresses sur le SWC2.

- La commande « **show run | include ip dhcp excluded-address** » est utilisée pour filtrer la configuration en cours d'un périphérique réseau afin d'afficher uniquement les lignes contenant des exclusions d'adresses IP pour le service DHCP. Cela permet de vérifier rapidement quelles plages d'adresses IP ont été exclues de l'attribution DHCP sans avoir à parcourir l'intégralité de la configuration. **Les figures 3.21** et **3.22** montre le résultat :

```
SWC1#show run | include ip dhcp excluded-address
ip dhcp excluded-address 10.150.2.127 10.150.2.251
ip dhcp excluded-address 10.150.3.127 10.150.3.251
ip dhcp excluded-address 10.150.4.127 10.150.4.251
ip dhcp excluded-address 10.150.5.127 10.150.5.251
ip dhcp excluded-address 10.150.6.127 10.150.6.251
ip dhcp excluded-address 10.150.7.127 10.150.7.251
ip dhcp excluded-address 10.150.8.127 10.150.8.251
ip dhcp excluded-address 10.150.9.127 10.150.9.251
ip dhcp excluded-address 10.150.10.127 10.150.10.251
ip dhcp excluded-address 10.150.11.127 10.150.11.251
ip dhcp excluded-address 10.150.12.127 10.150.12.251
ip dhcp excluded-address 10.150.13.127 10.150.13.251
ip dhcp excluded-address 10.150.14.127 10.150.14.251
```

Figure 3.25 : Affichage des adresses ip exclues de l'attribution DHCP sur le SWC1.

```
SWD2#show run | include ip dhcp excluded-address
ip dhcp excluded-address 10.150.2.1 10.150.2.126
ip dhcp excluded-address 10.150.3.1 10.150.3.126
ip dhcp excluded-address 10.150.4.1 10.150.4.126
ip dhcp excluded-address 10.150.5.1 10.150.5.126
ip dhcp excluded-address 10.150.6.1 10.150.6.126
ip dhcp excluded-address 10.150.7.1 10.150.7.126
ip dhcp excluded-address 10.150.8.1 10.150.8.126
ip dhcp excluded-address 10.150.9.1 10.150.9.126
ip dhcp excluded-address 10.150.10.1 10.150.10.126
ip dhcp excluded-address 10.150.11.1 10.150.11.126
ip dhcp excluded-address 10.150.12.1 10.150.12.126
ip dhcp excluded-address 10.150.13.1 10.150.13.126
ip dhcp excluded-address 10.150.14.1 10.150.14.126
```

Figure 3.26 : Affichage des adresses ip exclues de l'attribution DHCP sur le SWC2.

4.2.10 Configuration du Spanning-Tree Protocol

Le but du protocole STP est de désigner un root (route) primaire ou secondaire pour un VLAN. Nous l'avons configuré à la fois sur le SWC1 et le SWC2.

Les figures 3.27 et **3.28** présentent les commandes nécessaires pour la configuration du STP. Dans le cas du commutateur SWC1, il a été configuré afin d'être le root pour les VLANs de 2 à 7 avec une priorité de 4096 et le bridge pour les VLANs de 8 à 14 avec une priorité de 8192. Inversement le SWC2 sera root pour les VLANs de 8 à 14 avec une priorité de 4096 et le bridge pour les VLANs de 2 à 7 avec une priorité de 8192.

Les figures illustrent les commandes de configurations de STP :

```
SWC1(config)#spanning-tree mode rapid-pvst
SWC1(config)#spanning-tree vlan 2-7 priority 4096
SWC1(config)#spanning-tree vlan 8-14 priority 8192
SWC1(config)#
SWC1(config)#
```

Figure 3.27 : Configuration de STP sur SWC1.

```
SWC2(config)#spanning-tree mode rapid-pvst
SWC2(config)#spanning-tree vlan 2-7 priority 8192
SWC2(config)#spanning-tree vlan 8-14 priority 4096
```

Figure 3.28 : Configuration de STP sur SWC2.

- Pour vérifier la configuration du STP, on utilise la commande « **show spanning-tree** », Cette commande affichera les détails de la configuration STP sur le périphérique réseau, y compris les informations sur le bridge root, les ports de liaison et les états des ports.

```
SWC1(config)#do sh spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     0001.96A8.260D
              Cost        8
              Port        2(GigabitEthernet1/0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     00D0.9704.70B7
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi1/0/3          Desg FWD 4         128.3    P2p
Gi1/0/4          Desg FWD 4         128.4    P2p
Gi1/0/1          Desg FWD 4         128.1    P2p
Gi1/0/2          Root FWD 4         128.2    P2p

VLAN0002
  Spanning tree enabled protocol rstp
  Root ID     Priority    4098
              Address     00D0.9704.70B7
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4098  (priority 4096 sys-id-ext 2)
              Address     00D0.9704.70B7
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
```

Figure 3.29: Vérification de la configuration du STP sur SWC1.

4.2.11 Sécurité des ports et Bpdu guard

La sécurité des ports (port security) sur les commutateurs réseau contrôle l'accès en restreignant les adresses MAC autorisées sur une interface de switch. Bien qu'elle soit principalement configurée sur les commutateurs d'accès, elle peut aussi être appliquée aux commutateurs de niveau 3 pour protéger contre les accès non autorisés. **La figure 3.30** illustre cette configuration sur le switch d'accès SAPS (Switch d'Accès Production SAUCE) :

```
SAPS(config)#interface gig8/1
SAPS(config-if)# switchport mode access
SAPS(config-if)# switchport port-security
SAPS(config-if)# switchport port-security maximum 2
SAPS(config-if)# switchport port-security mac-address sticky
SAPS(config-if)# switchport port-security violation restrict
```

Figure 3.30 : Configuration de la sécurité des ports sur le switch SAPS.

La configuration de PortFast et BPDU Guard est essentielle pour améliorer les performances du réseau en réduisant le temps de convergence et pour protéger le réseau contre les boucles indésirables causées par des périphériques non autorisés.

- La commande « **spanning-tree portfast bpduguard default** » configure BPDU Guard globalement pour tous les ports PortFast.

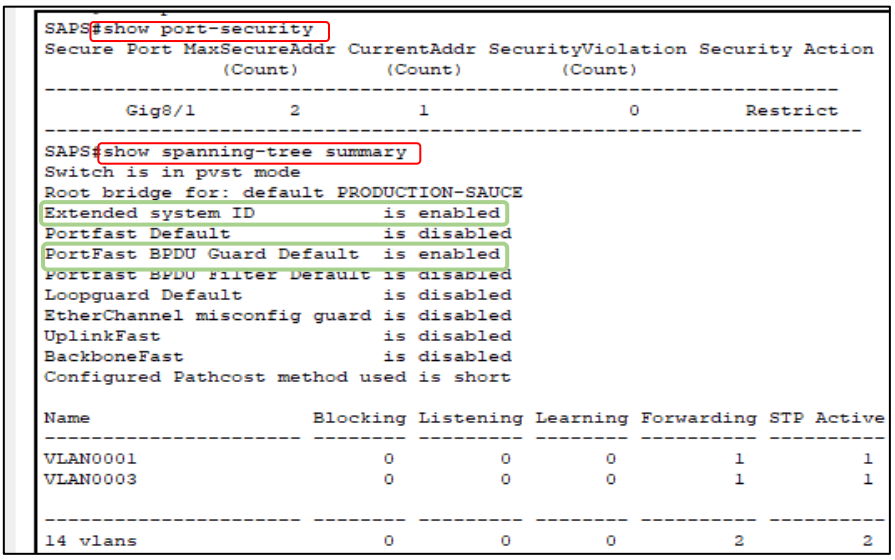
```
SAPS(config)#interface gigabitEthernet 8/1
SAPS(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on GigabitEthernet8/1 but will only
have effect when the interface is in a non-trunking mode.
SAPS(config-if)#
SAPS#
%SYS-5-CONFIG_I: Configured from console by console

SAPS#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SAPS(config)#spanning-tree portfast bpduguard default
```

Figure 3.31 : Configuration du Portfast et de BPDUGuard sur le switch d'accès SAPS.

Note 1 : PortFast doit être configuré uniquement sur les ports qui sont connectés à des périphériques finaux (comme des ordinateurs, des imprimantes, etc.), et non sur les ports de trunk ou uplinks.

Note 2 : BPDU est un message crucial pour la gestion et la prévention des boucles de commutation dans un réseau, assurant une topologie stable. BPDU Guard, quant à lui, est une fonctionnalité de sécurité qui protège le réseau en désactivant les ports configurés pour ne pas recevoir de BPDUs lorsqu'un BPDU indésirable y est détecté, prévenant ainsi les boucles de commutation indésirables.

- La sécurité des autres ports ainsi que la configuration de PortFast et de BPDU guard doivent être effectuée sur les ports de switchs qui sont connectés directement à des hôtes.
- Pour visualiser les configurations et états actuels de la sécurité des ports et de BPDU Guard sur notre switch on utilise les commandes suivante « **show port-security** » et « **show spanning-tree summary** ».



```
SAPS#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
-------------------------------------------------------------------------
       Gig8/1        2           1                0          Restrict
-------------------------------------------------------------------------
SAPS#show spanning-tree summary
Switch is in pvst mode
Root bridge for: default PRODUCTION-SAUCE
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                      0         0        0          1          1
VLAN0003                      0         0        0          1          1

---------------------- -------- --------- -------- ---------- ----------
14 vlans                      0         0        0          2          2
```

Figure 3.32 : visualisation des configurations et l'états actuels de la sécurité des ports et de BPDU Guard sur le switch SAPS.

✓ **Configuration Port-Security**

- **MaxSecureAddr (Count)** : Ce port est configuré pour accepter un maximum de 2 adresses MAC sécurisées.
- **CurrentAddr (Count)** : Actuellement, 1 adresse MAC est sécurisée sur ce port.
- **SecurityViolation (Count)** : Il n'y a eu aucune violation de sécurité sur ce port.
- **Security Action** : L'action en cas de violation de sécurité est de "Restreindre" (Restrict). Cela signifie que lorsque le nombre d'adresses MAC dépasse la limite autorisée, les paquets supplémentaires seront rejetés, mais le port restera actif.

✓ **Configuration Spanning-Tree**

- **Switch is in pvst mode** : Le switch utilise le mode PVST (Per-VLAN Spanning Tree), qui crée une instance STP distincte pour chaque VLAN.
- **Root bridge for** : Le switch est la racine (root bridge) pour les VLANs "default" et "PRODUCTION-SAUCE".
- **Extended system ID** : L'ID système étendu est activé, ce qui permet d'identifier les VLANs dans les BPDUs.
- **PortFast BPDU Guard Default** : La protection BPDU Guard est activée par défaut. Cela désactive un port si un BPDU est reçu, utile pour les ports configurés en PortFast.

4.2.12 Configuration du Hot standby Router Protocol

La mise en place de la haute disponibilité se réalise au niveau des switchs de distribution, (dans notre cas, la configuration de HSRP est effectuée au niveau de la couche Cœur). Son objectif est de désigner le routeur actif pour chaque VLAN en utilisant une priorité déterminée. Sur SWC1, nous avons configuré le HSRP en mode "actif" pour les VLANs 2 à 7,

tandis qu'il est configuré en mode "Standby" pour les VLANs 8 à 14. Inversement nous avons configuré l'HSRP sur SWC2 en mode « actif » pour les VLANs 8-14, et en mode « Standby » pour les VLANs 2-7.

✓ Mode « **Actif** » : VLANs 2-7 sur SWC1.

```
SWC1(config)#interface Vlan 2
SWC1(config-if)#standby 2 ip 10.150.2.254
SWC1(config-if)#standby 2 priority 110
SWC1(config-if)#standby 2 preempt
SWC1(config-if)#Exit
SWC1(config)#Int vlan 3
SWC1(config-if)#standby 3 ip 10.150.3.254
SWC1(config-if)#standby 3 priority 110
SWC1(config-if)#standby 3 preempt
SWC1(config-if)#Exit
```

Figure 3.33 : Configuration du HSRP en mode actif sur SWC1 pour les VLANs 2 et 3.

✓ Mode « **standby** » : VLANs 8-14 sur SWC1.

```
SWC1(config)#
SWC1(config)#Int vlan 8
SWC1(config-if)#Standby 8 ip 10.150.8.254
SWC1(config-if)#Exit
SWC1(config)#Int vlan 9
SWC1(config-if)#Standby 9 ip 10.150.9.254
SWC1(config-if)#Exit
SWC1(config)#Int vlan 10
SWC1(config-if)#Standby 10 ip 10.150.10.254
SWC1(config-if)#exit
SWC1(config)#Int vlan 11
SWC1(config-if)#Standby 11 ip 10.150.11.254
SWC1(config-if)#exit
SWC1(config)#Int vlan 12
SWC1(config-if)#Standby 12 ip 10.150.12.254
SWC1(config-if)#exit
SWC1(config)#Int vlan 13
SWC1(config-if)#Standby 13 ip 10.150.13.254
SWC1(config-if)#Exit
SWC1(config)#Int vlan 14
SWC1(config-if)#Standby 14 ip 10.150.14.254
SWC1(config-if)#
```

Figure 3.34 : Configuration du HSRP en mode standby sur SWC1 pour les VLANs 8-14.

✓ Mode « **actif** » : VLANs 8-14 sur SWC2.

```
SWC2(config)#Int vlan 8
SWC2(config-if)#Standby 8 ip 10.150.8.254
SWC2(config-if)#standby 8 priority 110
SWC2(config-if)#standby 8 preempt
SWC2(config-if)#Exit
SWC2(config)#Int vlan 9
SWC2(config-if)#Standby 9 ip 10.150.9.254
SWC2(config-if)#standby 9 priority 110
SWC2(config-if)#standby 9 preempt
SWC2(config-if)#Exit
```

Figure 3.35 : Configuration du HSRP en mode actif sur SWC2 pour les VLANs 8 et 9.

✓ Mode « **standby** » : VLANs 2-7 sur SWC2.

```
SWC2(config)#interface Vlan 2
SWC2(config-if)#standby 2 ip 10.150.2.254
SWC2(config-if)#exit
SWC2(config)#Int vlan 3
SWC2(config-if)#standby 3 ip 10.150.3.254
SWC2(config-if)#Exit
SWC2(config)#Int Vlan 4
SWC2(config-if)#standby 4 ip 10.150.4.254
SWC2(config-if)#Exit
SWC2(config)#Int vlan 5
SWC2(config-if)#standby 5 ip 10.150.5.254
SWC2(config-if)#exit
SWC2(config)#interface Vlan6
SWC2(config-if)#standby 6 ip 10.150.6.254
SWC2(config-if)#Exit
SWC2(config)#interface Vlan7
SWC2(config-if)#standby 7 ip 10.150.7.254
SWC2(config-if)#Exit
```

Figure 3.36 : Configuration du HSRP en mode standby sur SWC2 pour les VLANs 2-3.

- ✓ Nous avons vérifié la configuration de HSRP pour tous les VLANs avec la commande « **Show standby brief** » sur les deux switchs.

```
SWC1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
V12         2    110 P Active   local           10.150.2.253    10.150.2.254
V13         3    110 P Active   local           10.150.3.253    10.150.3.254
V14         4    110 P Active   local           10.150.4.253    10.150.4.254
V15         5    110 P Active   local           10.150.5.253    10.150.5.254
V16         6    110 P Active   local           10.150.6.253    10.150.6.254
V17         7    110 P Active   local           10.150.7.253    10.150.7.254
V18         8    100   Standby  10.150.8.253    local           10.150.8.254
V19         9    100   Standby  10.150.9.253    local           10.150.9.254
V110        10   100   Standby  10.150.10.253   local           10.150.10.254
V111        11   100   Standby  10.150.11.253   local           10.150.11.254
V112        12   100   Standby  10.150.12.253   local           10.150.12.254
V113        13   100   Standby  10.150.13.253   local           10.150.13.254
V114        14   100   Standby  10.150.14.253   local           10.150.14.254
```

Figure 3.37 : Vérification de la configuration de HSRP de l'ensemble des VLANs au niveau de SWC1.

```
SWC2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
V12         2    100   Standby  10.150.2.252    local           10.150.2.254
V13         3    100   Standby  10.150.3.252    local           10.150.3.254
V14         4    100   Standby  10.150.4.252    local           10.150.4.254
V15         5    100   Standby  10.150.5.252    local           10.150.5.254
V16         6    100   Standby  10.150.6.252    local           10.150.6.254
V17         7    100   Standby  10.150.7.252    local           10.150.7.254
V18         8    110 P Active   local           10.150.8.252    10.150.8.254
V19         9    110 P Active   local           10.150.9.252    10.150.9.254
V110        10   110 P Active   local           10.150.10.252   10.150.10.254
V111        11   110 P Active   local           10.150.11.252   10.150.11.254
V112        12   110 P Active   local           10.150.12.252   10.150.12.254
V113        13   110 P Active   local           10.150.13.252   10.150.13.254
V114        14   110 P Active   local           10.150.14.252   10.150.14.254
```

Figure 3.38 : Vérification de la configuration de HSRP de l'ensemble des VLANs au niveau de SWC2.

4.2.13 Attribution des adresses ip aux interfaces des périphériques (routeurs, switchs et serveur)

- **Au niveau du routeur Cojek**

```
Routeur-Cojek(config)#interface GigabitEthernet4/0
Routeur-Cojek(config-if)# ip address 172.16.3.1 255.255.255.252
Routeur-Cojek(config-if)#exit
Routeur-Cojek(config)#interface GigabitEthernet5/0
Routeur-Cojek(config-if)# ip address 192.168.1.1 255.255.255.252
Routeur-Cojek(config-if)#exit
Routeur-Cojek(config)#interface GigabitEthernet6/0
Routeur-Cojek(config-if)# ip address 192.168.2.1 255.255.255.252
Routeur-Cojek(config-if)#exit
```

Figure 3.39 : Attribution des adresses ip aux interfaces du routeur Cojek EL-KSEUR.

- **Au niveau des switch cœur**

```
SWC1(config)#int gig 1/0/5
SWC1(config-if)#no switchport
SWC1(config-if)#ip address 172.16.1.1 255.255.255.252
SWC1(config-if)#ex
```

Figure 3.40 : Attribution des adresses ip a l'interface du SWC1.

```
SWC2(config)#interface gig 1/0/5
SWC2(config-if)#no switchport
SWC2(config-if)#ip add 172.16.2.1 255.255.255.252
SWC2(config-if)#ex
```

Figure 3.41 : Attribution des adresses ip a l'interface du SWC2.

- **Au niveau du serveur Cojek situer au niveau de la DM Z**

L'attribution manuelle de l'adresses IP au serveur Cojek situés au niveau de la zone démilitarisé DMZ garantit un contrôle précis sur les paramètres réseau, excluant ainsi l'utilisation du DHCP pour éviter toute fluctuation non autorisée des adresses IP assignées.

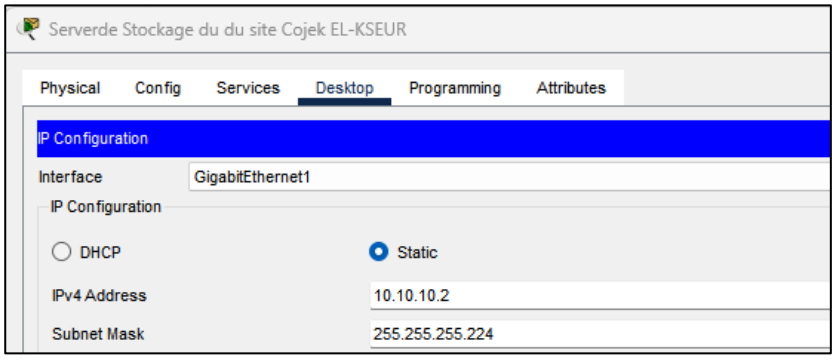


Figure 3.42 : Attribution des adresses ip a l'interface du serveur Cojek.

- L'attribution des adresses ip aux interfaces des autres périphériques se fait de la même manière.
- Pour afficher les adresses IP configurées sur un routeur ou un switch dans Packet Tracer, on utilise la commande **« show ip interface brief »** en mode privilégié. Cette commande

affiche un résumé des interfaces réseau en listant les adresses IP configurées ainsi que l'état de chaque interface (up ou down).

4.2.14 Configuration de l'OSPF

Pour assurer un routage efficace et dynamique, nous avons configuré le protocole OSPF (Open Shortest Path First) sur les switchs Coeur du site EL-KSEUR, ainsi que sur les routeurs et les pare-feu. Pour le site EL-KSEUR, le réseau utilisé est 10.150.0.0/16 et pour la DMZ (zone démilitarisée), le réseau utilisé est 10.10.10.0/27.

- **OSPF sur SWC1 du site EL-KSEUR :**

➢ Nous avons alloué le process OSPF numéro 1 et défini area 0.

➢ Nous avons saisi les réseaux directement connectés.

```
SWC1(config)#router ospf  1
SWC1(config-router)#network 172.16.1.0 0.0.0.3 area 0
SWC1(config-router)#network 10.150.0.0 0.0.255.255 area 0
SWC1(config-router)#
```

Figure 3.43 : Configuration du protocole OSPF au niveau du SWC1.

La configuration au niveau du switch SWC2 se fait de la même manière que SWC1.

- **OSPF sur les Routeurs**

➢ Chaque routeur relié aux switchs cœur utilise le même process OSPF et l'aire 10.

➢ Les réseaux connectés à ces équipements sont également configurés pour participer à l'OSPF.

➢ Un masque inversé (wildcard mask) est utilisé pour préciser les sous-réseaux dans les déclarations OSPF.

```
Routeur-Cojek(config)#router ospf 1
Routeur-Cojek(config-router)#network 172.16.3.0 0.0.0.3 area 0
Routeur-Cojek(config-router)#network 192.168.1.0 0.0.0.3 area 0
Routeur-Cojek(config-router)#network 192.168.2.0 0.0.0.3 area 0
```

Figure 3.44 : Configuration du protocole OSPF au niveau du routeur Cojek du site EL-KSEUR.

```
Router-algrie-Tlcom-1(config)#router ospf 1
Router-algrie-Tlcom-1(config-router)#network 192.168.1.0 0.0.0.3 area 0
Router-algrie-Tlcom-1(config-router)#network 192.168.3.0 0.0.0.3 area 0
Router-algrie-Tlcom-1(config-router)#exit
```

Figure 3.45 : Configuration du protocole OSPF au niveau du routeur Algérie télécom 1.

```
Router-algrie-Tlcom-2(config)#router ospf 1
Router-algrie-Tlcom-2(config-router)#network 192.168.2.0 0.0.0.3 area 0
Router-algrie-Tlcom-2(config-router)#network 192.168.4.0 0.0.0.3 area 0
Router-algrie-Tlcom-2(config-router)#exit
```

Figure 3.46 : Configuration du protocole OSPF au niveau du routeur Algérie télécom 2.

```
Router-site-central(config)#router ospf 1
Router-site-central(config-router)#network 192.168.5.0 0.0.0.3 area 0
Router-site-central(config-router)#network 192.168.4.0 0.0.0.3 area 0
Router-site-central(config-router)#network 192.168.3.0 0.0.0.3 area 0
Router-site-central(config-router)#exit
```

Figure 3.47 : Configuration du protocole OSPF au niveau du routeur du site Central de béjaia.

- Pour afficher la configuration OSPF (Open Shortest Path First) sur un routeur ou un switch de niveau 3 dans Packet Tracer, on utilise la commande **« show ip ospf database »,** cette commande permet d'afficher le contenu de la base de données OSPF, qui contient des informations sur les **L**ink **S**tate **A**dvertisements (LSAs) échangés entre les routeurs OSPF dans le réseau.
- La commande « **show ip route** » sur un routeur et un switch Cisco affiche la table de routage IP complète, incluant toutes les routes connues par le dispositif. Cette commande est essentielle pour vérifier les routes configurées et pour diagnostiquer des problèmes de routage.

```
Routeur-Cojek#sh ip ospf database
            OSPF Router with ID (192.168.2.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link cou
192.168.2.1     192.168.2.1     1338        0x80000015 0x00f024 3
1.1.1.1         1.1.1.1         1338        0x80000015 0x00a1f5 3
192.168.4.2     192.168.4.2     1334        0x8000000f 0x00d2cc 2
192.168.5.1     192.168.5.1     1334        0x80000015 0x007d2c 3
192.168.3.1     192.168.3.1     1334        0x8000000f 0x00acfa 2
172.16.1.1      172.16.1.1      44          0x8000009b 0x0061ad 14
1.1.2.2         1.1.2.2         6           0x80000048 0x007b96 2
172.16.2.1      172.16.2.1      4           0x8000009c 0x00524e 14

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.16.3.1      192.168.2.1     1310        0x80000004 0x0086b7
172.16.1.1      172.16.1.1      1324        0x80000004 0x0030b8
172.16.2.1      172.16.2.1      1319        0x8000002b 0x00dfec
10.150.12.253   172.16.2.1      1318        0x8000002c 0x00c065
10.150.11.253   172.16.2.1      1317        0x8000002d 0x006da9
192.168.2.2     192.168.4.2     1316        0x80000004 0x00415f
192.168.3.2     192.168.5.1     1315        0x8000000a 0x002ffd
10.150.5.253    172.16.2.1      1313        0x8000002e 0x006383
10.150.8.253    172.16.2.1      1313        0x8000002f 0x007e5e
 --More--
```

Figure 3.48 : Affichage du contenu de la base de données OSPF sur le routeur Cojek.

```
SWC1#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
O       10.10.10.0/27 [110/6] via 172.16.1.2, 09:01:28, GigabitEthernet1/0/5
C       10.150.2.0/24 is directly connected, Vlan2
C       10.150.3.0/24 is directly connected, Vlan3
C       10.150.4.0/24 is directly connected, Vlan4
C       10.150.5.0/24 is directly connected, Vlan5
C       10.150.6.0/24 is directly connected, Vlan6
C       10.150.7.0/24 is directly connected, Vlan7
C       10.150.8.0/24 is directly connected, Vlan8
C       10.150.9.0/24 is directly connected, Vlan9
C       10.150.10.0/24 is directly connected, Vlan10
C       10.150.11.0/24 is directly connected, Vlan11
C       10.150.12.0/24 is directly connected, Vlan12
C       10.150.13.0/24 is directly connected, Vlan13
C       10.150.14.0/24 is directly connected, Vlan14
     172.16.0.0/30 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, GigabitEthernet1/0/5
O       172.16.2.0 [110/2] via 10.150.2.253, 00:51:09, Vlan2
                   [110/2] via 10.150.3.253, 00:51:09, Vlan3
                   [110/2] via 10.150.4.253, 00:51:09, Vlan4
                   [110/2] via 10.150.5.253, 00:51:09, Vlan5
                   [110/2] via 10.150.6.253, 00:51:09, Vlan6
                   [110/2] via 10.150.7.253, 00:51:09, Vlan7
                   [110/2] via 10.150.8.253, 00:51:09, Vlan8
                   [110/2] via 10.150.9.253, 00:51:09, Vlan9
                   [110/2] via 10.150.10.253, 00:51:09, Vlan10
                   [110/2] via 10.150.11.253, 00:51:09, Vlan11
                   [110/2] via 10.150.12.253, 00:51:09, Vlan12
 --More-- |
```

Figure 3.49 : Affichage de la table de routage sur le SWC1

```
Routeur-Cojek#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
O       10.10.10.0/27 [110/4] via 192.168.1.2, 09:03:25, GigabitEthernet5/0
                      [110/4] via 192.168.2.2, 09:03:25, GigabitEthernet6/0
O       10.150.2.0/24 [110/3] via 172.16.3.2, 00:53:21, GigabitEthernet4/0
O       10.150.3.0/24 [110/3] via 172.16.3.2, 00:53:21, GigabitEthernet4/0
O       10.150.4.0/24 [110/3] via 172.16.3.2, 00:54:18, GigabitEthernet4/0
O       10.150.5.0/24 [110/3] via 172.16.3.2, 00:53:21, GigabitEthernet4/0
O       10.150.6.0/24 [110/3] via 172.16.3.2, 00:53:21, GigabitEthernet4/0
O       10.150.7.0/24 [110/3] via 172.16.3.2, 00:53:21, GigabitEthernet4/0
O       10.150.8.0/24 [110/3] via 172.16.3.2, 00:53:21, GigabitEthernet4/0
O       10.150.9.0/24 [110/3] via 172.16.3.2, 00:53:21, GigabitEthernet4/0
O       10.150.10.0/24 [110/3] via 172.16.3.2, 00:53:21, GigabitEthernet4/0
O       10.150.11.0/24 [110/3] via 172.16.3.2, 00:53:21, GigabitEthernet4/0
O       10.150.12.0/24 [110/3] via 172.16.3.2, 00:53:21, GigabitEthernet4/0
O       10.150.13.0/24 [110/3] via 172.16.3.2, 00:53:21, GigabitEthernet4/0
O       10.150.14.0/24 [110/3] via 172.16.3.2, 00:53:21, GigabitEthernet4/0
     172.16.0.0/30 is subnetted, 3 subnets
O       172.16.1.0 [110/2] via 172.16.3.2, 09:03:25, GigabitEthernet4/0
O       172.16.2.0 [110/2] via 172.16.3.2, 09:03:25, GigabitEthernet4/0
C       172.16.3.0 is directly connected, GigabitEthernet4/0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, GigabitEthernet5/0
     192.168.2.0/30 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, GigabitEthernet6/0
     192.168.3.0/30 is subnetted, 1 subnets
 --More--
```

Figure 3.50 : Affichage de la table de routage sur le routeur Cojek.

4.2.15 Configuration du pare-feu

a) Configuration de base ainsi que les interfaces des pare-feu

La configuration de base des pare-feu implique la définition des paramètres essentiels et des interfaces principales pour sécuriser le réseau. Chaque pare-feu est doté d'interfaces spécifiques, telles qu'Outside (externe), Inside (interne), et éventuellement DMZ (zone démilitarisée) pour les serveurs accessibles depuis Internet. Chaque interface reçoit une adresse IP et un niveau de sécurité, déterminant la confiance accordée à cette zone. Cette configuration contrôle et sécurise efficacement le trafic réseau tout en assurant la connectivité et l'isolation nécessaires selon les besoins de l'organisation.

```
FW-EL-KSEUR(config)#hostname FW-EL-KSEUR
FW-EL-KSEUR(config)#enable password firewall
FW-EL-KSEUR(config)#interface gig 1/1
FW-EL-KSEUR(config-if)#ip add 172.16.3.2 255.255.255.252
FW-EL-KSEUR(config-if)#nameif OUTSIDE
FW-EL-KSEUR(config-if)#security-level 0
FW-EL-KSEUR(config-if)#exit
FW-EL-KSEUR(config)#interface gi 1/2
FW-EL-KSEUR(config-if)#ip add 172.16.1.2 255.255.255.252
FW-EL-KSEUR(config-if)#nameif INSIDE1
FW-EL-KSEUR(config-if)#security-level 100
FW-EL-KSEUR(config-if)#exit
FW-EL-KSEUR(config)#interface gi 1/3
FW-EL-KSEUR(config-if)#ip add 172.16.2.2 255.255.255.252
FW-EL-KSEUR(config-if)#nameif INSIDE2
FW-EL-KSEUR(config-if)#security-level 100
FW-EL-KSEUR(config-if)#exit
FW-EL-KSEUR(config)#wr mem
Building configuration...
Cryptochecksum: ld552aac 2485058c 1a300ac9 6c65308a

1226  bytes copied in 2.637 secs (464 bytes/sec)
[OK]
```

Figure 3.51 : Configuration de base et les interfaces du pare-feu FW-EL-KSEUR.

```
ciscoasa(config)#hostname FW-Du-Site-Central
FW-Du-Site-Central(config)#enable password firewall
FW-Du-Site-Central(config)#interface gig 1/1
FW-Du-Site-Central(config-if)#ip add 192.168.5.2 255.255.255.252
FW-Du-Site-Central(config-if)#nameif OUTSIDE
INFO: Security level for "OUTSIDE" set to 0 by default.
FW-Du-Site-Central(config-if)#security-level 0
FW-Du-Site-Central(config-if)#exit
FW-Du-Site-Central(config)#interface gi 1/2
FW-Du-Site-Central(config-if)#ip add 10.10.10.1  255.255.255.224
FW-Du-Site-Central(config-if)#nameif DMZ
INFO: Security level for "DMZ" set to 0 by default.
FW-Du-Site-Central(config-if)#security-level 70
FW-Du-Site-Central(config-if)#exit
FW-Du-Site-Central(config)#wr mem
Building configuration...
Cryptochecksum: ld552aac 2485058c 1a300ac9 6c65308a

1194  bytes copied in 2.888 secs (413 bytes/sec)
[OK]
```

Figure 3.52 : Configuration de base et les interfaces du pare-feu du site central béjaia.

- Pour afficher la configuration de base sur un pare-feu Cisco ASA, on utilise la commande « **show running-config** » et pour afficher les adresses ip assignés au diffèrent interface on utilise la commande « **show ip address** ».

```
FW-EL-KSEUR#sh ip address
System IP Addresses:
Interface              Name                IP address      Subnet mask     Method
GigabitEthernet1/1     OUTSIDE             172.16.3.2      255.255.255.252 manual
GigabitEthernet1/2     INSIDE1             172.16.1.2      255.255.255.252 manual
GigabitEthernet1/3     INSIDE2             172.16.2.2      255.255.255.252 manual
GigabitEthernet1/4                         unassigned      unassigned      unset
GigabitEthernet1/5                         unassigned      unassigned      unset
GigabitEthernet1/6                         unassigned      unassigned      unset
GigabitEthernet1/7                         unassigned      unassigned      unset
GigabitEthernet1/8                         unassigned      unassigned      unset
Management1/1                              unassigned      unassigned      unset

Current IP Addresses:
Interface              Name                IP address      Subnet mask     Method
GigabitEthernet1/1     OUTSIDE             172.16.3.2      255.255.255.252 manual
GigabitEthernet1/2     INSIDE1             172.16.1.2      255.255.255.252 manual
GigabitEthernet1/3     INSIDE2             172.16.2.2      255.255.255.252 manual
GigabitEthernet1/4                         unassigned      unassigned      unset
GigabitEthernet1/5                         unassigned      unassigned      unset
GigabitEthernet1/6                         unassigned      unassigned      unset
GigabitEthernet1/7                         unassigned      unassigned      unset
GigabitEthernet1/8                         unassigned      unassigned      unset
Management1/1                              unassigned      unassigned      unset
```

Figure 3.53 : Les adresses ip asignés aux differentes interfaces du parfe-feu du site EL-KSEUR.

b) Configuration du protocole OSPF sur les pare-feu

La configuration du protocole OSPF au niveau d'un pare-feu, suit généralement plusieurs principes pour assurer un routage efficace et sécurisé au sein du réseau comme le montre les figures :

```
FW-Du-Site-Central(config)#router ospf 1
FW-Du-Site-Central(config-router)#network 192.168.5.0 255.255.255.252 area 0
FW-Du-Site-Central(config-router)#network 10.10.10.0 255.255.255.252 area 0
FW-Du-Site-Central(config-router)#
```

Figure 3.54 : Configuration du protocole OSPF au niveau du pare-feu du site central de béjaia.

```
FW-EL-KSEUR(config)#router ospf 1
FW-EL-KSEUR(config-router)#network  172.16.1.0 255.255.255.252 area 0
FW-EL-KSEUR(config-router)#network  172.16.2.0 255.255.255.252 area 0
FW-EL-KSEUR(config-router)#network  172.16.3.0 255.255.255.252 area 0
```

Figure 3.55 : Configuration du protocole OSPF au niveau du pare-feu EL KSEUR.

Bien que les masques inversés soient souvent utilisés pour la configuration OSPF sur les routeurs et les switchs en raison de la syntaxe spécifique à OSPF, les pare-feus peuvent opter pour des masques de sous-réseau normaux pour des raisons de convention ou de compatibilité avec leurs systèmes d'exploitation respectifs.

- La commande « **show running-config** » affiche toute la configuration en cours, y compris la section relative à OSPF.

- ✓ La commande « **show route** » sur un pare-feu Cisco ASA affiche la table de routage, incluant toutes les routes connues par le pare-feu. Cette table de routage contient des informations sur les routes connectées, statiques, et dynamiques comme OSPF.

```
FW-EL-KSEUR#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
O       10.10.10.0 255.255.255.224 [110/5] via 172.16.3.1, OUTSIDE, 08:35:36, GigabitEthernet1/1
O       10.150.2.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:25:22, GigabitEthernet1/2
                                 [110/2] via 172.16.2.1, INSIDE2, 00:25:22, GigabitEthernet1/3
O       10.150.3.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:25:22, GigabitEthernet1/2
                                 [110/2] via 172.16.2.1, INSIDE2, 00:25:22, GigabitEthernet1/3
O       10.150.4.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:26:21, GigabitEthernet1/2
                                 [110/2] via 172.16.2.1, INSIDE2, 00:26:21, GigabitEthernet1/3
O       10.150.5.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:25:22, GigabitEthernet1/2
                                 [110/2] via 172.16.2.1, INSIDE2, 00:25:22, GigabitEthernet1/3
O       10.150.6.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:25:22, GigabitEthernet1/2
                                 [110/2] via 172.16.2.1, INSIDE2, 00:25:22, GigabitEthernet1/3
O       10.150.7.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:25:22, GigabitEthernet1/2
                                 [110/2] via 172.16.2.1, INSIDE2, 00:25:22, GigabitEthernet1/3
O       10.150.8.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:25:22, GigabitEthernet1/2
                                 [110/2] via 172.16.2.1, INSIDE2, 00:25:22, GigabitEthernet1/3
O       10.150.9.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:25:22, GigabitEthernet1/2
                                 [110/2] via 172.16.2.1, INSIDE2, 00:25:22, GigabitEthernet1/3
O       10.150.10.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:25:22, GigabitEthernet1/2
                                  [110/2] via 172.16.2.1, INSIDE2, 00:25:22, GigabitEthernet1/3
O       10.150.11.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:25:22, GigabitEthernet1/2
                                  [110/2] via 172.16.2.1, INSIDE2, 00:25:22, GigabitEthernet1/3
O       10.150.12.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:25:22, GigabitEthernet1/2
                                  [110/2] via 172.16.2.1, INSIDE2, 00:25:22, GigabitEthernet1/3
O       10.150.13.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:25:22, GigabitEthernet1/2
                                  [110/2] via 172.16.2.1, INSIDE2, 00:25:22, GigabitEthernet1/3
O       10.150.14.0 255.255.255.0 [110/2] via 172.16.1.1, INSIDE1, 00:25:22, GigabitEthernet1/2
                                  [110/2] via 172.16.2.1, INSIDE2, 00:25:22, GigabitEthernet1/3
     172.16.0.0/30 is subnetted, 4 subnets
```

Figure 3.56 : Affichage de la table de routage sur le pare-feu FW EL-KSEUR.

c) Configuration des ACL sur les pare-feu

La configuration des ACL (Listes de Contrôle d'Accès) étendues sur les pare-feu permet de définir des règles précises de filtrage du trafic réseau, renforçant ainsi la sécurité de l'infrastructure. Les ACL étendues peuvent filtrer le trafic basé sur les adresses IP source et destination, les protocoles et les numéros de ports. Dans ce travail Nous allons configurer des ACL étendues sur les pare-feu du site central et de El-Kseur.

Le tableau 3.6 fournit une référence des ports utilisés par différents protocoles pour être utilisée dans la configuration ACL.

Protocoles	Port (TCP)	Port (UDP)
FTP /FTP Données	20/21	-
DNS	53	53
DHCP	-	67, 68
HTTP	80	-

Tableau 3.6 : Configuration des ACL - Protocoles et Ports autorisés au niveau des pare-feu**.**

Les lignes de configuration suivantes définissent des listes de contrôle d'accès (ACL) et les appliquent aux interfaces spécifiques sur les pare-feu du site central et de El Kseur.

```
FW-EL-KSEUR(config)#access-list RES extended permit icmp any any
FW-EL-KSEUR(config)#access-list RES extended permit tcp any any eq 80
FW-EL-KSEUR(config)#access-list RES extended permit tcp any any eq 53
FW-EL-KSEUR(config)#access-list RES extended permit udp any any eq 53
FW-EL-KSEUR(config)#access-list RES extended permit tcp any any eq 20
FW-EL-KSEUR(config)#access-list RES extended permit tcp any any eq 21
FW-EL-KSEUR(config)#access-list RES extended permit udp any any eq 67
FW-EL-KSEUR(config)#access-list RES extended permit udp any any eq 68
FW-EL-KSEUR(config)#
FW-EL-KSEUR(config)#
FW-EL-KSEUR(config)# access-group RES in interface OUTSIDE
```

Figure 3.57 : Configuration des ACL au niveau du Pare-Feu du site EL KSEUR.

```
FW-Du-Site-Central(config)#access-list RES extended permit icmp any any
FW-Du-Site-Central(config)#access-list RES extended permit tcp any any eq 80
FW-Du-Site-Central(config)#access-list RES extended permit tcp any any eq 53
FW-Du-Site-Central(config)#access-list RES extended permit udp any any eq 53
FW-Du-Site-Central(config)#access-list RES extended permit tcp any any eq 20
FW-Du-Site-Central(config)#access-list RES extended permit tcp any any eq 21
FW-Du-Site-Central(config)#access-list RES extended permit udp any any eq 67
FW-Du-Site-Central(config)#access-list RES extended permit udp any any eq 68
FW-Du-Site-Central(config)#
FW-Du-Site-Central(config)#access-group RES in interface DMZ
FW-Du-Site-Central(config)#access-group RES in interface OUTSIDE
```

Figure 3.58 : Configuration des ACL au niveau du Pare-Feu du site central Béjaia.

- **Définition des Règles ACL** : Les règles ACL définissent quels types de trafic (ICMP, TCP, UDP) et quels ports (HTTP, DNS, FTP, DHCP) sont autorisés entre n'importe quelles adresses IP.
- **Application des ACL aux Interfaces** : Les ACL sont appliquées aux interfaces spécifiques (DMZ et OUTSIDE) pour contrôler le trafic entrant sur ces interfaces.

5 Vérification de la communication

Après avoir déployé notre réseau, nous entamons l'étape cruciale de validation de son bon fonctionnement. Cette phase implique la vérification de la connectivité entre tous les équipements en utilisant la commande **Ping**.

Nous commencerons par tester les équipements tels que les switchs, avant de vérifier la communication inter-VLAN, intra-VLAN et inter-site. Il est important de souligner que la Commande « **Ping** » est un outil efficace pour confirmer la réactivité d'un dispositif au sein du réseau.

Exemple : Test réussi entre les deux switchs cœurs SWC1 et SWC2.

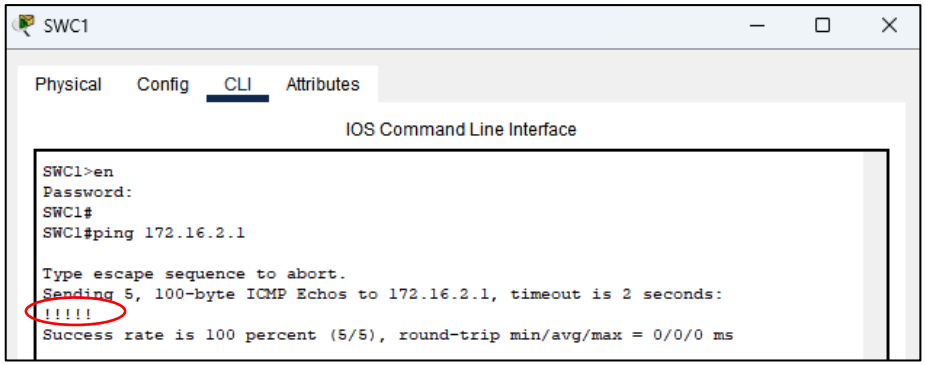


Figure 3.59 : Test de communication entre le switch SWC1 et SWC2.

Ces lignes représentent la sortie d'une commande « **ping** » exécutée sur le switch SWC1 en direction de l'adresse IP 172.16.2.1 du Switch SWC2.

« !!!!! » : Les cinq points d'exclamation représentent les réponses reçues du périphérique cible, indiquant une connectivité réussie.

5.1 Test intra-VLAN

La communication intra VLAN se réfère aux échanges de données entre dispositifs qui appartiennent au même VLAN.

Exemple : Tests réussis entre PC 8 (10.150.12.127) et le PC 9 (10.150.12.128) qui

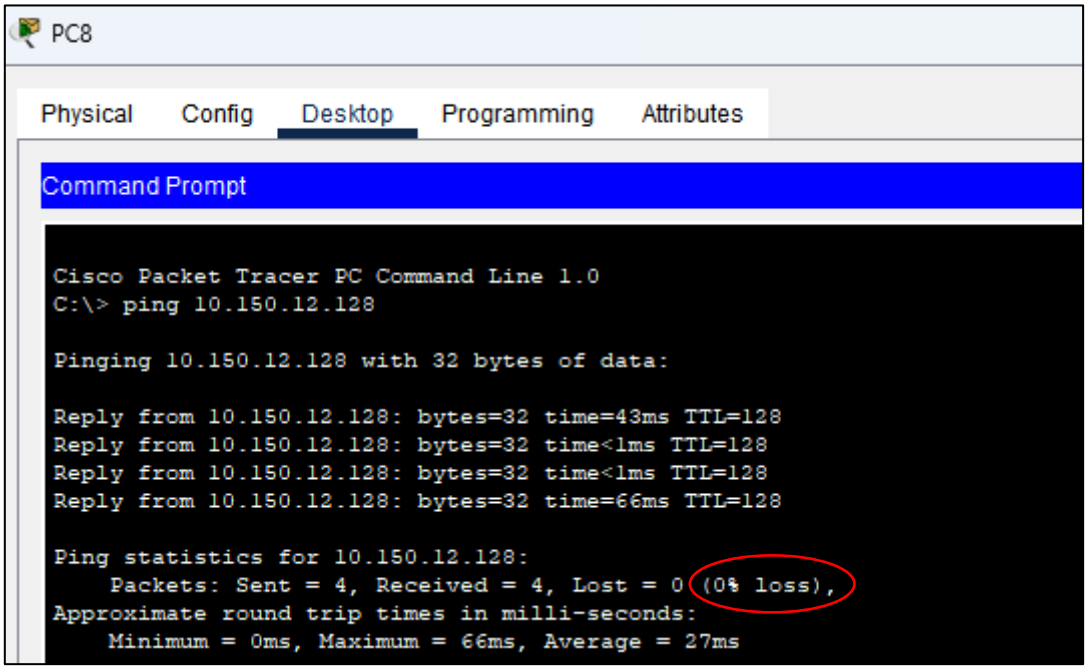


Figure 3.60 : Test de communication intra-VLAN entre le PC8 et le PC9.
appartiennent au même Vlan12.

Les lignes Reply from 10.150.12.128 confirment que toutes les requêtes ping ont été transmises avec succès et ont reçu une réponse. Les statistiques indiquent qu'il n'y a eu aucune perte de paquets (Lost = 0) et les temps de réponse sont très rapides (entre 0 et 10 ms, avec une

moyenne de 2 ms). Cela démontre une excellente connectivité réseau avec l'adresse IP 10.150.12.128.

5.2 Test inter-VLAN

La communication inter VLAN se réfère aux échanges de données entre dispositifs appartenant à des VLANs différents, nécessitant un routage via un routeur ou un switch de couche 3.

Exemple : Test réussi entre PC2 (10.150.4.1) et PC4 (10.150.7.1) qui appartiennent à différentes VLANs.

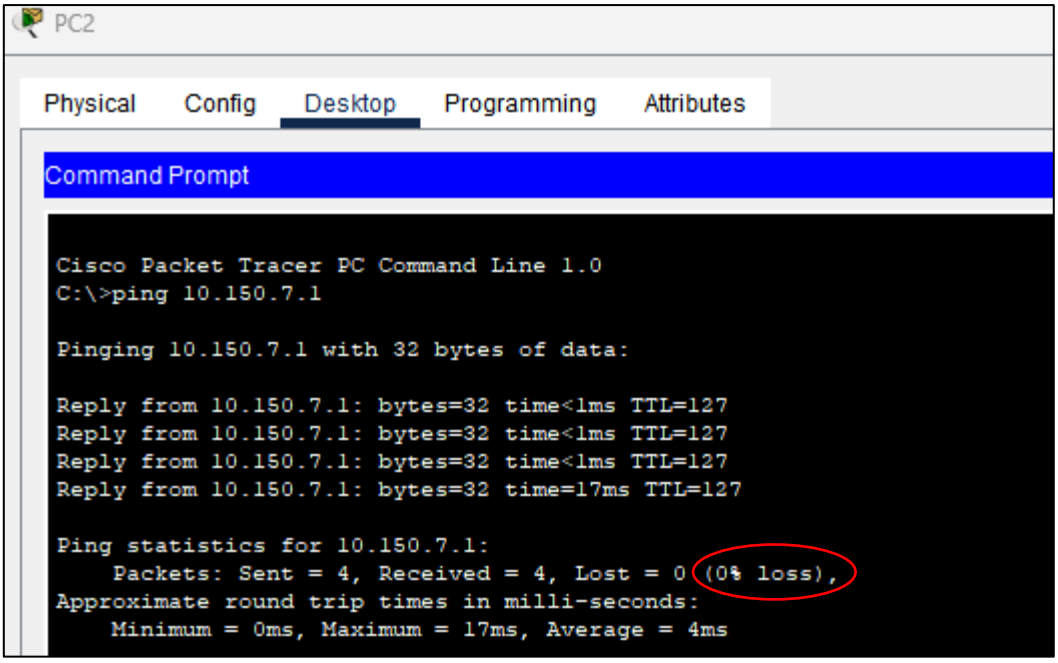


Figure 3.61 : Test de communication inter-VLAN entre le PC 2 et le PC 4.

Les lignes Reply from 10.150.7.1 montrent que les réponses ont été reçues pour toutes les requêtes envoyées, et les statistiques de ping confirment qu'il n'y a eu aucune perte de paquet (Lost = 0). Les temps de réponse (entre 0 et 12 ms) indiquent que les communications sont rapides et stables. Ainsi, le ping a bien été transmis et reçu sans aucune perte, confirmant une bonne connectivité réseau.

5.3 Test d'accès à distance

a) Comment vérifier si la connexion a abouti :

Pour tester si la connexion SSH est réussie, nous effectuons les étapes suivantes sur le PC8 administrateur avec l'IP static 10.150.12.127 :

1. Ouvrir une fenêtre de commande sur le PC.
2. Exécuter la commande SSH :

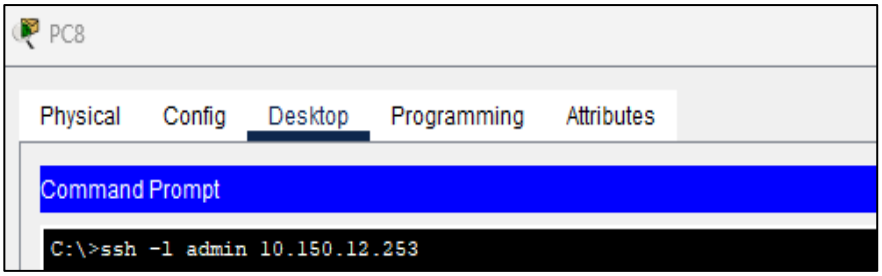


Figure 3.62 : Test de connexion SSh.

Cette commande essaie de se connecter au système à l'adresse IP 10.150.12.253 en utilisant le nom d'utilisateur admin via le protocole SSH. Une fois exécutée, elle demandera le mot de passe associé à cet utilisateur (admin) pour compléter la connexion sécurisée.

3. Saisir le mot de passe :

- Lorsque on est invité à entrer le mot de passe, entrons “cevital”.

b) Vérification de la connexion réussie :

- Si la connexion SSH est réussie, nous verrons le prompt du switch dans la fenêtre de commande.

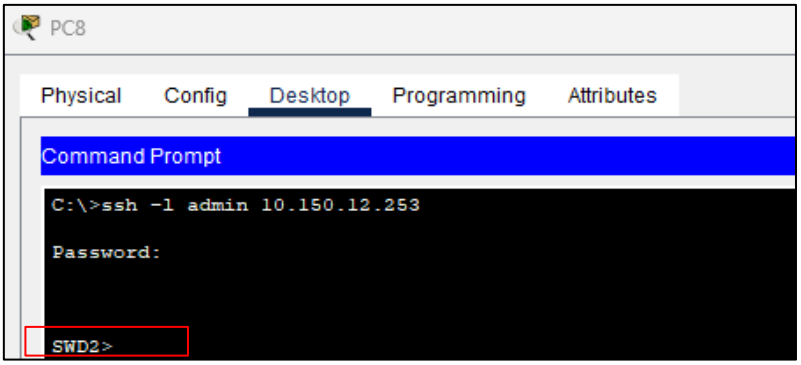


Figure 3.63 : Connexion SSh réussie.

- Si la connexion échoue, des messages d'erreur peuvent s'afficher, comme le montre **la figure 3.64 :**

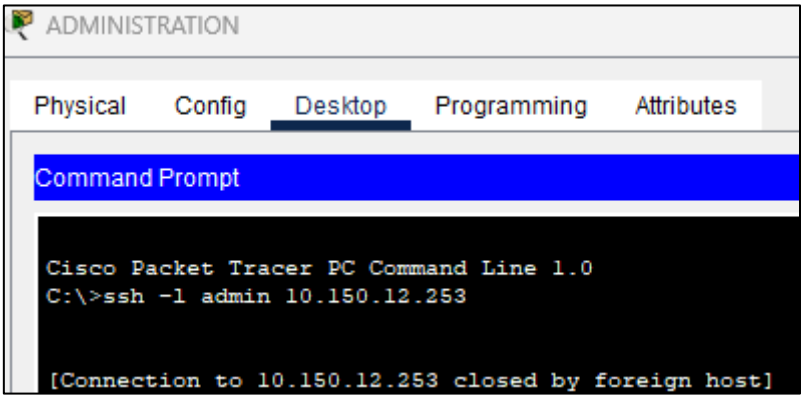


Figure 3.64 : Connexion SSh échouer.

Le message **[Connection to 10.150.12.253 closed by foreign host]** indique simplement que la connexion SSH depuis une adresse IP non autorisée (10.150.9.2) vers le switch

(10.150.12.253) a été fermée par le switch lui-même, en raison des règles d'ACL restrictives qui limitent l'accès aux seules adresses IP spécifiées dans l'ACL.

5.4 Test de Spanning-Tree Protocol

Exemple pour le VLAN 2 : on lance la commande « **show Spanning-Tree vlan 2** » sur le switch de distribution SWDS on remarque que les ports Gi 1/0/1, Gi 1/02, Gi 1/0/3, Gi 1/0/5, Gi 1/0/6 sont en état de forwarding, et le port Gi 1/0/4 est en état bloqué.

Rappel : l'état **forwarding** est l'état final et fonctionnel d'un port dans STP, où il participe pleinement au trafic réseau tout en continuant à surveiller la topologie pour assurer qu'aucune boucle ne se forme.

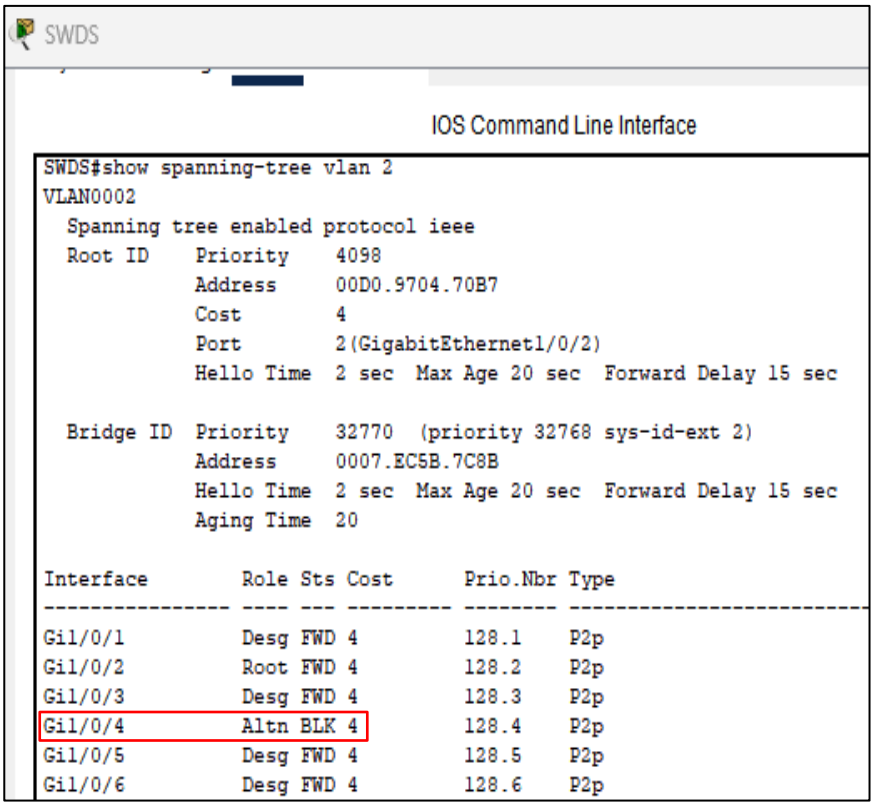


Figure 3.65: Test de spanning-tree.

Ensuite on bloque le port Gi1/0/2 et le port Gi1/0/4 passe par plusieurs états avant d'atteindre l'état de forwarding :

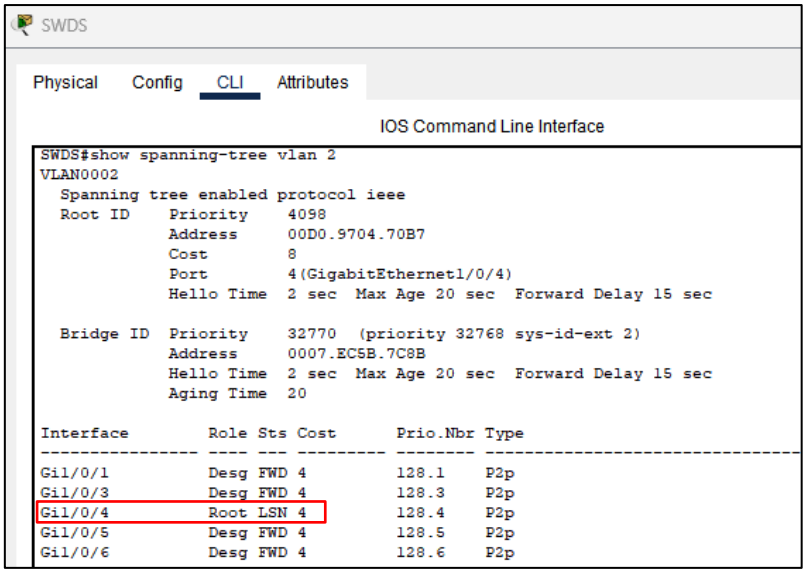


Figure 3.66 : Etat listening pour le port Gi1/0/4.

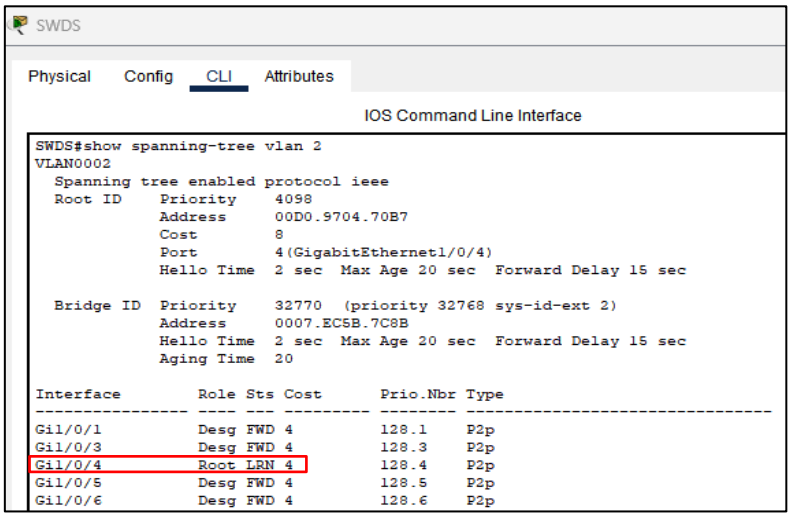


Figure 3.67 : Etat learning pour le port Gi1/0/4.

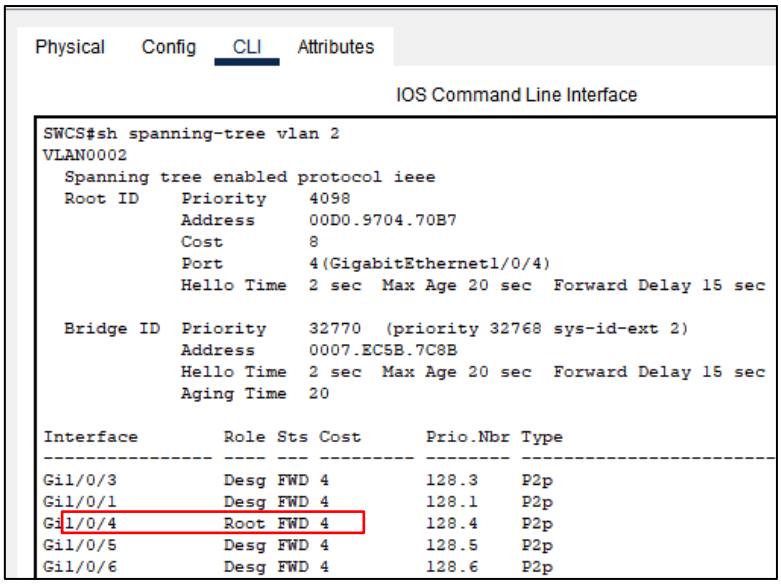


Figure 3.68 : Etat forwarding pour le port Gi1/0/4.

5.5 Simulation d'une panne sur le réseau

Nous avons débuté par un ping continu entre l'adresses IP du PC SAUCE (10.150.2.1) et le PC ADMINISTRATION (10.150.9.127). Par la suite, nous avons volontairement mis en mode « **Shutdown** » le root principal du VLAN 2, représenté par l'interface Gi1/0/2 au niveau du switch SWDS.

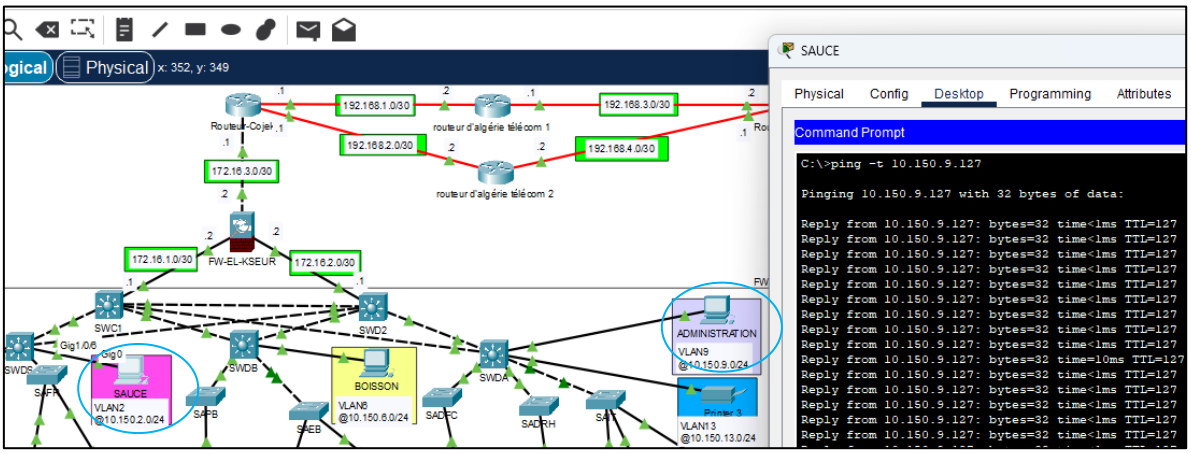


Figure 3.69 : Ping continu réussie vers le PC ADMINISTRATION.

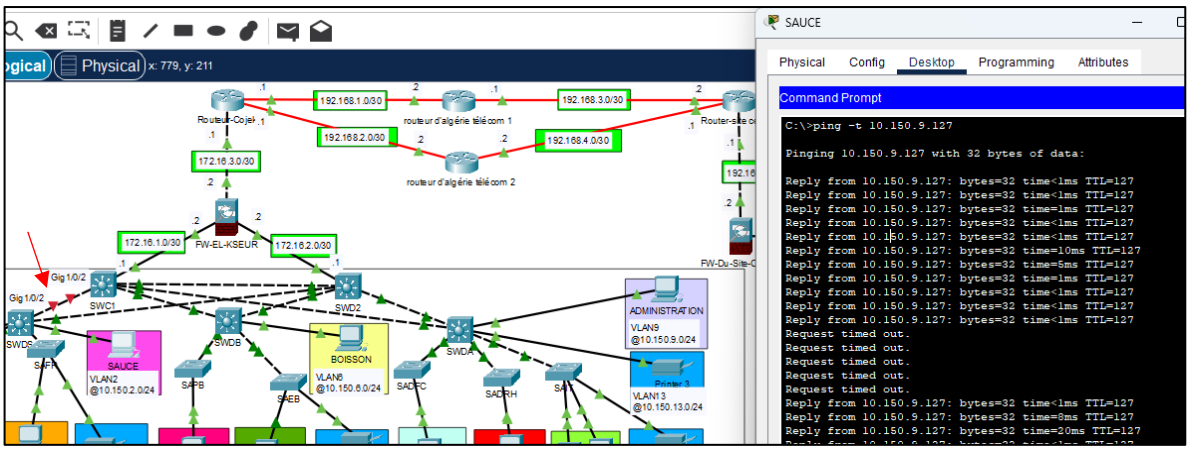


Figure 3.70 : Ping lors de la désactivation du port vers SWC1.

Avant de bloquer le port, le ping fonctionnait correctement, puis s'est arrêté temporairement avant de reprendre. La désactivation du root d'un VLAN met hors service le routeur principal, ce qui déclenche le recalcul des chemins STP par les commutateurs. Ce processus ajuste la topologie du réseau pour éviter les boucles et rétablir la connectivité, permettant ainsi au réseau de maintenir sa stabilité opérationnelle malgré la défaillance du root principal.

5.6 Test de HSRP (Hot Standby Router Protocol)

Nous avons simulé un ping entre le PC1 (10.150.3.1) et le PC5 (10.150.8.127). Ensuite, nous avons provoqué une panne en mettant cette fois l'interface Gi1/0/1 du SWC1 qui est relié avec le SWC2 en mode « **Shutdown** ».

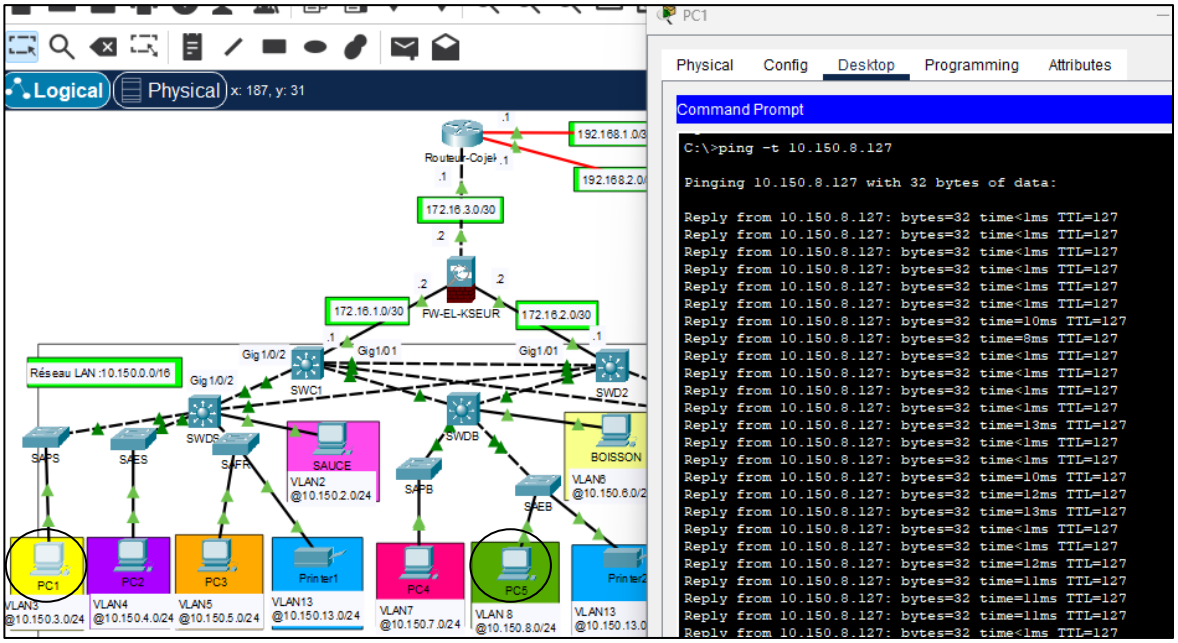


Figure 3.71 : Ping continu réussie vers le PC 5.

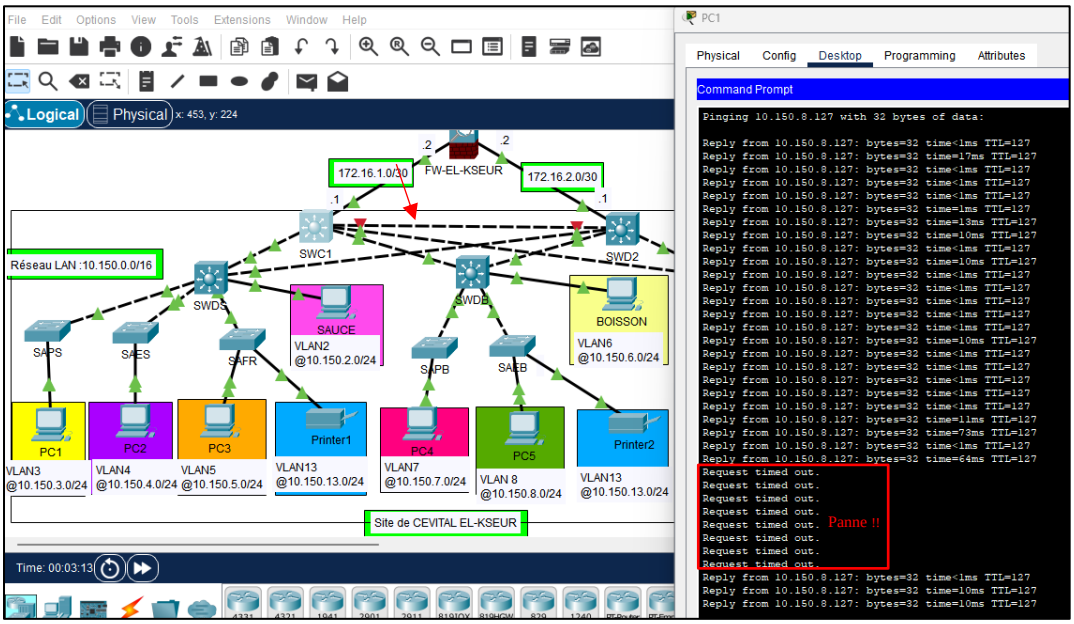


Figure 3.72 : Ping lors de la désactivation du port vers SWC2.

La figure illustre le résultat du ping après avoir provoqué la panne. Nous constatons que le ping s'arrête instantanément et ne passe plus. Après quelques interruptions, grâce au protocole HSRP, le SWC1 communique avec le SWC2 pour signaler sa panne. Le SWC2 active alors automatiquement le root en mode « **standby** » pour le passer en mode « **actif** ».

Comme illustré dans **la figure 3.72** le ping reprend, prouvant ainsi que la route a été redirigée vers le SWC2.

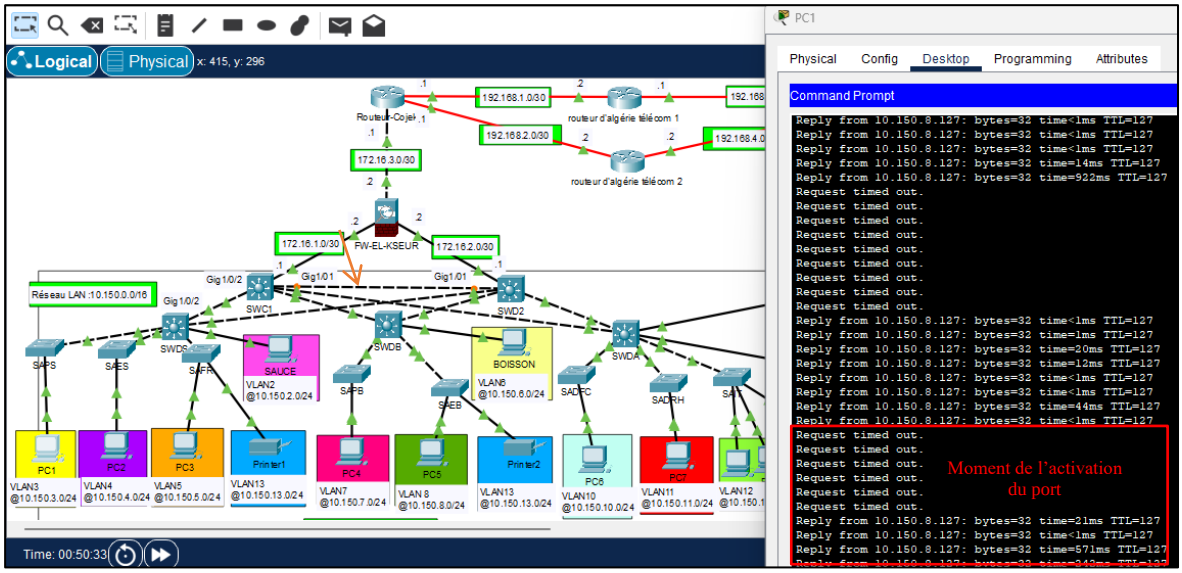


Figure 3.73 : Ping lors de l'activation du port sur le SWC1

Pour vérifier que le « **preempt** » du HSRP fonctionne correctement, nous avons réactivé l'interface principale sur le SWC1 pour observer s'il reprend sa route principale. **La figure 3.73** illustre le résultat du ping après cette réactivation. Nous constatons que le ping s'interrompt de nouveau, le temps que les deux commutateurs discutent des priorités, puis reprend immédiatement. Cela démontre que les protocoles HSRP et OSPF, mis en place pour gérer les défaillances du réseau, fonctionnent parfaitement.

5.7 Test inter-site

Après avoir confirmé le bon fonctionnement du réseau LAN du site El-Kseur et la fluidité des communications internes, la prochaine étape consiste à tester la connectivité avec le serveur situé dans la zone démilitarisée (DMZ) au site central de Béjaïa.

L'objectif est de s'assurer que les dispositifs du LAN d'El-Kseur peuvent accéder au serveur de la DMZ, tout en respectant les politiques de sécurité en vigueur.

Pour cela les outils utilisés et les étapes à suivre sont :

- ✓ **Ping** : Pour tester la connectivité de base entre un PC du LAN El-Kseur (**EX : 10.150.2.1**) et le serveur de stockage du site EL-KSEUR situer au niveau de la DMZ à Béjaïa (**10.10.10.2)**.
- ✓ **Traceroute** : Pour vérifier le chemin parcouru par les paquets et diagnostiquer les points de défaillance éventuels. **La figure 3.75** montre les résultats de deux exécutions du « **traceroute** » vers l'adresse IP 10.10.10.2

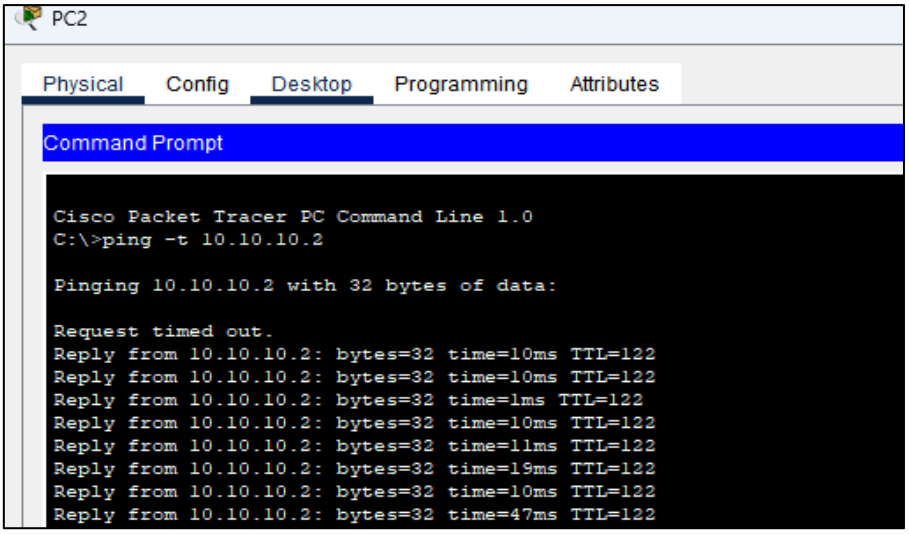


Figure 3.74 : Ping réussi entre un PC du LAN EL-KSEUR et son serveur de stockage situer au niveau de la DMZ à Béjaia.

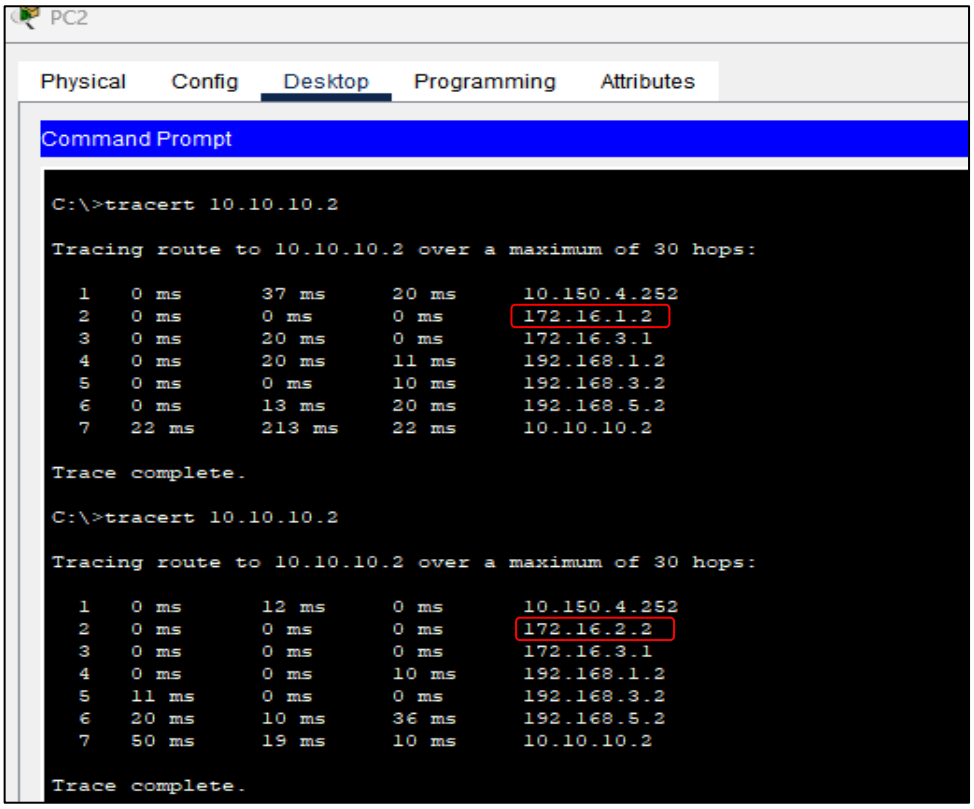


Figure 3.75 : Résultats de deux exécutions du tracert au niveau du PC2 vers l'adresse ip du serveur de stockage du site EL-KSEUR.

6 Synthèse

Dans cette partie de notre projet, nous avons d'abord évalué l'architecture réseau existante, identifié ses limitations et proposé un modèle de réseau hiérarchique avec des

couches de distribution et d'accès redondantes. Nous avons détaillé la planification du déploiement, incluant la nomination des équipements, l'adressage des interfaces et des VLANs. La mise en œuvre a été réalisée à l'aide de configurations spécifiques pour chaque équipement, garantissant l'accès à distance, la sécurité par ACL et la robustesse grâce à des protocoles comme HSRP et OSPF. Enfin, nous avons vérifié la communication intra- et inter-VLAN, testé la résilience du réseau face à des pannes simulées et validé la configuration du protocole de redondance.

Cette approche méthodique nous a permis de créer un réseau solide et fiable, capable de répondre aux besoins de l'entreprise tout en assurant une haute disponibilité et une sécurité renforcée.

7 Conclusion

Ce chapitre a été dédié à l'amélioration de la sécurité et de la disponibilité du réseau de Cevital. La simulation de la topologie a révélé des résultats satisfaisants. Nous avons proposé des solutions pour corriger les insuffisances en matière de sécurité et de disponibilité du réseau et nous avons pu démontrer que cette solution constituait une réponse adéquate à la problématique initiale

Conclusion générale

La mise en place d'un réseau LAN sécurisé et redondant au sein de Cevital représente une avancée significative pour améliorer l'efficacité opérationnelle et renforcer la sécurité des communications internes. Ce projet a débuté par une analyse approfondie de l'infrastructure existante de Cevital, mettant en lumière ses défis et ses lacunes. Nous avons alors proposé une architecture réseau optimisée intégrant des concepts avancés tels que les VLANs, le protocole STP pour la redondance, le HSRP pour la haute disponibilité des routeurs, ainsi que des protocoles de sécurité comme SSH et les ACL.

La refonte de l'architecture a été guidée par la création de modèles hiérarchiques, l'implémentation judicieuse de la redondance, et la sécurisation avec une zone démilitarisée (DMZ), démontrant notre engagement envers la protection des données et la continuité des opérations. La mise en œuvre pratique de ces solutions a été méthodique, comprenant des configurations détaillées et des tests rigoureux pour garantir la performance et la fiabilité du réseau.

Les tests de vérification ont confirmé que notre nouvelle architecture répond pleinement aux exigences de sécurité et de performance, tout en minimisant les risques d'interruption des services critiques. En conclusion, ce projet représente non seulement une évolution technique significative, mais également une réponse stratégique aux défis croissants de gestion et de sécurisation des réseaux d'entreprise. Il positionne Cevital sur une voie solide pour soutenir sa croissance future tout en assurant une connectivité fiable et sécurisée pour tous ses utilisateurs et services.

Bibliographie

[1] Source interne de l'entreprise CEVITAL.

[2] G. PUJOLLE, Les Réseaux, 5 éd., Paris: EYROLLES, 2006, pp. 6-7.

[3] J.-F. Pillou, Tout sur les Réseaux et Internet, 5 éd., DUNOD, 2020, p. 4.

[4] D. DROMARD et D. SERET, Architecture des Réseaux, paris: Pearson Education France, 2009.

[5] D. M. YAZID, «Réseaux Informatiques,» Université A. MIRA de Béjaia Faculté des Sciences Exactes Département d'Informatique, Béjaia, 2016/21017.

[6] T. Dean, Réseaux Informatique, 2 éd., RYNALD GOULET, 2001.

[7] Apprenez le fonctionnement des réseaux TCP/IP, OPENCLASSROOMS, 2013.

[8] P. ATELIN et J. DORDOIGNE, Réseaux informatique Notions fondamentales Normes, Architecture, Modèle OSI, TCP/IP; Ethernet, Wi-Fi,..., ENI éd., 2006, p. 61.

[9] G. PUJOLL, Les réseaux, 8 éd., Eyrolles, Éd., Paris, 2008.

[10] E. Lalitte , Apprenz le fonctionnement des réseaux TCP/IP, 4 éd., EYROLLES, 2009.

[11] S. Balaji Sivasubramanian et . R. T. Froom, Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide : Foundation Learning for SWITCH 642-813, Cisco Press, 2013.

[12] B. Kercheval, DHCP: a guide for TCP/IP network configuration, P. Hall, Éd., 1999.

[13] V. A, Cisco CCNA, ENI édition, 2010.

[14] T. George, *Introduction to Spanning Tree Protocol*, vol. 6, Contemporary Controls Systems, INC , 2005.

[15] N. Salmoon, «Redondance de routeur avec HSRP >>> HSRP : Hot Standby Routing Protocol,» n° %1226, 2011.

[16] F. B. Andrew Faulkner, «Avantages et faiblesses du protocole SSH,» n° %12, 2009.

[17] OFPPT, « Module : SECURITE DE RESEAUX INFORMATIQUES Support de cours & Aide-Mémoire V1.0».

Webographie

[W1] https://www.netacad.com/fr/courses/packet-tracer/faq#01

[W2] https://openclassrooms.com/fr/courses/6944606-concevez-votre-reseau-tcp-ip/7236472-prenez-du-recul-sur-votre-pratique-grace-au-modele-osi

[W3] https://isrdoc.wordpress.com/wp-content/uploads/2010/11/a12.png

[W4] https://www.frameip.com/hsrp-cisco-securite/

ANNEXE : Configuration du réseau existant de Cevital EL-KSEUR

1. Pour la configuration des équipements du réseau existant

Nous allons utiliser une topologie de réseau qui implique un routeur et des switchs de niveau 2. Nous présenterons également un exemple de configuration pour chaque équipement de cette topologie

a) Configuration de base des équipements réseau

Cette configuration nous permet tout d'abord d'affecter des noms significatifs aux équipements pour faciliter leur identification. De plus, elle nous offre la possibilité de restreindre l'accès aux personnes non autorisées en protégeant l'accès au mode privilégié, en Sécurisant la ligne consol ainsi que les ligne VTY avec des mots des passe solides.

Nous avons renommé le router et le switch et sécurisés avec le mot de passe "CEVITAL" comme le montre **la figure 1** et **2** :

- ✓ **Au niveau du routeur**

```
router(config)#hostname ROUTER
ROUTER(config)#enable secret cevital
ROUTER(config)#line consol 0
ROUTER(config-line)#pass CONSOL
ROUTER(config-line)#login
ROUTER(config-line)#exit
ROUTER(config)#line vty 0 15
ROUTER(config-line)#pass VTY
ROUTER(config-line)#login
ROUTER(config-line)#exit
ROUTER(config)#ex
```

Figure 1 : Configuration du nom et des mots de passe sur le routeur.

- ✓ **Au niveau du switch**

```
switch(config)#hostname SWITCH
SWITCH(config)#enable secret cevital
SWITCH(config)#line consol 0
SWITCH(config-line)#pass CONSOL
SWITCH(config-line)#login
SWITCH(config-line)#exit
SWITCH(config)#line vty 0 15
SWITCH(config-line)#pass VTY
SWITCH(config-line)#login
SWITCH(config-line)#exit
```

Figure 2 : Configuration du nom et des mots de passe sur le switch.

- Nous appliquons la même procédure pour les autres commutateurs (Switch).

b) Création et configuration des VLANs

Nous Créon 13 VLANs sur le routeur et sur chaque commutateur, commençant du vlan 2 jusqu'au vlan 14 tout en leur attribuant les noms qui leur correspondent. **Les figures 3** et **4** montres les étapes de la création des VLANs :

- ✓ **Au niveau du router**

```
ROUTER#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.
```

```
ROUTER(vlan)#VLAN 2 NAME SAUCE
VLAN 2 modified:
    Name: SAUCE
ROUTER(vlan)#vlan 3 name PRODUCTION-SAUCE
VLAN 3 modified:
    Name: PRODUCTION-SAUCE
ROUTER(vlan)#vlan 4 name EXPEDITION-SAUCE
VLAN 4 modified:
    Name: EXPEDITION-SAUCE
```

Figure 3 : Création des Vlans au niveau du routeur.

- Nous appliquons la même procédure pour créer les autres VLANs au niveau du routeur.

- ✓ **Au niveau du switch**

```
Password:
SWITCH#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#vlan 2
SWITCH(config-vlan)#Name SAUCE
SWITCH(config-vlan)#vlan 3
SWITCH(config-vlan)#NAME PRODUCTION-SAUCE
SWITCH(config-vlan)#vlan 4
SWITCH(config-vlan)#NAME EXPEDITION-SAUCE
SWITCH(config-vlan)#vlan 5
SWITCH(config-vlan)#NAME FROMMAGE
```

Figure 4 : Création des VLANs au niveau du switch.

- Les autres VLANs seront créés en suivant le même principe.
- Nous appliquons la même procédure pour les autres commutateurs (Switch).

- ➢ Afin de visualiser tous les VLANs qui ont été créés nous utilisons la commande « **show vlan brief ».**

✓ **Au niveau du routeur**

```
ROUTER#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    SAUCE                            active
3    PRODUCTION-SAUCE                 active
4    EXPEDITION-SAUCE                 active
5    FROMMAGE                         active
6    BOISSON                          active
7    PRODUCTION-BOISSON               active
8    EXPEDITION-BOISSON               active
9    ADMINISTRATION                   active
10   DFC                              active
11   DRH                              active
12   IT                               active
13   IMPRIMANTE                       active
14   SERVEUR                          active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
ROUTER#
```

Figure 5 : Visualisation des VLANs au niveau du routeur.

✓ **Au niveau du switch :**

```
SWITCH#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- ---------
1    default                          active
2    SAUCE                            active
3    PRODUCTION-SAUCE                 active
4    EXPEDITION-SAUCE                 active
5    FROMMAGE                         active
6    BOISSON                          active
7    PRODUCTION-BOISSON               active
8    EXPEDITION-BOISSON               active
9    ADMINISTRATION                   active
10   DFC                              active
11   DRH                              active
12   IT                               active
13   IMPRIMANTE                       active
14   SERVEUR                          active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SWITCH#
```

Figure 6 : Visualisation des VLANs au niveau du SWITCH.

La configuration des VLANs sur un routeur implique généralement la création de sous-interfaces dédiées à chaque VLAN. Pour ce faire, une sous-interface logique est établie sur l'interface physique du routeur associée au réseau local de chaque VLAN. Chaque sous-interface reçoit une adresse IP spécifique correspondant au sous-réseau du VLAN auquel elle est assignée. Ainsi, chaque sous-interface est configurée avec une adresse IP appartenant au sous-réseau du VLAN correspondant.

Nous avons configuré les sous-interfaces des VLANs précédemment créés. La méthode est décrite dans **la figure 7**, exposant la configuration des interfaces de manière illustrative.

```
ROUTER(config-subif)#interface gigabitEthernet 0/0.2
ROUTER(config-subif)#encapsulation dot1Q 2
ROUTER(config-subif)#IP ADD 10.10.2.254 255.255.255.0
ROUTER(config-subif)#interface gigabitEthernet 0/0.3
ROUTER(config-subif)#encapsulation dot1Q 3
ROUTER(config-subif)#IP ADD 10.10.3.254 255.255.255.0
ROUTER(config-subif)#interface gigabitEthernet 0/0.4
ROUTER(config-subif)#encapsulation dot1Q 4
ROUTER(config-subif)#IP ADD 10.10.4.254 255.255.255.0
ROUTER(config-subif)#interface gigabitEthernet 0/0.5
ROUTER(config-subif)#encapsulation dot1Q 5
ROUTER(config-subif)#IP ADD 10.10.5.254 255.255.255.0
```

Figure 7 : Configuration des sous-interfaces VLANs.

Le protocole Dot1q (**ou IEEE 802.1Q)** est une norme de mise en réseau qui permet le balisage des trames Ethernet pour supporter des VLANs. Il ajoute un en-tête de 4 octets aux trames Ethernet pour identifier le VLAN auquel elles appartiennent, permettant ainsi la segmentation logique du réseau en plusieurs VLANs sur une même infrastructure physique, améliorant ainsi la gestion du trafic et la sécurité.

- Après avoir configuré toutes les interfaces des VLANs, nous avons utilisé la commande **"show ip interface brief"** pour examiner l'état de toutes les interfaces.

```
ROUTER#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES unset  up                    up
GigabitEthernet0/0.2   10.10.2.254     YES manual up                    up
GigabitEthernet0/0.3   10.10.3.254     YES manual up                    up
GigabitEthernet0/0.4   10.10.4.254     YES manual up                    up
GigabitEthernet0/0.5   10.10.5.254     YES manual up                    up
GigabitEthernet0/0.6   10.10.6.254     YES manual up                    up
GigabitEthernet0/0.7   10.10.7.254     YES manual up                    up
GigabitEthernet0/0.8   10.10.8.254     YES manual up                    up
GigabitEthernet0/0.9   10.10.9.254     YES manual up                    up
GigabitEthernet0/0.10  10.10.10.254    YES manual up                    up
GigabitEthernet0/0.11  10.10.11.254    YES manual up                    up
GigabitEthernet0/0.12  10.10.12.254    YES manual up                    up
GigabitEthernet0/0.13  10.10.13.254    YES manual up                    up
GigabitEthernet0/0.14  10.10.14.254    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
```

Figure 8 : Vérification de l'état des sous interfaces VLANs.

c) Configuration du DHCP

Plutôt que d'assigner manuellement les adresses IP à chaque hôte connecté, le DHCP nous permet de les attribuer automatiquement grâce à une configuration effectuée sur le routeur. Nous avons activé le DHCP pour tous les VLANs en suivant la méthode illustrée dans **la figure 9**

```
ROUTER(config)#ip dhcp pool VLAN2
ROUTER(dhcp-config)#network 10.10.2.0 255.255.255.0
ROUTER(dhcp-config)#default-router 10.10.2.254
ROUTER(dhcp-config)#ex
ROUTER(config)#ip dhcp pool VLAN3
ROUTER(dhcp-config)#network 10.10.3.0 255.255.255.0
ROUTER(dhcp-config)#default-router 10.10.3.254
ROUTER(dhcp-config)#ex
ROUTER(config)#ip dhcp pool VLAN4
ROUTER(dhcp-config)#network 10.10.4.0 255.255.255.0
ROUTER(dhcp-config)#default-router 10.10.4.254
ROUTER(dhcp-config)#ex
```

Figure 9 : Configuration de DHCP.

- On suit la même procédure pour la configuration du DHCP des autres VLANs.
- Après avoir appliqué cette méthode à chaque VLAN, nous avons vérifié leur activation en utilisant la commande **« show running-config »**

```
ip dhcp pool VLAN2
 network 10.10.2.0 255.255.255.0
 default-router 10.10.2.254
ip dhcp pool VLAN3
 network 10.10.3.0 255.255.255.0
 default-router 10.10.3.254
ip dhcp pool VLAN4
 network 10.10.4.0 255.255.255.0
 default-router 10.10.4.254
ip dhcp pool VLAN5
 network 10.10.5.0 255.255.255.0
 default-router 10.10.5.254
ip dhcp pool VLAN6
 network 10.10.6.0 255.255.255.0
 default-router 10.10.6.254
```

Figure 10 : Vérification de l'activation du DHCP.

d) Configuration des ports

- **Configuration des liens trunks**

Un port configuré en mode trunk permet la circulation/multiplexage de plusieurs VLANs dans un même lien physique.

```
SWITCH(config)#interface GigabitEthernet1/1
SWITCH(config-if)#ex
SWITCH(config)#interface GigabitEthernet2/1
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#ex
SWITCH(config)#interface GigabitEthernet3/1
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#ex
SWITCH(config)#interface GigabitEthernet4/1
SWITCH(config-if)#switchport mode trunk
```

Figure 11 : Configuration des liens trunks.

- **Configuration des liens access**

Un port configuré en mode access permet la circulation d'un seul VLAN dans un lien donné.

```
SAUCE1(config)#interface FastEthernet3/1
SAUCE1(config-if)#
SAUCE1(config-if)#switchport mode access
SAUCE1(config-if)#
SAUCE1(config-if)#exit
SAUCE1(config)#interface FastEthernet4/1
SAUCE1(config-if)#
SAUCE1(config-if)#switchport mode access
SAUCE1(config-if)#
```

Figure 12 : Configuration des liens access sur le switch SAUCE1.

- Nous appliquons la même procédure pour les autres commutateurs (Switch).
- Nous avons ensuite vérifié la configuration à l'aide de la commande « **show interface trunk »**

```
SWITCH#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Gig0/1      on           802.1q         trunking      1
Gig1/1      on           802.1q         trunking      1
Gig2/1      on           802.1q         trunking      1
Gig3/1      on           802.1q         trunking      1
Gig4/1      on           802.1q         trunking      1
Gig5/1      on           802.1q         trunking      1
Gig6/1      on           802.1q         trunking      1
Gig7/1      on           802.1q         trunking      1
Gig8/1      on           802.1q         trunking      1
Gig9/1      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Gig0/1      1-1005
Gig1/1      1-1005
Gig2/1      1-1005
Gig3/1      1-1005
Gig4/1      1-1005
Gig5/1      1-1005
Gig6/1      1-1005
Gig7/1      1-1005
Gig8/1      1-1005
 --More--
```

Figure 13 : Vérification des trunk.

e) Attribution des ports des commutateurs aux VLANs

- Chaque port sur un commutateur est assigné à un VLAN spécifique. Cela permet de contrôler quelles données peuvent passer à travers chaque port en fonction du VLAN auquel il est assigné.
- En attribuant des ports à des VLANs spécifiques, il est possible de contrôler la sécurité du réseau en limitant l'accès aux ressources sensibles. De plus, cela permet de gérer efficacement la bande passante en isolant le trafic au sein de VLANs distincts.

La figure 14 représente la configuration des interfaces du switch SAUCE1. Et démontre la méthode de configuration.

```
SAUCE1(config)#interface FastEthernet3/1
SAUCE1(config-if)#switchport mode access
SAUCE1(config-if)#switchport access vlan 2
SAUCE1(config-if)#exit
SAUCE1(config)#interface FastEthernet4/1
SAUCE1(config-if)#switchport mode access
SAUCE1(config-if)#switchport access vlan 2
SAUCE1(config-if)#ex
```

Figure 14 : Attribution des ports aux VLANs.

- Nous appliquons la même procédure pour les autres commutateurs (Switch).

f) Vérification des adresses IP attribués par le DHCP aux PCs

La figure 15 montre l'adresse IP attribuée par le DHCP au PC 1 qui appartient au VLAN SAUCE.

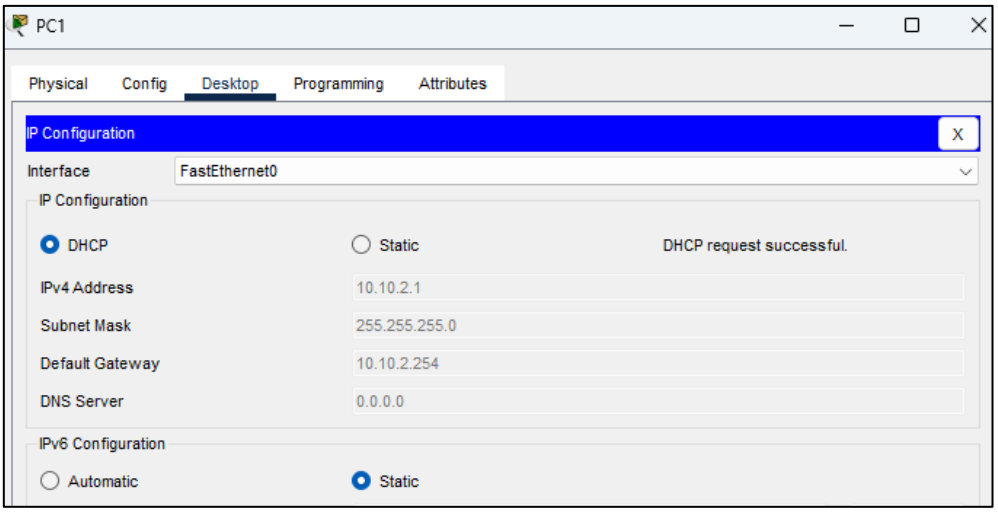


Figure 15 : Adresse IP attribuée automatiquement au PC 1 par le protocole DHCP.

- La vérification se fera pour tous les PCs.

2 Vérification de la connectivité

a) Test intra-VLAN

Nous avons évalué la connectivité entre les ordinateurs situés dans des mêmes VLANs en utilisant la commande « **Ping** » pour tester la connectivité IP entre les adresses attribuées PCS.

Par exemple **la figure 16** représente le résultat du Ping entre l'adresse IP du PC 7 qui appartient au VLAN FROMMAGE (10.10.5.1) et l'adresse IP du PC 9 qui appartient au même VLAN (10.10.5.4.)

b) Test inter-VLANs

Nous avons confirmé la connectivité entre les ordinateurs appartenant à des VLANs

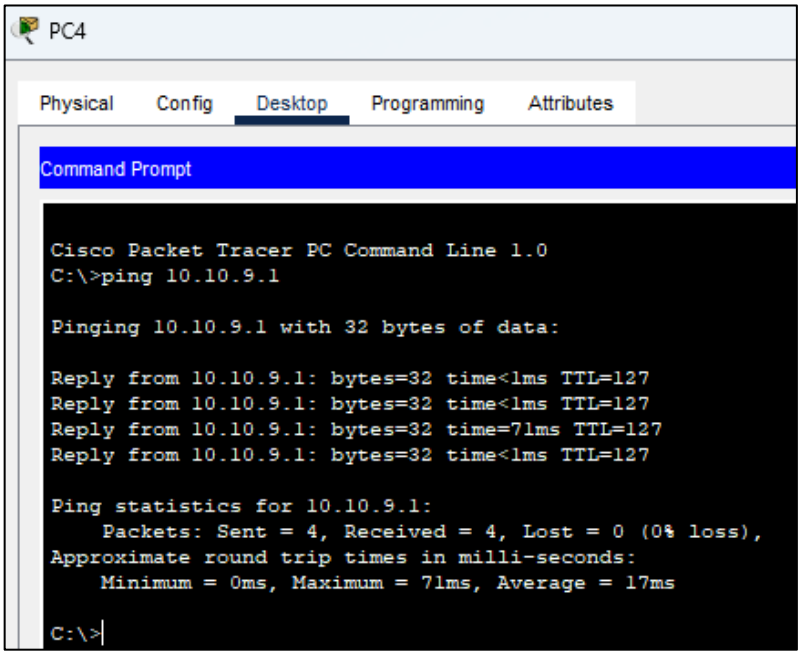


Figure 16 : Test inter-VLANs entre le PC4 et le PC 19.

distincts en réalisant un test Ping entre leurs adresses IP respectives.

La figure 17 représente le résultat du Ping entre l'adresse IP du PC 4 qui appartient au VLAN EXPEDITION-SAUCE (10.10.3.2) et l'adresse IP du PC 19 qui appartient au VLAN ADMINISTRATION (10.10.9.1).

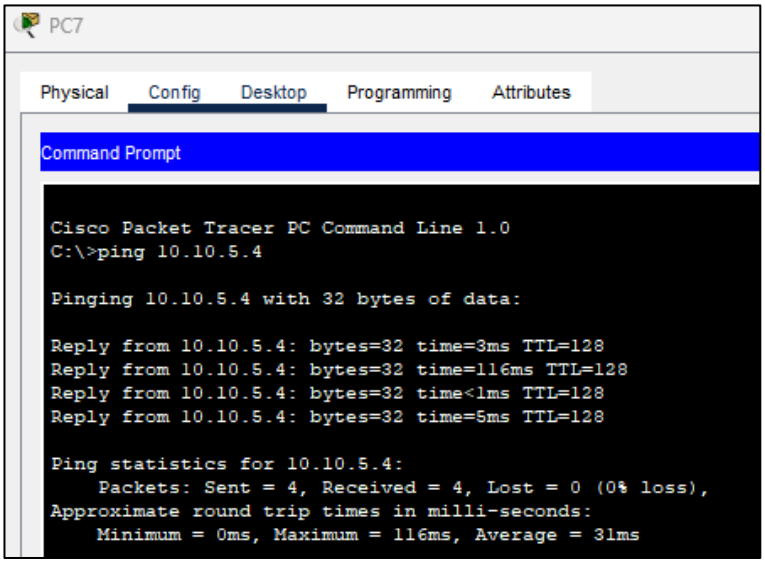


Figure 17 : Test intra-VLANs entre le PC 7 et le PC 9.

Résumé

Ce mémoire résulte d'un stage de fin d'études réalisé au sein de l'entreprise CEVITAL EL-KSEUR, où nous avons proposé une solution visant à centraliser les équipements et les ressources utilisés par les employés. Dans un premier temps, nous avons présenté l'entreprise, en soulignant ses atouts et ses faiblesses. Ensuite, nous avons décrit les concepts généraux des réseaux. Par la suite, nous avons proposé des améliorations pour le réseau de l'entreprise, en étudiant les solutions appropriées. Enfin, nous avons procédé à la mise en œuvre de ces solutions.

Mots-clés : STP, VTP, VLAN, DHCP, HSRP, OSPF, PACKET TRACER.

Abstract

This thesis is the result of an end-of-study internship carried out at the company CEVITAL EL-KSEUR, where we proposed a solution aimed at centralizing the equipment and resources used by the employees. Initially, we presented the company, highlighting its strengths and weaknesses. Then, we described the general concepts of networks. Subsequently, we proposed improvements to the company's network by studying appropriate solutions. Finally, we implemented these solutions.

Keywords : STP, VTP, VLAN, DHCP, HSRP, OSPF, PACKET TRACER.