République Algérienne Démocratique et Populaire
Université Abderrahmane MIRA de Béjaia
Faculté des Sciences Exactes

Département d'Informatique

Mémoire Présenté pour L'obtention du Diplôme de Master
en Informatique

Spécialité : Administration et Sécurité des Réseaux

Implémentation d'une infrastructure réseaux avec des protocoles de routage

Présenté par :
MASSIL HAIL
MOHAMED TAHAR HANNACHI

Sous la direction de : Dr Lachemi KHNOUS

Devant le jury composé de :

M^me^ Houha Amel	M.A. classe/ A	Président de jury	UAMB - Bejaia.
M Moktefi Mohand	M.C. classe/ B	Examinateur	UAMB - Bejaia.
M Chekrid Mohamed	M.A. classe/ A	Examinateur	UAMB - Bejaia.
M^me^ Battat Nadia	M.C. classe/ B	Examinatrice	UAMB - Bejaia.

Année Universitaire 2024 – 2025

Remerciements

Nous tenons à exprimer nos sincères remerciements à nos chers parents et à nos familles pour leur soutien moral, leur patience et leurs encouragements constants. Sans leur appui indéfectible, ce travail n'aurait pas pu voir le jour.

Nous exprimons également toute notre reconnaissance à Monsieur **Lachemi KHNOUS**, notre encadrant universitaire, pour sa disponibilité, ses conseils avisés et son accompagnement tout au long de l'élaboration de ce mémoire.

Nos remerciements les plus chaleureux vont aussi à tout le personnel de l'entreprise **CEVITAL – Bejaïa**, en particulier à Monsieur **SLIMANI Mennad**, notre encadrant de stage, pour sa patience, son sérieux et son engagement durant toute la durée du stage.

Nous remercions également l'ensemble de nos professeurs de l'Université de Bejaïa pour les solides bases théoriques qu'ils nous ont transmises, et sur lesquelles nous nous sommes appuyés pour mener à bien ce travail.

Enfin, nous adressons nos remerciements à toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de ce mémoire de fin d'études.

Dédicace

Avec un immense plaisir, un cœur rempli de gratitude et une profonde émotion, je dédie ce modeste travail :

À mes très chers et respectueux parents, pour leur patience, leurs sacrifices et leur soutien indéfectible tout au long de mon parcours universitaire.

À mes trois sœurs adorées : **Mélissa, Anaïs et Malak**, pour leur amour, leur présence rassurante et leurs encouragements constants.

À toute ma famille, qui m'a toujours entouré d'affection, de prières et de confiance.

À mes amis et camarades avec qui j'ai partagé des moments de travail, de motivation et de solidarité.

Et à toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de ce mémoire.

Massil

À mes très chers et respectueux parents, pour leurs sacrifices, leur patience et leurs encouragements constants.

À mes deux frères, **Ayoub et Chouib**, pour leur tendresse, leur soutien et leur présence précieuse à mes côtés.

À toute ma famille, pour leur bienveillance, leur confiance et leurs prières.

À mes camarades de promotion et amis proches, pour leur accompagnement, leurs encouragements et leur esprit de partage.

Et à toutes les personnes qui, de près ou de loin, ont contribué à l'aboutissement de ce travail.

Tahar

Table des matières

Table des figures

Liste des tableaux

Liste d'abriviations et notations

ACL	Access Control List
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
CLI	Command Line Interface
CPU	Central Processing Unit
DSI	Direction des Systèmes d'Information
DHCP	Dynamic Host Configuration Protocol
HSRP	Hot Standby Router Protocol
HP	Hewlett-Packard
IoT	Internet of Things (Internet des objets)
IP	Internet Protocol
IOS	Internetwork Operating System (système d'exploitation Cisco)
MAC	Media Access Control
OSPF	Open Shortest Path First
PC	Personal Computer
PRTG	Paessler Router Traffic Grapher
QoS	Quality of Service (Qualité de service)
SSH	Secure Shell
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol

Introduction générale

Dans un monde de plus en plus interconnecté, les réseaux informatiques sont devenus un pilier fondamental dans le fonctionnement quotidien des entreprises, des institutions et des particuliers. Ils permettent le partage rapide d'informations, la centralisation des ressources, et l'accès à des services variés, tout en garantissant une communication fluide et sécurisée. Face à l'évolution constante des besoins numériques, les entreprises doivent adapter leurs infrastructures pour offrir des solutions performantes, évolutives et sûres.

Ce mémoire vise à explorer en profondeur la conception, le fonctionnement et la mise en œuvre d'une infrastructure réseau moderne, basée sur des protocoles de routage dynamiques adaptés aux besoins actuels. Nous avons choisi de concentrer notre étude sur le protocole OSPF (Open Shortest Path First), reconnu pour sa capacité à assurer une convergence rapide, une gestion efficace des routes, et une adaptabilité aux architectures hiérarchiques complexes. Ce choix s'inscrit dans une logique de performance, de fiabilité et d'optimisation du trafic réseau.

La première partie de notre mémoire est consacrée aux bases théoriques des réseaux informatiques. Elle présente les différentes typologies de réseaux, les modèles de communication comme OSI et TCP/IP, les types de transmission, ainsi que les équipements essentiels à leur déploiement. Cette fondation est indispensable pour comprendre les enjeux de la configuration d'une infrastructure réseau fiable.

Ensuite, nous nous sommes intéressés aux protocoles de routage, avec un accent particulier sur OSPF. Nous avons détaillé son mode de fonctionnement, ses avantages par rapport aux autres protocoles, ses métriques et sa capacité à s'adapter aux grandes structures organisationnelles. Cela a permis de mieux saisir l'intérêt de ce protocole dans une architecture réseau professionnelle.

Enfin, la seconde partie du mémoire s'appuie sur une étude de cas pratique. Elle aborde la conception logique et physique d'un réseau d'entreprise, sa configuration dans un environnement simulé, et les tests réalisés pour valider sa performance. À travers cette démarche, nous avons cherché à démontrer la pertinence d'une approche structurée et professionnelle dans la mise en œuvre d'une architecture réseau moderne et fonctionnelle.

Ce travail représente à la fois une synthèse des compétences acquises durant notre parcours académique et une mise en situation professionnelle réaliste, en lien avec les exigences du domaine de l'administration et de la sécurité des réseaux.

1

Présentation de l'organisme d'accueil

Introduction

Ce chapitre est consacré à la présentation de l'entreprise d'accueil, **CEVITAL**, dans le cadre de notre stage de fin d'études en Master 2 « Administration et Sécurité des Réseaux ». Il s'articule autour de deux parties principales : la première présente le groupe CEVITAL dans ses aspects historiques, organisationnels et techniques ; la seconde expose l'architecture réseau actuelle de l'entreprise ainsi que les problématiques identifiées, qui justifient les propositions d'optimisation abordées dans les chapitres suivants.

1.1 Présentation générale de l'entreprise CEVITAL

1.1.1 Historique et positionnement

Le groupe **CEVITAL**, fondé en 1998 par M. Issad Rebrab et ses enfants, est l'une des plus grandes entreprises privées algériennes. Son siège social est à Garidi Kouba (Alger), avec un important complexe industriel à Béjaïa. Grâce à ses unités modernes et un réseau de distribution performant, CEVITAL est leader dans les secteurs du sucre, des huiles et des margarines.

1.1.2 Organisation structurelle

CEVITAL est structuré en plusieurs directions :

— Direction des Finances et Comptabilité
— Direction Commerciale
— Direction des Ressources Humaines
— Direction Industrielle
— Direction des Systèmes d'Information (DSI)

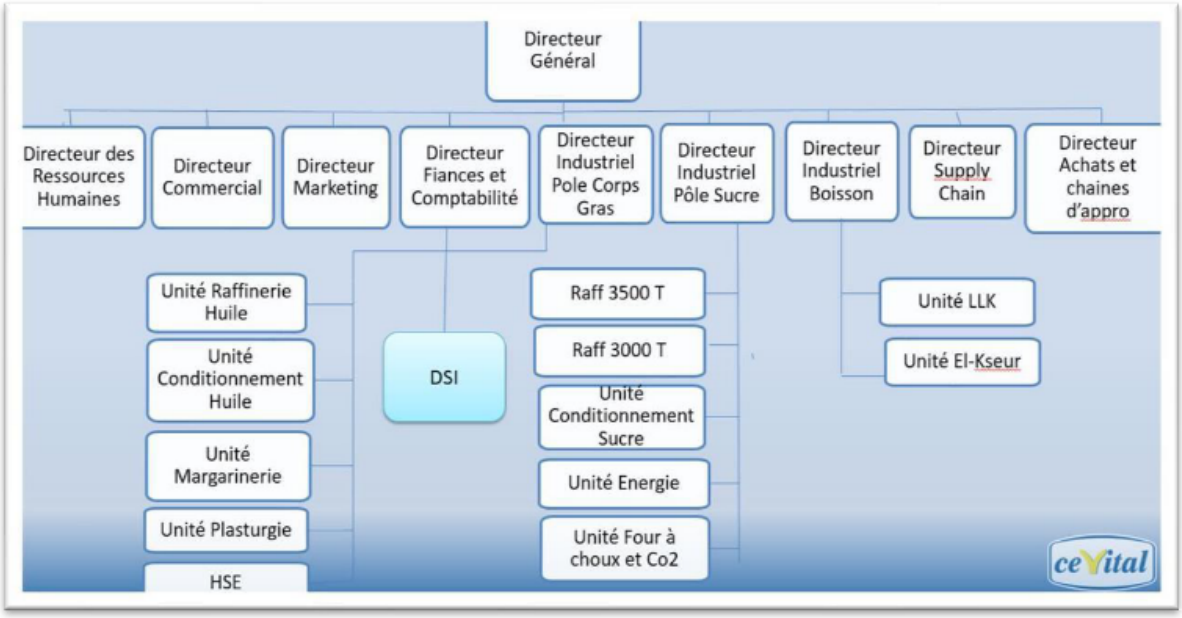

FIGURE 1.1 – Organigramme général du groupe CEVITAL

1.1.3 Organigramme de la Direction des Systèmes d'Information

La DSI est organisée en :
- Département technique
- Département des applications métiers
- Département data et transformation digitale
- Département sécurité

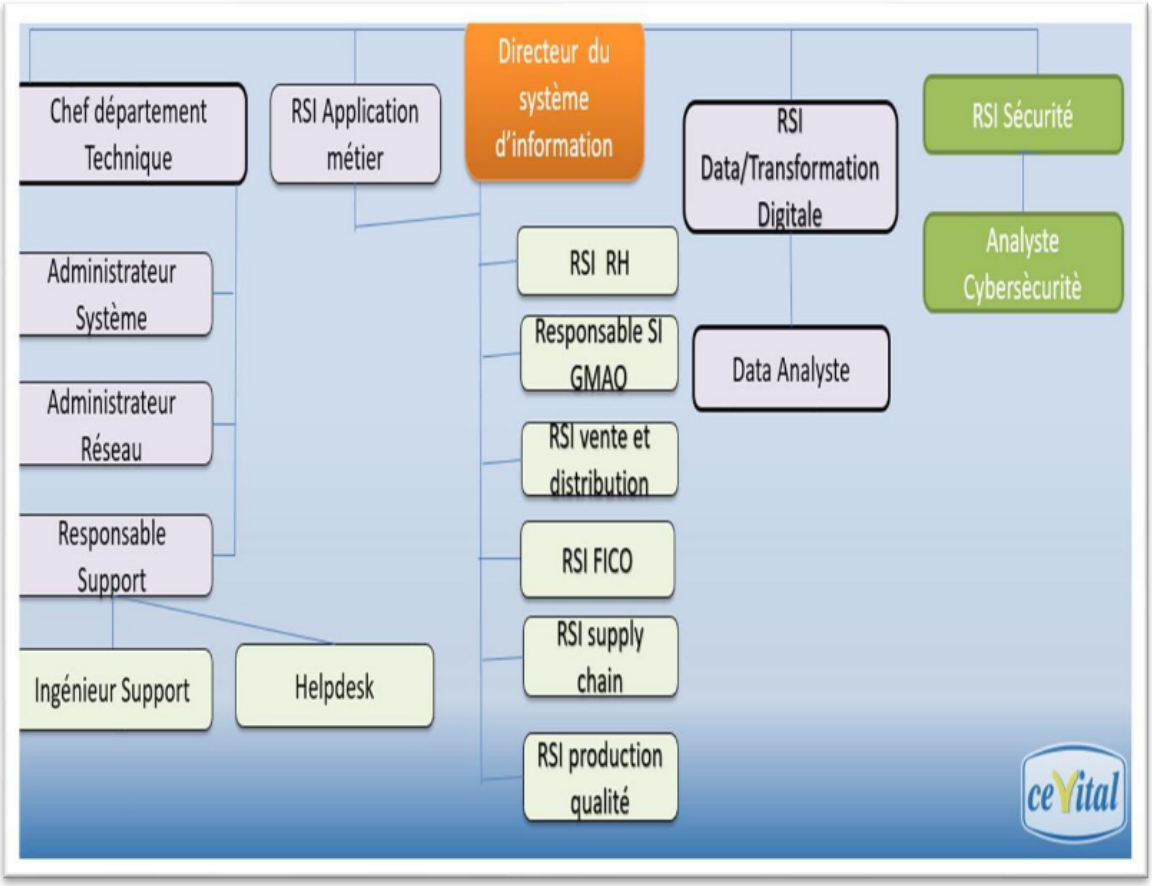

FIGURE 1.2 – Organigramme de la DSI de CEVITAL

1.2 Architecture et équipements du réseau informatique de CEVITAL

1.2.1 Description de l'infrastructure réseau

L'architecture réseau repose sur un modèle hiérarchique en trois couches :
— **Couche Core** : centralise le trafic et assure la connectivité externe via OSPF/BGP.
— **Couche Distribution** : interface entre Core et Access, applique les ACLs et gère les VLANs.
— **Couche Accès** : connecte les utilisateurs finaux, utilise VLANs, PoE, port-security, etc.

1.2.2 Conception du routage et connectivité inter-sites

Les technologies utilisées :
— **MPLS** : qualité de service et sécurité inter-sites.
— **VPN IPsec** : tunnels sécurisés pour connexions distantes.
— **Carte GDL** : connectivité de secours sans fil.

1.2.3 Description de l'Architecture Réseau

Cette topologie représente une infrastructure réseau d'entreprise répartie sur deux sites interconnectés, avec une hiérarchie organisée et plusieurs VLANs.

1. Composants Principaux

— 2 routeurs (**Router0** et **Router1**)
— 3 commutateurs multilayer (niveau 3) : **3560-24PS**
— 4 commutateurs de niveau 2 (**2960-24**) : gèrent les PC finaux
— 1 serveur **TFTP**
— 16 postes clients répartis sur plusieurs VLANs

2. Répartition des VLANs

— **VLAN 10** : PC0 à PC4
— **VLAN 20** : PC5 à PC8
— **VLAN 40** : PC9 à PC13
— **VLAN 50** : PC10 à PC14
— **VLAN 100** : PC15

3. Connexions

— Les commutateurs de niveau 3 relient les commutateurs de niveau 2.
— Les commutateurs de niveau 2 distribuent les connexions aux PC selon les VLANs.
— Les deux sites sont reliés via les routeurs (Gig0/1 vers Gig0/0).
— Une interconnexion par **trunk** existe entre les switches multilayer et les switches de niveau 2 (liaisons pointillées dans Packet Tracer).

Analyse Critique de l'Architecture

Points Positifs

1. **Bonne segmentation logique via les VLANs** : chaque groupe d'utilisateurs est isolé.
2. **Hiérarchisation claire** : *core* (routeurs), *distribution* (commutateurs L3), *accès* (commutateurs L2).
3. **Utilisation de commutateurs multilayer** : permet un *routage inter-VLAN* efficace sans dépendre uniquement des routeurs.
4. **Présence d'un serveur TFTP** : utile pour la gestion des configurations ou les mises à jour réseau.
5. **Connexion inter-site** : indispensable pour les entreprises à implantation multiple.

1.2.4 Critiques et Améliorations Possibles

1. Sécurité

— Aucune indication d'**ACLs**, **DHCP Snooping**, ou **Port Security**.

— *Suggestion* : Implémenter des mécanismes de sécurité pour protéger contre les attaques internes (*Rogue DHCP*, spoofing, etc.).

2. Absence de Redondance

— Il n'y a pas de lien de secours, ni de protocoles de haute disponibilité tels que **HSRP/VRRP** entre les routeurs ou les multilayer switches.

— *Suggestion* : Ajouter des liens de secours et des protocoles de redondance pour éviter un point de panne unique.

3. Pas d'indication sur les Protocoles de Routage

— On ne sait pas si le routage inter-VLAN est réalisé via **OSPF**, **EIGRP**, **BGP**, ou simplement via des interfaces VLAN (**SVI**).

— *Suggestion* : Documenter et configurer un protocole de routage dynamique adapté à la topologie.

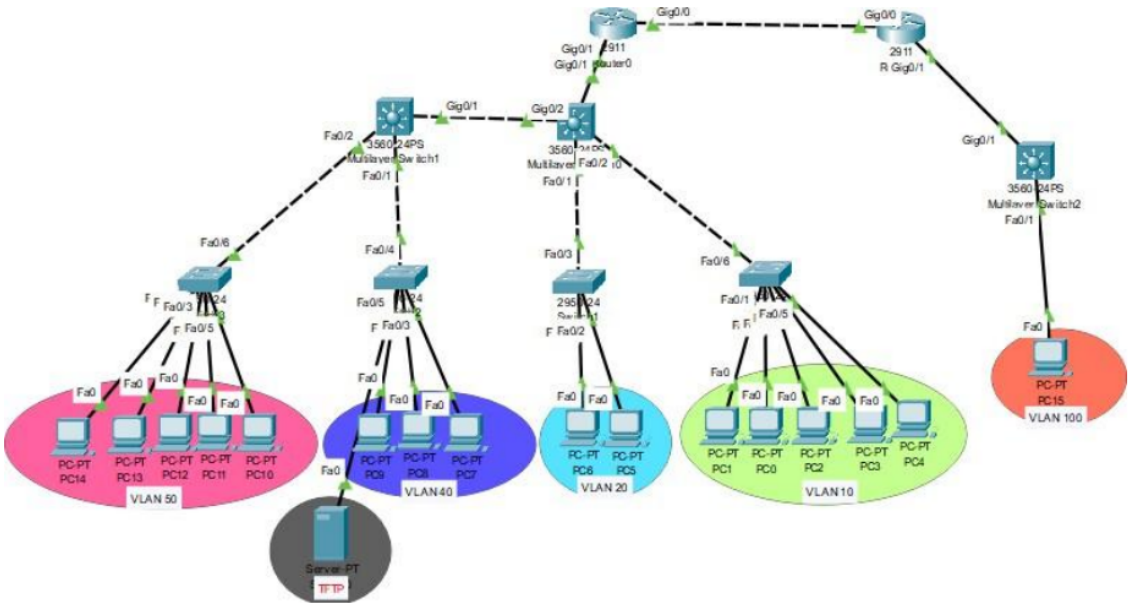

FIGURE 1.3 – Topologie simplifiée du réseau simulé

1.3 Outils et matériels utilisés

1.3.1 Logiciel de simulation

Utilisation de **Cisco Packet Tracer** pour la modélisation, la configuration et la validation de l'architecture réseau simulée.

1.3.2 Équipements réseau simulés

— Routeurs pour le routage inter-VLAN

— Switches multicouches (Distribution)
— Switches d'accès
— Postes clients (PCs) associés à des VLANs spécifiques

1.4 Matériel informatique réel utilisé par CEVITAL

1.4.1 Modèles et nombre des équipements

Équipement	Nombre	Marques
Ordinateurs personnels	1400	HP, Lenovo
Imprimantes	150	Canon
Téléphones IP	700	Alcatel Lucent
Routeurs	2	Cisco
Switches	55	Cisco
Serveurs physiques	40	HP
Serveurs virtuels	22	-
Pare-feux	4	Fortinet
Points d'accès Wi-Fi	26	Ruckus
Caméras	473	Samsung, Dahua, etc.

TABLE 1.1 – Modèles et nombre des équipements informatiques utilisés

1.4.2 Switches obsolètes (EOL/EOS)

— Plusieurs switches sont en fin de vie ou de support.
— 27 sur 55 sont considérés comme obsolètes.

Modèle	Nombre
C9200-L-48P-4G	3
WS-C2960X-48FPS-L	6
WS-C2960X-24PS-L V06	12
WS-C2960-48PST-L	10
WS-C2960-24TC-L	13

TABLE 1.2 – Extrait des modèles de switches utilisés

1.5 Problématiques et enjeux identifiés

— Obsolescence d'une partie des équipements (switches)
— Architecture complexe au niveau de la couche Distribution
— Manque de segmentation logique (peu de VLANs utilisés)
— Absence de routage dynamique (pas de OSPF/BGP)
— Surveillance et sécurité réseau insuffisantes

Conclusion

Ce diagnostic met en évidence la nécessité d'une modernisation de l'infrastructure réseau, tant au niveau matériel que logiciel. Le prochain chapitre propose une architecture optimisée intégrant les protocoles OSPF et BGP, une meilleure hiérarchisation, ainsi que des mécanismes de supervision et de sécurité renforcés.

2

Concepts fondamentaux sur les reseux informatique

Introduction

Les réseaux informatiques qui permettaient à leur origine de relier des terminaux passifs à de gros ordinateurs centraux autorisent à l'heure actuelle l'interconnexion de tous types d'ordinateurs, que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques. Les services qu'ils offrent font partie de la vie courante des entreprises et administrations (banques, gestion, commerce, bases de données, recherche,...) et des particuliers (messagerie, loisirs, services d'informations et Internet ...)[1].

2.1 Définition d'un réseau informatique

On peut définir le réseau informatique de plusieurs manières :

— C'est un ensemble d'ordinateurs et de périphériques connectés les uns aux autres pour échanger des informations et partager des ressources.
— C'est un ensemble d'équipements matériels et logiciels permettant d'échanger des données sous forme numérique.
— C'est un ensemble de terminaux passifs (clients) reliés à de gros ordinateurs serveurs centraux afin d'offrir des services[1].

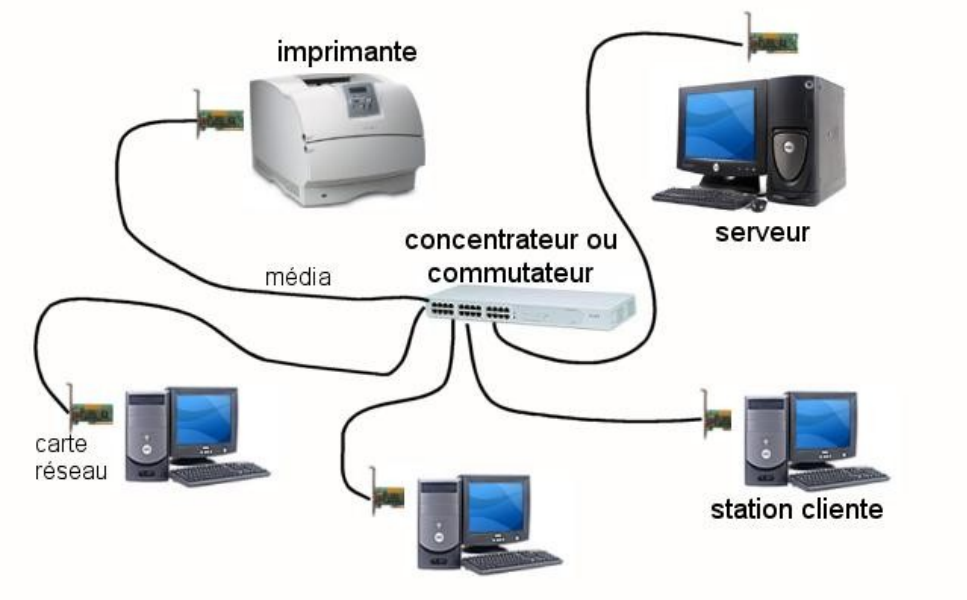

FIGURE 2.1 – Exemple d'un réseau informatique.

2.2 Intérêt d'un réseau

Un ordinateur est une machine permettant de manipuler des données. L'homme a vite compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations. Voici un certain nombre de raisons pour lesquelles un réseau est utile, un réseau permet :

- Le partage de fichiers et d'applications.
- La communication entre personnes (grâce au courrier électronique, la discussion en direct, etc.).
- La communication entre processus (entre des machines industrielles).
- La garantie de l'unicité de l'information (bases de données).
- Le jeu à plusieurs.
- Le transfert de la parole, de la vidéo et des données (réseaux à intégration de services ou multimédia).

Les réseaux permettent aussi de standardiser les applications, on parle généralement de group ware., comme par exemple la messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement[2].

2.3 Avantages de tels systèmes

Les réseaux informatiques présentent de nombreux avantages, parmi lesquels on peut citer :

- La diminution des coûts grâce au partage des données et des périphériques.
- La standardisation des applications.
- L'accès aux données en temps utile.
- Une communication et une organisation plus efficaces[3].

2.4 Les différents types de réseaux

On distingue généralement deux types de réseaux bien différents, ayant tout de même des similitudes.

2.4.1 Les réseaux Client/serveur

Un certain nombre de machines sont désignées comme serveur et centralisent les ressources communes du réseau qui seront exploitées par les autres machines du réseau qu'on appelle clients (Figure2.2).

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en terme de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion,

Les services sont exploités par des programes, appelés programmes clients, s'exécutant sur les machines clientes.On parle ainsi declien tFTP,client de messagerie,...,lorsquel'on désigne un programme, tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès du serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client messagerie il s'agit de courrier électronique)[4].

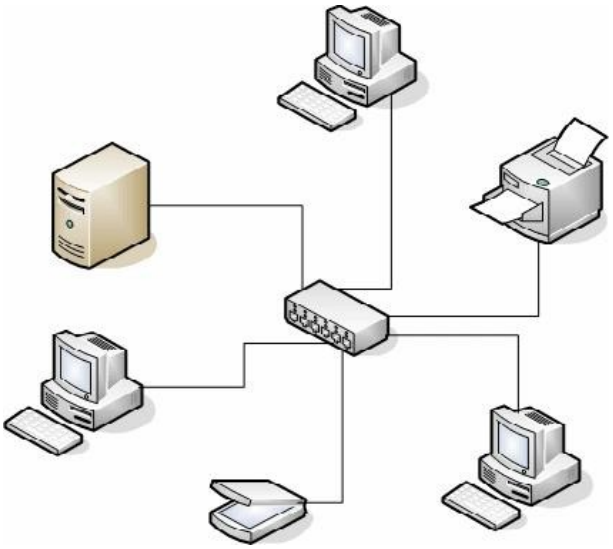

FIGURE 2.2 – Leréseau Client/serveur

a) Avantages de l'architecture client/serveur

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité. Ses principaux atouts sont :

— **Des ressources centralisées** : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction.

— **Une meilleure sécurité** : car le nombre de points d'entrée permettant l'accès aux données est moins important.
— **Une administration au niveau serveur** : les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés.
— **Un réseau évolutif** : grâce à cette architecture, il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modifications majeures[4].

b) Inconvénients du modèle client/serveur

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :
— **Un coût élevé** : dû à la technicité du serveur.
— **Un maillon faible** : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est construit autour de lui. Heureusement, le serveur a une grande tolérance aux pannes[4].

2.4.2 Architecture poste à poste

Dans une architecture poste à poste(dans sa dénomination anglaise peer to peer),il n'y a pas des serveur dédié, il n'ya donc pas de centralisation des ressources, les machines sont Autonomes et chaque utilisateur choisit les ressources qu'il veut mettre à disposition sur le réseau (Figure 2.3)[5].

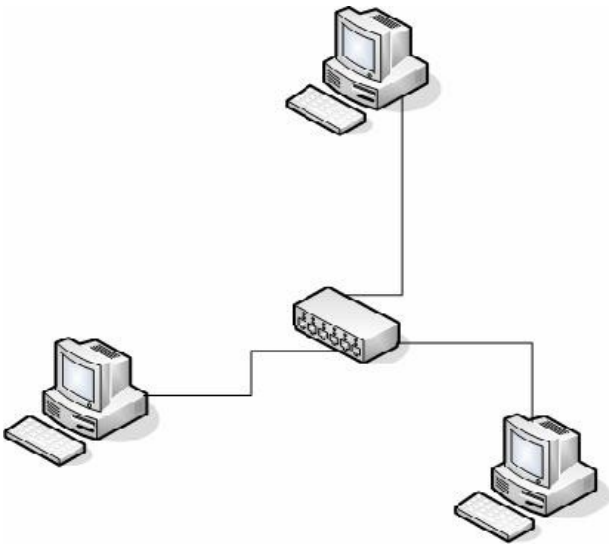

FIGURE 2.3 – Le réseau poste à poste.

a) Inconvénients des réseaux poste à poste

Les réseaux poste à poste ont les inconvénients suivants :
— Ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer.
— La sécurité est très peu présente.

— Il n'est pas fiable.

Ainsi, les réseaux poste à poste ne sont valables que pour un petit nombre d'ordinateurs (généralement une dizaine), et pour des applications ne nécessitant pas une grande sécurité. Il est donc déconseillé de les utiliser dans un réseau professionnel manipulant des données sensibles.

b) Avantages de l'architecture poste à poste

L'architecture poste à poste a tout de même quelques avantages parmi lesquels :

— Un coût réduit (les coûts engendrés par un tel réseau sont le matériel, les câbles et la maintenance).

— Une simplicité dans la réalisation.

2.5 Classification des réseaux

a) Classification par leur taille

On peut faire une classification des réseaux à l'aide de leur taille comme on peut le voir dans la figure 2.4.

— **Les bus** : interconnectent plusieurs composants (mémoires, périphériques d'entrée-sortie, processeurs, etc.). Ils sont considérés comme des réseaux dédiés à des tâches très spécifiques.

— **La structure d'interconnexion** : est basée sur la liaison des différents matériels (ordinateur, imprimante, scanner, USB, etc.) d'un même utilisateur.

— **Réseau local (LAN - Local Area Network)** : peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut couvrir plusieurs bâtiments.

— **Réseau métropolitain (MAN - Metropolitan Area Network)** : interconnecte plusieurs lieux situés dans une même ville, comme les différents sites d'une université.

— **Réseau étendu (WAN - Wide Area Network)** : permet de communiquer à l'échelle d'un pays ou de la planète, avec des infrastructures terrestres ou satellites[6].

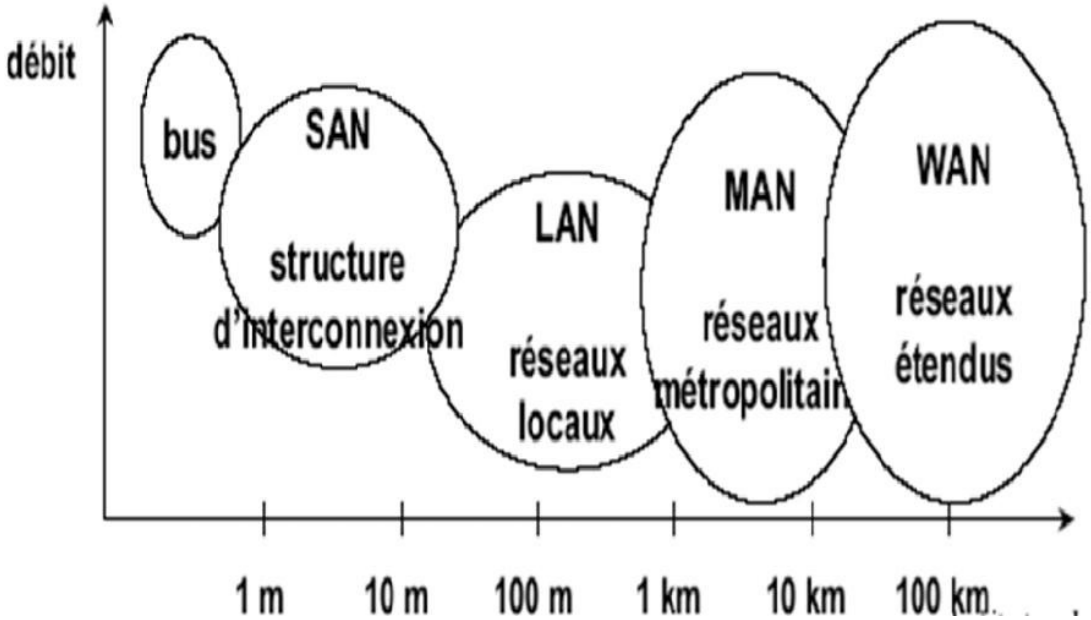

FIGURE 2.4 – Classification des réseaux.

On parle aussi de réseaux :

— **Homogènes** : tous les ordinateurs sont du même constructeur (exemple : AppleTalk).
— **Hétérogènes** : les ordinateurs reliés au réseau sont de constructeurs divers (exemple : Ethernet).

b) Classification par leur topologie

La topologie des réseaux décrit la configuration selon laquelle leurs stations sont interconnectées via le support de transmission. On distingue principalement quatre types de topologies :

— **Topologie en étoile** : un contrôleur central relie directement toutes les stations. Toute communication passe par ce nœud central[6].

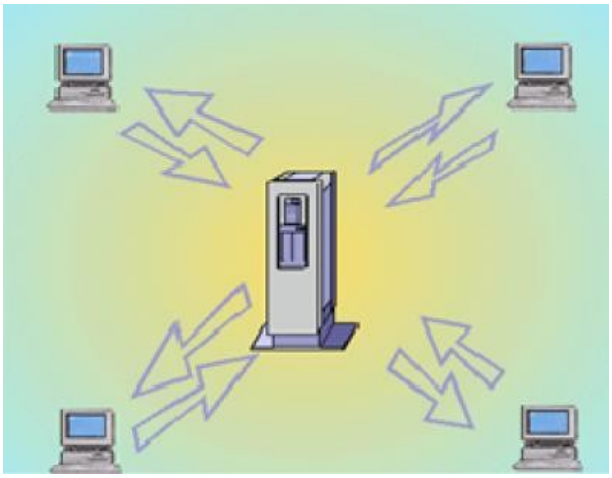

FIGURE 2.5 – Topologie en étoile.

— **Topologie en bus** : chaque station est attachée à un canal commun. Le bus peut être unidirectionnel ou bidirectionnel.

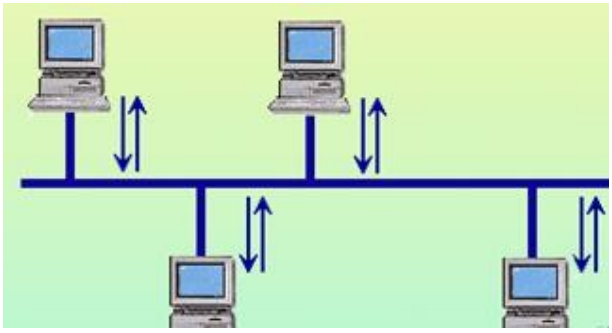

FIGURE 2.6 – Topologie en bus.

— **Topologie en anneau** : les stations sont connectées en boucle via des répéteurs. L'information circule dans un seul sens.

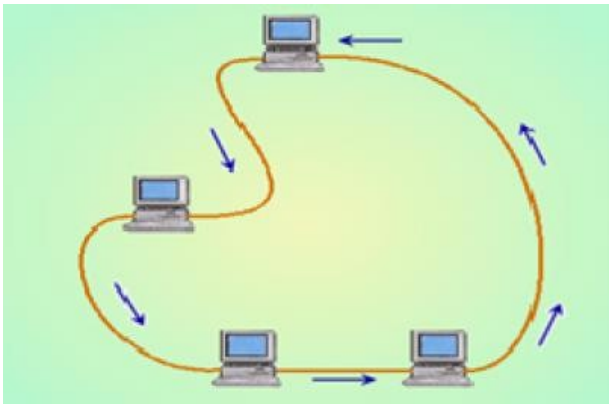

FIGURE 2.7 – Topologie en anneau.

— **Topologie maillée** : utilisée dans les grands réseaux de distribution. Elle offre des routes multiples et redondantes[6].

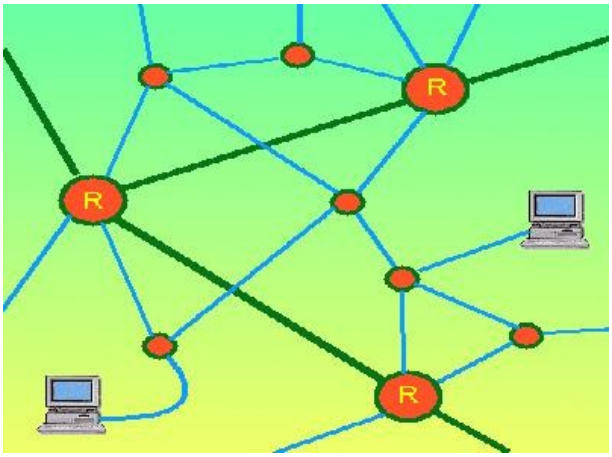

FIGURE 2.8 – Topologie maillée.

c) Classification par leur mode de connexion

— **Le mode avec connexion** :

Le mode avec connexion contient de négociation entre l'émetteur et le récepteur sur quelques paramètres définissant les limites admissibles pour le transfert des données, c'est la négociation de la qualité de service.

La transmission des données dans le mode avec connexion est sécurisée puisque l'émetteur et le récepteur se mettent d'accord, et par la suite lecontrôle est effectué, au moins, au niveau des deux extrémités.

— **Le mode sans connexion** :

Le mode sans connexion ne contient pas de négociation entre l'émetteur et le récepteur. Pour mettre en place cette connexion, il faut penser à une logistique afin de s'assurer du transfert des données : c'est la structure en couches, telle que chaque couche rend service à celle qui est inférieure.

Le mode sans connexion réside en l'établissement du contrôle de communication par le gestionnaire de réseau qui doit prendre des précautions [8].

d) Classification par leur méthode d'accès

— **La méthode d'accès CSMA/CD (Carrier Sense Multiple Access / Collision Detection)** :

CSMA/CD (Carrier Sens Method Access / Collision Detection) est un ensemble de règles qui déterminent la façon dont les périphériques du réseau répondent lorsque deux de ces périphériquestententdetransmettresimultanémentdesdonnéessurleréseau. La transmission simultanée de données par plusieurs ordinateurs provoque une collision. Tous les ordinateurs du réseau, clients et serveurs, vérifient le câble sur lequel s'effectue le trafic réseau. Un ordinateur ne transmet des données que lorsqu'il détecte que le câble

est libre. Une fois que l'ordinateur a transmis des données sur le câble, aucun autre ordinateur ne peut transmettre des données tant que les données d'origine n'ont pas atteint leur destination, libérant ainsi le câble. Lorsqu'il détecte une collision,un périphérique attend pendant un délai aléatoire , puis tente de retransmettre le message. S'il détecte de nouveau une collision, il attendra deux fois plus longtemps avant de retransmettre le message.

— **La méthode d'accès par jeton** :

Un jeton est une séquence spéciale de bits qui transitent sur l'anneau. Un ordinateur ne peut pas transmettre des données tant qu'il n'est pas en possession du jeton ; tant que ce jeton est utilisé par un ordinateur, les autres ordinateurs ne peuvent pas transmettre de données.

Lorsquele premier ordinateur de l'anneau se retrouve en ligne, le réseau génère un jeton. Ce jeton transite sur l'anneau jusqu'à ce que l'un de ces ordinateurs prenne le contrôle du jeton. Cet ordinateur envoie alors une trame de données sur le réseau. Cette trame parcourt l'anneau jusqu'àcequ'elleatteignel'ordinateurdontl'adresse correspond à l'adresse de destination de la trame. L'ordinateur destinataire copie la trame en mémoire et la marque pour indiquer que les informations ont été reçues. La trame continue à parcourir l'anneau jusqu'à l'ordinateur expéditeur, sur lequel la transmission est réussie. L'ordinateur qui a transmis les données retire alors la trame de l'anneau, et envoie sur celui-ci un nouveau jeton[7].

2.5.1 Architecture des réseaux

a) Modèle OSI

Le modèle OSI (*Open System Interconnection*) a été défini par l'ISO (International Standard Organisation) afin d'unifier les standards de communication entre ordinateurs sur un réseau.

À l'origine, chaque constructeur utilisait son propre système (système propriétaire), ce qui entraînait la coexistence de nombreux réseaux incompatibles. Le modèle OSI propose une architecture en sept couches hiérarchiques, où chaque couche remplit une fonction spécifique :

— **Couche physique** : Gère la connexion physique entre une machine et le réseau (supports, tensions, synchronisation, etc.).
— **Couche liaison de données** : Assure le transfert fiable de trames de données entre deux équipements directement connectés.
— **Couche réseau** : Définit l'unité de données transférée entre deux sites distants. Elle s'occupe notamment de l'adressage logique et du routage.
— **Couche transport** : Garantit un contrôle de bout en bout, permettant à un processus de communiquer directement avec un autre, tout en assurant l'intégrité des données.
— **Couche session** : Gère les sessions de communication entre applications (établissement, maintien, terminaison de session).
— **Couche présentation** : S'occupe de la représentation des données (conversion, compression, cryptage), afin d'assurer une compréhension mutuelle entre les systèmes.
— **Couche application** : Contient les applications réseau (ex : messagerie électronique, transfert de fichiers, navigation web, etc.)[9].

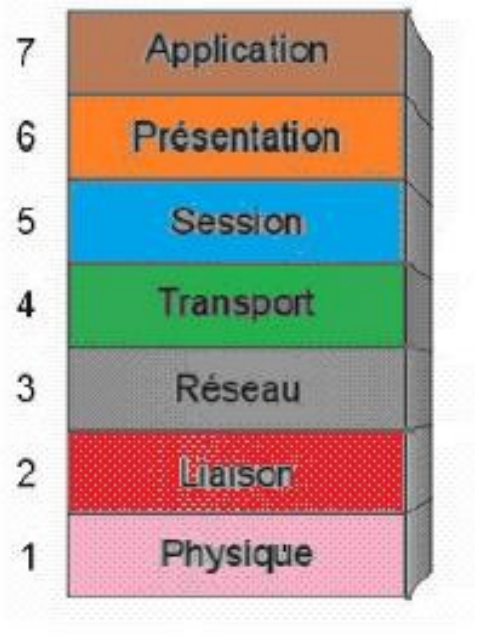

FIGURE 2.9 – Modèle de référence OSI selon l'ISO.

Encapsulation des données

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, ensemble d'informations qui garantissent la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état original[10].

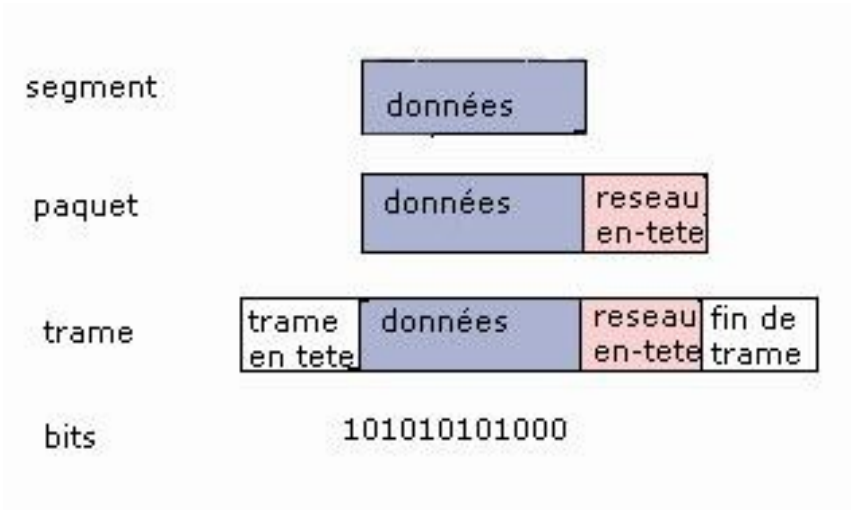

FIGURE 2.10 – principe d'encapsulation.

b) Modèle TCP/IP

Le modèle TCP/IP (*Transmission Control Protocol / Internet Protocol*) est un ensemble de protocoles utilisés pour la communication sur Internet. Il repose sur la notion d'adressage IP, qui permet d'identifier chaque machine d'un réseau afin d'acheminer les paquets de données vers leur destination.

- **TCP (Transmission Control Protocol)** : Ce protocole est responsable du découpage des messages en datagrammes, de leur réassemblage à l'arrivée (dans le bon ordre), ainsi que de la retransmission des paquets perdus.
- **IP (Internet Protocol)** : Il prend en charge le routage des datagrammes à travers le réseau.

La suite TCP/IP est organisée en quatre couches logicielles, reposant sur une couche matérielle (Figure 2.11) :

- **Couche accès réseau** : Interface entre l'ordinateur et le réseau, elle inclut les pilotes matériels du système d'exploitation ainsi que la carte réseau.
- **Couche Internet (IP)** : Gère la circulation et le routage des paquets dans le réseau. Elle comprend également les protocoles ICMP (Internet Control Message Protocol) et IGMP (Internet Group Management Protocol).
- **Couche transport** : Assure une communication fiable de bout en bout (avec TCP) ou non fiable (avec UDP). Elle régule le flux et garantit l'ordre des données transmises.
- **Couche application** : Contient les programmes utilisateurs tels que Telnet (accès distant), FTP (transfert de fichiers), SMTP (messagerie électronique), etc.[11][12]

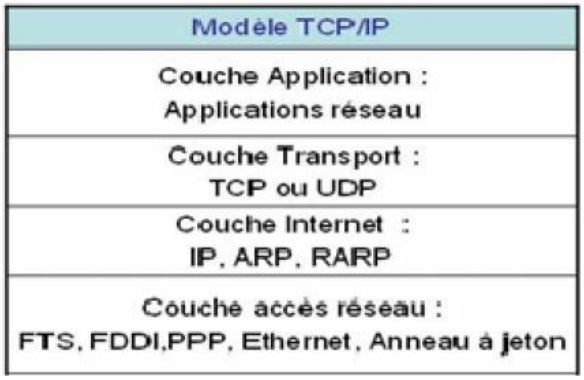

FIGURE 2.11 – Modèle de référence TCP/IP.

c) TCP/IP et le modèle OSI

Le modèle TCP/IP, inspiré du modèle OSI, reprend le principe de l'approche modulaire (utilisation de couches), mais ne comporte que quatre couches. Le tableau suivant met en évidence la correspondance entre les deux modèles [13] :

Modèle TCP/IP	Modèle OSI
Couche Application	Couche Application Couche Présentation Couche Session
Couche Transport (TCP/UDP)	Couche Transport
Couche Internet (IP)	Couche Réseau
Couche Accès réseau	Couche Liaison de données Couche Physique

TABLE 2.1 – Comparaison entre le modèle TCP/IP et le modèle OSI.

Comme on peut le constater, les couches du modèle TCP/IP ont des fonctions plus larges, certaines d'entre elles regroupant plusieurs couches du modèle OSI.

d)Dispositifs de communication

Les réseaux hétérogènes formant Internet sont reliés entre eux grâce à des dispositifs d'interconnexion (passerelles, routeurs, ponts, etc.) assurant le transfert des données.

1-Les ponts

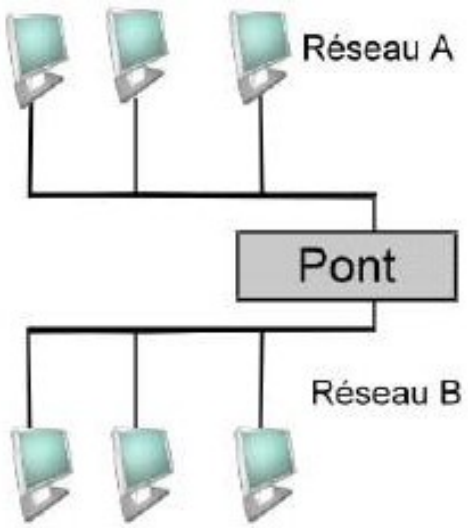

FIGURE 2.12 – Deux réseaux reliés avec un pont.

Ce sont des dispositifs matériels ou logiciels, permettant de relier des réseaux travaillant avec les mêmes protocoles. Le pont filtre les données et ne laisse passer que les données destinées aux ordinateurs situés de l'autre côté du pont (figure 2.12).

Un pont possède deux connexions à deux réseaux distincts. Lorsqu'il reçoit un paquet de données sur l'une de ses interfaces, il analyse l'adresse physique (MAC) du destinataire et

de l'émetteur.Sijamaislepontneconnaîtpasl'émetteur,ilstockesonadresse dans une table afin de savoir de quel côté du réseau se trouve l'émetteur.

Ainsi le pont est capable de savoir si l'émetteur et le destinataire sont situés du même côté ou bien de part et d'autre du pont. Dans le premier cas le pont ignore le message, dans le second le pont transmet la trame sur l'autre réseau[14].

2-Les passerelles

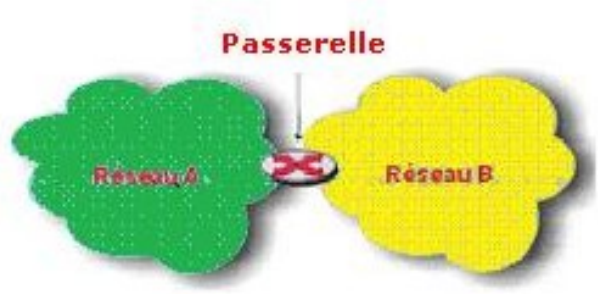

FIGURE 2.13 – Deux réseaux reliés avec une passerelle.

Ce sont des systèmes matériels et/ou logiciels permettant de faire des liaisons entre plusieurs réseaux de protocoles différents. L'information est codée et transportée différemment sur chacun des réseaux (Figure 2.13). Elles permettent aussi de manipuler les données afin de pouvoir assurer le passage d'un type de réseau à un autre. Les réseaux ne peuvent pas faire circuler la même quantité de données simultanément en terme de taille de paquet de données, mais la passerelle réalise cette transition en convertissant les protocoles de communication de l'un vers l'autre. Cette opération ralentie le transfert de données[14].

3-Les routeurs

Ce sont des dispositifs matériels ou logiciels, permettant de choisir le chemin qu'un message doit emprunter. De plus, ils permettent de manipuler les données (qui circulent sous forme de datagrammes) afin de pouvoir assurer le passage d'un type de réseau à un autre (contrairement aux ponts). Ainsi, les réseaux ne peuvent pas faire circuler la même quantité simultanée d'information en terme de taille de paquets de données. Les routeurs ont donc la possibilité de fragmenter les paquets de données pour permettre leur circulation (figure 2.14).

Ils fonctionnent grâce à des tables de routage et des protocoles de routage. Les routeurs intègrent souvent une fonction de passerelle leurs permettant d'acheminer les paquets quelque soit l'architecture[15].

4-Les hubs (concentrateurs)

Le hub, ou concentrateur, est un boîtier électronique qui relie plusieurs postes et périphériques au réseau. Il agit comme un répéteur, en transférant les données reçues vers tous les ports du réseau, y compris ceux qui ne sont pas destinataires[15].

FIGURE 2.14 – Routeur connecté à deux réseaux locaux.

5-Les switchs (commutateurs)

Le switch, ou commutateur, est un dispositif similaire au hub, mais plus intelligent. Il assure les connexions entre les équipements du réseau tout en optimisant le trafic. Contrairement au hub, il transfère les données uniquement vers le destinataire concerné, ce qui améliore la performance et libère de la bande passante[15].

e)Les protocoles du modèle OSI

Introduction

Un protocole est une méthode standard qui permet la communication entre deux machines, c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon le type de communication souhaitée. Certains protocoles sont spécialisés dans l'échange de fichiers (comme FTP), d'autres servent à gérer l'état de la transmission ou les erreurs (comme ICMP)[16].

Dans le modèle OSI, de nombreux protocoles sont utilisés. Voici une présentation des plus importants :

a) Protocole TCP

Le protocole TCP (Transmission Control Protocol) est un protocole sécurisé d'échange de données. Il a été conçu pour établir une communication fiable entre deux tâches exécutées sur des ordinateurs autonomes connectés à un réseau. C'est un protocole orienté connexion[16].

b) Protocole UDP

UDP (User Datagram Protocol) est un protocole plus léger que TCP. Il établit une communication sans contrôle d'erreur et sans accusé de réception, ce qui le rend plus rapide mais moins fiable. Il n'est pas orienté connexion[16].

c) Protocole DNS

Le DNS (Domain Name System) permet la mise en correspondance entre les adresses IP (physiques) et les noms de domaine (logiques). Grâce à sa structure hiérarchique, il simplifie l'accès aux sites web. Par exemple, il est plus simple de mémoriser `www.exemple.com` que l'adresse IP correspondante. Le DNS permet donc la « résolution de noms »[16].

d) Protocole DHCP

DHCP (Dynamic Host Configuration Protocol) attribue automatiquement des adresses IP aux équipements qui se connectent au réseau. Lorsqu'un appareil se connecte, il envoie une requête au serveur DHCP qui lui attribue une adresse IP et d'autres paramètres réseau[16]. Il fonctionne avec le protocole BOOTP.

e) Protocole FTP

FTP (File Transfer Protocol) est un protocole de transfert de fichiers entre deux machines via un réseau TCP/IP. Il permet d'envoyer, de recevoir, de renommer ou de supprimer des fichiers sur un serveur distant[16].

f) Protocole HTTP

HTTP (Hyper Text Transfer Protocol) est utilisé pour le transfert de pages Web. Il permet de transférer des fichiers HTML, des images, des vidéos, etc. sur le Web. C'est le protocole fondamental de la navigation Internet[16].

g) Protocole ARP

ARP (Address Resolution Protocol) permet d'obtenir l'adresse physique (adresse MAC) d'une machine à partir de son adresse IP. Il est essentiel pour le fonctionnement des réseaux locaux[16].

h) Protocole ICMP

ICMP (Internet Control Message Protocol) est utilisé pour envoyer des messages de contrôle ou d'erreur entre les équipements réseau. Par exemple, il est utilisé par la commande `ping`.[16]

i) Protocole IP

Le protocole IP (Internet Protocol) permet d'acheminer les paquets de données à travers un ensemble de réseaux interconnectés. Il assure également la fragmentation des paquets lorsqu'un segment du réseau impose une taille maximale différente.[16]

3
Protocole de routage

Introduction

Le protocole de routage permet à un routeur de partager avec d'autres routeurs des informations sur les réseaux qu'il connaît, ainsi que sur leur proximité avec d'autres routeurs. Les informations qu'un routeur reçoit d'un autre routeur, à l'aide d'un protocole de routage, servent à construire et à mettre à jour une table de routage On a plusieurs protocoles de routage :

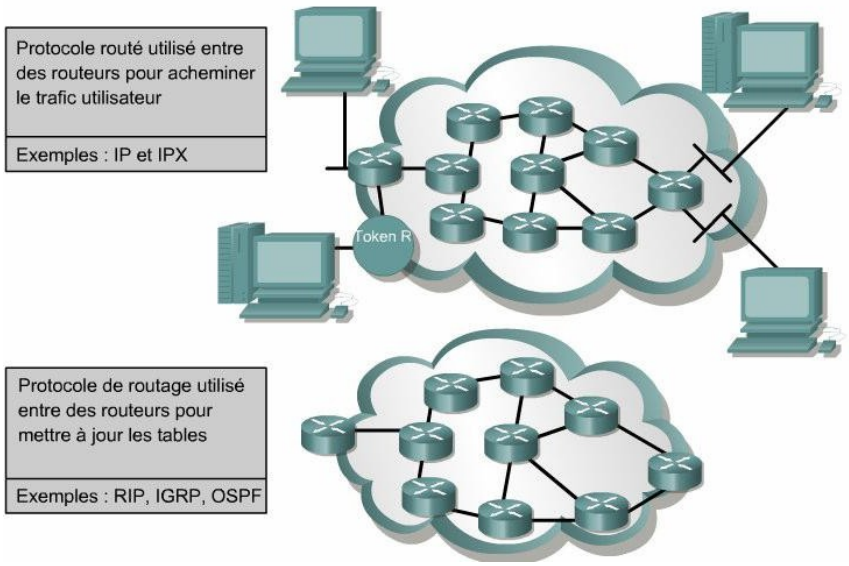

FIGURE 3.1 – Présentation des protocoles de routage.

— Protocole d'informations de routage (RIP)
— Protocole IGRP (Interior Gateway Routing Protocol)
— Protocole EIGRP (Enhanced Interior Gateway Routing Protocol)

— Protocole OSPF (Open Shortest Path First)[17]

3.1 Routage IP

Le routage est l'une des fonctionnalités principales de la couche IP et consiste à choisir la manière de transmettre un datagramme IP à travers les divers réseaux d'un internet. Ainsi un routeur réémettra des datagrammes venus d'une de ses interfaces vers une autre, alors qu'un ordinateur sera soit l'expéditeur initial, soit le destinataire final d'un datagramme. D'une manière générale on distingue le routage directe, qui correspond au transfert d'un datagramme entre deux ordinateurs du même réseau, et la le routage indirect qui est mise en œuvre dans tous les autres cas, c'est-à-dire quand au moins un routeur sépare l'expéditeur initial et le destinataire final[17].

3.2 Méthodes de routage IP

a) Routage Direct

Le routage direct se produit quand la machine de destination se trouve sur le même réseau physique que la machine émettrice. Dans ce cas, un datagramme IP peut être émis directement, sans passer par un routeur, après avoir été encapsulé dans une trame correspondant au type du réseau local. C'est ce qu'on appelle la remise directe[5][6].

b) Routage Indirect

Si la machine de destination du datagramme ne se trouve pas sur le même réseau que la machine émettrice, il faut passer par un routeur. L'adresse de la première passerelle par laquelle il faut passer pour atteindre la destination est appelée la route indirecte.

En fait, la machine émettrice ne s'occupe pas de connaître le chemin complet jusqu'à la destination, elle doit juste connaître l'adresse de cette première passerelle.

Si la destination se trouve sur le même réseau physique mais sur un sous-réseau différent, c'est le routage indirect qui sera utilisé. Ce qui implique qu'un routeur est nécessaire pour acheminer le trafic entre deux sous-réseaux.

Un routeur n'est pas nécessairement une machine séparée. Cela peut très bien être une station de travail ordinaire[5][6].

c) Routage par table

Les machines communiquant avec TCP/IP possèdent une table de routage IP. Il s'agit d'un ensemble de correspondances entre une adresse de réseau IP et l'adresse de la première passerelle à emprunter.

Quand une machine émet un datagramme, elle vérifie d'abord si l'adresse du réseau (pas de la machine) de destination est reprise dans cette table. Si c'est le cas, elle peut y lire l'adresse de la passerelle vers laquelle il faut envoyer le datagramme[5][6].

d) Routage par défaut

Si la table de routage IP ne contient aucune entrée faisant référence à la destination du datagramme, celui-ci est alors envoyé vers une passerelle dite *passerelle par défaut* (default gateway), dont l'adresse est généralement stockée dans la table de routage[5][6].

3.3 Table de routage

La table de routage spécifique à chaque routeur qui permet de déterminer vers quelle voie de sortie envoyer un datagramme destiné à un réseau quelconque. Évidemment, à cause de la structure localement arborescente d'Internet la plupart des tables de routage ne sont pas très grandes. Par contre, les tables des routeurs interconnectant les grands réseaux peuvent atteindre des tailles très grandes ralentissant d'autant le trafic sur ces réseaux. D'un point de vue fonctionnel une table de routage contient des paires d'adresses du type (D, R) où D est l'adresse IP d'une machine ou d'un réseau de destination et R l'adresse IP du routeur suivant sur la route menant à cette destination[18].

3.4 Les critères des protocoles de routage

Les critères de routage s'appuient généralement sur les éléments suivants :

— **Longueur du trajet** : Définit un critère de décision à partir du nombre de liens qu'un paquet doit traverser pour se rendre du point d'origine au point de destination.
— **Fiabilité** : Définit un critère de décision fondé sur la fiabilité de chaque lien du réseau.
— **Délai de transmission** : Définit un critère de décision fondé sur le temps requis afin d'acheminer un paquet du point d'origine au point de destination.
— **Largeur de bande** : Définit un critère de décision fondé sur la capacité de transmission d'un lien.
— **Charge** : Définit un critère de décision fondé sur les ressources d'un routeur comme le nombre de paquets traités par seconde, la mémoire disponible, etc.
— **Coût de la communication** : Définit un critère de décision fondé sur un coût appliqué à un lien (notamment pour des raisons économiques)[18].

3.5 Types de routage

a) Le routage statique

Une route donnée liée aux routes statiques est dirigée par un administrateur. Cet itinéraire est similaire à une route statique, car le chemin jusqu'à la destination est toujours le même et nécessite une mise à jour manuelle par l'administrateur.

Les opérations de routage statique s'articulent comme suit :

— L'administrateur réseau configure la route.
— Le routeur insère la route dans la table de routage.
— Les paquets sont acheminés à l'aide de la route statique[1].

3.6 Avantages et inconvénients du routage statique

a) Avantages du routage statique

- Plus facile à comprendre par l'administrateur.
- La configuration est simple.
- Effectue des traitements sur le processeur minimal.

b) Inconvénients du routage statique

- La configuration et la maintenance posent un problème de temps.
- Risques d'erreurs sur la configuration, surtout dans les grands réseaux.
- L'intervention de l'administrateur est requise pour assurer la mise à jour des informations relatives aux routes[1].

3.7 Le Routage à système autonome

Un système autonome est un ensemble de réseaux gérés par un administrateur commun et partageant une stratégie de routage commune (figure 3.2). Pour le monde extérieur, un système autonome est perçu comme une entité unique. Il peut être exécuté par un ou plusieurs opérateurs tout en présentant au monde extérieur une vue cohérente du routage.

L'Inter NIC(Internet Network Information Center),un fournisseur de services ou en core un administrateur attribue un numéro d'identification à chaque système autonome .Ce numéro est un nombre à 16 bits. Les protocoles de routage, tels que l'IGRP de Cisco, nécessitent l'attribution d'un numéro de système autonome unique[1].

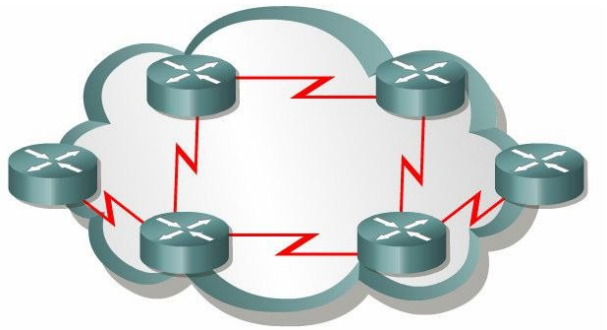

FIGURE 3.2 – Routeurs sous administrateur commune.

3.8 Le Routage dynamique

Utilise une route qu'un protocole de routage modifie automatiquement en fonction de changements de topologie ou de trafic, Les informations permettent aux routeurs de découvrir de nouveaux réseaux et également de trouver d'autres chemins en cas d'échec d'un lien vers un réseau actif[1][3].

3.8.1 Avantages et inconvénients du routage dynamique

a) Avantages du routage dynamique

— La maintenance de la configuration est simplifiée pour l'administrateur lors de l'ajout et de la suppression de réseaux.
— Plus évolutif, l'expansion du réseau ne présente généralement pas de problème.
— Les protocoles réagissent automatiquement aux modifications topologiques.
— La configuration présente moins de risques d'erreurs.

b) Inconvénients du routage dynamique

— Les ressources du routeur sont utilisées : cycle de processeur, mémoire et bande passante du lien, etc.
— La configuration nécessite davantage de connaissances de la part de l'administrateur, notamment pour le dépannage et le contrôle[1][3].

3.8.2 Fonctionnement des protocoles de routage dynamique

Le schéma de la figure 3.3 montre comment le protocole de routage dynamique construit et met à jour la table de routage. Le fonctionnement d'unprotocole de routage dynamique peut-être

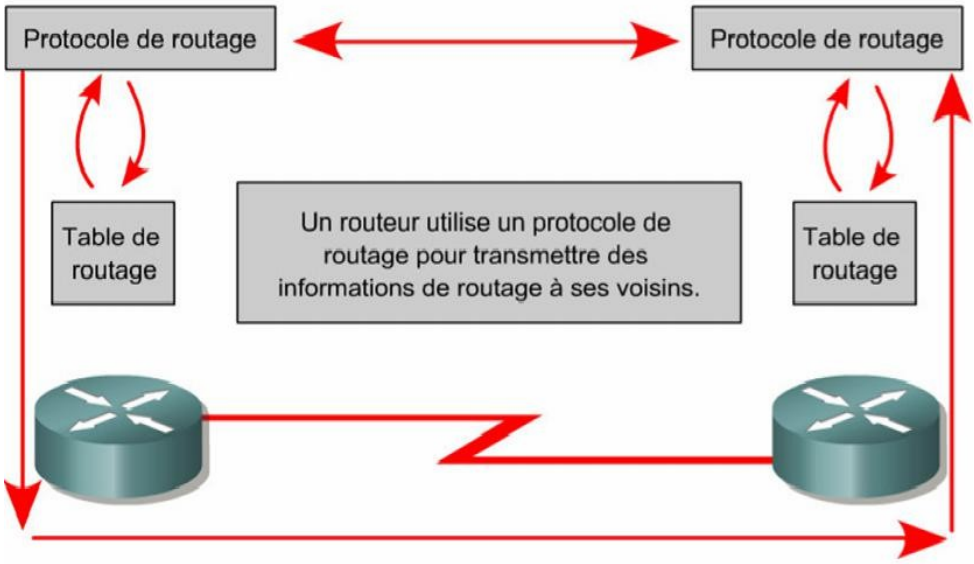

FIGURE 3.3 – Fonctionnement du routage dynamique.

décrit de la manière suivante :

— Le routeur envoie et reçoit des messages de routage sur ses interfaces.
— Le routeur partage les messages et les informations de routage avec d'autres routeurs qui utilisent le même protocole de routage.
— Les routeurs échangent des informations de routage pour découvrir des réseaux distants.
— Lorsqu'un routeur détecte une modification de topologie ,le protocole de routage peut l'annoncer aux autres routeurs.

On peut définir les composants d'un protocole de routage :

— Structures de données : pour fonctionner, certains protocoles de routage utilisent des tables et/ou des bases de données. Ces informations sont conservées dans la mémoire vive.

— Algorithme : un algorithme est une liste précise d'étapes permettant d'accomplir une tâche. Les protocoles de routage utilisent des algorithmes pour faciliter l'échange d'informations de routage et déterminer le meilleur chemin d'accès.

— Messages de protocoles de routage : les protocoles de routage utilisent différents types de messages pour découvrir les routeurs voisins, échanger des informations de routage et effectuer d'autres tâches afin d'obtenir et de gérer des informations précises sur le réseau[3].

3.8.3 Les différents protocoles de routage dynamique

Les protocoles de routage peuvent être classés dans différents groupes selon leurs caractéristiques. Les protocoles de routage les plus couramment utilisés sont les suivants :

— RIP : Protocole de routage interne à vecteur de distance.

— IGRP : Protocole de routage interne à vecteur de distance de Cisco.

— OSPF : Protocole de routage intérieur à état de liaisons.

— EIGRP : Protocole de routage intérieur à vecteur de distance avancé de Cisco.

— BGP : Protocole de routage extérieur à vecteur de distance[3].

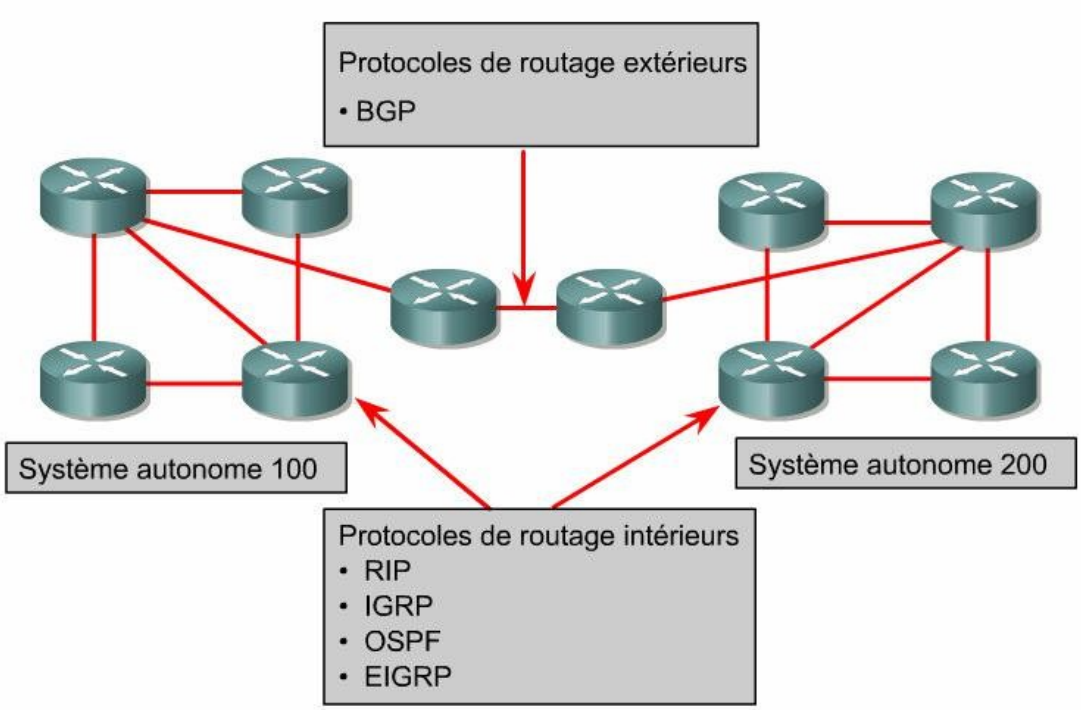

FIGURE 3.4 – Classification des protocoles de routage dynamique.

Au niveau de la couche Internet de l'ensemble de protocoles de la pile TCP/IP, un routeur peut utiliser un protocole de routage IP pour réaliser le routage par la mise en œuvre d'un algorithme de routage particulier. Les protocoles suivants sont des exemples de protocoles de routage IP :

a) Protocole RIP

Le protocole RIP a été initialement défini dans la RFC 1058. Ses principales caractéristiques sont les suivantes :

— Il s'agit d'un protocole de routage à vecteur de distance.
— Il utilise le nombre des auts comme métrique pour la sélection du chemin.
— Si le nombre des auts est supérieur à 15, le paquet est éliminé.
— Par défaut, les mises à jour du routage sont diffusées toutes les 30 secondes[2].

b) Protocole IGRP (Interior Gateway Routing Protocol)

Le protocole IGRP est un protocole propriétaire développé par Cisco. De par sa conception, le protocole IGRP est doté, entre autres, des caractéristiques suivantes :

— Il s'agit d'un protocole de routage à vecteur de distance.
— La bande passante, la charge, le délai et la fiabilité sont utilisés pour créer une métrique composite.
— Par défaut, les mises à jour du routage sont diffusées toutes les 90 secondes[7].

c) Protocole OSPF (Open Shortest Path First)

Le protocole OSPF est un protocole de routage à état de liens non propriétaire. Les caractéristiques clés de ce protocole sont les suivantes :

— Il s'agit d'un protocole de routage à état de liens.
— C'est un protocole de routage de norme ouverte décrit dans les requêtes pour commentaires RFC 2328.
— Il utilise l'algorithme SPF pour calculer le coût le plus bas vers une destination.
— Les mises à jour du routage sont diffusées à mesure des modifications de topologie[3][7].

d) Protocole EIGRP

Le protocole EIGRP est un protocole de routage à vecteur de distances améliorées et propriétaire développé par Cisco. Les caractéristiques clés de ce protocole sont les suivantes :

— Il s'agit d'un protocole de routage à vecteur de distance amélioré.
— Il utilise l'équilibrage de charge en coût différencié.
— Il utilise une combinaison de fonction à vecteur de distance et à état de liens.
— Il utilise l'algorithme DUAL (Diffused Update Algorithm) pour calculer le chemin le plus court.
— Les mises à jour du routage sont diffusées en mode multicast en utilisant l'adresse 224.0.0.10 et sont déclenchées par des modifications topologiques[7].

e) Protocole BGP (Border Gateway Protocol)

Le protocole BGP est un protocole de routage extérieur. Les caractéristiques clés de ce protocole sont les suivantes :

— Il s'agit d'un protocole de routage extérieur à vecteur de distance.
— Il est utilisé pour la connexion entre les FAI ou entre les FAI et les clients.
— Il est utilisé pour acheminer le trafic Internet entre des systèmes autonomes[19].

3.8.4 Les fonctions de base des protocoles de routage

Détermination du chemin et commutation

En règle générale, un routeur détermine le chemin que doit emprunter un paquet entre deux liaisons à l'aide des deux fonctions de base suivantes :

— La détermination du chemin.
— La commutation[14].

a) La Détermination du chemin

La détermination du chemin se produit au niveau de la couche réseau. La fonction de détermination de chemin permet à un routeur d'évaluer les chemins vers une destination donnée et de définir le meilleur chemin pour traiter un paquet. Le routeur se sert de la table de routage pour déterminer le meilleur chemin et transmet ensuite le paquet en utilisant la fonction de commutation[7].

b) La commutation

La fonction de commutation est le processus interne qu'utilise un routeur pour accepter un paquet sur une interface et le transmettre à une deuxième interface sur le même routeur. La fonction de commutation a pour responsabilité principale d'encapsuler les paquets dans le type de trame approprié pour la prochaine liaison.

Le routeur utilise la portion réseau de l'adresse pour sélectionner le chemin qui permettra de transmettre le paquet au prochain routeur situé sur le chemin et une fois arrivé au routeur local, il utilise la partie hôte pour déterminer le port vers lequel envoyer le paquet[7][19].

3.8.5 L'objectif des protocoles de routage dynamique

Les protocoles de routage sont utilisés pour faciliter l'échange d'informations de routage entre des routeurs. Ils permettent aux routeurs de partager de manière dynamique des informations sur les réseaux distants et d'ajouter automatiquement ces informations à leurs propres tables de routage.

Les protocoles de routage déterminent le meilleur chemin vers chaque réseau, lequel est ensuite ajouté à la table de routage. L'un des principaux avantages de l'utilisation d'un protocole de routage dynamique est l'échange d'informations de routage entre des routeurs dès lors qu'une topologie est modifiée.

Les protocoles de routage dynamique requièrent une charge administrative moindre. Toutefois, l'utilisation de protocoles de routage dynamique implique qu'une partie des ressources d'un routeur est dédiée au fonctionnement du protocole[7][19].

3.9 Les protocoles de routage à vecteurs à distances et l'état de liaisons

3.9.1 Fonctionnement des protocoles de routage à vecteur de distance

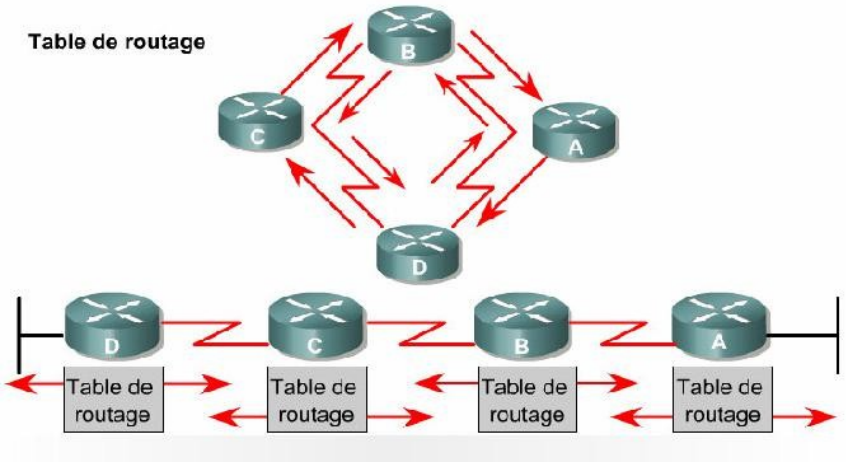

FIGURE 3.5 – Table de routage aux routeurs voisins et cumul des vecteurs de distance.

Les algorithmes de routage à vecteur de distance transmettent régulièrement des copies de table de routage d'un routeur à l'autre (Figure II.5). Ces mises à jour régulières entre les routeurs permettent de communiquer les modifications topologiques. Les algorithmes de routage à vecteur de distance sont également appelés algorithmes Bellman-Ford .

Chaque routeur reçoit une table de routage des routeurs voisins auxquels il est directement connecté. Le routeur B reçoit des informations du routeur A. Le routeur B ajoute un nombre de vecteurs (par exemple, un nombre de sauts) qui allonge le vecteur de distance. Ensuite, le routeur B transmet la nouvelle table de routage à son voisin, le routeur C. La même procédure est répétée étape par étape dans toutes les directions entre les routeurs directement adjacents.

L'algorithme cumule les distances afin de tenir à jour la base de données contenant les informations sur la topologie du réseau. Cependant, les algorithmes de routage à vecteur de distance ne permettent pas à un routeur de connaître la topologie exacte d'un inter réseau,étant donné que chaque routeur voit uniquement ses voisins.

3.9.2 Fonctionnement des protocoles à état de liaisons

Les routeurs à état de liens utilisent une «carte» identique du réseau. Un routeur à état de liens utilise les informations d'état de liens pour créer une topologie et sélectionner le meilleur chemin vers tous les réseaux de destination de la topologie.

Avec certains protocoles de routage à vecteur de distance, les routeurs envoient des mises à jour régulières de leurs informations de routage à leurs voisins. Les protocoles de routage à état de liens n'utilisent pas de mises à jour régulières. Une fois que le réseau a convergé, une mise à jour d'état de liens est envoyée uniquement en cas de modification de la topologie.

Avec l'algorithme de Dijkstra ou algorithme SPF (shortest path first ou du plus court chemin d'abord). Ils gèrent une base de données complexe d'informations topologiques. Les protocoles

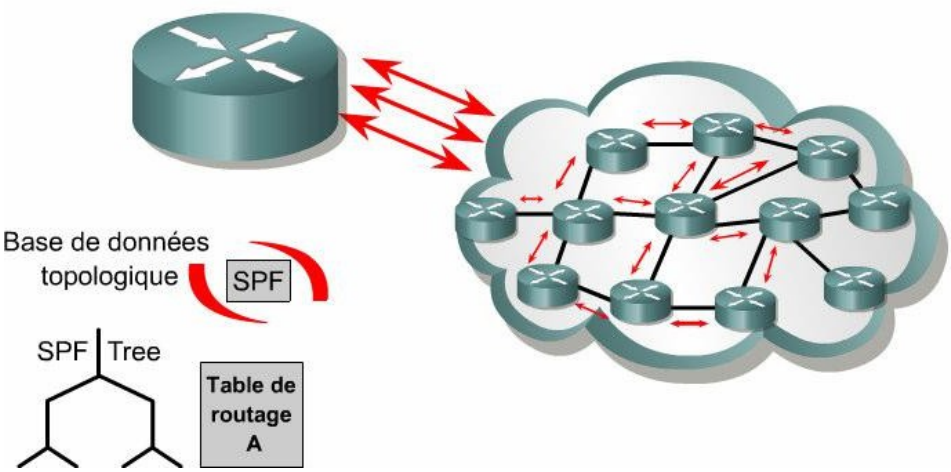

FIGURE 3.6 – Fonctionnement des protocoles à état de liaisons.

à état de liaisons sont tout particulièrement adaptés dans les situations suivantes :

— Réseau conçu de manière hiérarchique (il s'agit généralement de grands réseaux).
— Administrateurs ayant une bonne connaissance du protocole de routage à état de liaisons implémenté.
— Réseau pour lequel une convergence rapide est primordiale.

Les protocoles de routage à état de liaisons nécessitent davantage de mémoire et de capacités de calcul que les protocoles de routage à vecteur de distance. Les routeurs doivent disposer d'une mémoire suffisante pour stocker toutes les informations des différentes bases de données, l'arbre topologique et la table de routage[7][14].

3.10 Métriques et protocoles de routage

Paramètres de métrique et champ de métrique

a) Paramètres de métrique

Les métriques utilisées par les protocoles de routage varient en fonction du protocole. La métrique utilisée par un protocole de routage n'est pas comparable à celle utilisée par un autre protocole. Deux protocoles de routage peuvent choisir des chemins différents avec une même destination par les métriques identifiées.

Le protocole RIP choisit le chemin impliquant le moins de sauts, tandis que le protocole OSPF choisit celui qui présente la bande passante la plus élevée.

Les métriques suivantes sont utilisées dans les protocoles de routage IP :

— **Fiabilité** : est la variation de la probabilité d'échec d'un lien, calculée à partir du nombre d'erreurs de l'interface ou des défaillances du lien.
— **Nombre de sauts** : métrique simple qui compte le nombre de routeurs.
— **Coût** : est la valeur déterminée par l'IOS ou par l'administrateur réseau. Le coût peut représenter une métrique, une combinaison de métriques ou une stratégie.
— **Bande passante** : est la sélection du chemin en préférant celui dont la bande passante est la plus élevée.

— **Charge** : est l'utilisation d'un lien spécifique en termes de trafic.
— **Délai** : est le temps nécessaire à un paquet pour parcourir un chemin.

b) Champ de métrique dans la table de routage

Métrique utilisée par chacun des protocoles de routage :
— **IGRP et EIGRP** : Délai, charge, bande passante et fiabilité. Le meilleur chemin est la route présentant la plus petite valeur de métrique composite, calculée à partir de ces différents paramètres. Par défaut, seuls la bande passante et le délai sont utilisés.
— **OSPF** : Coût. Le meilleur chemin est la route associée au coût le plus faible.
— **RIP** : Nombre de sauts. Le meilleur chemin est la route présentant le nombre de sauts le plus faible[3][5].

3.11 Comparaison des protocoles de routage dynamique

On peut comparer les protocoles de routages de vecteur à distance et à l'état de liaisons par la table 3.1 suivante [7][9][14] :

Protocoles à vecteur de distance	**Protocoles à état de liaison**
Un routeur connaît ses voisins uniquement lors de la transmission de mise à jour de leur part.	Chaque routeur doit connaître ses voisins avant d'échanger des informations.
Les routeurs envoient des mises à jour régulières de leurs informations de routage à leurs voisins.	Les protocoles de routage à état de liens n'utilisent pas de mises à jour régulières. La mise à jour est envoyée uniquement en cas de modification de la topologie.
Un routeur à vecteur de distance fait confiance à un autre routeur pour lui indiquer la distance réelle jusqu'au réseau de destination.	Les routeurs à état de liens utilisent une carte pour déterminer leur chemin préféré vers une autre destination.
Temps de convergence est lent à cause de la détection des boucles.	Temps de convergence est plus rapide.
Les protocoles à vecteur distance sont des protocoles publics (RIP) ou propriétaires (IGRP).	Les protocoles à état de liaison sont uniquement publics (OSPF).

TABLE 3.1 – Comparaison des protocoles de vecteur à distance et l'état de liaison

3.12 Identification des classes des protocoles de routage dynamique

La plupart des algorithmes de routage peuvent être rangés dans l'une des catégories suivantes :
— Vecteur de distance

— État de liaisons

Le routage à vecteur de distance détermine la direction (vecteur) et la distance jusqu'à une liaison quelconque de l'inter réseau. L'approche à état de liaison, également appelée routage

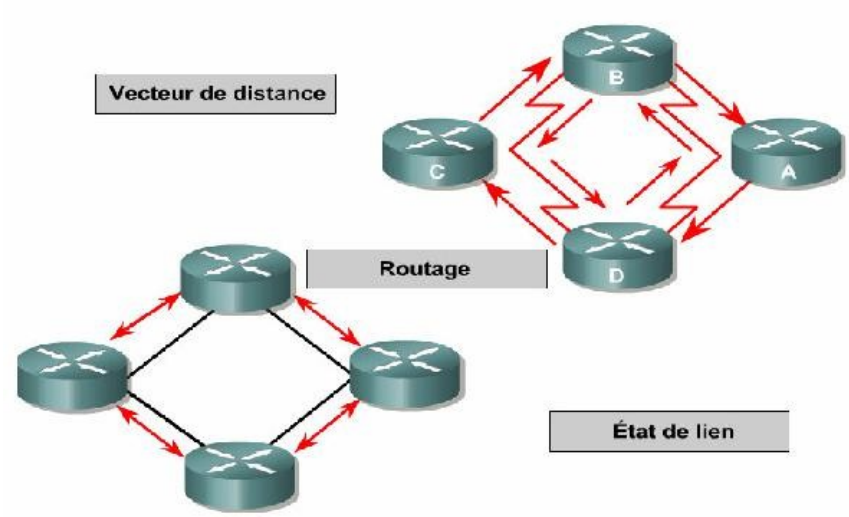

FIGURE 3.7 – Présentation des classes des protocoles de routage dynamique.

par le chemin le plus court, recrée la topologie exacte de l'intégralité du réseau (tient compte de la qualité des liaisons)[4].

3.13 Convergence des protocoles de routage

Il ya convergence si les tables de routage de tous les routeurs sont cohérentes. Le réseau a convergé lorsque tous les routeurs disposent d'informations complètes et précises sur le réseau. Le temps de convergence est le temps nécessaire aux routeurs pour partager des informations ,calculer les meilleurs chemins et mettre à jour leur stables de routage. Un réseau n'est pas complètement opérationnel tant qu'il n'a pas convergé.

Les routeurs partagent des informations les uns avec les autres, mais doivent calculer chacun de leur côté l'impact des modifications de la topologie sur leurs propres routes donc La convergence est à la fois collaborative et indépendante.

Les propriétés deconvergence incluent la vitesse de propagation des informations de routage et le calcul des chemins optimaux. Les protocoles de routage peuvent être classés en fonction de leur vitesse de convergence : une convergence rapide améliore un protocole de routage[6].

4
Mécanisme de sécurité

Introduction

Dans le cadre de la conception de mon infrastructure réseau, le protocole **OSPF** (Open Shortest Path First) est particulièrement adapté aux environnements d'entreprise nécessitant une organisation structurée, une gestion efficace du trafic et une convergence rapide. Grâce à sa capacité à diviser le réseau en zones, OSPF permet une meilleure hiérarchisation, une réduction de la taille des tables de routage, et une plus grande facilité d'administration. Ces caractéristiques répondent parfaitement aux exigences de stabilité, de performance et de scalabilité que je vise dans mon projet. C'est dans cette logique que l'implémentation d'OSPF a été privilégiée pour assurer un routage fiable et optimisé au sein de l'infrastructure simulée.

Ce chapitre est structuré en deux parties : la première est consacrée au protocole de routage à état de liens **OSPF**, et la seconde porte sur les mécanismes de **surveillance, maintenance et sécurité** du réseau[7].

4.1 Le protocole de routage a état de liens (OSPF)

4.1.1 Introduction

OSPF (Open Shortest Path First) est un protocole de routage IGP (Interior Gateway Protocol) de type link-state, standardisé par l'IETF (RFC 2328). Il calcule les routes optimales en utilisant l'algorithme SPF (Dijkstra), garantissant une convergence rapide et évitant les boucles de routage. Adapté aux grands réseaux, il supporte le VLSM (Variable LengthSubnetMask) et le CIDR.

4.1.2 Fonctionnement

— **Topologie Link-State** :
Chaque routeur maintient une base de données (LSDB) identique dans une zone, contenant les états des liens (coûts, voisins).
— **Établissement des Voisins** :
Des paquets *Hello* sont diffusés périodiquement pour découvrir les voisins (adresse multicast `224.0.0.5`).
— **Synchronisation des LSDB** :
Échange de **LSA** (Link State Advertisements) via différents types de paquets :
— **DBD (Database Description)** : Résumé de la LSDB.
— **LSR (Link State Request)** : Demande de LSA manquants.
— **LSU (Link State Update)** : Envoi des LSA.
— **LSAck (Acknowledgment)** : Accusé de réception[4].

4.1.3 Avantages et Inconvénient

a) Avantages du protocole OSPF

— **Convergence rapide**
— Détection des pannes en quelques secondes grâce aux paquets Hello (défaillance après 4x l'intervalle Hello).
— Recalcul immédiat des routes avec l'algorithme SPF (Dijkstra).
— **Architecture hiérarchique (zones)**
— Réduction du trafic : les LSA sont confinés dans chaque zone.
— Optimisation des ressources : seuls les routeurs frontières (ABR) traitent les routes inter-zones.
— **Évolutivité**
— Supporte les très grands réseaux (ex. : opérateurs télécoms) grâce au découpage en zones.
— Jusqu'à 1 000 routeurs par zone (recommandation pratique).
— **Support avancé du routage**
— VLSM/CIDR : allocation flexible d'adresses IP.
— Multipath : équilibrage de charge sur jusqu'à 16 chemins (coût identique).
— **Résistance aux boucles**
— Algorithme link-state garantissant une topologie sans boucle (vs. protocoles à vecteur de distance comme RIP).

b) Inconvénients du protocole OSPF

— **Complexité de configuration**
— Gestion fastidieuse des zones (surtout dans les réseaux multi-zones).
— Paramétrage avancé nécessaire pour les zones spéciales (NSSA, Stub).
— **Consommation de ressources**
— CPU/Mémoire : l'algorithme SPF est gourmand lors des recalculs de topologie.
— Bande passante : synchronisation initiale intensive (échange de LSDB).
— **Sensibilité aux erreurs humaines**

  - Risque d'instabilité si :
    - La zone 0 (backbone) est fragmentée.
    - Filtrage incorrect des LSA.
- **Sécurité insuffisante sans configuration**
  - Authentification non activée par défaut, vulnérabilité aux attaques.
  - MD5 obsolète (nécessité de migrer vers SHA-256/512).
- **Limitations techniques**
  - Broadcast Domains : nécessite des routeurs dédiés dans chaque sous-réseau (coût matériel).
  - Interopérabilité : variations d'implémentation entre constructeurs (Cisco vs. Juniper)[5].

4.1.4 LesVLANs(VirtualLocalAreaNetworks)

Les VLANs jouent un rôle essentiel dans une architecture réseau en permettant une segmentation efficace, ce qui améliore la sécurité, les performances et la gestion du réseau. Les VLANs utilisés dans notre architecture sont illustrés dans le tableau 4.1 : Les VLANs, où chaque direction est associée à un VLAN spécifique.

DIRECTION	VLAN
Comptabilité	VLAN10
DRH	VLAN20
DSI	VLAN40
Invités	VLAN50
Management	VLAN99
Administratif (site2)	VLAN100

TABLE 4.1 – Les VLANs

4.1.5 Justificationdela hiérarchisation

- **Performance** : réduction du domaine de broadcast grâce aux VLANs.
- **Maintenance** : séparation des responsabilités par niveau facilite la supervision.
- **Sécurité** : chaque VLAN peut être isolé avec des ACL [4].

4.1.6 Répartition des protocoles

4.1.6.1 Routage interne : OSPF

OSPF est adapté à un grand réseau avec des politiques de routage flexibles.

4.1.6.2 DHCP (Dynamic Host Configuration Protocol)

Le protocole DHCP est utilisé pour attribuer automatiquement des adresses IP à des dispositifs (clients) sur un réseau. Il est configuré sur les switches Core pour attribuer aux switches d'accès des adresses IP automatiques[7].

4.1.7 Techniquesd'optimisationdestablesderoutage

4.1.7.1 Agrégation et récapitulation des routes

Réduire la taille des tables de routage.
Exemple : résumer toutes les routes des VLANs 10, 20, 40 en une seule route vers la distribution.

4.1.7.2 Prévention des boucles

— **Split Horizon** : empêche un routeur d'envoyer une route par l'interface par laquelle elle a été apprise.
— **Route Poisoning** : désactive les routes invalides en les rendant inaccessibles[22].

Technique	Application dans le projet
Agrégation et récapitulation des routes	Résumer les VLANs du site 1
Split Horizon	Automatique sur OSPF
Route Poisoning	Automatique sur OSPF (LSA update)

TABLE 4.2 – Techniques d'optimisation des tables de routage

4.2 Surveillance Maintenance et Sécurité du Réseau

4.2.1 Introduction

Dans un environnement informatique, la surveillance, la maintenance et la sécurité du réseau constituent des éléments cruciaux pour garantir la fiabilité, la performance et la résilience de l'infrastructure. Après avoir conçu et optimisé la topologie du réseau, cette phase vise à mettre en place les mécanismes nécessaires pour assurerle bon fonctionnement continu du système,anticiperles incidents et protéger les flux de données contre les menaces internes et externes[25].

4.2.2 SurveillanceduRéseau

4.2.2.1 Introduction

La surveillance du réseau est essentielle pour garantir la disponibilité, la performance et la sécurité des infrastructures. Elle permet de détecter les défaillances, de diagnostiquer les problèmes et d'optimiser les ressources réseau. Trois technologies principales sont largement utilisées : SNMP, NetFlow, et sFlow.

4.2.2.2 SNMP (Simple Network Management Protocol)

a) Définition SNMP est un protocole d'application standardisé utilisé pour collecter et organiser les informations des équipements réseau, modifier ces informations afin de gérer ces équipements[20].

b) Fonctionnement Architecture basée sur :
- Manager SNMP (serveur NMS comme SolarWinds, PRTG, etc.)
- Agents SNMP (installés sur les routeurs, switchs, etc.)
- MIB (Management Information Base) : base de données contenant les objets managés.
- Utilise le port UDP 161 (requêtes) et 162 (traps).
- Trois versions principales :
  - SNMPv1/v2c : simple, mais peu sécurisé (authentification par ”community”).
  - SNMPv3 : apporte chiffrement, intégrité et authentification[21].

c) Avantages
- Léger et simple à mettre en œuvre
- Compatible avec presque tous les équipements réseau
- Permet la supervision en temps réel (traps)

d) Limites
- Peu sécurisé (sauf SNMPv3)
- Ne donne pas une vision détaillée du trafic (contrairement à NetFlow/sFlow)

4.2.2.3 NetFlow

a) Définition NetFlow est une technologie développée par Cisco pour surveiller et analyser les flux de données IP transitant par les équipements réseau.

b) Fonctionnement
- Collecte des ”flows” (flux IP) :
  - Adresse IP source et destination
  - Numéro de port source et destination
  - Protocole, taille des paquets, temps de début/fin
- Composants :
  - Exporter (routeur ou switch qui génère les données)
  - Collector (réception et stockage des données)
  - Analyzer (visualisation, reporting)

c) Avantages
- Fournit une vue détaillée sur le trafic
- Permet l’analyse de performance, la détection d’anomalies
- Très utile pour l’optimisation de bande passante

d) Limites
- Consomme plus de CPU que SNMP
- Initialement limité aux équipements Cisco (aujourd’hui standardisé via IPFIX)[22]

4.2.2.4 sFlow (Sampled Flow)

a) Définition sFlow est une alternative open standard à NetFlow, basée sur l'échantillonnage du trafic réseau[23] (sampling).

b) Fonctionnement
- Prélève un échantillon de paquets à intervalles réguliers
- Envoie ces échantillons à un collecteur sFlow
- Composants :
  - sFlow Agent intégré à l'équipement réseau
  - sFlow Collector pour analyse et visualisation[23]

c) Avantages
- Moins de charge CPU que NetFlow
- Supporte des vitesses élevées (10G, 40G)
- Compatible avec un grand nombre de constructeurs (Juniper, HP, Extreme...)

d) Limites
- Résultats approximatifs (échantillonnage)
- Moins précis que NetFlow pour analyses fines

4.2.3 Maintenance du Réseau

4.2.3.1 Introduction

La maintenance proactive vise à prévenir les défaillances avant qu'elles n'affectent la disponibilité du réseau. Contrairement à la maintenance corrective (intervention après panne), la maintenance proactive repose sur l'anticipation des incidents, la sauvegarde régulière, la redondance des équipements et la mise à jour continue de la configuration.

Parmi les outils clés de cette approche figurent :
- **TFTP** : pour les sauvegardes et restaurations automatisées de configurations.
- **HSRP** : pour assurer la redondance des routeurs et une continuité de service même en cas de panne d'un routeur principal[24][25].

4.2.3.2 TFTP–Trivial File Transfer Protocol

a) Définition TFTP est un protocole léger de transfert de fichiers, fonctionnant sur **UDP/69**. Il est principalement utilisé pour :
- Sauvegarder la configuration d'un switch ou routeur.
- Restaurer des fichiers de configuration.
- Transférer des images IOS (firmware)[24].

b) Fonctionnement
- Aucun mécanisme d'authentification.
- Utilise un serveur TFTP (ex : dans Cisco Packet Tracer ou via un logiciel TFTP sur PC).
- Nécessite que le routeur/switch ait une connectivité IP vers le serveur[24].

c) Avantages
- Permet de sauvegarder automatiquement la configuration après modification.
- Utile en cas de remplacement d'un équipement ou de réinitialisation.
- Facile à intégrer dans des scripts d'automatisation (via cron, Python, etc.).

4.2.3.3 HSRP–Hot Stand by Router Protocol

a) Définition HSRP est un protocole de redondance de passerelle développé par Cisco. Il permet à plusieurs routeurs de partager une adresse IP virtuelle et d'élire un routeur actif et un routeur de secours[25].

b) Fonctionnement
- L'utilisateur configure plusieurs routeurs dans un même groupe HSRP.
- Un routeur actif prend en charge le trafic.
- Un routeur en veille (*standby*) surveille l'état de l'actif et prend le relais en cas de panne.
- Une adresse IP virtuelle est utilisée comme passerelle par les PC[25].

c) Avantages
- Haute disponibilité de la passerelle par défaut.
- Basculement automatique rapide.
- Transparence pour les utilisateurs : la passerelle IP reste la même.

4.2.4 Sécurité du Réseau

4.2.4.1 Les ACLS(Access Control Lists)

a) Définition Les ACLs sont des règles de filtrage du trafic qui permettent de contrôler les paquets qui transitent sur un réseau. Elles sont appliquées sur les interfaces des routeurs ou des switches de niveau 3 afin de permettre ou refuser le trafic selon des critères définis : adresse IP source ou destination, protocole, port, etc[19].

b) Fonctionnement
- Les ACLs permettent de :
  - Restreindre l'accès des VLAN invités à certains serveurs.
  - Bloquer l'accès à Internet depuis une plage IP spécifique.
  - Autoriser uniquement les connexions SSH vers les équipements réseau[18].

c) Avantages
- **Renforcement de la sécurité** : Contrôle de l'accès aux ressources du réseau.
- **Blocage du trafic non autorisé** (ex. : accès externe, ports sensibles).
- **Réduction du trafic inutile** : Filtrage des paquets indésirables à l'entrée ou à la sortie du réseau.
- **Meilleure utilisation de la bande passante**.
- **Contrôle granulaire** : Filtrage par IP, protocole, port ou plage d'adresses.
- **Autorisation ou refus précis** du trafic.

— **Facilité d'implémentation** : Simple à configurer via l'interface CLI des équipements Cisco.
— **Compatible avec les routeurs et switches de niveau 3**.

4.2.4.2 Port Security

a) Définition *Port Security* est une fonctionnalité des switches Cisco qui permet de restreindre l'accès aux ports physiques en contrôlant les adresses MAC autorisées à s'y connecter. Elle permet de limiter le nombre de périphériques connectés à un port d'accès[17].

b) Fonctionnement Si une nouvelle adresse MAC inconnue essaie d'accéder au port, le switch applique une action de sécurité selon le mode configuré :
— **protect** : ignore le trafic de la MAC inconnue.
— **restrict** : ignore le trafic et envoie une alerte SNMP/syslog.
— **shutdown** : désactive le port (port en *err-disabled*).

c) Avantages
— Protection contre les connexions non autorisées : bloque les périphériques non connus.
— Facile à configurer et sans matériel supplémentaire : utilisable sur tout switch Cisco L2/L3.
— Complémentaire à d'autres mécanismes (802.1X, ACL) : ajoute une couche physique de sécurité.
— Compatible avec les VLANs : peut s'appliquer dans chaque VLAN indépendamment.

d) Limites
— Pas de détection de *MAC spoofing* avancée : un attaquant peut changer sa MAC pour usurper une MAC autorisée.
— Pas de tolérance à la mobilité : un PC déplacé vers un autre port provoque un blocage.
— Nécessite une surveillance régulière : sinon les *sticky MAC* deviennent obsolètes après remplacement matériel[16].

4.2.4.3 DHCP Snooping

a) Définition *DHCP Snooping* est une fonctionnalité de sécurité des switches Cisco qui agit comme un pare-feu entre les clients DHCP et les serveurs DHCP, permettant de bloquer les faux serveurs DHCP (*rogue DHCP*) et de filtrer les messages DHCP non autorisés[15].

b) Fonctionnement DHCP Snooping fonctionne en classant les ports du switch en deux catégories :
— **Ports trusted** : vers des serveurs DHCP légitimes → laissent passer les messages DHCP.
— **Ports untrusted** : vers les clients ou tout autre port → bloquent les messages `DHCPOFFER/ACK` non autorisés[20].

Le switch :
— Surveille tous les échanges DHCP.
— Construit une table de *bindings* (liaisons) entre :

— Adresse MAC
— IP attribuée
— VLAN
— Port physique

c) Avantages
— Protection contre les *rogue DHCP* : empêche les affectations IP malveillantes.
— Intégration avec d'autres mécanismes : supporte DAI, IP Source Guard, etc.
— Création de table de bindings fiable : table IP/MAC/VLAN utilisée comme base de sécurité.
— Facile à auditer et surveiller via `show ip dhcp snooping binding` et `show ip dhcp snooping`.

d) Limites
— Dépend du bon fonctionnement DHCP : ne fonctionne que pour les clients utilisant DHCP.
— Pas de détection de spoofing manuel : n'empêche pas un attaquant de fixer manuellement son IP/MAC.
— Maintenance accrue : la table de bindings doit être surveillée (notamment en cas de mobilité)[18].

4.2.4.4 DAI

a) Définition *DAI (Dynamic ARP Inspection)* est un mécanisme de sécurité des switches Cisco qui protège le réseau contre les attaques ARP spoofing en interceptant, vérifiant et filtrant les paquets ARP non valides ou falsifiés[17].

b) Fonctionnement de DAI
— DAI se base sur la table *DHCP snooping binding* (liste des adresses MAC et IP associées aux ports).
— Lorsqu'un paquet ARP est reçu, le switch compare l'adresse IP, l'adresse MAC source et l'interface avec les données de cette table.
— Si les informations sont cohérentes, le paquet est autorisé.
— Sinon, le paquet est bloqué, car il est considéré comme une tentative d'usurpation d'identité.
— DAI protège donc la couche 2 du modèle OSI, qui est vulnérable par défaut aux attaques ARP[17].

c) Avantages
— **Protection contre ARP spoofing** : Empêche les attaques Man-in-the-Middle et les détournements de trafic ARP.
— **Validation basée sur IP/MAC réels** : Utilise des informations DHCP valides pour vérifier les trames ARP.
— **Intégration avec DHCP Snooping** : Fonctionne de manière complémentaire pour un filtrage cohérent.

— **Logs et alertes** : Génère des logs en cas de trames ARP non conformes, ce qui facilite l'audit et le dépannage[14].

d) Limites

— **Requiert DHCP Snooping** : Sans table de binding, DAI ne peut pas valider les trames ARP.
— **Pas compatible avec IP statiques par défaut** : Les hôtes configurés manuellement sont rejetés sans ACL ou exceptions.
— **Maintenance nécessaire** : Il faut mettre à jour les ACL ARP ou autoriser les hôtes statiques.
— **Complexité en environnement mixte** : Risque de blocages si mal configuré[16].

La figure 4.1 présente une illustration de la configuration.

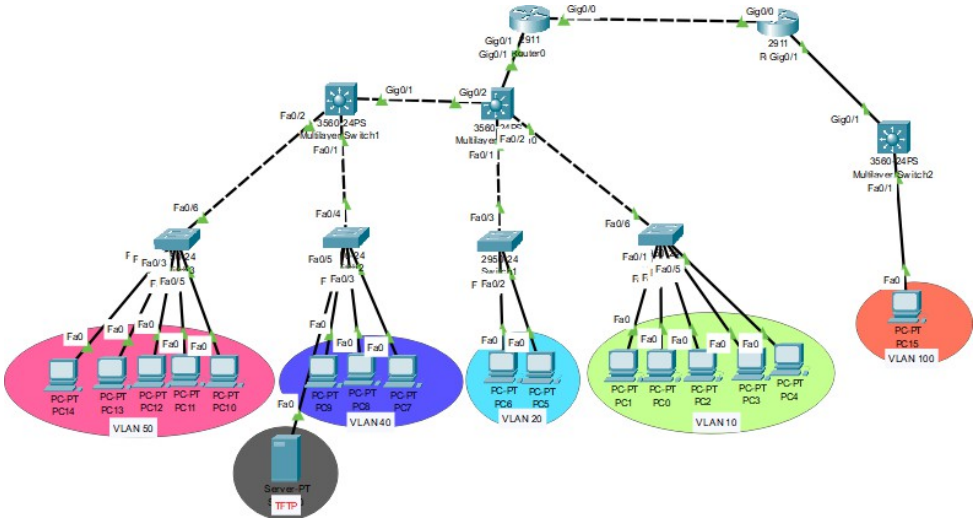

FIGURE 4.1 – Topologie Configuré

4.3 Conclusion

Dans ce chapitre, nous avons proposé une conception et optimisation de l'architecture réseau de l'entreprise CEVITAL. Nous avons proposé des améliorations au niveau de Surveillance Maintenance et Sécurité du Réseau. Pour pallier les faiblesses identifiées précédemment, garantissant ainsi l'efficacité et la stabilité du réseau. Dans le chapitre suivant, nous allons montrer la mise en œuvre et les tests effectués pour la mise en place de l'architecture. Le chapitre suivantse concentrera sur l'application concrète del'architecture conçue, à travers la configuration des équipements,la mise en place des protocoles, ainsi que la réalisation de tests visant à vérifier la conformité, la performance du réseau.

5
Mise en oeuvre et Test

Introduction

La dernière étape de notre travail porte sur la mise en œuvre de notre architecture. Durant cette phase, nous ferons lasimulation de la solution proposée. Pour ce faire, nous débuterons par la présentation du simulateur utilisé, suivie d'une explication détaillée des différentes étapes à suivre.

5.1 Présentation du simulateur "CiscoPacketTracer"

Packet Tracer est un simulateurdematériel réseau développéparCiscoSystem. Cet outil est fourni gratuitement aux centres de formation, aux étudiants et aux diplômés participants ou ayant participé aux programmes de formation Cisco (Cisco Networking Academy). L'objectif de Packet Tracer est de permettre aux élèves et aux professeurs d'apprendre les principes du réseau tout en acquérant des compétences spécifiques aux technologies Cisco. Il peut être utilisé pour s'entraîner, se former, préparer les examens de certification Cisco, ainsi que pour la simulation d'architectures réseaux. La figure IV.1 montre l'interface de packet tracer.

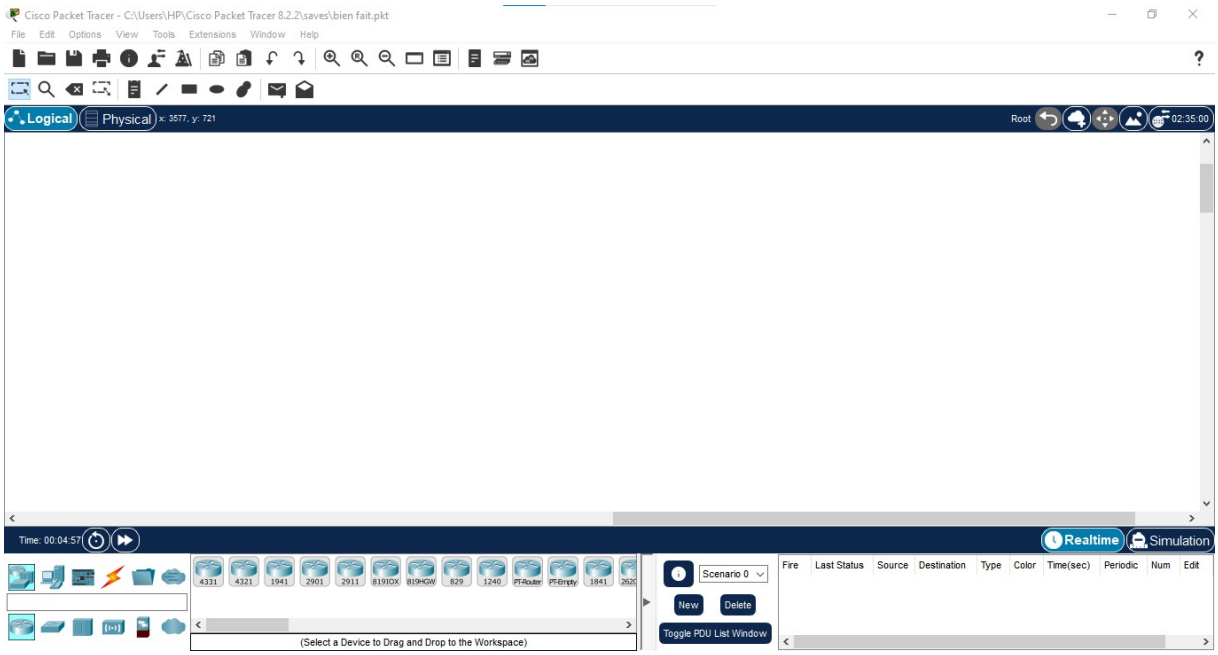

FIGURE 5.1 – Interface Packet Tracer

5.2 Configuration des équipements

5.2.1 Configuration des commutateurs

Nous allons commencer par la création des VLANs surles switches niveau 3, sachant qu'il yaura en tout 6VLANs, voici la figure 5.2 de création de VLANs.

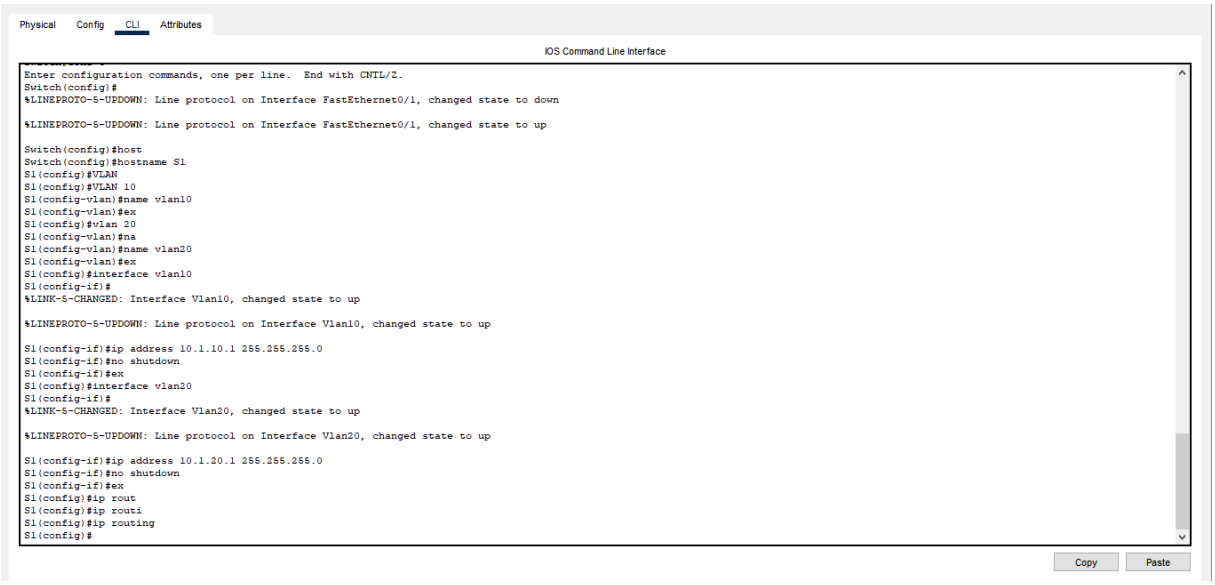

FIGURE 5.2 – Création VLANs

5.2.2 Configuration des Interfaces

Nous allons configurer les liaisons entre les commutateurs en mode Trunk (Figure 5.3). Par contre les interfaces en mode accès se trouvent au niveau des liens entre les commutateurs d'accès et les PC (Figure 5.4). Les figures suivantes illustrent les configurations effectuées.

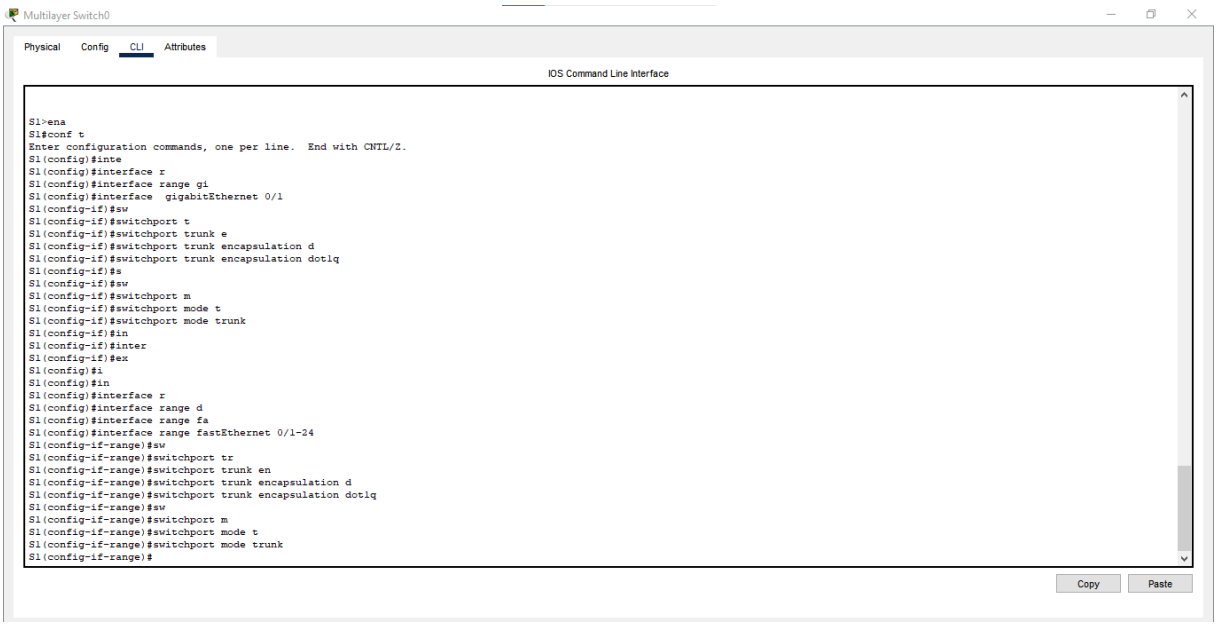

FIGURE 5.3 – Activation des liens Trunk

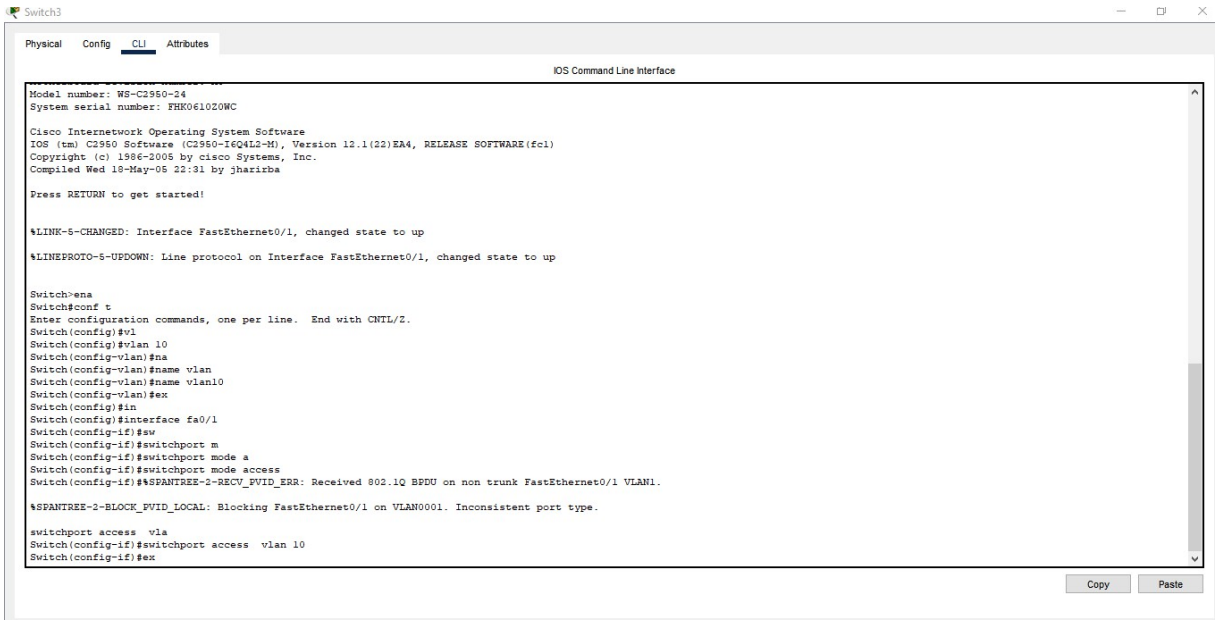

FIGURE 5.4 – Activation des liens Access

5.2.3 Configuration de OSPF

Maintenant,nousallonsconfigurerleprotocole OSPF,enprendexempleleswitch.(Voirla figure 5.5).

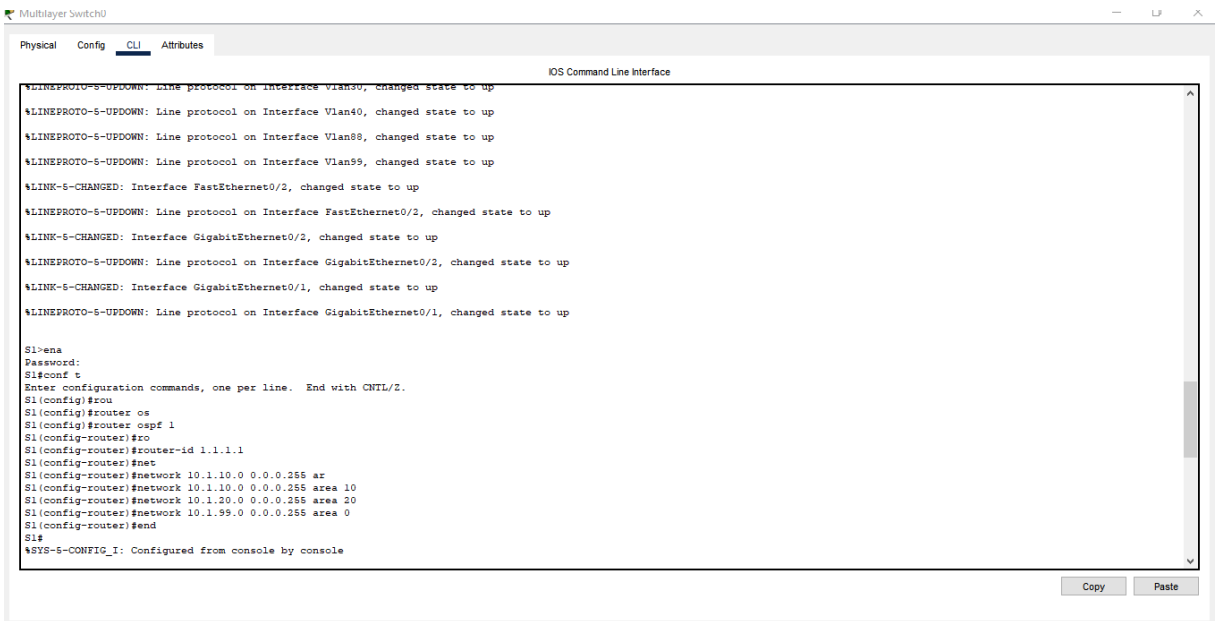

FIGURE 5.5 – Configuration de OSPF

5.2.4 Configuration de Mécanisme de sécurité OSPF

Maintenant, nousallons configurer le Mécanisme de sécurité OSPF,on prend exemple le Routeur.(Voirlesfigures 5.6)

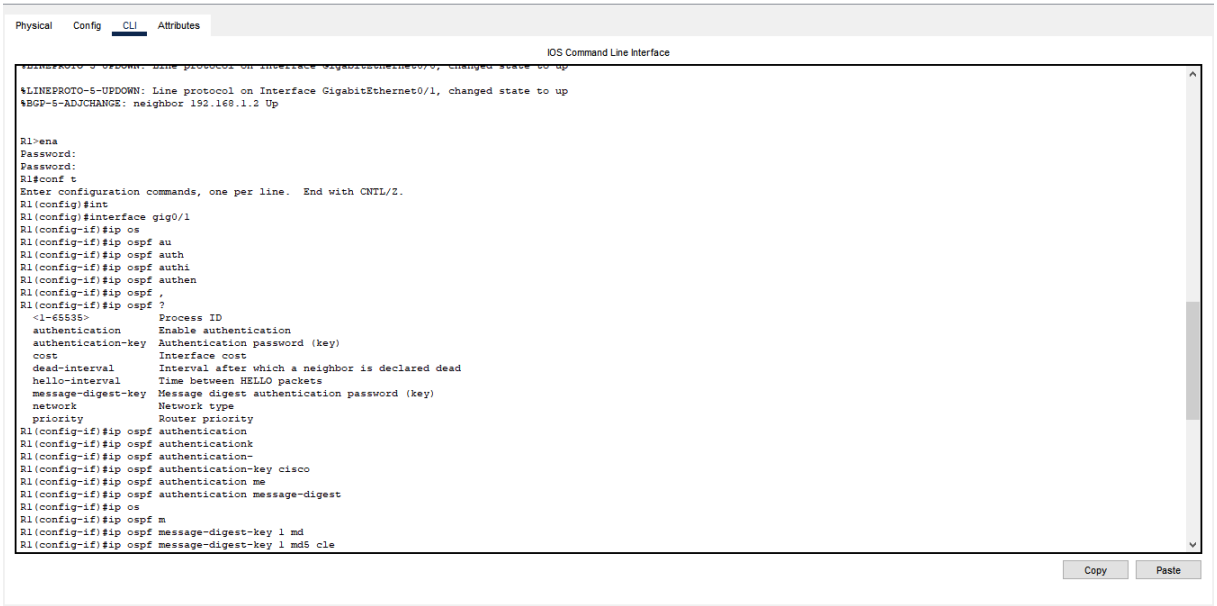

FIGURE 5.6 – Mécanisme de sécurité OSPF

5.2.5 Configuration de DHCP

Pour configurer le serveur DHCP,nous devons créer des pools d'adresses qui comporteront les noms des VLANs tout en introduisant les Gateway et le nombre maximum d'adresses. Nous continuons avec en exemple le switch.(voir les figures 5.7)

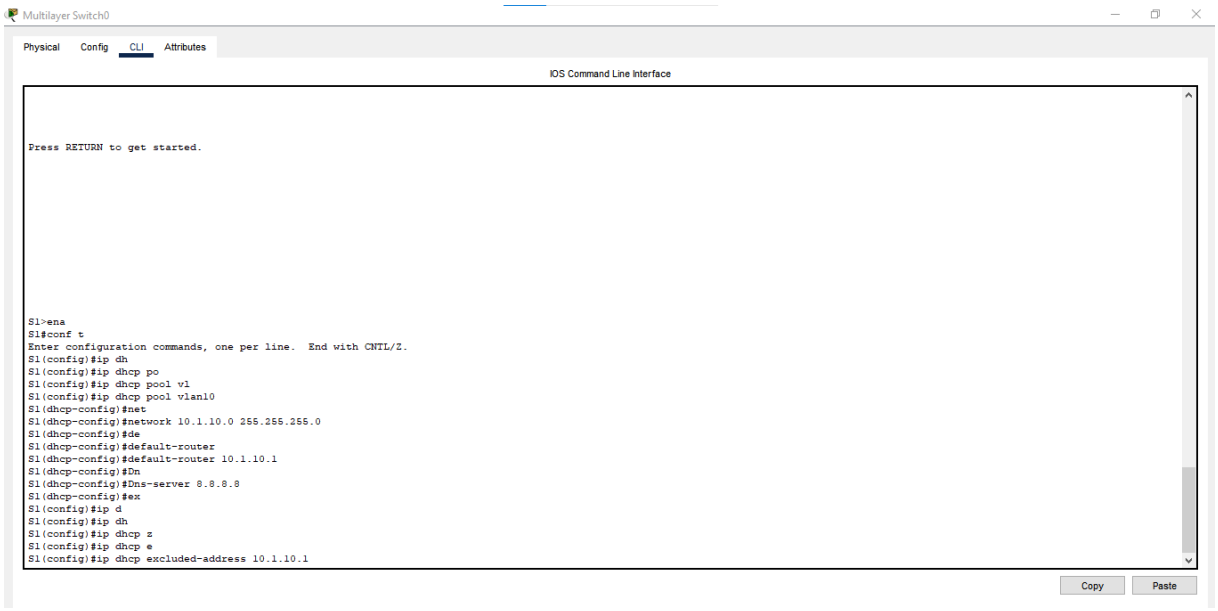

FIGURE 5.7 – Configuration de DHCP

5.2.6 Configuration de L'ACL

Maintenant,nous allons configurer les ACL dans les switches niveau3. (Voir lesfigures **??**)

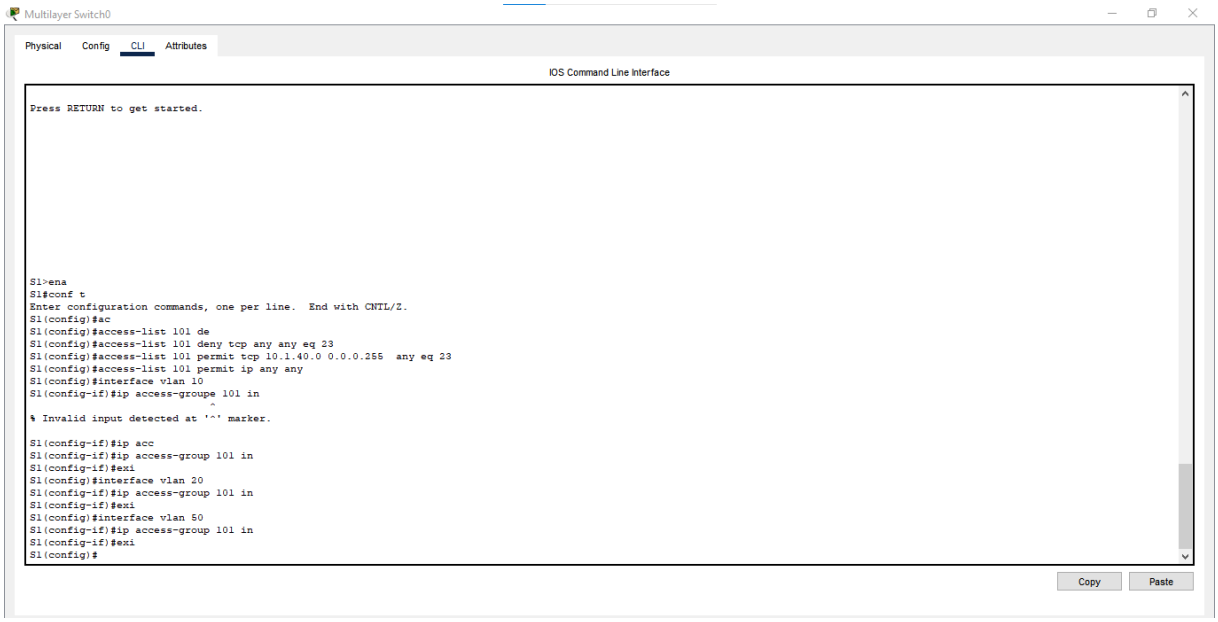

FIGURE 5.8 – Configuration de L'ACL

5.2.7 Configuration du HSRP

La configuration du protocole HSRP sur les deux switches niveau3 est illustré sur la figure 5.9.

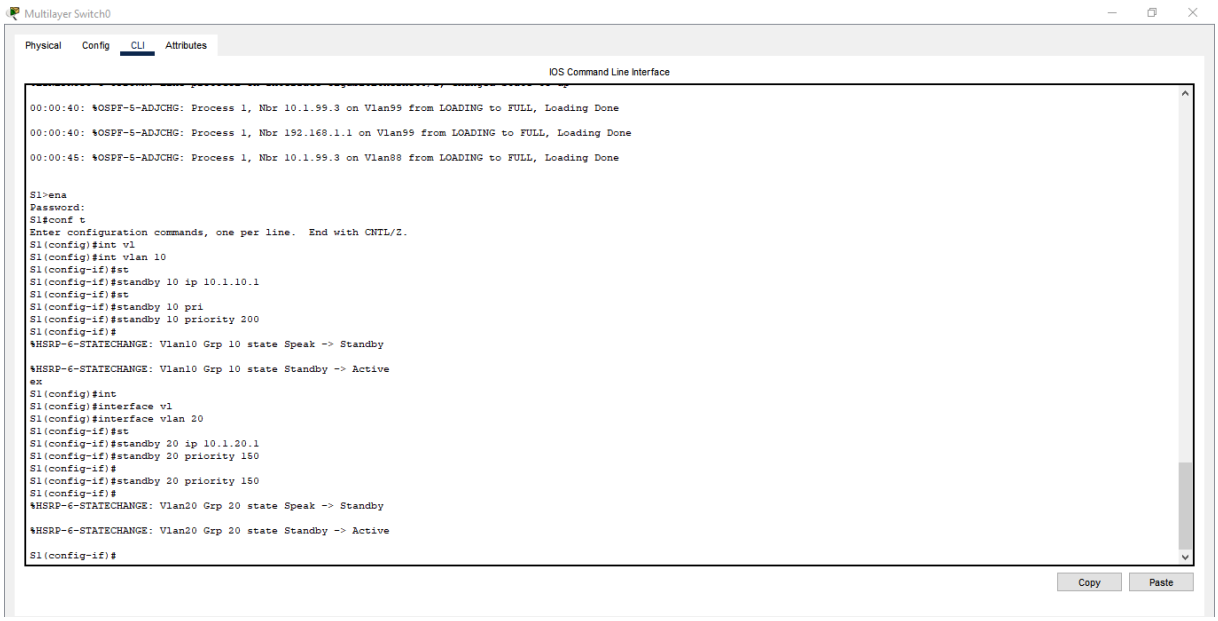

FIGURE 5.9 – Configuration du HSRP

5.2.8 Configuration du port security

Activer pour limiter le nombre de MAC autorisées par portet bloquerles connexions inconnues.(Commeillustré sur la figure 5.10).

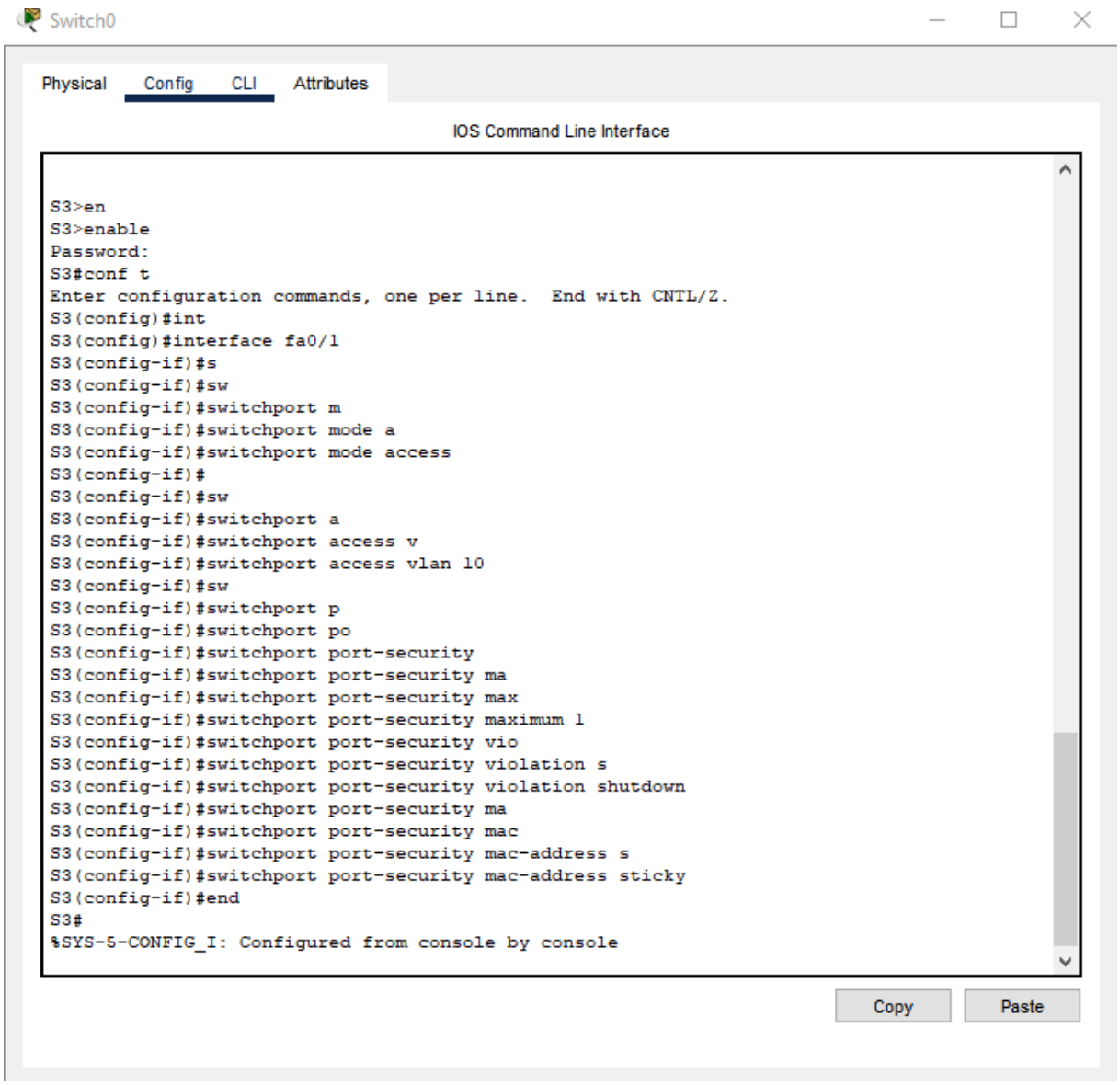

FIGURE 5.10 – Configuration port security

5.2.9 Configuration du DHCP snooping

Activé pour bloquer les faux serveurs DHCP surles ports non autorisés.(Voir lafigure 5.11).

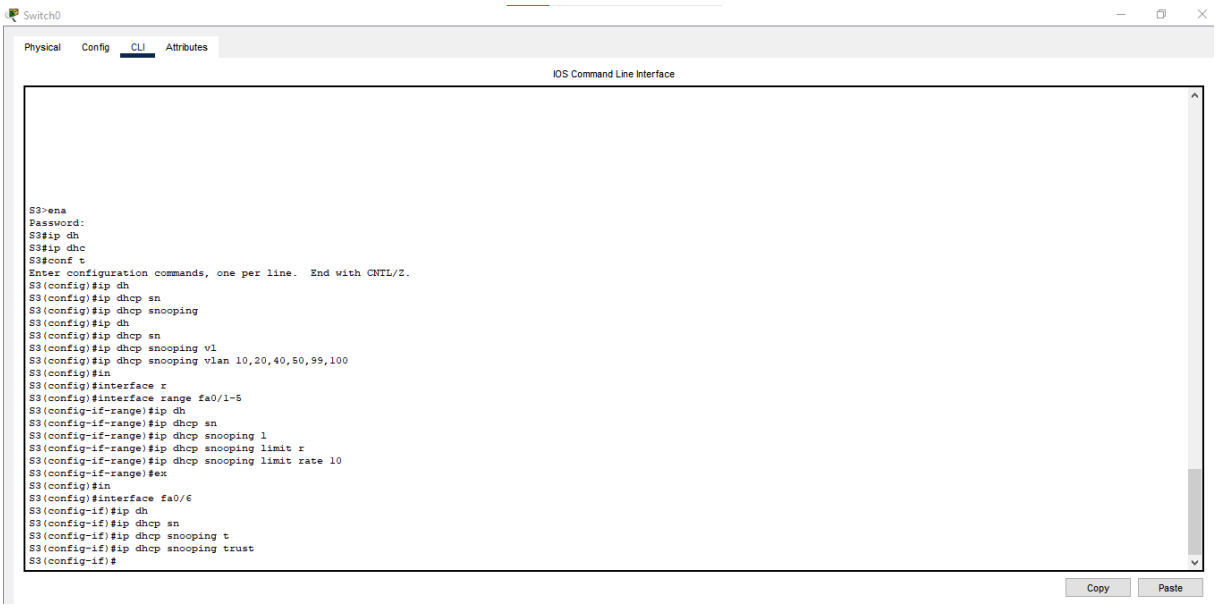

FIGURE 5.11 – Configuration du DHCP snooping

5.2.10 Configuration du DAI(Dynamic ARP Inspection)

Permet de bloquer les requêtes ARP falsifiées grâce aux données DHCP Snooping.(voirla figure 5.12).

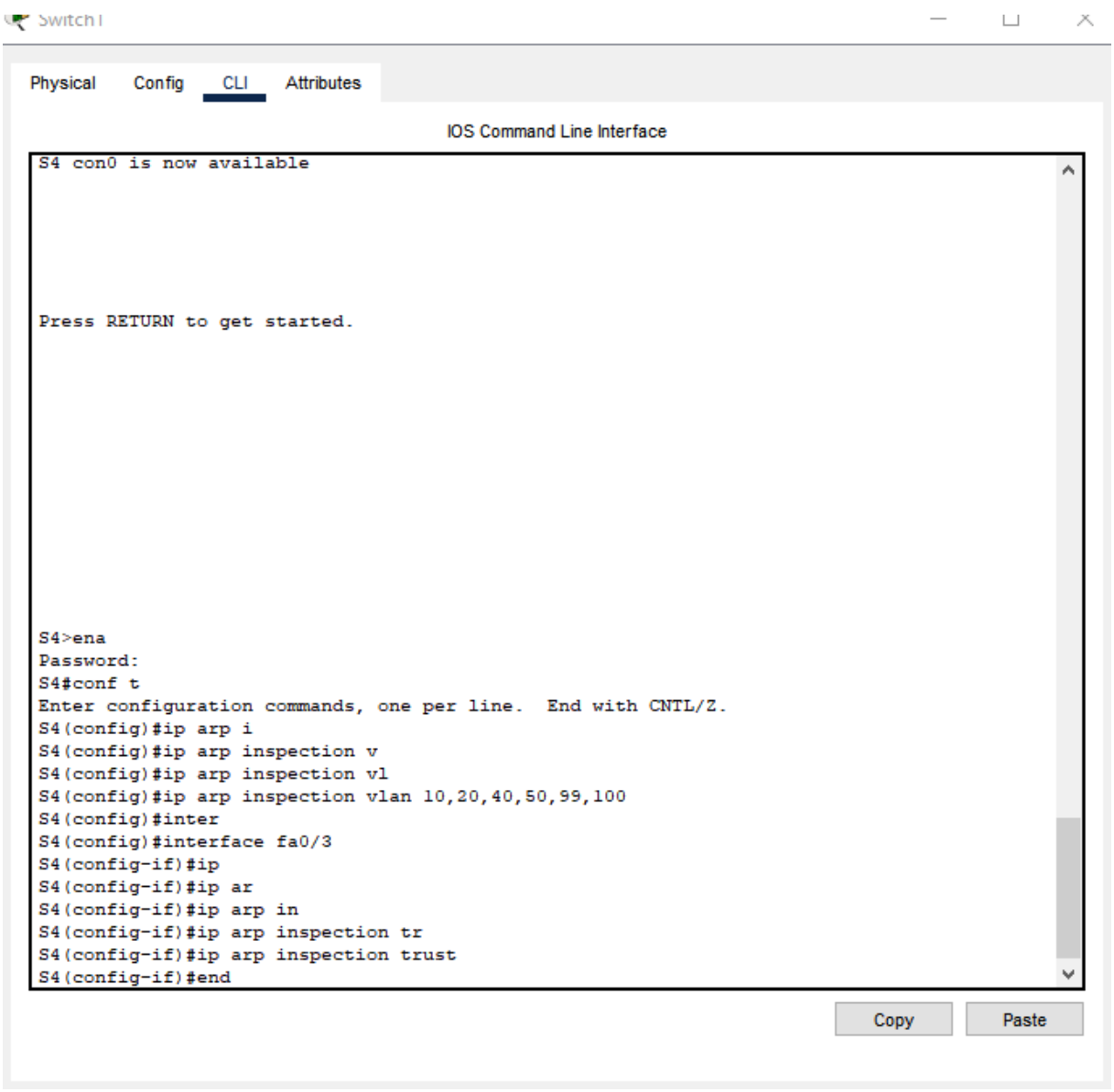

FIGURE 5.12 – Configuration du DAI (Dynamic ARPInspection)

5.3 Test et validation de la configuration

Dans cette section, nous allons vérifier la connectivité entre les différents équipements de l'architecture. Cette vérification sera réalisée à l'aide de la commande ¡ping¿.

5.3.1 Test intra-VLAN

Ce test vérifie la connectivité entre Pc-0(10.1.10.3)et Pc-2(10.1.10.5) d'un même Vlan10. (VoirFigure 5.13)

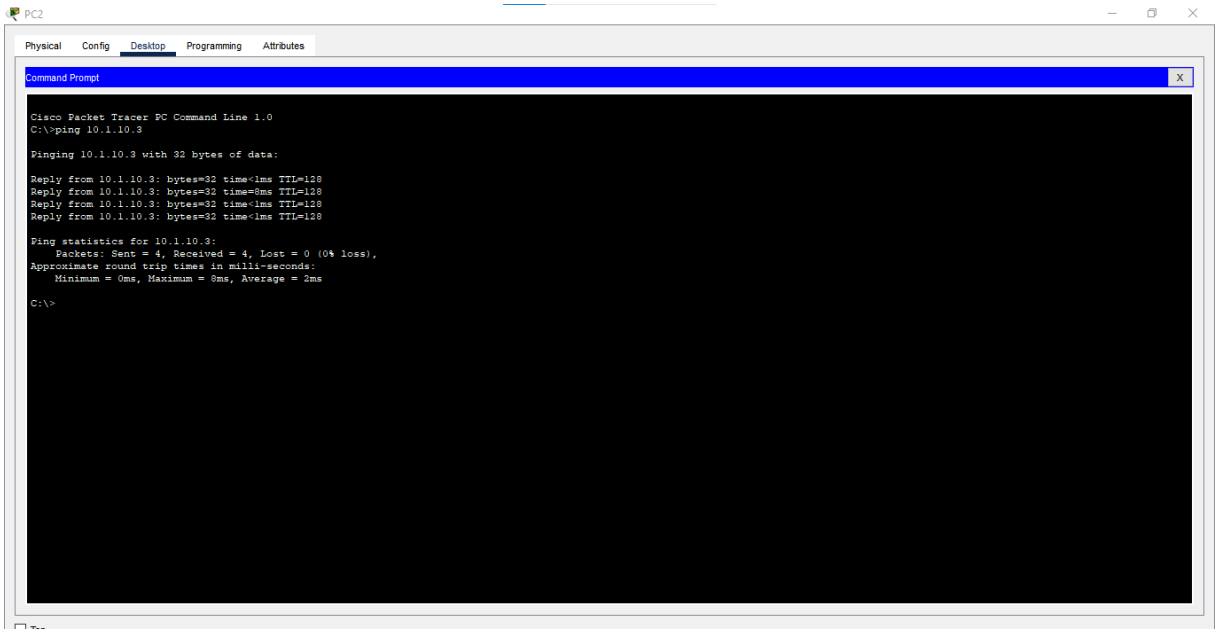

FIGURE 5.13 – Test intra-VLAN

5.3.2 Test inter-VLAN

Cetest vérifie la connectivité entre Pc-0(10.1.10.3) dans Vlan10. et Pc-7(10.1.40.5)dans Vlan40. (Voir figure 5.14)

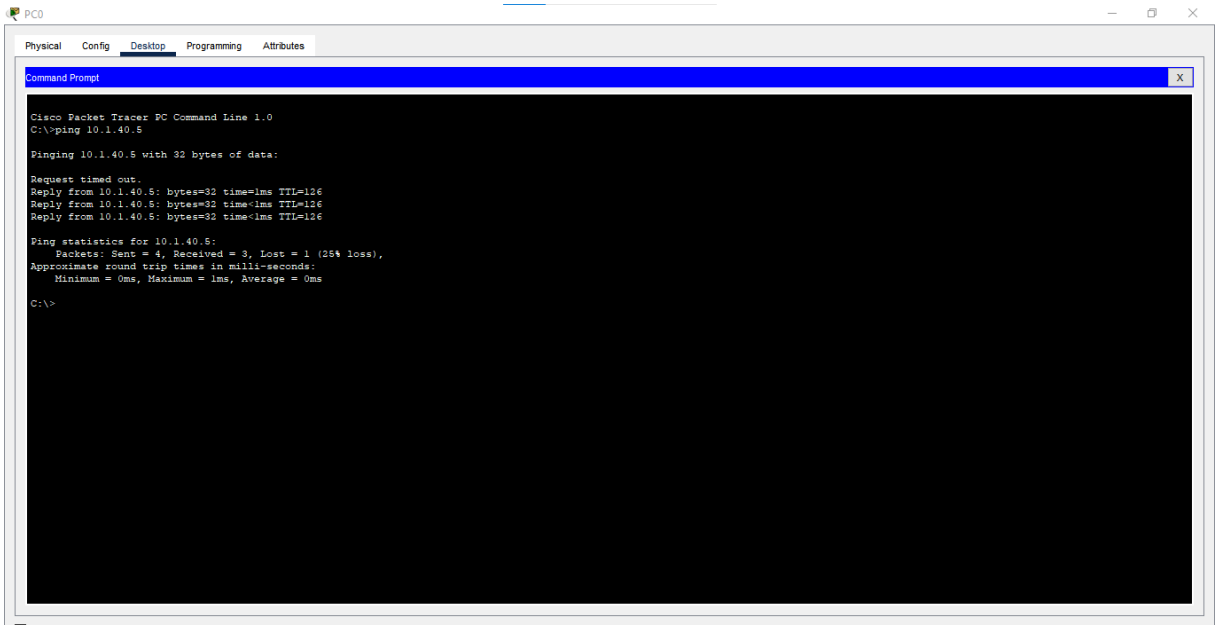

FIGURE 5.14 – Test inter-VLAN

5.4 Conclusion

Ce dernier chapitre décrit la phase de mise en œuvre de l'ensemble des configurations des équipements réseau, ainsi que les tests de connectivité nécessaires pour la mise en place de l'architecture réseau de **CEVITAL**.

Conclusion générale et travaux futures

Au terme de ce mémoire, nous avons pu démontrer l'importance cruciale des réseaux informatiques dans le fonctionnement des systèmes d'information actuels, ainsi que la nécessité de concevoir des infrastructures efficaces, sécurisées et adaptées aux besoins spécifiques de chaque organisation. L'évolution rapide des technologies et des usages numériques impose une maîtrise rigoureuse des concepts de base des réseaux, mais aussi des outils et des protocoles de routage les plus pertinents.

La première partie de ce travail nous a permis de revoir en profondeur les fondements des réseaux informatiques, notamment les types de réseaux, les architectures, les équipements et les modèles de communication. Ces notions sont essentielles pour comprendre comment les données circulent dans une organisation et comment garantir leur fiabilité, leur confidentialité et leur disponibilité.

Nous avons ensuite exploré les protocoles de routage, avec une focalisation sur OSPF, en analysant ses mécanismes, ses avantages et ses domaines d'application. Ce protocole, basé sur l'état des liens, permet une convergence rapide et une grande souplesse dans les réseaux de moyenne et grande envergure. Son intégration dans une architecture bien structurée constitue une solution fiable pour assurer la connectivité interne et optimiser les chemins empruntés par les paquets.

La dernière partie de ce mémoire a été dédiée à la mise en pratique de ces concepts à travers une simulation complète d'un réseau d'entreprise. À l'aide de l'outil Cisco Packet Tracer, nous avons conçu, configuré et testé une architecture intégrant des VLANs, le routage inter-VLAN, le protocole OSPF, ainsi que des mécanismes de sécurité et d'adressage dynamique. Les résultats obtenus ont confirmé l'efficacité de notre conception, tant en termes de performance que de robustesse.

Ce projet a été l'occasion de mobiliser et d'appliquer nos compétences en ingénierie réseau, tout en nous préparant à répondre aux exigences du monde professionnel. Il constitue une étape importante dans notre parcours, et ouvre la voie à des perspectives d'approfondissement, notamment dans l'automatisation, la supervision avancée ou l'intégration de technologies émergentes comme le SDN.

Nous espérons que ce travail apportera une contribution pertinente et utile dans le domaine de la conception et de la gestion des réseaux informatiques.

Bibliographie

[1] J. Havez, *Routage Statique, Dynamique avec Ripv1, Ripv2 et OSPF*, Ed. UTBM, 2005.

[2] C. Hedrick, *Routing Information Protocol*, Internet Request For Comments RFC 1058, June 1988.

[3] J. Moy, *OSPF Version 2*, Internet Request For Comments RFC 1583, March 1994.

[4] G. Pujolle, *Cours réseaux et télécom*, Ed. Eyrolles, 2004.

[5] I. Rudenko, *Configuration IP des routeurs Cisco*, Ed. Eyrolles, 2005.

[6] D. Seab, *Interconnexion des réseaux à l'aide des routeurs commutateurs*, Ed. ENI, Novembre 2003.

[7] G. Steve, *Synthèse de protocoles courants*, Ed. Degouet Fabien, 1999.

Sites Web :

— [8]http://www.reseaux-telecoms.fr
— [9]http://www.commentcamarche.com
— [10]http://www.guill.net
— [11]http://www.bet.be
— [12]http://www.egs-howto.com
— [13]http://www.linux-france.org
— [14]http://www.supinfo.com
— [15]http://www.cisco.fr
— [16]http://www.commentcamarche.net/forum
— [17]http://www.ipsec-howto.org
— [18]http://www.hsc.fr
— [19]http://www.ietf.org
— [20]https://datatracker.ietf.org/doc/html/rfc1157 — SNMP RFC 1157
— [21]https://datatracker.ietf.org/doc/html/rfc3411 — Architecture SNMPv3 RFC 3411-3418
— [22]https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html — Cisco NetFlow
— [23]https://sflow.org — sFlow Protocol
— [24]https://datatracker.ietf.org/doc/html/rfc1350 — TFTP Protocol RFC 1350
— [25]https://datatracker.ietf.org/doc/html/rfc2281 — HSRP Protocol RFC 2281

Résumé

Ce mémoire porte sur la conception et l'optimisation d'une infrastructure réseau utilisant des protocoles de routage avancés. L'objectif principal est de démontrer la mise en œuvre d'une architecture réseau fiable et performante à l'aide du protocole OSPF (Open Shortest Path First), particulièrement adapté aux réseaux internes d'entreprise. Ce travail est structuré en deux parties principales : la première présente les concepts théoriques fondamentaux des réseaux informatiques, les types de topologies, ainsi que le rôle des protocoles de routage. La deuxième partie se concentre sur l'étude de cas pratique, où une architecture réseau est conçue et simulée dans un environnement virtuel, intégrant les VLANs, le routage inter-VLAN et les mécanismes de sécurité. Les résultats obtenus démontrent l'efficacité de la solution proposée, en termes de performance et de fiabilité du réseau simulé.

Mots clés : réseaux informatiques, routage OSPF, infrastructure réseau, simulation réseau, VLAN, inter-VLAN, fiabilité réseau

Abstract

This thesis focuses on the design and optimization of a network infrastructure using advanced routing protocols. The primary goal is to demonstrate the implementation of a reliable and high-performing network architecture using the OSPF (Open Shortest Path First) protocol, which is particularly suited for internal corporate networks. This work is divided into two main sections : the first presents the fundamental theoretical concepts of computer networks, types of topologies, and the role of routing protocols. The second part focuses on the practical case study, where a network architecture is designed and simulated in a virtual environment, incorporating VLANs, inter-VLAN routing, and security mechanisms. The results show the effectiveness of the proposed solution in terms of network performance and reliability.

Keywords : computer networks, OSPF routing, network infrastructure, network simulation, VLAN, inter-VLAN, network reliability