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

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Réseaux et télécommunications

Thème

Elaboration d'un plan de continuité d'activité(PCA) robuste pour assurer la résilience des systèmes informatiques -Cas EPB-

Préparé par :

Mlle DJENADI Chiraz et **Mlle REDOUANI** Ouarda

Membre de jury :

Mme BOUNCER. S	**Université de Bejaia**	**Présidente**
Mlle ACHOUR. L	**Université de Bejaia**	**Examinatrice**
Mme ZENADJI. S	**ESTIN**	**Encadrant université**
Mr MANSOUR. A	**Université de Bejaia**	**Encadrant entreprise**

Année universitaire : 2023/2024

Remerciements

En premier lieu nous tenons à remercier « le bon Dieu » pour la patience et la santé qu'il nous a offertes tout au long de nos études.

Nous remercions notre promotrice ***« M^{me} ZENADJI S »*** *d'avoir acceptée de nous encadrer et de nous orienter pour la réalisation de notre projet, ainsi que pour sa confiance, ses encouragements, ses corrections et pour Ses conseils qu'elle nous a apportés nous remercions aussi* ***« M^{me} Zaidi N »*** *pour son aide et ses conseils.*

Nos sincères remerciements s'adressent également à ***« M^{r} MANSOUR A »*** *notre promoteur à l'Entreprise Portuaire de Bejaia pour son accueil et tous ses conseils prestigieux ainsi qu'à son soutien dans les moments difficiles rencontrés durant cette épreuve, Un grand merci pour l'organisme d'accueil EPB, qui nous a accepté comme stagiaires et qui nous a donné une chance pour découvrir le domaine professionnel.*

Nous tenons également à remercier l'ensemble des membres de jury pour l'intérêt qu'ils ont portés à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.

Un grand merci également à tous nos enseignants de département ATE qui nous ont accompagnés durant notre parcours universitaire, pour le savoir qu'ils nous ont transmis, et aussi parce qu'ils nous ont appris à aimer la spécialité RT.

Enfin, nous tenons à exprimer nos sincères remerciements à nos familles, nos amies et à tous ceux qui ont contribué à la réalisation de ce mémoire fin d'étude.

Dédicaces

Avec un énorme plaisir, un cœur ouvert et une immense joie, que je dédie ce modeste travail :

À mes très chers parents, pour leurs patiences, leur amour, leurs encouragements et leurs sacrifices tout au long de mon parcours ;

À mes petites sœurs : ***Kahina****,* ***Karima****,* ***iline****,* ***Amel****,* ***ritadj****.*

À toute ma famille ***REDOUANI****;*

À ma binôme ***CHIRAZ****, celle qui m'a accompagné tout au long de notre parcours, je t'exprime ma gratitude ;*

À tous mes amis et camarades, en particulier ***IMENE****,* ***NONOCH****,* ***NASSIM****,* ***AMINE****. Je garde en souvenir les bons moments et tout ce que nous avons vécu ensemble. ET à tous ceux qui m'ont aidé dans l'élaboration de ce travail.*

OUARDA*.*

Avec gratitude, et des plus profondes, je dédie ce modeste travail :

À mes chers parents, mes frères, ma sœur et ma belle sœur ;
À mon frère ***FOUAD*** *qui, malgré la distance, reste présent et à mes côtés ;*

À ma binôme ;

À toute personne qui m'a encouragé tout au long de ce parcours

CHIRAZ*.*

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

A

ADSL : *Asymetric digital subscriber line.*

B

BIA : *Bilan impact d'activité.*

BPDU *Bridge Protocol Data Unit.*

D

DHCP : *Dynamic Host Configuration Protocol.*

DMIA : *Temps d'interruption maximum autorisé.*

DSI : *Direction des systèmes informatiques.*

E

EIGRP : *Enhanced Interior Gateway Routing Protocol.*

EPB : *Entreprise portuaire de Bejaia.*

F

FDDI : *Fibre Distributed data interface.*

H

HSRP : *Hot Standby Routing Protocol.*

I

ID : *Identifiant.*

IEEE : *Institute of Electrical and Electronics Engineers.*

IP : *Internet Protocol.*

ISO : *International Standards Organization.*

L

LACP : *Link Aggregation Control Protocol.*

LAN : *Local Area Network.*

M

MAC : *Media Access Control.*

MAN : *Metropolitan Area Network.*

MCA : *Management de la Continuité d'Activité.*

O

OMCA : *Objectif minimum de continuité d'activité.*

OSPF : *Open Shortest Path First.*

P

PAN : *Personal Area Network.*

PAgP : *Port Aggregation Protocol.*

PCA : *Plan de continuité d'activité .*

PMDT : *Perte de données maximale tolérable.*

PRA : *Plan reprise d'activité.*

PSI : *plan de secours informatique .*

R

RIP : *Routing Information Protocol.*

RSSI : *Responsable de la sécurité du système d'information.*

S

S.I : *Système informatique.*

SSH : *Secure Socket Shell.*

STP : *Spanning-Tree Protocol.*

T

TTL : *Time to live .*

U

USB : *Universal Serial Bus.*

V

Vlan : *Virtual Local Area Network.*

VRRP : *Virtual Router Redundancy Protocol.*

VTP : *Vlan trunking Protocol.*

VTY : *Virtual terminal line.*

W

WAN : *Wide Area Network.*

WiMAX : *Worldwide interoperability for microwave access.*

Introduction générale

L'Importance des systèmes informatiques dans le fonctionnement des entreprises modernes n'est plus à démontrer. En effet, ces systèmes sont devenus des outils indispensables pour la communication, la collaboration, la gestion des données, l'accès aux ressources et bien d'autres fonctions vitales pour l'entreprise.

Cependant, la disponibilité de ces systèmes est souvent mise à rude épreuve par des pannes matérielles ou logicielles, des cyberattaques, des catastrophes naturelles et d'autres facteurs de risque. Les interruptions des systèmes informatiques peuvent avoir des conséquences désastreuses sur le fonctionnement de l'entreprise, entraînant des pertes financières, des perturbations dans les activités quotidiennes et une perte de confiance des clients et des partenaires.

Pour répondre à cette problématique, le site de secour et la redondance des réseaux sont devenus des solutions de plus en plus populaires pour garantir la continuité des activités de l'entreprise. Un site de secour est conçu pour offrir une disponibilité maximale en cas de panne ou de défaillance, en fournissant des liens de secours, des mécanismes de basculement automatique et d'autres fonctionnalités de résilience. Ce mémoire vise à fournir une étude théorique et pratique de la continuité d'activité pour L'EPB, en présentant ses activités, ses risques, les solutions et les résultats de l'implémentation de cette solution. Le présent mémoire comporte trois chapitres :

1. Les concepts de base d'un plan de continuité d'activité : Ce chapitre présente les fondements théoriques et les étapes clés de l'élaboration d'un PCA. Il est divisé en deux sections : la première section fournit une vue d'ensemble des PCA, la deuxième détaille les étapes précédant son élaboration.
2. Plan de Continuité d'activité dans les systèmes informatiques : Ce chapitre se concentre spécifiquement sur les défis et les particularités liés aux systèmes informatiques. Il comprend deux sections : la première aborde les généralités sur les systèmes informatiques, et la deuxième examine l'application concrète d'un PCA dans ce domaine.
3. Conception et réalisation : Au cours de ce chapitre, nous allons présenter l'organisme

d'accueil EPB, son historique et les nombreux départements qui font partie de son infrastructure. Nous identifions les risques en exposant la problématique de notre travail et quelques éventuelles solutions. Dans la deuxième section de ce chapitre, nous parlerons de la conception du réseau LAN, incluant la procédure de préparation, la nomination des équipements, la désignation des interfaces et les VLAN à travers le simulateur Packet Tracer. Puis, nous allons interconnecter ce modèle vers d'autres sites distants de secours.

Nous clôturons avec des tests de validation de la configuration globale utilisée, dans le souci de vérifier si les objectifs ont été atteints.

1

Concepts de base d'un plan de continuité d'activité

Introduction

Les entreprises sont constamment confrontées à des défis imprévus, l'importance de la résilience et de la préparation ne peut être surestimée. Le plan de continuité d'activité (PCA) est un élément crucial pour assurer la pérennité des opérations face à des perturbations de toutes sortes, qu'il s'agisse de catastrophes naturelles, de cyber attaques ou d'autres crises.

Ce chapitre vise à explorer les concepts fondamentaux d'un PCA, en fournissant une compréhension approfondie de ses composants essentiels et des étapes nécessaires pour sa mise en œuvre. Pour mieux comprendre nous allons aborder les deux sections suivantes :

- La première section : Généralité sur un plan de continuité.
- La deuxième section : Préparation à l'élaboration d'un plan de continuité d'activité.

Ces sections fournissent une feuille de route complète pour comprendre, préparer un plan de continuité d'activité robuste, indispensable pour la résilience organisationnelle.

1.1 Section 1 : Généralités sur un Plan de continuité d'activité (PCA)

Via cette section, nous posons les bases en définissant ce qu'est un PCA, ses mots clés, son importance pour les organisations et ses acteurs. Cette partie met en lumière les avantages d'un plan bien structuré et les risques encourus en son absence.

1.1.1 C'est quoi un PCA

Il s'agit d'un plan qui décrit comment une organisation continuera à fonctionner pendant ou après une sorte d'urgence, de catastrophe ou d'événement. Cela implique de planifier la manière dont les services peuvent garantir la poursuite et la reprise des activités. [W1]

Autrement dit un PCA est une suite de procédure,de consignes qui forment un plan à suivre par des responsables concernés permettant à une entreprise de maintenir ou de reprendre ses activités essentielles en cas de perturbations.

1.1.2 Les conséquences d'une interruption d'activité

Une interruption de l'activité peut entrainer des conséquences néfastes pour une entreprise :

- ➢ Un ralentissement de l'activité opérationnelle, ce qui fait un retard dans les opérations quotidiennes de l'entreprise.
- ➢ Une perte de données qui peut être dangereuse pour l'activité.
- ➢ Perte de clients de réputations permet aux concurrents de profiter de l'occasion et renforcer leurs présences dans le marché et gagner la confiance des clients.
- ➢ Perte financière.
- ➢ Risques juridiques due à l'interruption d'activités peut entrainer des litiges contractuels ou des poursuites juridiques pour le non-respect des engagements contractuels suite aux retards dans les fournitures de biens ou de services à des clients.

1.1.3 Les éléments clés d'un PCA

Un PCA est indispensable pour assurer la résilience organisationnelle. Voici les éléments clés à considérer lors de sa mise en place :

- ➢ **Identification des fonctions critiques :** il s'agit de déterminer les activités indispensables à la survie de l'entreprise ainsi que les ressources nécessaires à leur fonctionnement.

➢ **Analyses des risques :** lors de cette étape, il faut identifier les risques auxquels l'entreprise est exposée tels que les catastrophes naturelles, les pannes techniques, les cybers attaques ...Cependant elle vise à fournir une étude approfondie des menaces potentilles afin de développer des stratégies de gestion adaptées pour assurer la continuité d'activités d'un PCA.

➢ **Stratégies de continuité :** Développer des stratégies de continuité pour maintenir les opérations essentielles pendant et après un événement perturbateur. Cela peut inclure la mise en place de sites de secours, la virtualisation des infrastructures ou la décentralisation des opérations.

1.1.4 Types d'un PCA

La différence entre un PCA simplifiée et PCA complet :

Caractéristique	**PCA complet**	**PCA simplifié**
Entreprise concerné	Entreprises qui disposent d'une analyse préalable des risques et d'une stratégie de gestion des risques bien établie.	Entreprises qui ont besoin d'une approche plus ciblée
Objectif principal	Assurer la continuité totale ou partielle des activités essentielles et Planifier la reprise complète des opérations après une crise.	Maintenir les activités essentielles pendant une crise et préparer une réponse rapide à un scenario spécifique
Portée	Englobe toutes les mesures et processus pour anticiper les conséquences d'une crise sur les activités principales de l'entreprise.	Se concentre uniquement sur les actions majeures prioritaires nécessaires pour faire face à une crise spécifique
Analyse des risques	Analyse approfondie des risques et Evaluations de leurs impacts.	Analyses simplifiées des risques spécifiques à un scenario particulier
Adaptabilité	Plus flexible pour faire face à différents types de crises et de scenarios.	Simple et rapide à mettre en œuvre

Table 1.1 – Type de Plan de continuité d'activité [W2].

1.1.5 Rôle d'un PCA dans la gestion des crises

Le rôle d'un (PCA) dans la gestion des crises est de fournir une structure et des procédures pour assurer la continuité des opérations essentielles de l'entreprise pendant et après une crise. Il joue un rôle en aidant les entreprises à se préparer, à réagir et à se rétablir rapidement et efficacement face à des événements imprévus pouvant menacer leurs opérations.

- ➢ **Préparation :** Le PCA prépare l'entreprise à faire face à une variété de scénarios de crise en identifiant les risques potentiels, en évaluant leurs impacts sur les opérations et en élaborant des stratégies pour y faire face.
- ➢ **Réduction des perturbations :** En mettant en œuvre des mesures préventives et des plans de réponse, le PCA vise à réduire les perturbations et les dommages potentiels causés par une crise sur les opérations commerciales.
- ➢ **Rétablissement rapide :** Le PCA prévoit des procédures spécifiques pour rétablir rapidement les opérations critiques après une crise, en minimisant ainsi les temps d'arrêt et les pertes financières.
- ➢ **Coordination des efforts :** Pendant une crise, le PCA définit clairement les rôles et responsabilités de chaque membre de l'équipe de gestion de crise, ce qui facilite la coordination des efforts pour une réponse efficace.
- ➢ **Communication :** Le PCA comprend des protocoles de communication pour assurer une diffusion rapide et précise des informations aux parties prenantes internes et externes, y compris les employés, les clients, les fournisseurs et les autorités réglementaires.
- ➢ **Évaluation et amélioration continue :** Après la crise, le PCA permet d'évaluer les performances de l'entreprise dans sa gestion de la crise, en identifiant les points forts et les domaines à améliorer pour renforcer la préparation future.

1.1.6 Les acteurs d'un PCA

- ➢ **La direction générale :** La responsabilité première et ultime du management de la continuité d'activité devrait s'établir au niveau du comité de direction. Après tout, il s'agit de la survie de l'entreprise ! Le rôle de la direction générale est déterminant dans la mesure où elle doit impulser, promouvoir, rendre visible et contrôler le PCA.

  Au-delà, ils interviennent à trois moments cruciaux de la démarche.

  Les responsables de la Direction Générale sont essentiels à différentes étapes d'un projet de PCA :

  - Au début du projet, lors de la phase initiale de bilan d'impact sur l'activité (BIA), ils définissent les niveaux minimums acceptables.
  - Pendant la mise en œuvre du projet (phase de conduite du changement), ils participent à la sensibilisation, à la formation, et à la diffusion d'informations dans leurs domaines de compétence.

- Lorsque le PCA est opérationnel (en régime établi), ils contribuent aux exercices de tests, à la maintenance (notamment la mise à jour des informations les concernant), et se soumettent aux contrôles nécessaires. [1]

➢ **Le risk manager :** c'est la personne généralement liée directement à la direction générale est idéalement positionnée pour jouer un rôle clé dans la mise en œuvre d'un PCA, son rôle est la supervision globale des risques d'entreprise.

➢ **Les directions métier :** Les responsabilités des directions métier dans la mise en œuvre et le maintien en conditions opérationnelles d'un PCA sont vitales, la première étant l'esprit de collaboration, Au-delà, elles interviennent à trois moments cruciaux de la démarche et se soumettent aux contrôles nécessaires [1].

➢ Le responsable du PCA :

- Contrôler le plan de manière cohérente et persévérante, en appliquant les actions correctives nécessaires.
- Être prêt à déclencher le plan avec sang-froid et coordination en cas de besoin.
- Communiquer efficacement pour organiser les formations et les tests du plan. [1]

➢ **Le Responsable de la sécurité du système d'information (RSSI) :** Les responsabilités d'un RSSI sont la mise en place de procédures de sécurité, la communication, la gestion des incidents, et le suivi des risques. Il joue un rôle de conseil, d'assistance, d'information, de sensibilisation, d'alerte, et d'interface entre les différents acteurs de l'entreprise. Ses compétences de base, généralement techniques, lui donnent une posture avantageuse pour compléter un éventuel tandem de projet avec le risk manager qui lui a souvent plus une compétence de gestion. [W3]

1.2 Section 2 : Préparation d'un plan de continuité d'activité

Cette section se concentre sur les préparatifs nécessaires avant de concevoir un PCA. Elle détaille les évaluations des risques, les analyses d'impact (BIA) et l'identification des ressources critiques, fournissant un cadre méthodique pour une planification efficace

1.2.1 Formation et sensibilisation sur la continuité d'activités

Avant toute démarche de planification de la continuité d'activité (PCA), la formation et la sensibilisation des employés sont essentielles. Elles préparent le personnel à réagir en cas d'incident, garantissant ainsi une mise en œuvre efficace des plans de PCA et favorisant une culture de préparation au sein de l'entreprise.

1.2.1.1 Programme de sensibilisation

L'objectif de la sensibilisation est d'attirer l'attention et de faire évoluer les habitudes. Elle est destinée à toucher les comportements.

Les objectifs d'un programme de sensibilisation des parties prenantes :

- ➢ Prendre le temps de reconnaître et de comprendre le rôle à jouer en période de perturbation : Une façon de résoudre ce problème consiste à fournir des réponses aux questions suivantes : de quelles manières puis-je m'assurer d'être tenu au courant des derniers développements concernant la situation ? Quelle est la manière appropriée de soumettre un rapport à votre superviseur ? Faut-il simplement rentrer chez soi et attendre des conseils supplémentaires ? Ou bien faut-il se rendre à l'emplacement alternatif désigné pour que le personnel puisse poursuivre ses opérations ?
- ➢ Comprendre l'amélioration continue des systèmes de gestion, de la continuité des activités.
- ➢ Être conscient de tout non-respect des exigences du système de gestion de la continuité d'activités impliquées : par la sensibilisation des nouveaux collègues par des différents moyens tels que : faire des sessions de formations, des exercices pratiques, des réunions...etc.

1.2.1.2 Programme de formation

La finalité de la formation est d'acquérir des compétences c'est à dire la capacité de mettre en pratique des connaissances, des compétences et des savoir-être.

Il est essentiel de respecter les recommandations de la norme ISO 22301. Il est nécessaire :

- ➢ D'identifier les compétences indispensables à développer.
- ➢ Assurez que les individus sélectionnés possèdent des compétences basées sur une formation initiale ou professionnelle et une expérience adéquate.
- ➢ Prendre des mesures pour développer les compétences requises et évaluer l'efficacité de ces mesures.

1.2.2 Développement d'un bilan d'impacts d'activités (BIA)

Une étape essentielle de la démarche qui signifie l'évaluation des activités de l'entreprise et leurs impacts. Il vise à fournir une compréhension globale des conséquences positives et négatives de l'activité afin d'aider à prendre des décisions pour mettre en œuvre des mesures d'atténuation si nécessaire. L'exactitude des résultats du BIA est essentielle pour obtenir un PCA qui répond aux besoins de l'entreprise.

1.2.2.1 Les paramètres d'un BIA

Pour chaque activité, le BIA évalue trois paramètres :

- **DMIA (Temps d'interruption maximum autorisé)** en anglais le RTO ou Recovery Time Objective, Il s'agit de la durée maximale acceptable pendant laquelle une brique

IT (serveur, réseau, ordinateur, application) peut ne pas être fonctionnelle suite à une interruption majeure de service. Cette durée est définie à l'avance. le DMIA classe les activités par priorité de reprise après sinistre. [W4]

- **La PMDT (Perte de données maximale tolérable)** est un concept important dans le domaine de la gestion des données et de la continuité des activités. Elle représente la quantité maximale de données qu'une organisation peut se permettre de perdre sans compromettre son fonctionnement ou sa capacité à reprendre ses activités normales après un incident. Par exemple, aucune perte de données, perte de données sur 24 heures, etc.[W5]
- **L'OMCA (l'objectif minimum de continuité d'activité)** définit la capacité d'une entreprise à maintenir un niveau minimal d'activité malgré les dommages subis . Par exemple, à la fin du DMIA, l'activité peut travailler avec la moitié de l'effectif nominal, ce qui marque le début du retour à l'activité .

Pour déterminer l'éligibilité aux activités prioritaires, il faut justifier ces derniers en mesurant l'impact des pertes financières, les pertes d'images et les pertes de productivité liées à la désorganisation.

1.2.2.2 L'objectif du BIA

- ➢ Comprendre les produits et les services clés de l'entreprise et les activités qui les fournissent.
- ➢ Déterminer les priorités et les délais de reprise des activités.
- ➢ Déterminer les ressources/moyens et dépendances nécessaires à la continuité des activités.
- ➢ Déterminer les dépendances (internes et externes, y compris les fournisseurs) nécessaires à la continuité et à la reprise des activités.

1.2.2.3 Elaboration d'un BIA

L'élaboration d'un BIA se résume en 5 étapes :

Étape 1 : Évaluer les activités de la société. En règle générale, se base sur la cartographie des processus qui se divise en sous-processus et activités.

Les étapes indispensables à la prestation de produits et services et les procédures qui soutiennent leur domaine d'activité et constituent l'infrastructure de l'entreprise : les opérations d'achat, les recrutements, l'informatique, la comptabilité, etc. [W6]

Étape 2 : Élaborer une base de données pour qualifier les impacts.

Il est nécessaire d'identifier un référentiel unique pour comparer la gravité des impacts. Il nous donnera la possibilité de trier toutes les activités de l'entreprise en fonction de leur priorité. Il est nécessaire que la direction générale valide ce référentiel de qualification des impacts.

Une fois cette étape est terminée on reçoit le référentiel de qualification des impacts approuvés par la Direction générale. Il sera donc possible de comparer de manière équitable les

conséquences sur chaque activité. [W6]

Étape 3 : Évaluer les conséquences d'une pause dans les activités.

Après avoir développé le domaine d'application et le référentiel de qualification des niveaux d'impact, il sera possible d'évaluer chaque activité en leur attribuant des types et des niveaux d'impact.

Pour cette étape, détailler le quan, le qui et le comment.

- ➢ **Quand à l'évaluation des impacts, à quel moment ?**

  On évalue les conséquences en prenant en considération les éventuels problèmes de fonctionnement. Il est essentiel de se trouver à un moment crucial afin de maximiser l'effet.

- ➢ **Qui évalue les conséquences ?**

  La mesure des conséquences est réalisée en collaboration avec le responsable de l'activité et ses adjoints opérationnels.

- ➢ **Comment estiment-ils les conséquences ?**

  Il est possible de recueillir les informations en réalisant des entretiens, en envoyant un questionnaire ou en organisant un atelier impliquant plusieurs responsables d'activité. L'entretien est préparé en envoyant un ordre du jour. Il est nécessaire que les personnes interrogées valident le compte rendu de la réunion.

De toute manière, il est également nécessaire de faire valider par le directeur de l'activité les résultats fournis par les participants et donner une perspective plus exhaustive sur le fonctionnement de l'activité. À la fin de cette étape, on obtient pour chaque activité analysée, les DMIA, PMDT et OMCA, les ressources/moyens requis, ainsi que les parties intéressées.

Étape 4 : Évaluation des ressources/moyens requis pour les activités et leurs interactions.

Après avoir identifié les activités prioritaires, il est maintenant nécessaire de demander les ressources nécessaires (postes de travail, applications informatiques, moyens matériels, fournisseurs ou partenaires externes, etc.) pour un mode de fonctionnement considéré comme acceptable.

Étape 5 : Obtention de l'approbation de la Direction générale sur les résultats.

Les résultats du bilan d'impact sur l'activité de chaque activité devront ensuite être présentés à la Direction générale afin d'être validés. [W6]

1.2.3 Identification des risques

Cette étape nécessite une étude minutieuse des risques potentiels susceptibles de perturber les opérations de l'entreprise. Ces dangers peuvent provenir de sources internes telles que des difficultés opérationnelles ou technologiques, ou de sources externes telles que des catastrophes naturelles ou des modifications réglementaires. Les risques sont identifiés afin de déterminer les secteurs où l'entreprise est la plus exposée et requièrent une attention particulière dans le cadre de la continuité. [W7]

1.2.3.1 Les étapes d'identification des risques

La procédure d'identification des risques qui menacent une entreprise se résume en quatre étapes :

- ➢ **Déterminer les risques :** consiste à identifier les risques auxquels une entreprise pourrait être confortée. Ces risques peuvent varier, allant d'une catastrophe naturelle qui pourrait endommager et saboter ses systèmes appelant des risques majeurs ou d'autres types de ressources exposées à risques (ex bâtiment et infrastructure, informatique, outils et flux de production eau, électricité).le propriétaire d'entreprise doit être constamment conscient de ces derniers. Ce processus doit être continu et les responsables doivent prendre en compte toutes les évolutions potentielles chaque année.
- ➢ **Évaluation des risques :** cette étape a pour but de déterminer le niveau de criticité des risques . il s'agit à impliquer et à quantifier la probabilité que ces risques se produisent et d'analyser l'impact potentiel qu'ils pourraient avoir sur l'entreprise .Cette évaluation permet de les classer par priorité à la reprise immédiate.
- ➢ **Traitement des risques :** pour atténuer les risques, il est nécessaire de développer un plan d'action qui contient diverses mesures telles que des précautions préventives, des procédures d'urgences ou encore des politiques internes qui visent à minimiser le résultat négatif.
- ➢ **Le monitoring et reporting des risques :** Dans cette étape, l'entreprise surveille activement les risques identifiés pour détecter tout changement ou évolution, analyse les données collectées pour évaluer leur impact, et communique régulièrement ces informations à la direction et aux parties prenantes pour prendre des décisions éclairées et mettre en place des mesures correctives si nécessaire. [W8]

1.2.4 L'elaboration d'une stratégie

la stratégie d'un PCA est la dérnière étape de sa préparation.elle consiste à séléctionner des solutions pour chaque risque qui menace une activité précise. Elle devrait également la faire valider par la direction générale qui décidera en fonction de certains points ; en particulier : [W6]

- ➢ **L'appétence au risque :** chercher à réduire les risques ou accepter de vivre avec.
- ➢ **Le choix des priorités :** que décider pour les activités prioritaires (issues du BIA) ? Valider les délais maximaux d'interruption admissibles demandés par les responsables (les DMIA) ? Quel niveau de reprise paraît acceptable ?
- ➢ **Le choix de solutions :** Avec quels moyens (site de repli des positions de travail critiques, site de secours informatique, constitution de stocks de secours, etc.), quels effectifs et quelle montée en charge de positions de travail est préférable de mettre en place ?
- ➢ **Le choix de partenaires :** faire appel à des prestataires de solution de repli des positions de travail, de solution de secours informatique.
- ➢ **Le choix financier :** Quel budget consacrer à cela ? Quel planning ? Quelles priorités ?

Il y a diverses sortes de solutions pour assurer la continuité d'activité. Afin de développer la stratégie, il faudra sélectionner un ensemble cohérent de ces solutions :

- ➢ **Les solutions de prévention :** Avant que l'événement perturbateur ne survienne, des mesures de prévention sont prises. Elles visent à diminuer sa probabilité de se produire. Elles opèrent de façon proactive et nécessitent une amélioration constante.
- ➢ **Les solutions de détection de l'événement perturbateur :** Les dispositifs de détection sont mis en place avant que l'événement perturbateur ne se produise. Elles ont la capacité de diminuer l'impact en le repérant rapidement, ce qui permet de lancer rapidement une alerte.

➢ **Les solutions de protection, maintien et/ou reprise des activités prioritaires :** Les mesures de sécurité sont préparées et instaurées avant que l'événement perturbateur ne se produise. Afin d'être efficaces, ces mesures nécessitent une validation régulière. En se basant sur deux principes : les solutions de secours informatique qui correspondent globalement à trois concepts de base : les secours à froid, actif-passif ou actif-actif et les sites de repli des positions de travail.

1.2.4.1 Les études de la stratégie de la continuité d'activité

Après avoir connu les différents types de solutions maintenant la réalisation de la stratégie de continuité d'activité consiste à faire :

➢ **Une étude technique :** l'ensemble des solutions doit faire l'objet d'une étude de faisabilité technique au regard des délais exprimés dans le BIA.

➢ **Une étude financière :** l'ensemble des solutions internes et externes doit faire l'objet d'une évaluation chiffrée.

➢ **Une étude des avantages et des inconvénients :** Facilité et délai de mise en œuvre, capacité à évoluer, facilité de maintien en condition opérationnelle, facilité à être testée/validée. [W6]

Conclusion

Ce chapitre a fourni une vision complète et structurée de la mise en place et de la gestion d'un PCA, élément important pour la résilience des entreprises face aux crises. Il a mis en lumière l'importance d'un PCA bien conçu pour assurer la continuité des opérations et la résilience organisationnelle. En comprenant et en appliquant ces concepts de base, les entreprises peuvent se préparer à surmonter les crises avec succès et minimiser les impacts négatifs sur leurs activités.

2

Un plan de continuité d'activité dans les systèmes informatiques

Introduction

Actuellement, les systèmes informatiques sont importants dans toutes les infrastructures de l'entreprise. La perte de connectivité réseau peut entraîner des conséquences graves, allant des temps d'arrêt coûteux à la perte de données critiques. Pour éviter ces problèmes, les entreprises investissent dans des architectures réseau de secours.

Ce chapitre est divisé en deux sections principales :

- La première décrit des généralités sur les systèmes informatiques.
- La deuxième section décrit l'application d'un Plan de continuité d'activité sur ces systèmes.

Ce chapitre vise à fournir une compréhension globale des systèmes informatiques et des méthodes pour garantir leurs continuités.

2.1 Section1 : généralités sur les systèmes informatiques SI

Cette section explore en profondeur les divers aspects des systèmes informatiques et les défis de la sécurité informatique, en examinant les menaces potentielles et les meilleures pratiques pour faire face. Par la suite, nous nous focalisons plus sur la résilience des systèmes informatiques car c'est le point le plus important dans notre thème.

2.1.1 Qu'est-ce qu'un SI

Un système informatique est un ensemble interconnecté de composants matériels, logiciels et humains qui travaillent ensemble pour traiter, stocker et transmettre des données selon des règles bien définies.

Un système informatique peut être aussi simple qu'un ordinateur personnel utilisé pour des tâches courantes telles que la navigation sur le Web et le traitement de texte, ou aussi complexe qu'un réseau mondial de serveurs interconnectés soutenant des milliards d'utilisateurs et de services en ligne. La conception, la mise en œuvre et la maintenance des systèmes informatiques nécessitent une compréhension approfondie de leurs composants et de leur fonctionnement interne.

2.1.2 Les composantes d'un SI

Chaque système informatique est constitué de trois composantes, à savoir le matériel, les logiciels et l'humain.

- **Matériel :** Il s'agit de l'ensemble de l'environnement lié aux éléments matériels qui participent au système (ordinateur, écran, clavier, modem, clés USB, etc.).
- **Logiciel :** Il englobe chacun des éléments qui peuvent être classés dans les environnements liés aux programmes informatiques et applications. C'est la partie "software" du système qui fait référence aux informations et systèmes virtuels programmés, numériques et intangibles.
- **Humain :** La composante humaine (ressources humaines) est essentielle à tout système informatique. Elle regroupe tous les utilisateurs qui interviennent dans un réseau informatique, utilisent un ordinateur ou le programment[W9] .

2.1.3 Les réseaux informatiques

Un réseau informatique est un ensemble de dispositifs électroniques interconnectés, tels que des ordinateurs, des serveurs, des routeurs, des commutateurs, etc., qui communiquent entre eux pour partager des ressources, des données et des services. Ces dispositifs sont reliés par des liaisons physiques ou sans fil, permettant ainsi le transfert d'informations et la collaboration entre les utilisateurs et les systèmes au sein du réseau.

Figure 2.1 – Les composants d'un réseau informatique [2].

2.1.3.1 Classification des réseaux

Les réseaux informatiques se classifient en trois catégories distinctes :

- ➢ Selon la taille.
- ➢ Selon la topologie.
- ➢ Selon le mode de communication.

Figure 2.2 – Classification d'un réseau informatique [2].

2.1.3.1.1 Classification selon la taille

Généralement, ils sont présentés par quatre classes selon la taille géographique :

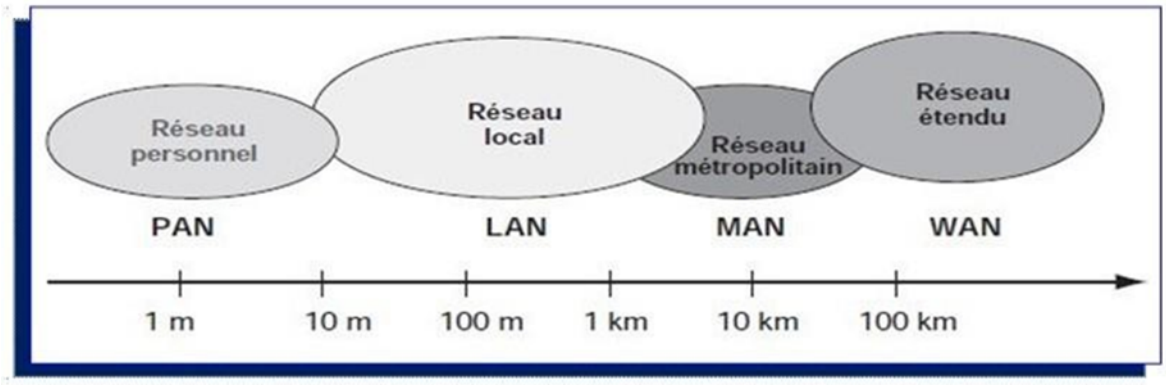

Figure 2.3 – La taille des différentes catégories de réseaux informatiques [2].

➢ **Réseau personnel (PAN, Personal Area Network) :**

Un réseau PAN aussi appelé réseau domestique ou réseau individuel regroupe des équipements dans un rayon de 10 mètres. Ces équipements appartiennent généralement à un même utilisateur comme : Un téléphone portable avec ses accessoires, un ordinateur avec ses périphériques et Bluetooth.

➢ **Réseau local (LAN, Local Area Network) :**

Un réseau local est un réseau informatique qui relie des ordinateurs et des périphériques dans une zone géographique limitée, comme un bureau, une maison ou un campus.

➢ **Réseau métropolitain (MAN, Metropolitan Area Network) :**

C'est un ensemble de réseaux de connexion à haut débit qui interconnectent plusieurs réseaux locaux en un seul réseau de grande taille avec un pont commun. Ce pont est appelé "backbonelines" qui est généralement établi par fibre optique pour augmenter la vitesse de transfert des données.

➢ **Réseau étendu (WAN, Wide Area Network) :**

C'est un réseau étendu qui s'étend sur de vastes zones géographiques et relie plusieurs réseaux plus petits comme LAN et MAN.

2.1.3.1.2 Classification selon la topologie

La topologie physique est la représentation géométrique de tous les liens et dispositifs entre eux. Elle est aussi appelée le schéma de base, l'architecture ou le plan. Les topologies peuvent être classées en deux types de la manière la plus fondamentale :

➢ **Topologie physique :**

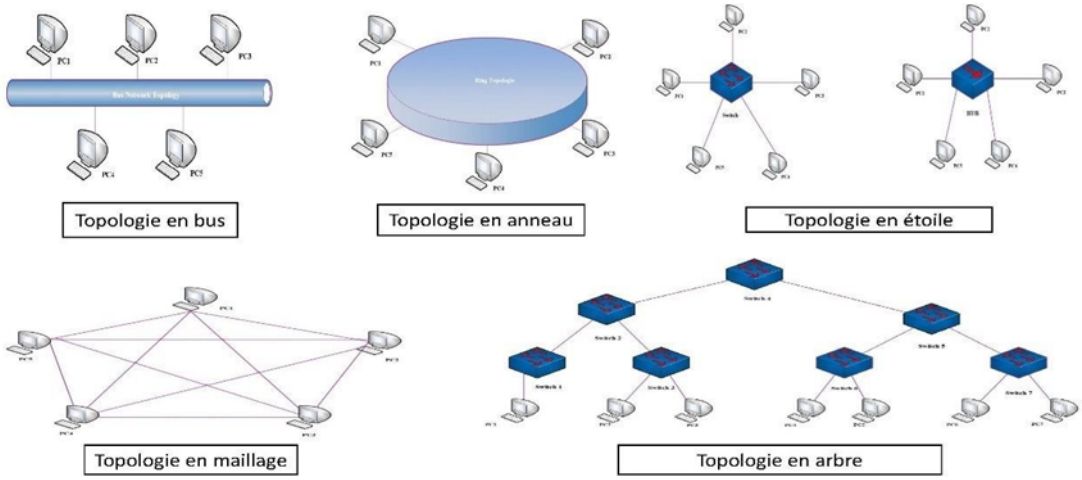

FIGURE 2.4 – Les topologies physiques [2].

➢ **Topologie logique :**

Par opposition à la topologie physique, elle représente la façon selon laquelle les données transitent sur les lignes de communication. Les topologies logiques les plus courantes sont : Ethernet, Token Ring et FDDI (pour Fibre Distributed data interface) [2].

2.1.3.1.3 Classification selon le mode de communication

On distingue généralement deux types de réseaux très différents en fonction de la nature des relations entre les sites, mais ils partagent des similitudes. Ils sont :

➢ **Réseau Client/serveur :**

Dans cette architecture, les ressources et les services sont fournis par un ou plusieurs serveurs à des clients. Les clients demandent des services au serveur, qui les fournit en retour. Cette architecture est souvent utilisée dans les entreprises pour gérer les données et les applications.

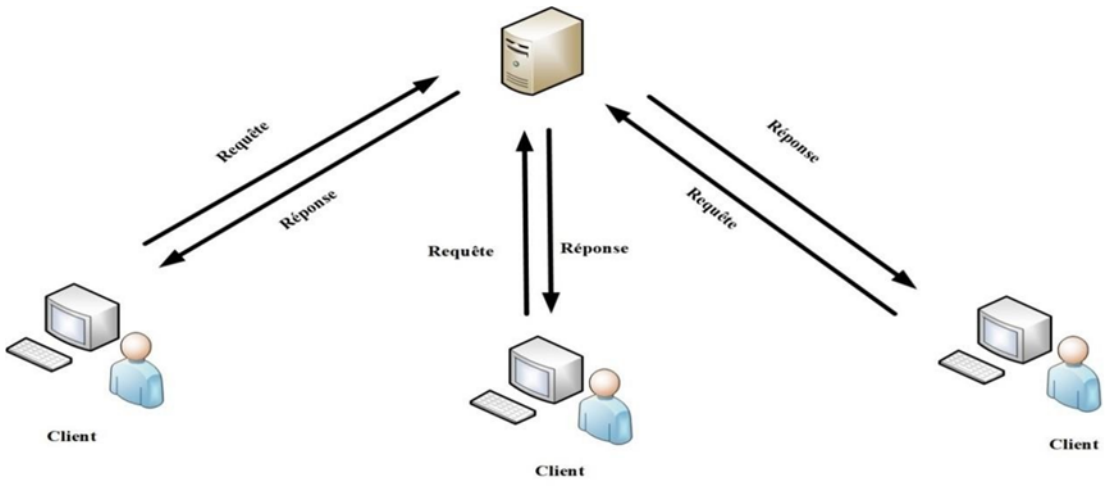

FIGURE 2.5 – Fonctionnement d'un client/serveur [2].

➢ **Réseau poste à poste :**

Dans cette architecture, chaque ordinateur est à la fois client et serveur, et peut échanger des données avec d'autres ordinateurs du réseau. Cette architecture est souvent utilisée pour le partage de fichiers et la collaboration.

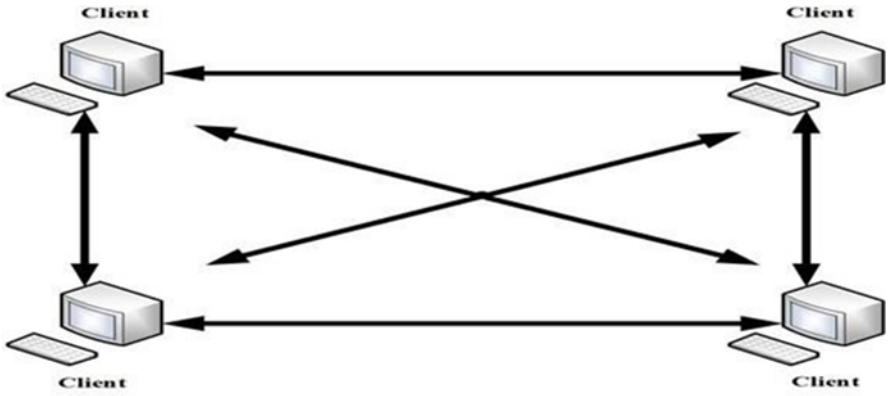

Figure 2.6 – Réseau poste à poste [2].

2.1.3.2 Modèle hiérarchique

Le modèle hiérarchique des réseaux est une approche de conception de réseaux informatiques qui organise l'infrastructure en plusieurs niveaux distincts, ou couches, chacun exerçant des responsabilités et des fonctions spécifiques, ce qui permet une conception modulaire du réseau. Cette approche facilite la gestion, la maintenance et l'expansion du réseau, tout en offrant des performances optimales et une sécurité renforcée. Le modèle hiérarchique des réseaux est largement utilisé dans les environnements d'entreprise pour créer des infrastructures réseau robustes et évolutives.

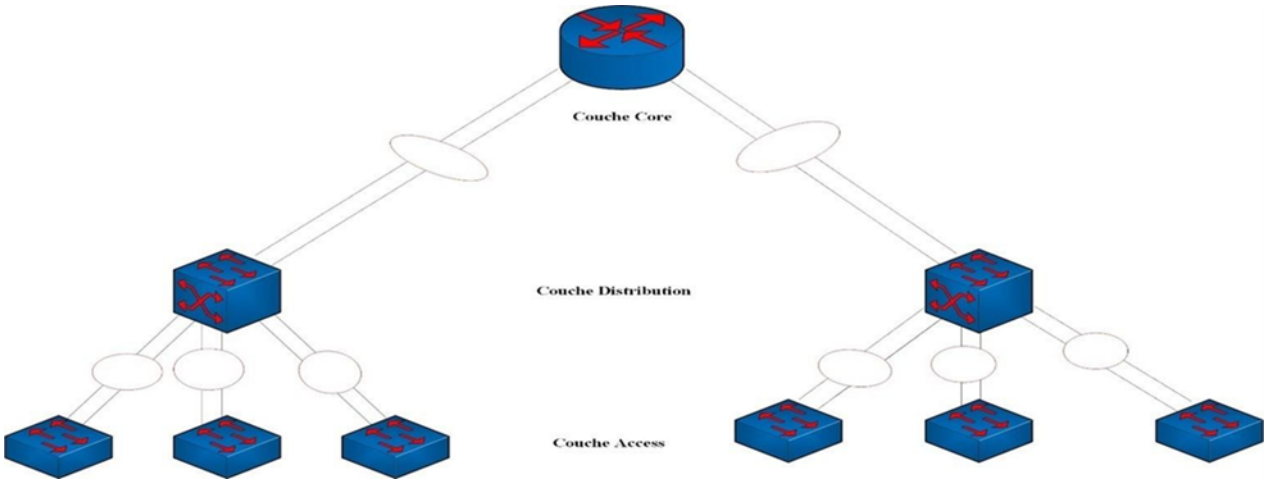

Figure 2.7 – Modèle de conception hiérarchique à trois couches.

➢ **La couche cœur (Core Layer) :**

C'est le niveau le plus élevé dans la hiérarchie, Il est responsable du transport de gros volumes de données entre les différents réseaux de distribution. Les dispositifs typiques de ce niveau sont les routeurs principaux ou les commutateurs centraux à haut débit. Son rôle principal est de fournir une connectivité rapide et fiable entre les différents segments du réseau.

➢ **La couche distribution (Distribution Layer) :**

Situé entre le niveau d'accès et le niveau central. Il agrège les connexions provenant de différents niveaux d'accès et les redistribue vers le niveau central ou d'autres niveaux d'accès. Il est souvent composé de commutateurs de distribution et de routeurs. Ses principales fonctions incluent la segmentation du trafic, le filtrage et la mise en couche pour optimiser les performances du réseau.

➢ **La couche d'accès (Access Layer) :**

C'est le niveau le plus bas de la hiérarchie. Il est directement en contact avec les utilisateurs finaux et leurs appareils, tels que les ordinateurs, les téléphones et les imprimantes. Les dispositifs typiques de ce niveau sont les commutateurs d'accès Ethernet et les points d'accès sans fil (Wi-Fi).

Son rôle principal est de fournir une connectivité réseau aux appareils finaux et de gérer les communications locales à faible latence.

2.1.4 La sécurité de l'information

La protection de l'information est l'ensemble des processus, des contrôles et des solutions qui protègent les affaires de votre entreprise avec un niveau de protection adapté par rapport à tous les niveaux (organisationnel, technique...) [3]

Sécuriser une information, c'est travailler et raisonner sur quatre variables :

- ❖ L'intégrité : l'information est précise et exhaustive.
- ❖ La disponibilité : l'information est disponible quand on en a besoin.
- ❖ La confidentialité : l'information est disponible uniquement aux personnes et aux ressources autorisées.
- ❖ La traçabilité : l'information est suivie dans son évolution, son parcours.

La protection d'une information ou sécurité informatique est donc le produit de ces quatre composantes. Mais on peut ajouter d'autres clés de contrôle comme la non-répudiation et la gestion des épreuves...etc. [3]

2.1.4.1 Les enjeux de la sécurité informatique

Les enjeux de la sécurité informatique font référence aux défis et aux risques auxquels sont confrontés les systèmes informatiques des données et de l'effet des enjeux de sécurité informatique qui peuvent être important, car une faille de sécurité peut entraîner des conséquences graves telles que le vol de données, la perte de confiance des utilisateurs et des dommages financiers importants pour les entreprises. Il est donc essentiel de les comprendre et de les gérer efficacement pour garantir la sécurité et la pérennité des systèmes informatiques.

Les principaux enjeux :

- La protection contre les cyber attaques.
- Enjeux environnementaux.
- La préservation de la confidentialité des informations .
- La garantie de l'intégrité des systèmes.
- La disponibilité continue des services informatiques.

2.1.5 La résilience des SI

2.1.5.1 Définition

La résilience des systèmes informatique est un concept majeur dans le domaine de la technologie et de l'information. C'est la capacité d'un système informatique à continuer à fonctionner en cas de panne, d'incident, de piratage ou d'augmentation des opérations commerciales. Pour y parvenir, il est essentiel de mettre en œuvre des protocoles et des systèmes de sécurité pour atténuer les pertes de données en cas d'incident majeur [W10].

2.1.5.2 L'importance de la résilience pour assurer la continuité des activités

Le point le plus important à retenir, est que la résilience des systèmes informatiques vise principalement à garantir la continuité des activités, notamment à travers la mise en place d'un Plan de Continuité d'Activité (PCA).

➢ Réduction des temps d'arrêt : l'interruption ne durera pas longtemps.

➢ Protection de la réputation.

➢ Réduction des pertes financières.

2.1.5.3 Mesures de résilience

Pour renforcer la résilience des systèmes informatiques, il est essentiel de mettre en place de mesures telles que la sauvegarde des données, des techniques de détection de menaces pour la surveillance à jour des systèmes, l'organisation efficace pour résoudre les problèmes et d'autres. Ainsi que des techniques de réplication (redondance) ou élaboration des plans de reprise d'activités.

2.1.5.3.1 Un plan de reprise d'activité

2.1.5.3.1.1 Vue d'ensemble sur le plan de reprise

Un Plan de Reprise d'Activité (PRA) représente un ensemble organisé de mesures documentées visant à soutenir une entreprise lors de situations de crise, permettant ainsi une reprise rapide de ses opérations commerciales.

Un PRA est centré sur la récupération des données informatiques et la restauration des systèmes, le PRA s'est étendu pour englober une gamme variée d'incidents, tels que les pannes informatiques, les désastres naturels et les erreurs humaines.

En tant qu'élément complémentaire du Plan de Continuité d'Activité (PCA), le PRA assure la résilience de l'entreprise en garantissant la continuité des opérations lors de perturbations majeures. Outre la restauration des données et des systèmes informatiques, il peut également inclure des stratégies pour maintenir les processus métier critiques, protéger les ressources humaines et matérielles, ainsi que communiquer efficacement avec toutes les parties prenantes.

2.1.5.3.1.2 Procédure de sauvegarde et de récupération de donnés

La restauration et la sauvegarde des données sont indispensables pour la sécurité de chaque entreprise. Elles désignent un processus global permettant la récupération des données d'une entreprise après incident.

2.1.5.3.1.3 Définitions

➢ La récupération des données consiste à restaurer les données perdues, altérées ou supprimées sur un serveur, un ordinateur ...

➢ La sauvegarde des données (ou préservation des données) c'est faire une copie et un archivage des informations informatiques afin de les rendre accessibles en cas de corruption ou de perte. c'est l'objectif le plus important d'un PCA dans les entreprises.

Il existe différents supports et systèmes de sauvegarde utilisés par chaque entreprise, qu'il s'agisse d'une clé USB, d'un disque dur, d'un serveur externe ou d'une sauvegarde en ligne dans le Cloud.

2.1.5.3.1.4 Solutions

Pour sauvegarder et restaurer les données d'une entreprise et assurer leur disponibilité continue, l'utilisation des solutions dédiées à la sauvegarde, la restauration et la récupération de donnés est essentielle. Parmi ces solutions on peut citer celle-ci :

- Logiciels de sauvegarde et de récupération des données : les logiciels de récupération sont la solution la plus courante. Cependant, cette solution informatique n'est pas professionnelle pour plusieurs raisons (fiabilité limitée, complexité, cout élevé ...)
- Stockage Cloud : sauvegarder les données critiques hors site et offrir une protection supplémentaire à distance.

- Sauvegardes automatisées et planifiées : la régularité des sauvegardes par automatisation est considérée aussi comme solution fiable pour réduire les risques de pertes

2.1.5.3.2 La réplication

C'est une technique qui permet la fiabilité et la disponibilité continue des données d'un système. Elle consiste à créer des copies d'une donnée et de les stocker dans des endroits différents, elle permet de ne plus dépendre d'un site central unique [4].

2.2 SECTION 2 : Application d'un Plan de continuité d'activité (PCA) dans un système informatique (SI)

Les systèmes informatiques jouent un rôle essentiel dans les entreprises, les protéger avec des solutions techniques ne suffit pas toujours pour faire face à un sinistre. Cependant, ils sont exposés à des risques, ces interruptions peuvent causer des pertes de données, ainsi que des dommages à la réputation. Pour s'en prémunir, les entreprises doivent élaborer des plans de continuité d'activité solides pour ces systèmes. Cela inclut des sauvegardes régulières, une sécurité renforcée et des procédures de gestion de crise claires. De plus, avoir des sites de secours et des systèmes redondants est essentiel pour assurer une disponibilité continue des services, même en cas de défaillance majeure. Ces mesures aident les entreprises à minimiser les interruptions et à rester opérationnelles face aux défis numériques actuels.

2.2.1 Evaluation des risques qui menacent les SI

Les risques d'un système informatique ou réseau sont nombreux, on peut les classer selon leurs origines comme suit :

➢ **Origines physiques :** par exemple :

- Désastre naturel (inondation, séisme, incendie).
- Environnement (intempéries, taux d'humidité de l'air, température).
- Panne matérielle.
- Panne du réseau.
- Coupure électrique. [5]

➢ **Origines humaines :** par exemple :

- Erreur de conception (bogue logiciel, mauvais dimensionnement du réseau).
- Porte dérobée.
- Piratage. [5]

➢ **Origines opérationnelles :** Elles sont liées à un état du système à un moment donné :

- Bogue logiciel.
- Dysfonctionnement logiciel. [5]

2.2.2 Techniques d'application d'un PCA sur les systèmes informatiques

Pour assurer la continuité d'activité et le bon fonctionnement d'un système informatique, on fait appel aux techniques de secours et de redondances.

2.2.2.1 Un plan de secours informatique (PSI)

Le PSI vise la reprise d'activité de l'entreprise après un sinistre important ayant atteint le système d'information. Il traite principalement la restauration de l'infrastructure informatique et des données. Les moyens de secours sont parfois très importants lorsque l'entreprise ne peut se permettre une interruption de service. Certaines organisations doublent l'intégralité de leur infrastructure afin de pouvoir transférer leurs utilisateurs dans un autre site identique et reprendre très vite leur activité, ce type de plan est une composante essentielle du Plan de Continuité d'Activité (PCA) global d'une entreprise. [W11]

2.2.2.1.1 Elaboration d'un PSI

Avant tout, il convient de désigner une personne responsable de l'élaboration et de la mise en œuvre du plan de secours. Cette fonction est très souvent assurée par le responsable informatique lui-même, ou le responsable qualité. Cette personne doit réunir plusieurs compétences :

- ➢ Une bonne connaissance dans le domaine de la sécurité, sans pour autant connaître en détail le fonctionnement des technologies. Il y a donc un minimum de connaissances à acquérir et à maintenir pour être crédible vis-à-vis des techniciens en sécurité informatique, mais aussi pour savoir apprécier les risques liés à l'utilisation du système d'information.
- ➢ Une vision transversale de l'activité de l'entreprise.
- ➢ Une aptitude à communiquer pour mener des missions de sensibilisation du personnel.
- ➢ Des capacités en matière d'organisation, car il sera le chef d'orchestre de la gestion du sinistre.

La réalisation d'un plan de secours informatique implique plusieurs étapes clés pour s'assurer que l'organisation est prête à faire face à toute perturbation majeure de ses opérations informatiques. Voici les étapes typiques pour élaborer un plan de secours informatique : [W11]

2.2.2.1.1.1 Analyse de risque et d'impact

Il s'agit de déterminer les menaces qui pèsent sur l'informatique de l'entreprise, elles peuvent être d'origine humaine (maladresse, attaque, malveillance) ou technique (panne), et être interne ou externe à l'entreprise. Il convient d'estimer la probabilité que chaque menace se concrétise.

L'analyse d'impact consiste à mesurer les conséquences d'un risque qui se matérialise. Cette évaluation essentiellement financière peut être segmentée en paliers pour lesquels les coûts s'aggravent. Exemple : à H (heure du sinistre).

+2h : . . .H+10h : . . .H+1 jour : . . .[W11]

2.2.2.1.1.2 Mise en place du plan de secours

Il s'agit de mettre en place des mesures préventives et curatives. Certaines de ces mesures reposent sur des outils, tandis que d'autres sont davantage liées au comportement des utilisateurs. Mais avant de mettre en place ces mesures, l'entreprise doit d'abord statuer sur deux questions :

- ➢ Quelle est la quantité maximale d'informations que je peux perdre et mettre en péril mon activité ?
- ➢ Quel est le délai maximum de reprise d'activité normal au-delà duquel le suivi de la société est compromis ?

La réponse à ces questions va déterminer le niveau de sécurité à mettre en place. Autrement dit, quelles informations faut-il protéger et rétablir en priorité en cas de sinistre.

- ➢ **Les mesures préventives :**

  Elles permettent d'éviter une discontinuité de l'activité. Voici les principaux points de vigilance.

  - Le plan de sauvegarde : il s'agit de déterminer la fréquence et le type de sauvegarde (complète, différentielle, incrémentale) pour chaque catégorie d'information (basique, sensible, stratégique) il est Important de ne pas stocker les supports de sauvegarde à côté du serveur ou de la machine qui contient les données.
  - La sécurité logique : il convient de mettre en place des outils de protection de base (anti-virus, pare-feu, anti-spam) et de les maintenir à jour. A cela peuvent s'ajouter des contrôles d'accès aux données par mot de passe ou certificat électronique.
  - La sécurité physique : il s'agit de la sécurité des locaux. Une attention particulière doit être portée à la sécurité du serveur de l'entreprise.
  - Le facteur humain : la sécurité des systèmes d'information n'est pas qu'une affaire d'outils. C'est aussi - voire surtout - une information régulière diffusée auprès des collaborateurs. Une charte informatique permet de responsabiliser et sensibiliser les salariés à la sécurité informatique.

- ➢ **Les mesures curatives :**

  Ces mesures sont nécessaires car aucune mesure préventive n'est efficace à 100%. Elles interviennent lorsqu'un sinistre survient.

  - Restauration des dernières sauvegardes.
  - Redémarrage des machines (serveurs, imprimantes / copieurs, boitiers, etc.).
  - Redémarrage des applications (bureautiques, métiers, etc.). Le temps de remise en route du système va dépendre de l'endommagement occasionné par le sinistre. Un renouvellement de matériel peut parfois être nécessaire[W11].

2.2.2.1.1.3 Maintenance du plan de secours

Il est important de vérifier que le plan est réalisable en termes de procédures, de budget et de temps nécessaires au redémarrage. Par ailleurs, le plan de secours doit être actualisé pour être en phase avec le développement de l'entreprise : création d'une nouvelle activité, mise en œuvre d'une nouvelle infrastructure, croissance externe, recrutement, etc. [W11]

2.2.2.2 La Redondance et les protocoles utilisés

La redondance des réseaux informatiques est une technique qui consiste à ajouter des chemins de communication supplémentaires pour garantir une disponibilité continue des réseaux, en minimisant les temps d'arrêt. Elle permet d'assurer la continuité de service en cas de défaillance d'un composant du réseau, tel qu'un routeur, un commutateur ou un câble. Elle permet également d'améliorer la performance et la capacité des réseaux, en tolérant la répartition de la charge de travail entre plusieurs chemins de communication. [W12]

La redondance des réseaux informatiques peut être mise en place de différentes manières, en fonction des besoins et des contraintes du réseau. Parmi les techniques courantes, on peut citer : [5]

- **Au niveau des connexions réseau :**

  En utilisant plusieurs connexions physiques pour assurer une redondance, comme l'agrégation de liens ou la redondance de liens. Si une connexion tombe en panne, le trafic est automatiquement redirigé vers les autres connexions.

- **Au niveau des commutateurs :**

  En utilisant des commutateurs redondants pour permettre un basculement automatique en cas de panne d'un commutateur.

- **Au niveau des routeurs :**

  En utilisant des protocoles de redondance tels que HSRP et VRRP pour assurer un basculement transparent, en cas de défaillance d'un routeur (actif) un autre en veille prendra le relai.

- **Au niveau des serveurs :**

  En configurant des serveurs en cluster pour permettre à un serveur de prendre le relais en cas de défaillance d'un autre serveur.

2.2.2.2.1 Les protocoles de redondance

Les protocoles réseau sont comme des guides qui aident les applications à envoyer des données à travers le réseau d'une entreprise. La disponibilité d'un réseau peut être assurée par plusieurs méthodes, parmi ces dernières, nous citons les protocoles suivants :

2.2.2.2.1.1 Protocol HSRP (Hot Standby Routing Protocol)

❖ Définition :

Le protocole HSRP (Hot Standby Routing Protocol) est un protocole de niveau 3 propriétaire de “continuité de service” implémenté dans les routeurs Cisco pour la gestion des “liens de secours”. Il sert à augmenter la tolérance de panne sur le réseau en créant un routeur virtuel à partir de 2 routeurs physiques : un “actif” et l’autre “en attente” (ou ”standby”) en fonction des priorités accordées à chacun de ces routeurs [6].

❖ Principe de fonctionnement :

Le protocole HSRP permettra aux routeurs situés dans un même groupe de former un routeur virtuel qui sera l’unique passerelle des hôtes du réseau local, Un routeur dans ce groupe est donc désigné comme actif et ce sera lui qui fera passer les requêtes d’un réseau à un autre.

Pendant que le routeur actif travaille, il envoie également des messages aux autres routeurs indiquant qu’il est toujours vivant et opérationnel. Si le routeur principal (élu actif) vient de tomber en panne, il sera automatiquement remplacé par un routeur qui était jusque-là passif et lui aussi membre du groupe HSRP. Cette réélection et ce changement de passerelle seront totalement invisibles, car ils auront toujours pour unique passerelle. Le routeur virtuel aura donc toujours la même adresse IP et adresse MAC des hôtes du réseau même si en réalité il y a un changement du chemin par lequel transitent les paquets [5].

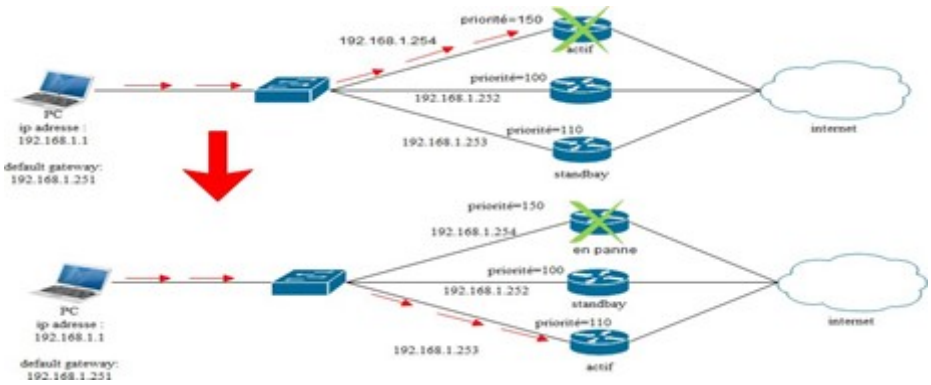

Figure 2.8 – Schéma montrant le principe de fonctionnement de protocole HSRP [7]

2.2.2.2.1.2 Protocol VRRP (Virtual Router Redundancy Protocol)

❖ Définition :

C’est un protocole de routage standard similaire à HSRP, il fonctionne sur d’autres routeurs que Cisco, il permet de partager une adresse IP virtuelle pour assurer la redondance de la passerelle par défaut d’un réseau local. Le groupe de routeurs partageant la même adresse IP virtuelle est appelé groupe VRRP. Le routeur ayant la priorité la plus élevée sera élu comme routeur actif appelé Master, les autres routeurs ayant la priorité inférieure au routeur Master sont des routeurs en attente appelés Backup [8].

❖ **Principe de fonctionnement :**

Tous les routeurs de groupe VRRP doivent être configurés avec la même adresse IP virtuelle, un même identifiant de groupe (ID) et une priorité.

Le routeur ayant la meilleure priorité est désigné comme routeur Master, il se charge de répondre aux requêtes, les autres routeurs ayant la priorité inférieure sont des routeurs Backup, tous les routeurs de groupe VRRP envoient périodiquement des messages VRRP pour signaler leurs présences. Les routeurs Backup surveillent le routeur Master, si un message VRRP de ce dernier n'est pas reçu par les routeurs Backup, la Master sera remplacée par un Backup ayant la priorité la plus élevée [7].

2.2.2.2.1.3 Le protocole STP (Spanning-Tree Protocol)

❖ **Définition :**

Le protocole Spanning-tree (STP) est un protocole de niveau 2 conçu pour les commutateurs. Il permet de créer un chemin sans boucle dans un environnement commuté et physiquement redondant. STP détecte et désactive ces boucles et fournit un mécanisme de liens de sauvegarde.

Toutefois, si les commutateurs acheminent le trafic de diffusion et multicast par tous les ports sauf celui d'origine et si les trames Ethernet ne disposent pas de durée de vie (TTL), divers problèmes peuvent alors apparaître [9].

❖ **Fonctionnement du protocole STP :**

Le fonctionnement du protocole STP se déroule en 4 étapes [5] :

- ➢ **Élection du Bridge Root :** tous les commutateurs du réseau envoient des messages BPDU (Bridge Protocol Data Unit) pour élire un commutateur qui servira de racine de l'arbre de couverture. Le commutateur ayant l'ID de pont le plus bas sera choisi comme racine.
- ➢ **Établissement de chemins de redondance :** le protocole STP sélectionne un chemin de transmission vers la racine de l'arbre pour chaque commutateur du réseau. Les chemins alternatifs sont mis en état de blocage pour éviter les boucles. Les ports des commutateurs rencontrent cinq états dont le "Blocking" qui ne transfère pas de trames de données et le "Forwarding" qui les transfère.
- ➢ **Détection de changement de topologie :** le protocole STP surveille constamment le réseau pour détecter les changements de topologie, tels que la défaillance d'un commutateur ou la mise en place d'une nouvelle connexion. Lorsqu'un changement est détecté, le protocole STP recalcule l'arbre de couverture pour s'adapter à la nouvelle topologie.
- ➢ **Rétablissement du réseau :** lorsqu'un commutateur ou une liaison échoue, le protocole STP active un chemin alternatif en débloquant le port correspondant. Également, le protocole STP surveille constamment le réseau pour détecter si le problème est résolu et si le chemin principal peut être rétabli.

2.2.2.2.1.4 EtherChannel

❖ **Définition :**

La technologie EtherChannel a initialement été développée par Cisco comme une technique de réseau local entre deux commutateurs permettant d'assembler plusieurs liens physiques Ethernet identiques en un seul lien logique. Cette technologie a pour but d'augmenter la bande passante et d'améliorer la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs [W13].

❖ **Protocoles d'agrégation de canaux :**

Il existe deux protocoles d'agrégation de lien pour configurer un EtherChannel, dits protocoles de négociation [5] :

- ➢ **PAgP :** c'est un protocole propriétaire de Cisco, il facilite la création automatique d'une liaison EtherChannel. Les modes PagP sont : on, PagP désirable et PagP auto.
- ➢ **LACP :** il fait partie d'une spécification IEEE qui permet également de regrouper plusieurs ports physiques dans un seul canal logique. Les modes LacP sont on, LacP active et LacP passive.

PAgP et LACP ne fonctionnent pas ensemble. Le mode ON existe pour PAgP et LACP pour réaliser un EtherChannel de manière inconditionnelle, sans leurs utilisations par défaut, aucun mode n'est configuré.

❖ **Avantages de l'EtherChannel :**

- ➢ La plupart des tâches de configuration peuvent être effectuées sur l'interface EtherChannel plutôt que sur chaque port individuel, ce qui assure la cohérence de la configuration à travers les liens.
- ➢ L'EtherChannel s'appuie sur les ports de commutation existants afin d'augmenter la bande passante. Aucune mise à niveau matérielle n'est nécessaire.
- ➢ L'équilibrage de charge est possible entre les liaisons qui font partie d'un même Etherchannel.
- ➢ L'EtherChannel crée une agrégation que STP reconnaît comme une seule liaison logique.
- ➢ L'EtherChannel garantit la redondance et la perte d'un lien physique ne génère pas de changement dans la topologie.

2.2.2.3 Les protocoles de gestion et configuration de réseau

2.2.2.3.1 Vlan (Virtual Local Area Network)

2.2.2.3.1.1 Définition

VLAN (Un Virtual Local Area Network) est un sous-réseau logique créé à l'intérieur d'un réseau physique. Contrairement à un réseau local traditionnel où tous les appareils sont sur le même segment de réseau, un VLAN permet de regrouper des appareils en fonction de critères comme la fonction, le département ou la sécurité. Chaque VLAN est indépendant des autres. Ceci permet de les configurer ou de les gérer de manière séparée [W14].

2.2.2.3.1.2 Avantage des vlans

La segmentation logique des ports au sein d'un ou plusieurs réseaux physiques permet de tirer plusieurs points positifs des vlans qui sont [W14] :

- ➢ Réduction de la diffusion du trafic sur le réseau ;
- ➢ Améliorer la sécurité en n'autorisant la communication qu'entre les machines du même VLAN ;
- ➢ Simplifier les tâches d'administrateur : le déplacement d'un poste de travail d'un VLAN à un autre ne nécessite aucune manipulation physique, mais elle est gérée au niveau du commutateur ;
- ➢ Flexibilité de segmentation du réseau ;
- ➢ Augmentation considérable des performances du réseau ;
- ➢ La technologie évolutive et faible coût ;
- ➢ La régulation de la bande passante.

2.2.2.3.2 Le protocole VTP (Vlan trunking Protocol)

2.2.2.3.2.1 Définition

C'est un protocole de niveau 2 qui permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur (le serveur) qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau (clients). Le VTP permet ainsi d'éviter toute incohérence de configuration des VLAN sur l'ensemble d'un réseau local. [5]

2.2.2.3.2.2 Fonctionnement de Protocol VTP

Le VTP possède trois modes de fonctionnement :

- **Serveur :** Il est associé à un domaine VTP. La déclaration des VLANs s'effectue sur le serveur. Lorsqu'on modifie la configuration VLAN sur un serveur VTP, que ce soit un ajout, une suppression ou bien une simple modification, elle est propagée surtout les switches du domaine VTP. Il tient à jour la liste des VLANs déclarés et la diffuse à l'ensemble des clients.
- **Client :** Il est associé à un domaine VTP. Il n'est pas possible de modifier la configuration des VLAN. Il reçoit la liste des VLANs, il la propage aux autres clients auxquels il est connecté et met à jour sa propre liste.
- **Transparent :** Il n'est associé à aucun domaine VTP. Sa liste de VLAN est locale et n'est pas mise à jour lorsqu'il reçoit une trame VTP. Cependant, il propage les listes de VLAN qu'il reçoit.

Les administrateurs peuvent changer les informations de VLAN sur les commutateurs fonctionnant en mode serveur uniquement. Une fois que les modifications sont appliquées, elles sont distribuées à tout le domaine VTP au travers des liens « trunk». En mode transparent, le switch reçoit les mises à jour et les transmet à ses voisins sans les prendre en compte. Il peut créer, modifier ou supprimer ses propres VLAN, mais ne les transmet pas. Les switches en mode client appliquent automatiquement les changements reçus du domaine VTP. [W15]

2.2.2.3.3 Protocol DHCP (Dynamic Host Configuration Protocol)

Le DHCP est un protocole réseau utilisé pour attribuer automatiquement des adresses IP et d'autres paramètres de configuration réseau à des appareils connectés à un réseau informatique. Plutôt que de devoir configurer manuellement chaque appareil avec une adresse IP, un masque de sous-réseau, une passerelle par défaut, etc., le DHCP permet à un serveur DHCP de gérer ces tâches de manière dynamique.

2.2.2.3.4 Protocol SSH (Secure Socket Shell)

Le protocole SSH (Secure socket Shell) est un protocole de réseau cryptographique qui permet une communication sécurisée entre deux systèmes informatiques. Il est largement utilisé pour l'accès à distance aux systèmes informatiques et pour l'exécution de commandes sur des machines distantes de manière sécurisée. Il permet de se connecter à un autre ordinateur sur un réseau, d'exécuter des commandes et de déplacer des fichiers d'un ordinateur à un autre.

2.2.2.4 Le routage

Le routage est le processus qui permet de diriger les paquets de données à travers un réseau de manière efficace et en fonction de leur destination. C'est un élément clé des réseaux informatiques, car il permet d'acheminer les données de manière fiable et rapide d'un point à un autre tout en évitant les congestions ou les temps d'arrêt.

Il est utilisé pour connecter des réseaux locaux (LAN) ou des réseaux étendus (WAN) entre eux, et pour permettre à des utilisateurs distants de se connecter aux ressources du réseau. Les routeurs sont les équipements du réseau qui effectuent cette tâche. Ils analysent les en-têtes de paquets de données et les transmettent au prochain routeur en fonction des informations de destination [W16].

Le routage peut être classé en deux catégories principales :

- **Routage statique :** dans le routage statique, les routes sont configurées manuellement sur chaque routeur. Cette méthode est souvent utilisée pour les réseaux simples ou lorsque la topologie du réseau est stable et ne change pas fréquemment.
- **Routage dynamique :** dans le routage dynamique, les routes sont calculées automatiquement par les routeurs en utilisant des protocoles de routage. Cette méthode est utilisée pour les réseaux complexes ou lorsque la topologie du réseau est susceptible de changer fréquemment.

2.2.2.4.1 Les protocoles de routage

Un protocole est un ensemble de règles et de conventions définissant comment les données sont échangées entre des dispositifs dans un réseau informatique ou dans tout autre système de communication. Il existe plusieurs protocoles de routage pour déterminer les chemins les plus efficaces pour transmettre des données d'un nœud à un autre. Parmi les plus courants :

2.2.2.4.1.1 OSPF (Open Shortest Path First)

C'est un protocole de routage d'état de lien qui est largement utilisé dans les réseaux IP. Il a été développé pour remplacer le protocole de routage de passerelle intérieure (IGRP), qui était un protocole de routage propriétaire de Cisco. De plus, OSPF utilise un algorithme de Dijkstra pour trouver la meilleure route de destination et maintenir une table de routage optimisée. Ce qui le rend plus adapté aux réseaux de plus grande taille.

2.2.2.4.1.2 RIP (Routing Information Protocol)

C'est un protocole de routage utilisé dans les réseaux informatiques. Il appartient à la famille des protocoles de routage à vecteur de distance, ce qui signifie qu'il se base sur des informations de distance pour déterminer le chemin optimal vers une destination. Il est principalement utilisé dans les réseaux de petite à moyenne taille.

L'idée de base derrière RIP est de partager des informations de routage entre les routeurs voisins afin de déterminer les chemins les plus courts vers les différentes destinations réseau. Les routeurs utilisent ces informations pour mettre à jour leurs tables de routage. RIP utilise une mesure de distance appelée "hop count" (nombre de sauts) pour évaluer la distance entre les routeurs.

2.2.2.4.1.3 EIGRP (Enhanced Interior Gateway Routing Protocol)

C'est un protocole de routage avancé utilisé dans les réseaux informatiques. Conçu par Cisco, EIGRP est un protocole de routage à vecteur de distance amélioré qui combine les meilleures caractéristiques des protocoles de routage à vecteur de distance et des protocoles de routage à état de lien.

EIGRP offre des fonctionnalités de redondance telles que l'équilibrage de charge, la redondance de lien, la redondance de routeurs et l'agrégation des liens pour améliorer la disponibilité et la redondance du réseau. Ces fonctionnalités lui permettent de fournir une haute disponibilité et une faible latence pour les applications critiques [10].

Conclusion

Ce chapitre a fourni une analyse complète sur les principes fondamentaux et les applications pratiques nécessaires pour garantir la résilience et la continuité des opérations informatiques. Nous avons mentionné qu'en combinant une compréhension approfondie des systèmes informatiques avec des stratégies de continuité robustes, les organismes peuvent mieux se préparer aux interruptions potentielles et assurer la sécurité, la disponibilité et l'efficacité continue de leurs opérations informatiques.

3

CONCEPTION ET REALISATION

Introduction

Ce chapitre présente la mise en œuvre d'un Plan de Continuité d'Activité (PCA) au sein de l'entreprise EPB où on a effectué notre stage. Nous avons utilisé le simulateur Cisco Packet Tracer qui est un point clé pour l'élaboration du PCA, la configuration des protocoles de redondance servent à la continuité d'activité, en permettant à chaque fois qu'un équipement tombe en panne, un autre de prendre le relais. L'objectif principal est de démontrer comment la théorie du PCA peut être appliquée dans un contexte réel, en offrant une vue d'ensemble des pratiques et des stratégies adoptées, ainsi que les outils utilisés, pour assurer la résilience des systèmes informatique et garantir la robustesse et la continuité des activités de l'entreprise.

3.1 SECTION 1 : Présentation de l'organisme d'accueil

Le transport maritime est le principal moyen de transport utilisé pour le déplacement de marchandises en grande quantité. Le port joue un rôle essentiel dans ces opérations, car il représente un abri naturel ou artificiel qui peut accueillir des navires, facilitant ainsi le déplacement des personnes et des marchandises.

Le port de Bejaia joue un rôle très important dans les transactions internationales vu sa place et sa position géographique. Aujourd'hui, il est classé $2^{\text{ème}}$ port d'Algérie en marchandises générales et $3^{\text{ème}}$ en pétrole.

3.1.1 Historique de la ville et du port

Au cœur de l'espace méditerranéen, la ville de Bejaïa possède de nombreux sites naturels et vestiges historiques, datant de plus de 10 000 ans, ainsi qu'une multitude de sites archéologiques,

recelant des trésors anciens remontant à l'époque du néolithique.

Bejaia joua un grand rôle dans la transmission du savoir dans le bassin méditerranéen. Grâce au dynamisme de son port, la sécurité de la région, la bonne politique et les avantages douaniers, Bougie a su attirer beaucoup de puissants marchands.

Dans l'Antiquité, Amsyouen, habitants des flans surplombant la côte, ne fréquentaient la côte que pour pêcher. Les premières nefs qui visitèrent nos abris naturels furent phéniciennes, ils y installèrent des comptoirs.

La Saldae romaine leur succéda et devint port d'embarquement de blé. Ce n'est qu'au 11ème siècle que la berbère Begaïeth, devenue Ennaciria, prit une place très importante dans le monde de l'époque. Le port de Bejaïa devint l'un des plus importants de la Méditerranée, ses échanges étaient très denses. L'histoire retiendra également, à cette époque, que par Fibonacci de Pise, fils d'un négociant pisan, s'étendirent dans le monde à partir de Bejaia, les chiffres aujourd'hui universellement utilisés.

La réalisation des ouvrages actuels du port débuta en 1834, elle fût achevée en 1987. C'est en 1960 que fût chargé le 1er pétrolier au port de Bejaïa [W17].

3.1.2 Historique de création de l'EPB

Le décret $n°$82-285 du 14 Août 1982 publié dans le journal officiel $n°$ 33 porta création de l'Entreprise Portuaire de Bejaia ; entreprise socialiste à caractère économique ; conformément aux principes de la charte de l'organisation des entreprises, aux dispositions de l'ordonnance $n°$ 71-74 du 16 Novembre 1971 relative à la gestion socialiste des entreprises et les textes pris pour son application à l'endroit des ports maritimes.

L'entreprise, réputée commerçante dans ses relations avec les tiers, fut régie par la législation en vigueur et soumise aux règles édictées par le susmentionné décret.

Pour accomplir ses missions, l'entreprise est substituée à l'Office National des Ports (ONP), à la Société Nationale de Manutention (SO.NA.MA) et pour partie à la Compagnie Nationale Algérienne de Navigation (CNAN).

Elle fut dotée, par l'Etat, du patrimoine, des activités, des structures et des moyens détenus par l'ONP, la SO.NA.MA et de l'activité Remorquage, précédemment dévolue à la CNAN, ainsi que des personnels liés à la gestion et aux fonctionnements de celles-ci.

En exécution des lois $n°$ 88.01, 88.03 et 88.04 du 02 Janvier 1988 s'inscrivant dans le cadre des réformes économiques et portants sur l'autonomie des entreprises, et suivant les prescriptions des décrets $n°$88.101 du 16 Mai 1988, $n°$88.199 du 21 Juin 1988 et $n°$88.177 du 28 Septembre 1988,

l'Entreprise Portuaire de Bejaia ; entreprise socialiste ; est transformée en Entreprise Publique Economique, Société par Actions (EPE-SPA) depuis le 15 Février 1989, son capital social fut fixé à Dix millions (10.000.000) de dinars algérien, actuellement, il a été augmenté à 3.500.000.000 de DA [W17].

3.1.2.1 Situation géographique

Le port de Bejaia est situé à une Latitude Nord 36°45'24" et une longitude Est 05°05'50". Son positionnement au cœur de la méditerranée occidentale et au centre de la côte algérienne présente une originalité économique et une place de choix sur les routes maritimes. Le port de Bejaïa jouit d'une situation géographique privilégiée. Bien protégé naturellement, sa rade est l'une des plus sûres.

Le port est situé dans la baie de la ville de Bejaïa, le domaine public, artificiel, maritime et portuaire est délimité par suite de l'arrêté $n°$ 93/1015/DRAG, ainsi :

- Au nord par la route nationale $n°9$.
- Au sud par les jetées de fermeture et du large sur une longueur de 2.750 m.
- A l'est par la jetée Est.
- A l'ouest par la zone industrielle de Bejaïa [11].

3.1.2.2 Activités et services de l'EPB

➢ **Ses activités :**

Les principales activités de l'entreprise sont [W17] :

- L'exploitation de l'outillage et des installations portuaires ;
- L'exécution des travaux d'entretien, d'aménagement et de renouvellement de la super structure portuaire ;
- L'exercice du monopole des opérations d'acconage et de manutention portuaire ;
- L'exercice du monopole des opérations de remorquage, de pilotage et d'amarrage ;
- La police et la sécurité portuaire dans la limite géographique du domaine public portuaire.

➢ **Ses services :**

Les principes service de port sont [11] :

- **L'acheminement des navires de la rade vers le quai :** Dans certains cas exceptionnels d'arrivée massive, les navires restent en attente sur la zone de mouillage (rade) jusqu'à obtention d'autorisation de joindre un poste à quai, délivrée par une conférence de placement au niveau de la direction capitainerie, et opérations d'aide à la navigation identifiée par le remorquage, pilotage, et le lamanage.
- **Le remorquage :** Tirer ou pousser le navire, pour effectuer les manœuvres d'accostage, de déhalage ou d'appareillage du navire, effectuer les opérations de convoyage et d'aide dans l'exécution des autres manœuvres.

- **Le pilotage :** Assuré de 24H/24 par la direction capitainerie, obligatoire en entrée et sortie du navire, afin d'assister le commandant dans la conduite de son navire à l'intérieur du port.
- **Le lamanage :** Amarré ou désamarrer le navire de son poste d'accostage. Le lamaneur procède aux opérations d'arrimage et de désarrimage du navire. Il coopère avec les remorqueurs et l'équipage du navire, reçoit les amarres lancées du navire et procède à leur capelage ou décapelage.
- **Les opérations de manutention et d'acconage des marchandises :**

  Ils consistent en :

  - Les opérations d'embarquement et de débarquement des marchandises.
  - La réception des marchandises
  - Le transfert vers les aires d'entreposage, hangars et terre-pleins, ports secs.
  - La préservation ou la garde des marchandises sur terre-pleins ou hangar et hors port.
  - Pointage des marchandises.
  - La livraison aux clients.
  - La manutention et l'acconage sont assurés, par un personnel formé dans le domaine. Il est exercé de jour comme de nuit, réparti sur deux vacations de 6h à 19h avec un troisième shift optionnel qui s'étale entre 19h et 01h du matin. Pour des exceptionnels, ce dernier peut s'étaler jusqu'à 7h du matin. D'autres prestations sont également fournies aux navires et au client telle que :
  - Enlèvement des déchets des navires et assainissement des postes à quai.
  - Pesage des marchandises (ponts bascules).
  - Location de remorqueurs ou vedettes (pour avitaillement des navires, transport de l'assistance médicale, assistance et sauvetage en haut mer.

3.1.2.3 Caractéristique technique

Parmi ces caractéristiques [W17] :

- **ACCES DU PORT :** Le port de Bejaia est accessible par un chenal extérieur large de 320 m et à 13,50 m. Les navires de marchandises générales accèdent aux bassins par le biais de deux passes, respectivement la passe ABDELKADER, large de 110 m et draguée à 12 m et la passe de la Casbah, large de 125 m et dragué à 12 m.
- **INFRASTRUCTURE PORTUAIRE :** Le port de Bejaia s'étale sur une superficie totale de 76 hectares. Sa surface d'entreposage s'étend sur 422.000 m^2 couverts. Il dispose de plus 3000 ml de quai, répartis, entre 16 postes à quais pour navires de marchandises générales, 03 postes à quais pour navires pétroliers, un poste RO/RO et un poste gazier.
- **LES BASSINS DU PORT :**

  Le port est composé de trois bassins :

- Bassin de l'Avant-Port : sa superficie est de 75 hectares et ses profondeurs varient entre 10,5 m et 13,5 m. Disposant d'installations spécialisées, l'avant-port est destiné à traiter les navires pétroliers.
- Bassin du Vieux Port : sa superficie est de 25 hectares et ses profondeurs de quai varient entre 8 et 9 m.
- Bassin de l'Arrière-Port : Sa superficie est de 55 hectares et ses profondeurs varient entre 10,5 m et 12 m.

- **DONNES PHYSIQUE :**
  - Vents dominants de Nord-Est à Est, en été et d'Ouest à Nord-Ouest en hiver.
  - Marrée inexistante, mais des différences de niveau peuvent atteindre 50 cm.
  - Ressac : jusqu'à 50 cm par gros temps d'Ouest à Nord-Ouest (Port pétrolier).
  - Visibilité excellente.

- **JETÉES ET BRISE- LAMES :**
  - A l'est : Jetée Est 650m
  - Au sud : Jetée en chevrons composée de trois éléments dont la longueur atteint 2.750 :
    - Jetée Sud,
    - Jetée du large,
    - Jetée de la fermeture.

- **MOUILLAGE :** Connue pour être l'une des meilleures de la côte algérienne, la rade de Bejaia offre d'excellentes potentialités en matière de protection et des fonds propices à un bon mouillage, avec des profondeurs allant de 10 m à plus de 20 m. Abritée de tous les vents sauf du Nord Est à l'Est, la rade est limitée par une ligne imaginaire s'étendant du Cap Carbon au Cap Aokas. Pour les pétroliers, la zone de mouillage est située à l'Est de l'axe du chemin d'accès.

3.1.3 L'organisation des structures de l'entreprise portuaire de Bejaia

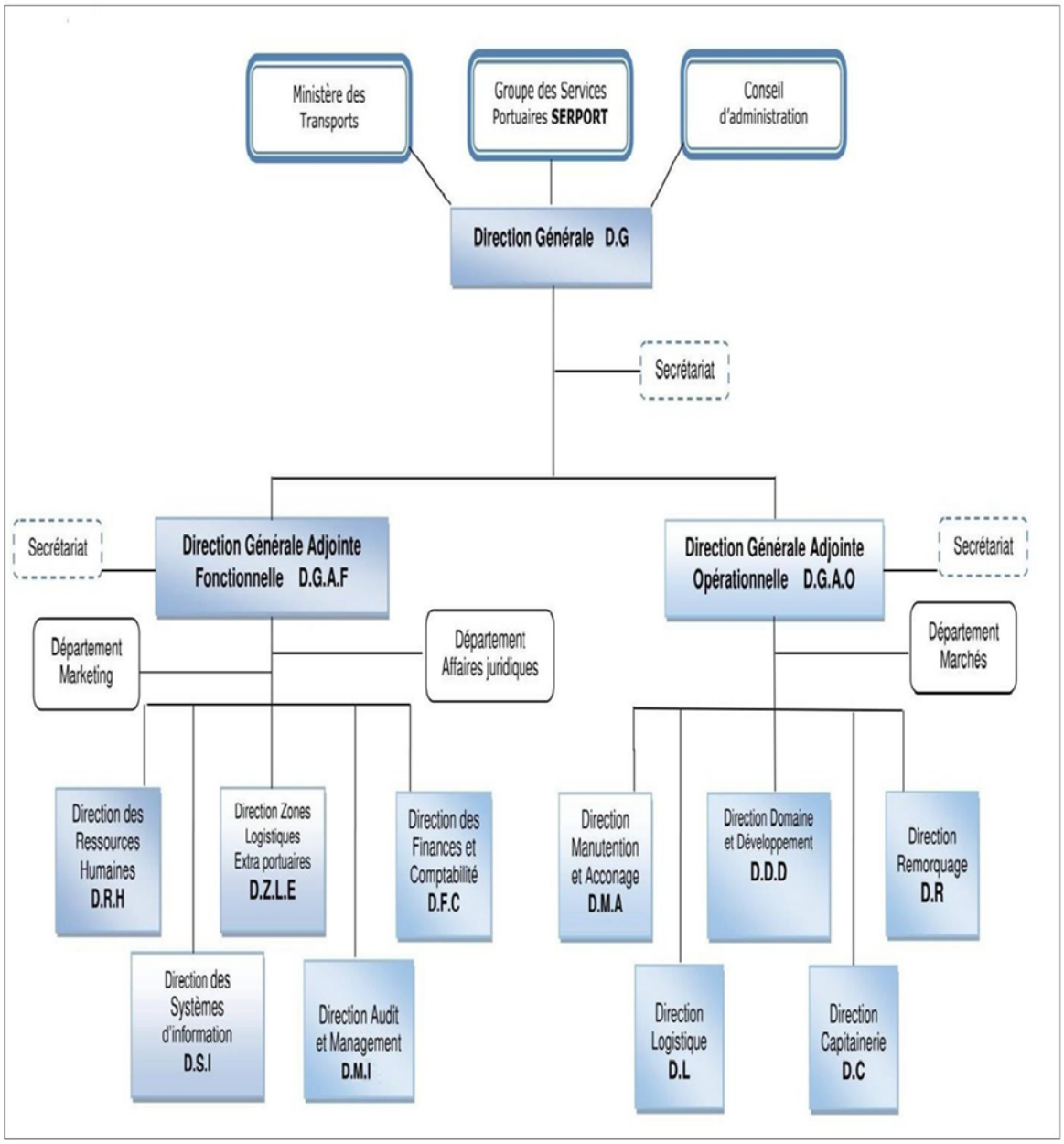

Figure 3.1 – L'organigramme de l'EPB [12].

L'organigramme de direction générale de l'EPB est organisé en directions fonctionnelles et opérationnelles :

- **Direction Opérationnelle :** Les structures d'activités du terrain en relation Directe avec les clients. Parmi ces directions :
  - **Direction Manutention et Acconage (DMA) :** Elle est chargée de prévoir, organiser, coordonner et contrôler l'ensemble des actions de manutention et d'acconage liées à l'exploitation du port.

- **Direction Domaine et Développement (DDD) :** elle est chargée de :
  - l'amodiation et location de terre-pleins, hangar, bureaux, immeubles, installations et terrains 'à usage industriel ou commercial.
  - l'enlèvement des déchets des navires et assainissement des postes à quai.
  - Pesage des marchandises (pont bascule).
  - Avitaillement des navires en eau potable.
- **Direction Capitainerie (DC) :** Elle est chargée de la sécurité portuaire, ainsi que de la bonne régulation des mouvements des navires, et la garantie de sauvegarde des ouvrages portuaires.
- **Direction Remorquage (DR) :** Elle est chargée d'assister le pilote du navire lors de son entrée et de sa sortie du quai. Son activité consiste essentiellement à remorquer les navires entrants et sortants, ainsi que la maintenance des remorqueurs. Les prestations sont : Le remorquage portuaire, le remorquage hauturier (haute mer) et le sauvetage en mer.
- **Direction Logistique (DL) :** Elle consiste à gérer tout ce qui concerne le transport et le stockage des produits de l'entreprise : véhicules nécessaires au transport, fournisseurs de l'entreprise, entrepôts, manutention, en optimisant leur circulation pour minimiser les couts et les délais.

- **Directions fonctionnelles :** Il s'agit des structures de soutien aux structures opérationnelles. Parmi ces directions :
  - **Direction du Management Intègre (DMI) :** Elle est chargée de :
    - La mise en œuvre, le maintien et l'amélioration continue du système de management intégré ;
    - L'animation et la coordination de toutes les activités des structures dans le domaine Qualité, Hygiène, Sécurité, Environnement, QHSE ;
  - **Direction Ressources Humaines (DRH) :** Elle est chargée de :
    - Gestion de la paie
    - Gestion des fournisseurs
    - Les moyennes générales
    - Gestion des recrutements
  - **Direction Finances et Comptabilité (DFC) :** Elle a pour mission :
    - La tenue de la comptabilité.
    - La gestion de la trésorerie (dépenses, recettes et placement).
    - La tenue des inventaires.
    - Le contrôle de gestion (comptabilité analytique et contrôle budgétaire).

- **Direction Zones Logistiques Extra Portuaires :** Elle a pour mission :
  - Elaborer les schémas de développement technique, organisationnel, commercial et opérationnel des zones logistiques extra-portuaires.
  - Suggérer les axes stratégiques pour le développement et la promotion des activités multimodales.
  - Elaborer les procédures de gestion et de fonctionnement opérationnel des sites logistiques.
  - Accompagner la Direction Générale pour l'obtention des différentes autorisations et agréments nécessaires pour l'opérabilité optimale du site.
- **Direction des Systèmes d'Information (DSI) :** Elle a pour mission :
  - La réalisation du schéma directeur par la conduite des projets d'informatisation en veillant à la cohérence fonctionnelle et technique ainsi qu'à la qualité et la sécurité des systèmes d'information.
  - La mise en œuvre des systèmes d'information à la fois flexibles et fiables. Le management des évolutions des systèmes d'information et des projets informatiques.

3.1.4 Présentation la DSI (direction des systèmes d'information)

Le système d'information (SI) représente un ensemble structuré de ressources conçu pour rassembler, stocker, traiter et distribuer des données. La direction des systèmes information, relevant directement de la direction fonctionnelle de l'EPB, est chargée de l'automatisation des activités de l'entreprise portuaire de Bejaïa. Il déploie les logiciels et les infrastructures nécessaires à la gestion du SI.

L'EPB déploie ces systèmes d'information dans le but d'accroître la productivité, d'automatiser les processus métier et d'améliorer le service client. Ces systèmes intègrent de plus en plus de fonctionnalités réseau pour connecter tous les utilisateurs à l'entreprise, ainsi que pour établir des liens avec la clientèle et les fournisseurs. Le réseau local de l'entreprise constitue désormais une valeur ajoutée en permettant l'intégration de nouveaux partenaires, fournisseurs et clients.

3.1.4.1 Missions de la DSI

La direction des systèmes d'information joue un rôle essentiel dans l'entreprise, la figure suivante résume les missions essentielles :

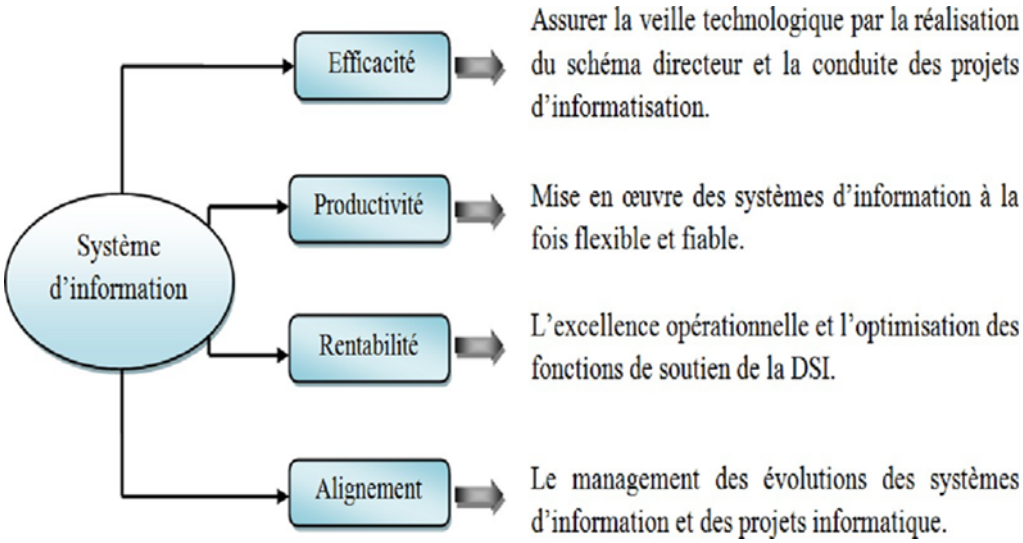

Figure 3.2 – Missions de système d'information de l'EPB [12].

3.1.4.2 Organigramme humain de la DSI (direction des systèmes informatique)

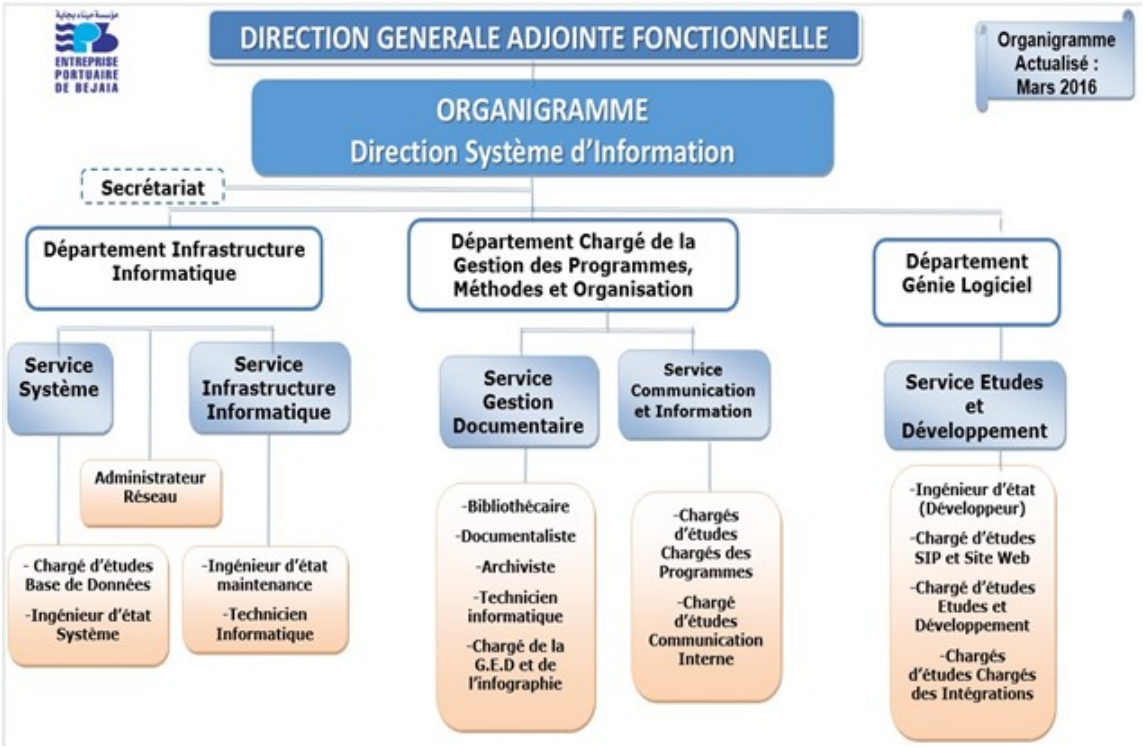

Figure 3.3 – Organigramme de la structure informatique [12].

- **Département Infrastructure informatique :** chargée de l'administration et du déploiement du réseau, des systèmes, de la sécurité, des serveurs, des bases de données ; des équipements
- **Département Génie Logiciel :** c'est le département chargé de l'administration et du suivi des applications enveloppées en interne ou acquises chez un fournisseur externe, d'étoilement et d'assistance chez les utilisateurs finaux.
- **Département Programme méthode et Organisation :** c'est une administration qui s'occupe des programmes méthode et organisations suivis des archives, de l'affichage dynamique, des communications internes. . .

3.1.4.3 Présentation des logiciels utilisés

L'EPB dispose d'un parc consistant des logiciels informatiques qui traitent les différentes activités du port (activités opérationnelles, activités de soutien...) pour une meilleure identification des logiciels disponibles, on distingue :

Nom	**Présentation**	**Utilisateurs**
LOGIMAC	Il est lié principalement à la gestion de la marchandise : • Affectation des équipes d'employés aux navires afin de débarquer ou embarquer les marchandises transportées ou à transporter par les navires. • Affectation des engins aux navires nécessaires pour l'embarquement ou le débarquement des marchandises • Gestion de la marchandise de chaque navire • Récupérer des statistiques à propos des marchandises importées et exportés en termes de tonnage, etc.	- Direction logistique. - Direction Générale (pour avoir des statistiques)

BIG-RH : Gestion des ressources Humaines	Il permet à l'EPB de gérer l'ensemble des aspects liés aux personnels (employé). Cela comprend : L'administration du personnel : gestion des informations personnelles et professionnelles des salariés, gestion des paies, gestion des temps et activités, gestion des congés et absences, gestion des contrats de travail, etc. Le recrutement et l'intégration : publication d'offres d'emploi, gestion des candidatures, sélection des candidats, intégration des nouveaux salariés, etc. La gestion des compétences : identification des compétences des salariés, évaluation des compétences, développement des compétences, gestion des carrières, etc. La gestion de la formation : identification des besoins en formation, organisation de formations, suivi des formations, évaluation de l'impact des formations, etc. La gestion de la paie : calcul de la paie, gestion des cotisations sociales, édition des bulletins de paie, etc. La gestion de la performance : définition des objectifs individuels et collectifs, évaluation de la performance, gestion des primes et des récompenses, etc. La gestion de la santé et sécurité au travail : évaluation des risques professionnels, mise en place de mesures de prévention, suivi des accidents du travail et des maladies professionnelles, etc. La communication interne : diffusion d'informations aux salariés, gestion des enquêtes de satisfaction, etc.	- Direction des ressources humaines.

GED (Gestion électronique des documents)	Le logiciel GED (Gestion électronique des documents) permet de gérer le cycle de vie des documents numériques au sein d'EPB. Il permet de : Numériser les documents papier existants. Stocker les documents numériques dans un référentiel sécurisé Organiser et classer les documents de manière structurée. Indexer les documents pour faciliter leur recherche. Gérer les accès aux documents en fonction des habilitations des utilisateurs. Suivre le cycle de vie des documents, de leur création à leur destruction. Automatiser certaines tâches liées à la gestion documentaire, comme la validation des workflows. Sécuriser les documents contre les accès non autorisés, les virus et les pertes de données. Respecter les réglementations en vigueur en matière d'archivage électronique	- Toutes les directions.

Table 3.1 – Les logiciels prioritaires de l'EPB.

3.1.4.4 Infrastructure informatique

3.1.4.4.1 Le réseau informatique de l'EPB

Le réseau du port de Bejaia s'étend du port pétrolier (n°16) aux ports 13 et 18 (parc à bois). La salle machine du réseau local de l'EPB contient principalement une armoire de brassage et une autre armoire optique de grande taille, ces deux armoires servent à relier les différents sites de l'entreprise avec le département informatique par fibres optiques de type 4, et 12 brins, comme l'illustre la figure (3.4) . Chaque site a une armoire de brassage contenant un/des convertisseur(s) média, un/plusieurs Switch où sont reliés les différents équipements par des câbles informatiques.

Figure 3.4 – Réseau fibre optique de L'EPB [12].

3.1.4.4.2 Présentation de l'architecture réseau de l'EPB

Dans cette partie, on présente les différentes composantes de l'architecture réseau LAN de l'EPB.

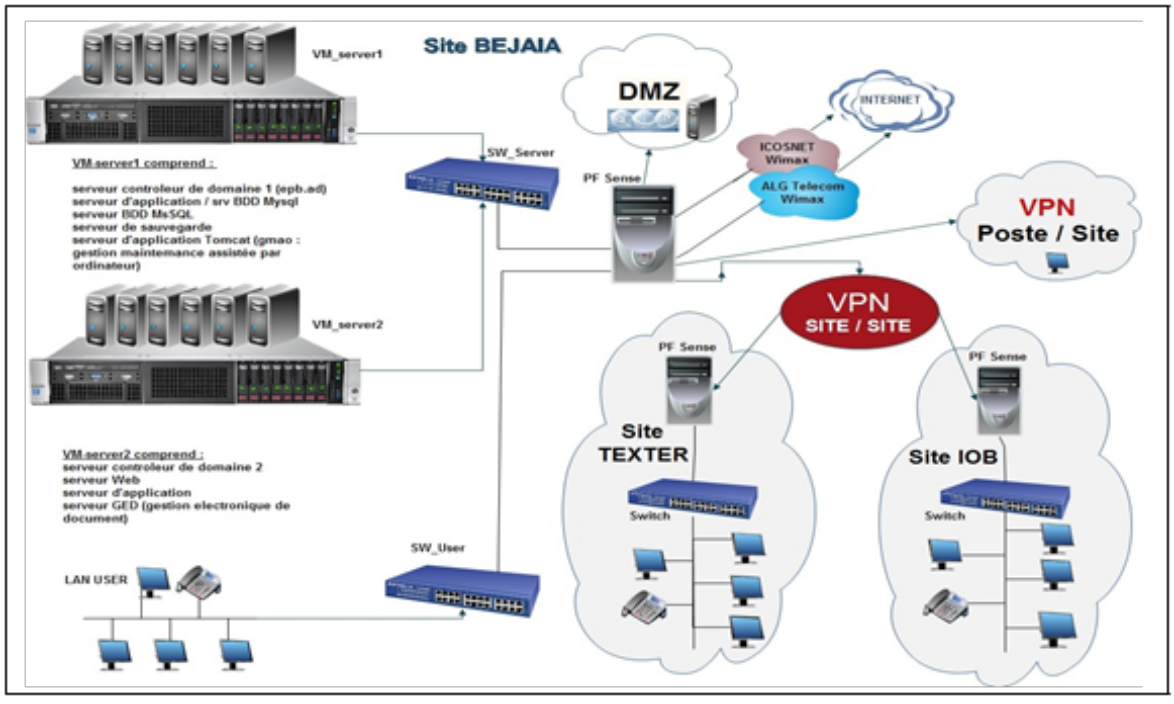

Figure 3.5 – L'architecture du réseau LAN de l'entreprise EPB..

3.1.4.4.2.1 Étude de l'architecture

- **Connexion Internet :** L'entreprise portuaire de Bejaia s'est dotée de deux connexions fournies par ALG TELECOM : WIMAX et ADSL.
  - La technologie ADSL permet d'assurer des transmissions numériques haut débit sur de la paire torsadée classique.
  - La technologie WiMAX permet quant à elle de se connecter à internet haut débit grâce à une antenne Outdoor qui communique par ondes hertziennes via une station de base située au mont Gouraya , d'une très grande fiabilité permettant ainsi d'éviter l'usage du câble et le risque d'une panne physique
- **Sécurité :**
  - ✓ Les postes clients sont interconnectés avec les serveurs par des switches, sous contrôle d'un pare-feu pfSense pour appliquer les stratégies d'accès et les règles de routages déterminant la manière dont les clients accèdent à Internet .
  - ✓ Une zone démilitarisée est utilisée pour avoir un accès au réseau local de manière privilégiée à partir de n'importe quel endroit .
  - ✓ Deux zones logistiques TEXTER et IGHIL OUBEROUAK qui sont reliées au réseau global via des tunnels VPN.
- **Salle machine :** La salle machine est le cœur du réseau toutes les activités du port reposent sur cette salle, elle regroupe en un seul endroit les ressources nécessaires au bon fonctionnement du LAN, en plus des Switches elle comporte les différentes équipements :
  - ✓ **Onduleur :** un onduleur afin de protéger les équipements réseau installés (switch, serveur. . .) ;
  - ✓ **Armoire optique :** une armoire de fibre optique qui relie les câbles de fibre optique sortant elle contient des convertisseurs, des jarretières et des tiroirs optiques ;
  - ✓ **Armoire de brassage :** contient une console KVM, des convertisseurs, des panneaux et cordons de brassage et deux serveurs physiques, contenant dedans d'autres serveurs virtuels tels que :
    - **Serveur de base de données (SQL server 2008 and My SQL) :**
      Un serveur de base de données répond à des demandes de manipulation de données stockées dans une ou plusieurs bases de données. Il s'agit de demande de recherche, de tri, d'ajout, de modification ou de suppression de données. Ces données sont utilisées par des serveurs web et des utilisateurs.
    - **Serveur de contrôleur de domaine DC1 (Active Directory) :**
      Sous Windows Server 2012 R2 l'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateur utilisant le système Windows. Il répertorie les éléments de ce réseau administré tel que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes...etc.

- **Serveur de contrôleur de domaine redondant DC2 (Active Directory) :**
  Il permet de conserver des réplicas de données de l'annuaire sur un autre contrôleur de domaine, cela garantit la disponibilité et la continuité.
- **Serveur application/fichier :**
  C'est un serveur sur lequel sont installées les applications utilisées par les usagers, ces applications sont chargées sur le serveur d'application pour y accéder à distance. Un serveur d'application peut être un serveur qui centralise toutes les applications utilisées par les postes clients.
- **Serveur de sauvegarde :**
  Il a pour rôle de sauvegarder en continu les données générées par l'entreprise. Si un employé efface par erreur un document ou qu'il y a un dysfonctionnement d'un ordinateur, le serveur est en mesure de récupérer le fichier perdu.

3.2 Section 2 : Réalisation d'un PCA au sein de l'EPB

3.2.1 Un premier pas dans le plan de continuité d'activité au sein de l'EPB

La continuité d'activité des équipements qui gèrent les logiciels critiques est essentielle pour maintenir les opérations de l'entreprise sans interruption. Une panne peut entraîner des pertes financières et nuire à la réputation de l'entreprise. Les logiciels critiques doivent fonctionner en continu. Pour cela, un Plan de Continuité d'Activité (PCA) est nécessaire, incluant des procédures de sauvegarde, de récupération et une maintenance proactive.

3.2.1.1 Plan de sensibilisation et formation sur PCA

Sensibiliser les employés de la Direction des Systèmes d'Information (DSI) et les acteurs du PCA sur son importance est une étape essentielle pour sa réussite au sein de l'entreprise. Ils doivent comprendre leurs rôles, adopter des bonnes pratiques et respecter les procédures de sécurité. Des formations régulières, des guides pratiques et des simulations de panne peuvent renforcer cet acte ou même des fiches de sensibilisation. En évaluant la participation et les connaissances des employés, l'entreprise peut améliorer continuellement son PCA. Ainsi, l'entreprise peut minimiser les impacts des perturbations et assurer le bon déroulement de ses opérations critiques.

Voici un exemple d'un flyer de sensibilisation qu'on a réalisé dans le cadre de la sensibilisation des employés de l'EPB sur le PCA :

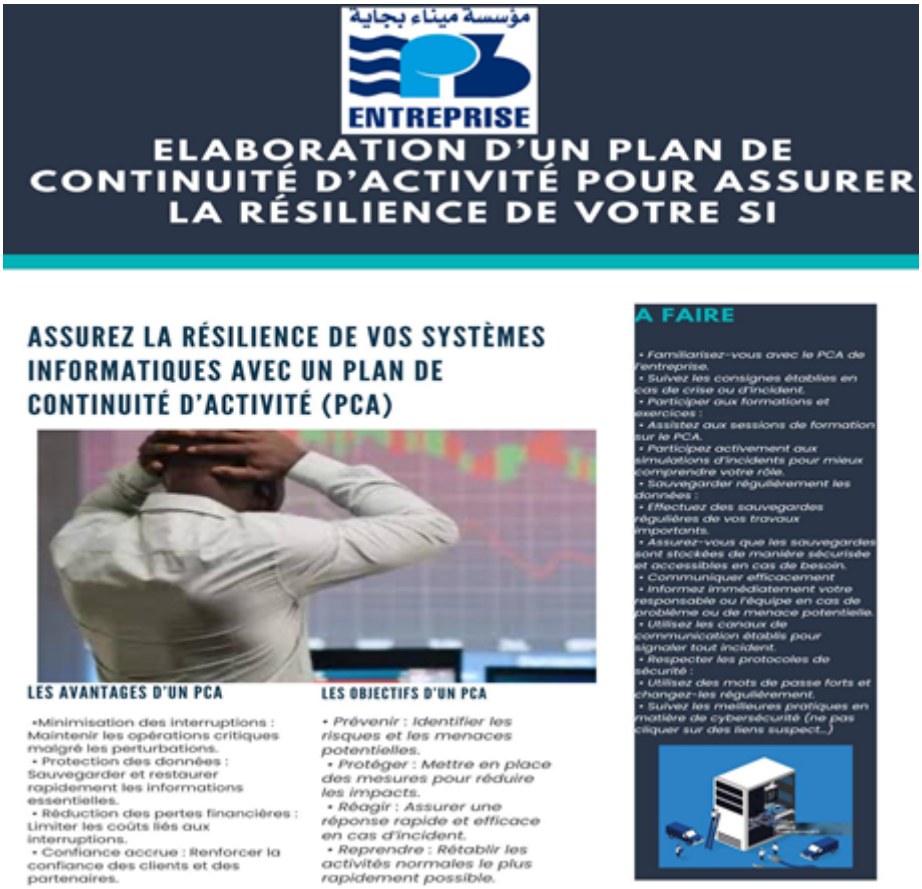

Figure 3.6 – Flyer de sensibilisation.

3.2.1.2 Fiche de BIA

Pour élaborer un PCA efficace au sein d'une entreprise portuaire, il faut d'abord identifier les activités critiques et les classer par ordre de priorité en fonction de leur importance pour la continuité des opérations en cas de perturbation.

Ce tableau représente un aperçu initial d'un BIA de quelques directions de l'EPB :

DMIA	**Activité**	**Type d'impact**	**Logiciel**
H+4	Affectation des équipes d'employés aux navires afin de débarquer ou embarquer les marchandises transportées ou à transporter par les navires.	Opérationnel	LOGIMAC
	Affectation des engins aux navires nécessaires pour l'embarquement ou le débarquement des marchandises.		
	Gestion de la marchandise de chaque navire		

	Récupérer des statistiques à propos des marchandises importées et exportées en termes de tonnage, etc. La gestion des navires pour avoir traçabilité à propos de séjour de navire au port de Bejaia : • Date d'annonce d'arrivée de navire. • Date d'arrivée en rade. • Date d'entrée au quai.		
H+12	**La gestion des compétences :** identification des compétences des salariés, évaluation des compétences, développement des compétences, gestion des carrières, etc.	Financier et opérationnel	GED
	La gestion de la formation : identification des besoins en formation, organisation de formations, suivi des formations, évaluation de l'impact des formations, etc.		
H+24	L'administration du personnel : gestion des informations personnelles et professionnelles des salariés, gestion des paies, gestion des temps et activités, gestion des congés et absences, gestion des contrats de travail, etc.	Image (réputation)	BIG-RH
	Le recrutement et l'intégration : publication d'offres d'emploi, gestion des candidatures, sélection des candidats, intégration des nouveaux salariés, etc.		
H+48	La gestion des navires pour avoir traçabilité à propos de séjour de navire au port de Bejaia : • Date d'annonce d'arrivée de navire. • Date d'arrivée en rade. • Date d'entrée au quai.	Opérationnel	LOGIMAC

Table 3.2 – Fiche BIA.

3.2.1.3 Identification et évaluation des risques

Dans le cadre de notre engagement pour renforcer la résilience de notre entreprise portuaire et son système informatique, nous avons réalisé une analyse des risques. Le tableau "Identification et évaluation des risques" synthétise cette analyse et sert d'outil de référence pour : Documenter les risques identifiés, évaluer leurs niveaux de criticité, examiner leurs impacts sur les opérations puis prendre des décisions éclairées pour renforcer la résilience.

Ce tableau contribuera à renforcer notre capacité à anticiper et à répondre efficacement aux défis futurs.

Les risques	Les impacts	Niveau du risque
Cyberattaques : Telles que, les logiciels malveillants et les attaques par déni de service ou piratages des sites utilisés dans la gestion générale de l'EPB.	Peuvent compromettre les systèmes informatiques critiques du port, entraînant des interruptions d'activité, la perte de données sensibles ou la violation de la confidentialité des informations.	Fort.
Catastrophes naturelles : Identifier les risques liés aux catastrophes naturelles telles que les tempêtes, les inondations ou les séismes.	Paralyser les opérations portuaires, des retards dans les livraisons ainsi que les dommages infrastructures...	Fort.
Interruptions de service : Les pannes matérielles, les erreurs humaines...	Peuvent entraîner des interruptions de service des systèmes informatiques critiques du port, perturbant les opérations et entraînant des pertes financières.	Modéré.
Fuites de données : Qu'elles soient accidentelles ou intentionnelles peuvent compromettre la confidentialité des informations sensibles telles que les données des clients, les plans opérationnels ou les informations financières.	Ce qui peut nuire à la réputation de l'entreprise et entraîner des sanctions réglementaires.	Moyen.

Table 3.3 – Identification et évaluation des risques.

3.2.1.3.1 Un scenario d'une cyberattaque sur un logiciel de l'EPB

Scénario concernant une Cyber-attaque qui cible un serveur hébergeant l'application suivante : Escale ou LOGIMAC.

Voici un exemple de procédure à appliquer après l'attaque :

a. **Identification et Évaluation de la Cyber-Attaque :**

- ➢ Des anomalies sont détectées par rapport à l'utilisation du logiciel LOGIMAC, indiquant une possible cyber-attaque.
- ➢ L'équipe informatique est alertée et elle doit commencer à enquêter sur l'incident.

b. **Isolation et Containement :**

- ➢ Les ordinateurs utilisant LOGIMAC vont être isolés du reste du réseau pour empêcher la propagation de l'attaque.
- ➢ Les journaux d'activité sont examinés pour identifier l'origine de l'attaque et les méthodes utilisées par les attaquants.

c. **Restauration des Systèmes Critiques :**

- ➢ LOGIMAC doit être restauré à partir de sauvegardes récentes pour permettre la reprise des opérations portuaires.
- ➢ Des mesures de sécurité supplémentaires, telles que l'authentification à deux facteurs, sont mises en place pour renforcer la sécurité du système restauré.

d. **Communication et Gestion des Parties Prenantes :**

- ➢ Les autorités portuaires doivent être informées de l'incident et des mesures prises pour remédier (Police, gendarmerie).
- ➢ Les compagnies maritimes et les autres parties prenantes (consignataire, transitaire, douane, clients, etc) doivent être notifiées des retards possibles dans les opérations portuaires et des mesures prises pour minimiser les impacts.

e. **Évaluation Post-Attaque et Améliorations Continues :**

- ➢ Une analyse postérieure de l'incident sera réalisée pour identifier les failles de sécurité et les lacunes dans le plan de continuité d'activité.
- ➢ Des mesures correctives, telles que des mises à jour logicielles et des formations supplémentaires pour le personnel, sont mises en œuvre pour renforcer la résilience de l'entreprise aux cyber-attaques futures.
- ➢ Le personnel sera sensibilisé aux risques cybernétiques lors de séances de formation dédiées.
- ➢ Des simulations d'attaques informatiques seront organisées pour permettre au personnel de pratiquer les procédures de réponse en cas d'incident réel.
- ➢ Des éventuels outils de surveillance continue seront déployés pour renforcer la détection des activités suspectes sur le réseau informatique du port.
- ➢ Mise en place d'un système d'alertes automatique pour informer immédiatement l'équipe informatique en cas de tentative d'intrusion ou de comportement anormal des systèmes.

3.2.1.4 Problématique et Solutions proposées

Les systèmes informatiques sont souvent exposés à différents risques, tels que des pannes matérielles ou logicielles, des cyberattaques, des catastrophes naturelles et d'autres facteurs de risque.

En raison de leur importance dans les entreprises, leur fonctionnement quotidien est indispensable. Ainsi, garantir la disponibilité des logiciels et leur résilience devient une priorité pour éviter des interruptions désastreuses des activités.

Pour répondre à cette problématique, il est important de mettre en place des solutions de redondance et de topologies de secours.

Une topologie de secours est une topologie alternative réseau LAN, tenue prête pour utilisation lors de la survenance d'un évènement menaçant la continuité d'activité. Elle sera activée en cas de sinistre privant l'organisation de son réseau principal.

3.2.1.4.1 Choix de localisation pour l'installation

L'EPB dispose de trois zones logistiques extra portuaires :

➢ La gare maritime : c'est un nouveau terminal à passagers s'étale sur une superficie de 34.145 m^2 et il est construit sur deux sites :

- Le bloc de débarquement à partir du bateau, situé dans l'enceinte du port avec une Surface totale de 19.460 m^2.
- Le bâtiment d'embarquement, situé à l'extérieur du port, avec une surface totale de 14 685 m^2.Les deux blocs sont reliés par deux passerelles fixes. [W17]

➢ Zone logistique de texter se situe dans la Daïra de Aïn Taghrout, Wilaya de Bordj BouArreridj. Elle est à environ : 190 km du Port de Bejaia, 30 Km de Bordj Bou Arreridj, 40 km de la Wilaya de Sétif, 100 km de la Wilaya de Msila et 130 Km de la Wilaya de Bouira. [W17]

➢ La zone logistique IGHIL OUBEROUAK Sis à environ 5 KM au Sud-Est du port et d'une superficie de 48 560 m^2, ce site a une capacité spatiale de 1040 EVP et une capacité commerciale de 19 000 EVP. Il est constitué de plusieurs parties et essentiellement de deux hangars de 10 200 m^2 et 750 m^2, et de deux entrées principales, dont l'une d'elles est reliée à la RN 09. [W17]

3.2.1.4.2 Critères déterminant le choix

Choisir la meilleure zone logistique comme site de secours est une décision importante pour assurer la résilience de l'entreprise en cas d'urgence. Après l'étude de quelques éléments essentiels telle que :

- **Accessibilité :** assure que la zone est facilement accessible en cas d'urgence, tant pour les employés que pour les secours.
- **Risques naturels :** choisir une zone moins exposée à ces risques ou prévoyez des mesures d'atténuation adéquates. Telles que les inondations sont les tremblements de terre, les tempêtes, les incendies de forêt.
- **Infrastructures :** Vérifiez la disponibilité et la fiabilité des infrastructures essentielles telles que l'électricité.
- **Taille et capacité :** La zone logistique doit être suffisamment grande pour accueillir tous les équipements et le personnel nécessaires en cas d'urgence, ainsi que pour stocker des fournitures et des ressources.
- **Sécurité :** Assure que la zone est clôturée et équipée de systèmes de surveillance adéquats.
- **Distance par rapport au site principal :** le site de secours devrait être situé à une distance raisonnable du site principal de l'entreprise, afin de pouvoir être rapidement opérationnel en cas d'urgence.
- **Coûts :** Évaluez les coûts associés à l'acquisition ou à la location de la zone logistique, ainsi que les coûts opérationnels continus.

3.2.1.4.3 Résultat du choix

Après avoir évalué les trois zones pour le choix de l'installation du site de secours, nous avons opté pour la zone maritime en raison de ses nombreux avantages. Cette zone offre un bon compromis entre coût et distance par rapport au site principal, permettant une réactivité rapide en cas de besoin tout en restant économiquement viable. Elle dispose de bonnes infrastructures pour garantir la sécurité des équipements. Sa taille et sa capacité sont également adéquates pour accueillir les équipements nécessaires sans compromettre la performance, ce qui renforce la résilience du site.

3.2.2 Mise en place d'un site de secours sur PACKET TRACER

Pour la mise en œuvre d'un site de secours dans l'architecture de l'EPB, nous avons opté pour l'utilisation d'une simulation sur de l'outil PACKET Tracer.

Ce logiciel nous offre la possibilité de représenter notre réseau et atteindre notre objectif principal, qui est de garantir la continuité des opérations ou des logiciels installés au sein de chaque direction de l'entreprise qui permettent de gérer leurs activités et leurs actions même en cas de défaillance ou de panne. C'est pourquoi nous avons choisi de mettre en place un réseau redondant (haute disponibilité) en installant les différents équipements tels que les routeurs, les commutateurs et des PCs en raison de ses caractéristiques avancées.

3.2.2.1 Présentation et utilisation de Packet Tracer

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible, pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc...

3.2.2.1.1 Description générale

La figure 3.7 montre un aperçu général de Packet Tracer. La zone (1) est la partie dans laquelle le réseau est construit. Les équipements sont regroupés en catégories accessibles dans la zone (2). Une fois la catégorie sélectionnée, le type d'équipement peut être sélectionné dans la zone (3). La zone (4) permet de passer du mode temps réel au mode simulation, la zone (5) permet d'ajouter des indications dans le réseau, enfin la zone (6) contient un ensemble d'outils :

- Select : pour déplacer ou éditer des équipements.
- Move Layout : permet de déplacer le plan de travail.
- Place Note : place des notes sur le réseau.
- Delete : supprime un équipement ou une note.
- Inspect : permet d'ouvrir une fenêtre d'inspection sur un équipement (table ARP, routage).

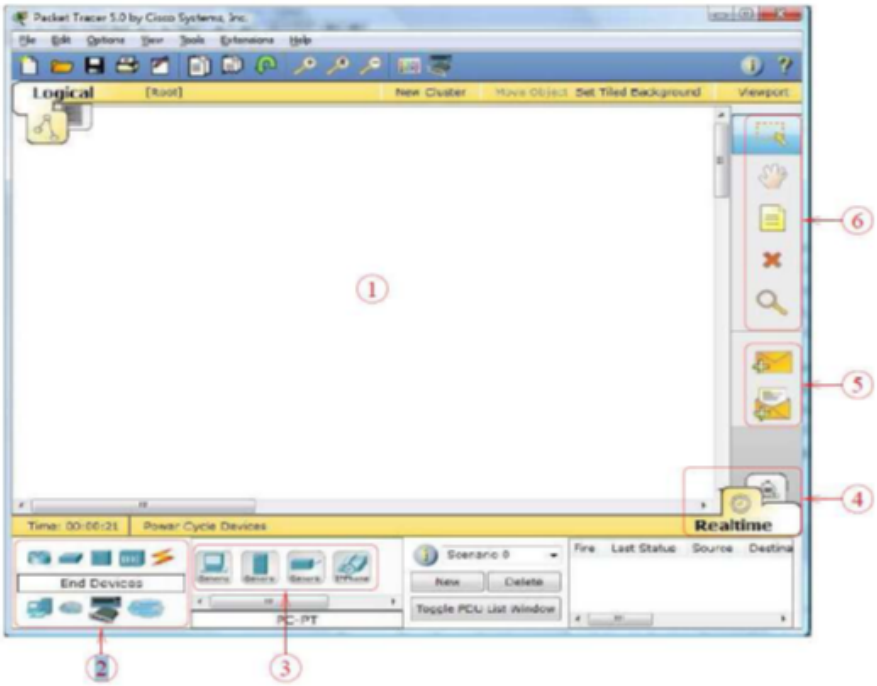

Figure 3.7 – Description de la fenêtre principale du CISCO packet tracer.

3.2.3 la mise en place de la topologie LAN sur Cisco

Avant de créer la topologie, nous avons procédé d'abord à représenter l'architecture de réseau local de l'EPB sur le logiciel CISCO packet tracer en utilisant les différents équipements nécessaires, puis les relier entre eux avec des câbles appropriés.

Figure 3.8 – Topologie LAN de l'EPB.

Le réseau local (LAN) de l'EPB est composé de trois couches : une couche cœur contenant deux commutateurs de niveau 3 (switch cœur), une couche de distribution composée de quatre commutateurs de niveau 2 (switch distribution), et une couche d'accès composée de 8 équipements terminaux qui sont des PCs.

3.2.3.1 Présentation des équipements utilisés

Couche	**Équipement du modèle type**	**Nombre**	**Nomination**
Couche cœur	Switch core (cisco catalystC6807-XL)	2	switchcoeur(n)
Couche distribution	Switch distribution (cisco Catalyst C3850-24S)	4	Switch(n)
Couche accès	PC	8	PC(n)

Table 3.4 – Èquipements utilisés.

3.2.3.2 Plan d'adressage

L'adresse du réseau LAN se basera sur une adresse qui est 172.16.0.0/24. C'est à partir de cette dernière que l'affectation des adresses IP pour l'ensemble des équipements et des VLANs va être accomplie.

3.2.3.3 Vlan de l'architecture

Les équipements terminaux affiliés à un Vlan vont prendre toutes les adresses IP d'une même adresse sous réseau.

On a désigné pour chaque direction de l'entreprise présentée sur l'architecture un Vlan spécifique. Le tableau suivant montre le plan d'adressage des VLANs.

Vlan	**Vlan 10**	**Vlan 20**	**Vlan 30**	**Vlan 40**
Direction	D.RH	D.C	D.FC	D.L
Adresse	172.16.10.252/24	172.16.20.252/24	172.16.30.252/24	172.16.40.252/24
DHCP	dynamique	dynamique	dynamique	dynamique

Table 3.5 – Vlan du réseau LAN.

3.2.4 Configuration des équipements utilisés

Après avoir installé les équipements nécessaires afin de réaliser la topologie de réseau local actuel de l'EPB et les avoir reliés pour qu'ils soient interconnectés, nous avons appliqué une série

de configurations.

Les équipements réseau comprenant les commutateurs de niveau 2 et 3 qui forment le réseau local des stations seront configurés. Diverses configurations ont été appliquées à ces équipements, chaque type étant illustrés par un exemple.

3.2.4.1 La configuration de base

3.2.4.1.1 Configuration des noms et des mots de passe au mode privilégié

Cette configuration consiste à l'attribution d'un nom et un mot de passe au mode privilégié pour les commutateurs :

```
switch(config)#hostname swc
swc(config)#enable secret swc
swc(config)#
```

Figure 3.9 – Configuration des noms et mots de passes du mode privilège.

3.2.4.1.2 Configuration des mots de passe pour les lignes consoles et VTY

Sécuriser des lignes consol et vty des commutateurs :

```
swc(config)#line console 0
swc(config-line)#password swc
swc(config-line)#login
```

```
swc(config)#line vty 0 15
swc(config-line)#password swc
swc(config-line)#login
```

Figure 3.10 – Configuration des mots de passe pour la ligne console et vty.

➢ Sauvegarder la configuration en cours dans la mémoire par la commande copy running-config startup-config ou simplement "wr" :

```
swc#wr
Building configuration...
[OK]
```

Figure 3.11 – La commande de sauvegarde.

3.2.4.2 Configuration des protocoles de gestion et de configuration de réseau LAN

3.2.4.2.1 Configuration du VTP mode server et client sur les commutateurs

- Sur Switch cœur : mode server.
- Sur Switch distribution : mode client.

```
swc(config)#vtp mode server
Device mode already VTP SERVER.
swc(config)#vtp version 2
swc(config)#vtp domain EPB.com
Changing VTP domain name from NULL to EPB.com
swc(config)#vtp password cisco
```

Figure 3.12 – Configuration VTP mode server.

```
DC(config)#vtp mode client
Device mode already VTP CLIENT.
DC(config)#vtp version 2
Cannot modify version in VTP client mode
DC(config)#vtp domain EPB.com
Domain name already set to EPB.com.
DC(config)#vtp password  cisco
Password already set to cisco
```

Figure 3.13 – Configuration VTP mode client.

➢ **Vérification du mode vtp avec la commande " show vtp status " :**

```
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : EPB.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0000.0CB7.1920
Configuration last modified by 172.16.10.252 at 3-1-93 01:24:10
Local updater ID is 172.16.10.252 on interface Vl10 (lowest numbered VLAN interface
found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 9
Configuration Revision          : 0
MD5 digest                      : 0x5E 0x8C 0xA0 0xDB 0x8F 0xD4 0xEA 0x75
                                  0xF2 0xB2 0x47 0xBD 0x28 0xD5 0x28 0x6E
```

```
DL#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : EPB.COM
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 000B.BE2A.EA00
Configuration last modified by 0.0.0.0 at 3-1-93 00:12:08

Feature VLAN :
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 255
Number of existing VLANs        : 6
Configuration Revision          : 0
MD5 digest                      : 0xA3 0xF0 0x8B 0xA0 0xB9 0x11 0x2B 0xC3
                                  0x3E 0xD2 0x06 0x68 0x06 0x9E 0x0F 0xAA
```

Figure 3.14 – La commande show VTP status.

3.2.4.2.2 Configuration des Vlan avec l'attribution d'adresse IP

La création de tous les VLANs du réseau LAN sur les deux Switchs cœur en attribuant une adresse pour chacun.

```
swc(config)#int vlan 10
swc(config-if)#ip add 172.16.10.252 255.255.255.0
swc(config-if)#ex
swc(config)#int vlan 20
swc(config-if)#ip add 172.16.20.252 255.255.255.0
swc(config-if)#ex
swc(config)#int vlan 30
swc(config-if)#ip add 172.16.30.252 255.255.255.0
swc(config-if)#ex
swc(config)#int vlan 40
swc(config-if)#ip add 172.16.40.252 255.255.255.0
swc(config-if)#ex
```

Figure 3.15 – Configuration des Vlan.

3.2.4.2.2.1 Configuration du service DHCP pour l'interface de chaque vlan

Créer un pool d'adresses pour chaque VLAN, puis leur définir une passerelle par défaut du sous-réseau.

```
swc(config)#int vlan10
swc(config-if)#ip add 172.16.10.252 255.255.255.0
swc(config-if)#ip dhcp pool vlan10
swc(dhcp-config)#network 172.16.10.252 255.255.255.0
swc(dhcp-config)#default-router 172.16.10.252
swc(dhcp-config)#dns-server 41.110.167.10
swc(dhcp-config)#
```

Figure 3.16 – Configuration DHCP.

➢ **Confirmation de la bonne attribution d'adresse au PCs et serveurs des autres Vlan :**

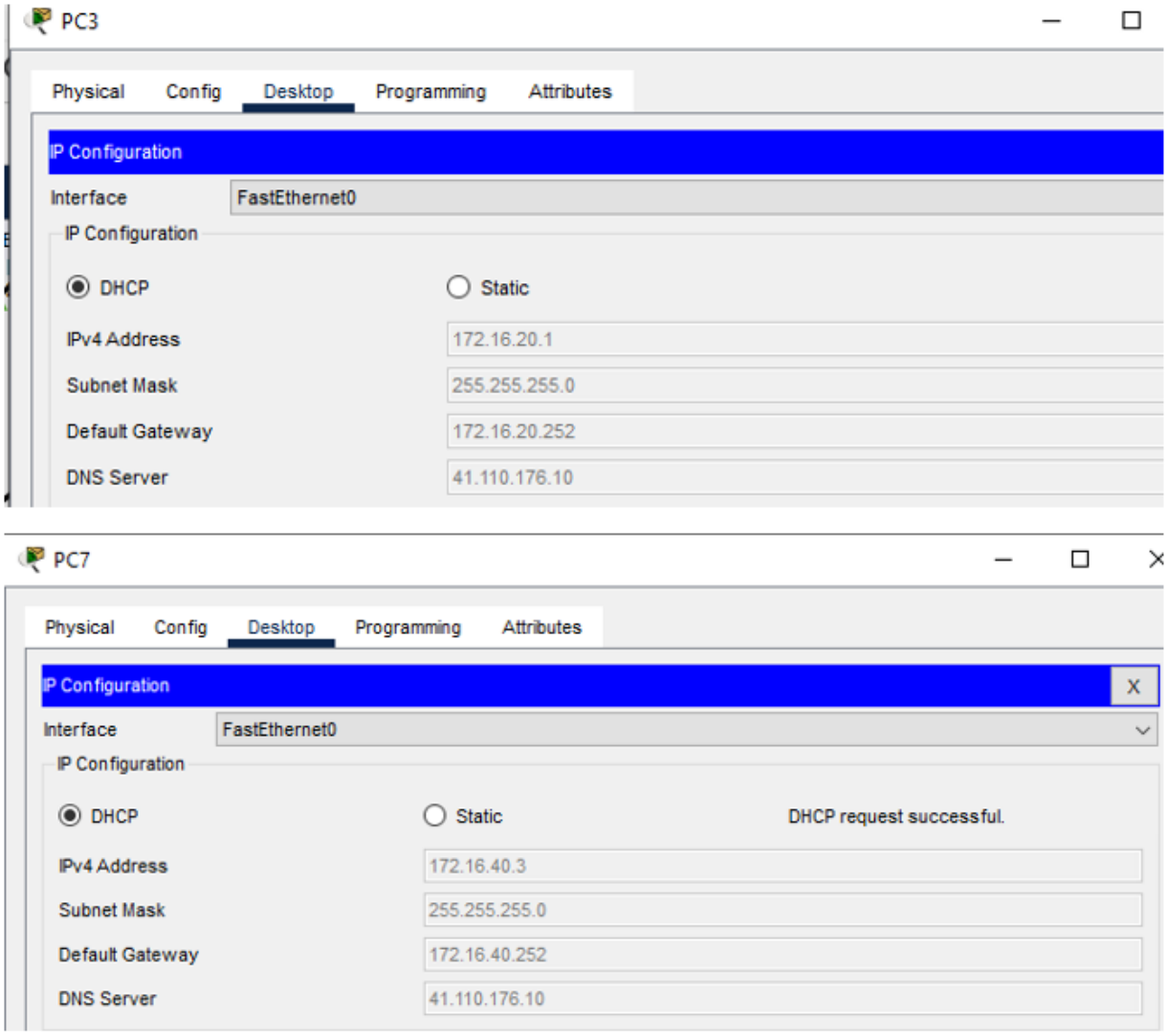

Figure 3.17 – Attribution adresses DHCP.

➢ **Vérification de la propagation des Vlans :**

```
swcl#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24
10   DRH                              active
20   DC                               active
30   DFC                              active
40   SDL                              active
70   log-LOGIMAC                      active    Gig0/1
80   log-BIGRH                        active    Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
swcl#%IP-4-DUPADDR: Duplicate address 172.16.70.254 on Vlan70, sourced by
0000.0C9F.F001
```

Figure 3.18 – La commande show vlan brief.

3.2.4.2.2.2 Attribution des ports aux VLANs

Au niveau de chaque switch distribution, nous avons attribué des interfaces pour chaque vlan. En effet, chaque port de cet équipement appartiendra à un vlan donné :

```
DC(config)#int f0/12
DC(config-if)#switchport mode access
DC(config-if)#switchport access vlan 20
DC(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

DC(config-if)#int f0/2
DC(config-if)#switchport mode access
DC(config-if)#switchport access vlan 20
DC(config-if)#ex
```

Figure 3.19 – Attributions des ports aux vlans.

3.2.4.2.2.3 Sécurisation d'accès à distance avec SSH (Secure socket Shell)

Activation de SSH sur les commutateurs de la couche cœur et distribution :

```
swc(config)#username admin password EPBSSH
swc(config)#ip domain-name cisco.com
swc(config)#crypto key generate rsa
The name for the keys will be: swc.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

swc(config)#line vty 04
*Mar 1 1:7:2.891: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 1:7:2.917: %SSH-5-ENABLED: SSH 1.5 has been enabled
swc(config-line)#transport input ssh
swc(config-line)#login
swc(config-line)#
```

Figure 3.20 – Configuration de SSH.

3.2.5 La création d'une topologie de secours

Dans cette architecture qu'on a proposé, on a réduit le nombre des équipements par rapport au LAN à deux Switch et deux PCs, chaque élément étant spécifiquement dédié à un logiciel critique.

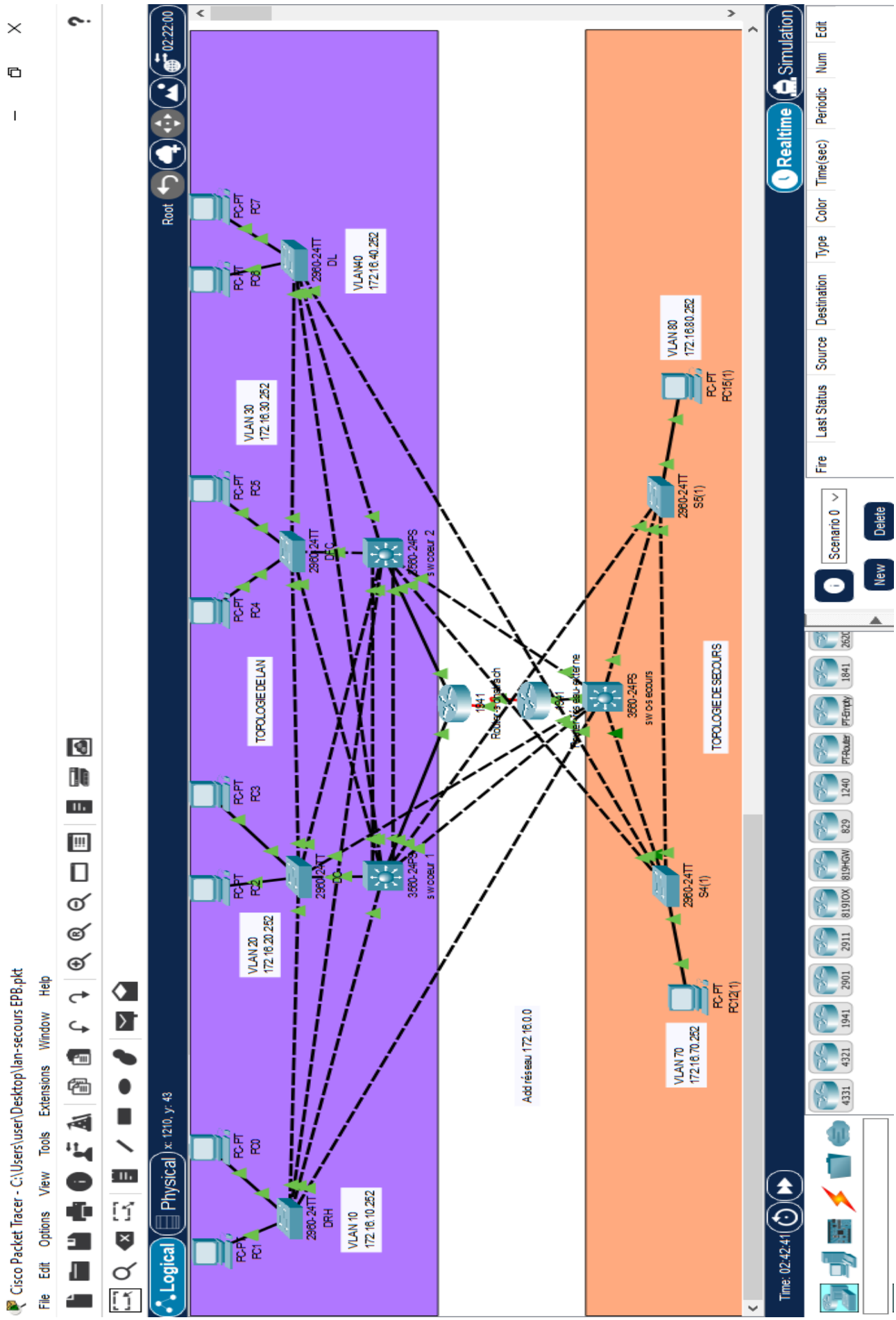

Figure 3.21 – Proposition de la topologie LAN+secours pour l'EPB.

3.2.5.1 Présentation des équipements utilisés

Équipement du modèle type	Nombre	Nomination
Switch core (cisco catalystC6807-XL)	1	Multilayer switch
Routeur ISR4331	2	Routeur(n)
Switch distribution (cisco Catalyst C3850-24S)	2	Switch(n)
PC	2	PC(n)

Table 3.6 – Présentation des équipements dans la topologie de secours.

3.2.5.2 Vlan de l'architecture de secours

On a désigné pour chaque logiciel critique dans une direction un vlan spécifique.

Le VLAN 70 est réservé au logiciel LOGIMAC de la direction Capitainerie, tandis que le VLAN 80 est dédié au secours du logiciel Big-RH de la direction des ressources humaines. Cette approche ciblée garantit une reprise immédiate et sans faille des opérations en cas de défaillance.

Vlan	Vlan 70	Vlan 80
Direction	D.RH	D.C
Adresse	172.16.70.1/24	172.16.80.1/24
DHCP	Dynamic	Dynamic

Table 3.7 – Architecture de secours.

3.2.5.3 Configuration des équipements

3.2.5.3.1 Configuration de base des équipements du réseau de secours

Configuration des noms et un mot de passe du mode privilège ainsi que la sécurisation des lignes consol et VTY :

```
sw(config)#hostname sw-secours
sw-secours(config)#enable secret sws
sw-secours(config)#line consol 0
sw-secours(config-line)#password sws
sw-secours(config-line)#login
sw-secours(config-line)#exit
sw-secours(config)#line vty 0 15
sw-secours(config-line)#password sws
sw-secours(config-line)#login
sw-secours(config-line)#exit
sw-secours(config)#
```

Figure 3.22 – Configuration de base des équipements de secours.

3.2.5.3.2 Configuration des protocoles de gestion et configuration de réseau de secours

3.2.5.3.2.1 Configuration du VTP mode server et client sur les commutateurs

- Sur sw-secours : mode server.
- Sur les switch distribution de secours : mode client.

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname sw-secours
sw-secours(config)#vtp mode server
Device mode already VTP SERVER.
sw-secours(config)#vtp version 2
sw-secours(config)#vtp domain EPB
Changing VTP domain name from NULL to EPB
sw-secours(config)#vtp password cisco
Setting device VLAN database password to cisco
```

Figure 3.23 – Configuration VTP mode server.

```
log-LOGIMAC(config)#VTP MODE CLIENT
Device mode already VTP CLIENT.
log-LOGIMAC(config)#VTP DOMAIN EPB.com
Changing VTP domain name from EPB to EPB.com
log-LOGIMAC(config)#vtp password cisco
Setting device VLAN database password to cisco
```

Figure 3.24 – Configuration VTP mode client.

➢ **Vérification du mode vtp avec la commande " show vtp status " :**

```
swcveille#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : EPB.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0000.0CB7.1920
Configuration last modified by 172.16.10.252 at 3-1-93 01:24:10
Local updater ID is 172.16.10.252 on interface Vl10 (lowest numbered VLAN interface
found)

Feature VLAN :
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 9
Configuration Revision            : 0
MD5 digest                        : 0x5E 0x8C 0xA0 0xDB 0x8F 0xD4 0xEA 0x75
                                    0xF2 0xB2 0x47 0xBD 0x28 0xD5 0x28 0x6E
```

```
DL#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : EPB.COM
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 000B.BE2A.EA00
Configuration last modified by 0.0.0.0 at 3-1-93 00:12:08

Feature VLAN :
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 6
Configuration Revision            : 0
MD5 digest                        : 0xA3 0xF0 0x8B 0xA0 0xB9 0x11 0x2B 0xC3
                                    0x3E 0xD2 0x06 0x68 0x06 0x9E 0x0F 0xAA
```

Figure 3.25 – La commande show VTP status.

3.2.5.3.2.2 Configuration des Vlan avec l'attribution d'adresse IP

La création des vlan 10-20-70-80 sur les deux switchs cœur en leur attribuant des adresses IP.

```
sw-secours(config)#int vlan70
sw-secours(config-if)#ip add 172.16.70.252 255.255.255.0
sw-secours(config-if)#no shut
sw-secours(config-if)#ex
sw-secours(config)#int vlan80
sw-secours(config-if)#ip add 172.16.80.252 255.255.255.0
sw-secours(config-if)#no shut
sw-secours(config-if)#
sw-secours(config)#int vlan10
sw-secours(config-if)#ip add 172.16.10.252 255.255.255.0
sw-secours(config-if)#no shut
sw-secours(config-if)#ex
sw-secours(config)#int vlan20
sw-secours(config-if)#ip add 172.16.20.252 255.255.255.0
sw-secours(config-if)#no shut
sw-secours(config-if)#ex
sw-secours(config)#
```

Figure 3.26 – Configuration des VLANs.

❖ **Configuration du service DHCP pour l'interface de chaque vlan**

```
sw-secours(config)#int vlan70
sw-secours(config-if)#ip add 172.16.70.252 255.255.255.0
sw-secours(config-if)#ip dhcp pool vlan70
sw-secours(dhcp-config)#network 172.16.70.252 255.255.255.0
sw-secours(dhcp-config)#default-router 172.16.70.252
sw-secours(dhcp-config)#dns-server 41.110.167.10
```

Figure 3.27 – Configuration DHCP.

➢ **Confirmation de la bonne attribution d'adresse au PCs et serveurs des autres Vlan :**

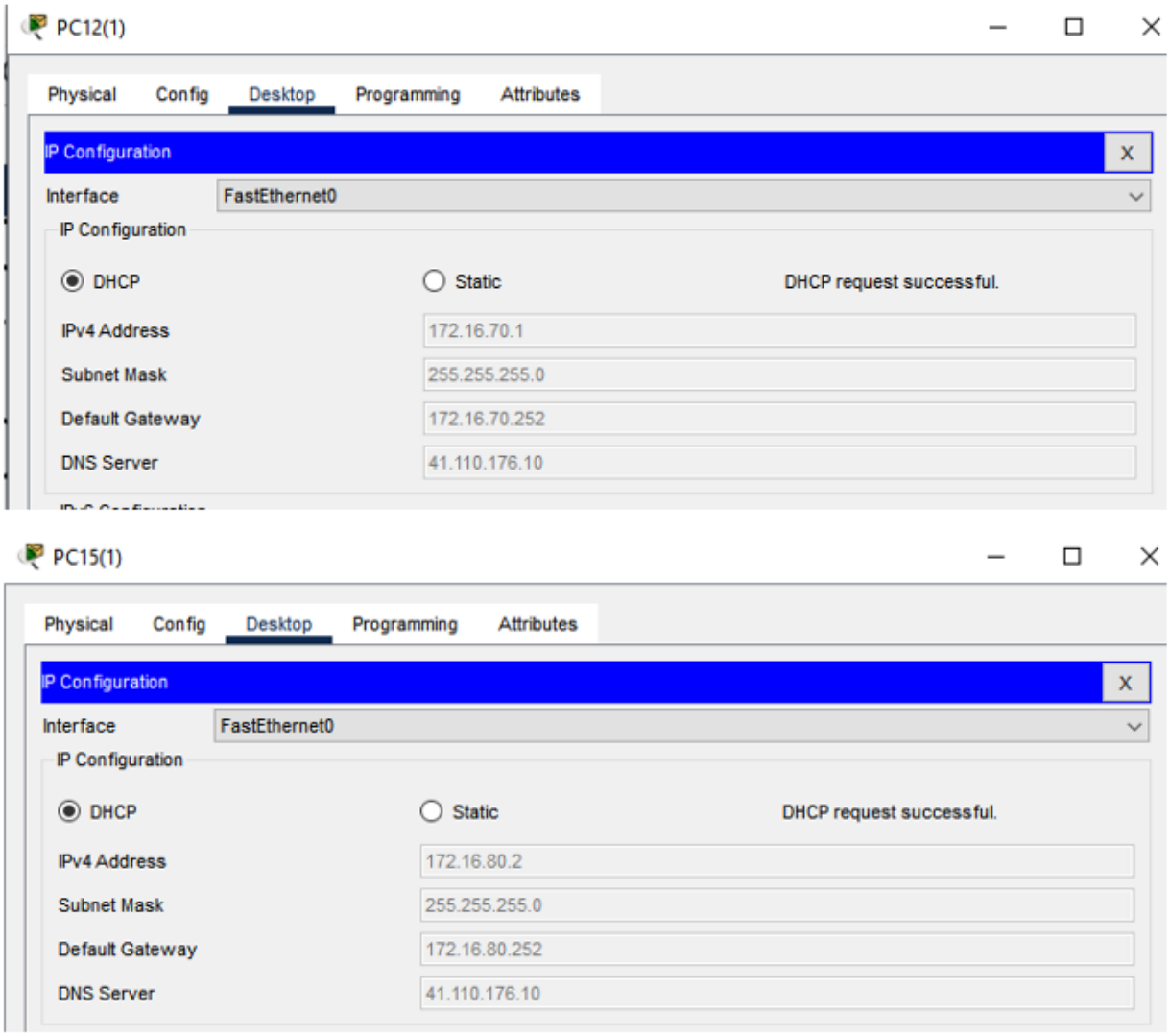

Figure 3.28 – Attribution adresses DHCP au PC.

➢ **Vérification de la propagation des Vlans :**

```
sw-secours#SH VLAN BRIEF

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                 Gig0/2
10   DRH                               active
20   DC                                active
70   log-LOGIMAC                       active
80   log-BIGRH                         active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
sw-secours#
```

Figure 3.29 – La commande show vlan brief.

3.2.5.3.2.3 Sécurisation d'accès à distance avec SSH (Secure socket Shell)

Activation de SSH sur les commutateurs de la couche cœur et distribution :

```
sw-secours(config)#username admin password EPBSSH
sw-secours(config)#ip domain-name cisco
sw-secours(config)#crypto key generate rsa
The name for the keys will be: sw-secours.cisco
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

sw-secours(config)#line vty 04
*Mar 1 0:9:49.83: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:9:49.83: %SSH-5-ENABLED: SSH 1.5 has been enabled
sw-secours(config-line)#transport input ssh
sw-secours(config-line)#login
```

Figure 3.30 – Configuration SSH.

3.2.5.3.3 Configuration des protocoles de redondance

3.2.5.3.3.1 Configuration des liens Etherchannel

Nous avons opté pour une agrégation des liens fastethernet entre les deux switchs cœurs sw cœur 1 et sw cœur 2 par la mise des deux ports fastethernet dans un groupe, puis activer le mode trunk.

```
swc#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
swc(config)#int range f0/1-2
swc(config-if-range)#channel-group 1 mode on
swc(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

swc(config-if-range)#exit
swc(config)#int port-channel 1
swc(config-if)#switchport trunk encapsulation dot1q
swc(config-if)#switchport mode trunk
swc(config-if)#
swc(config-if)#
```

Figure 3.31 – Configuration des liens Etherchannel.

➢ **Vérification de l'Etherchannel avec la commande " show etherchannel summary "**

```
swc#sh etherchannel sum
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


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

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           -      Fa0/1(P) Fa0/2(P)
swc#
```

Figure 3.32 – La commande show etherchannel summary.

3.2.5.3.3.2 Configuration du protocole STP

Configuration des deux premiers vlan 10-20 du réseau LAN en routes primaires et les vlan 70-80 en routes secondaires pour le sw cœur 1.

```
swc(config)#spanning-tree mode pvst
swc(config)#spanning-tree vlan 10-20 root primary
swc(config)#spanning-tree vlan 70-80 root secondary
swc(config)#
```

Configuration des deux premiers vlan 70-80 en routes primaires et les vlan 10-20 en routes secondaires pour le sw cœur 2.

```
sw-veille(config)#spanning-tree mode pvst
sw-veille(config)#spanning-tree vlan 70-80 root primary
sw-veille(config)#spanning-tree vlan 10-20 root secondary
sw-veille(config)#
```

Figure 3.33 – Configuration stp.

➢ Vérification de la configuration STP avec la commande "show spanning-tree" sur les commutateurs

```
spanning-tree mode pvst
spanning-tree vlan 10,20 priority 20480
spanning-tree vlan 70-80 priority 28672
!
spanning-tree mode pvst
spanning-tree vlan 70-80 priority 24576
spanning-tree vlan 10-20 priority 28672
!
```

Figure 3.34 – La commande show spanning-three.

3.2.5.3.3.3 Configuration hsrp

Configuration du protocole HSRP au niveau des switchs du réseau LAN et de celui de secours, au niveau de chaque interface de VLAN.

Configuration de vlan 10-20 comme vlans actifs au niveau de LAN avec une priorité 150 et 100 pour les vlan en veille 70-80, et inversement au niveau de la topologie de secours, c'est-à-dire configuration de vlan 70-80 comme vlans actifs au niveau de topologie de secours avec une priorité 150 et 100 pour les vlan en veille 10-20.

- **Au niveau du LAN :**

```
swc(config)#int vlan10
swc(config-if)#ip add 172.16.10.252 255.255.255.0
swc(config-if)#standby 10 ip 172.16.10.254
swc(config-if)#standby 10 priority 150
swc(config-if)#standby 10 preempt
swc(config-if)#ex
swc(config)#int vlan20
swc(config-if)#ip add 172.16.20.252 255.255.255.0
swc(config-if)#standby 20 ip 172.16.20.254
swc(config-if)#standby 20 priority 150
swc(config-if)#standby 20 preempt
swc(config-if)#int vlan70
swc(config-if)#ip add 172.16.70.252 255.255.255.0
swc(config-if)#standby 70 ip 172.16.70.254
swc(config-if)#standby 70 priority 100
swc(config-if)#standby 70 preempt
swc(config-if)#ex
swc(config)#int vlan80
swc(config-if)#ip add 172.16.80.252 255.255.255.0
swc(config-if)#standby 80 ip 172.16.80.254
swc(config-if)#standby 80 priority 100
swc(config-if)#standby 80 preempt
swc(config-if)#ex
swc(config)#
```

Figure 3.35 – Configuration du HSRP sur les switchs LAN.

- **Au niveau de la topologie de secours :**

```
sw-secours(config)#int vlan10
sw-secours(config-if)#ip add 172.16.10.252 255.255.255.0
sw-secours(config-if)#standby 10 ip 172.16.10.254
sw-secours(config-if)#standby 10 priority 100
sw-secours(config-if)#ex
sw-secours(config)#int vlan20
sw-secours(config-if)#ip add 172.16.20.252 255.255.255.0
sw-secours(config-if)#standby 20 ip 172.16.20.254
sw-secours(config-if)#standby 20 priority 100
sw-secours(config-if)#standby 20 preempt
sw-secours(config-if)#ex
sw-secours(config)#int vlan70
sw-secours(config-if)#ip add 172.16.70.252 255.255.255.0
sw-secours(config-if)#standby 70 ip 172.16.70.254
sw-secours(config-if)#standby 70 priority 150
sw-secours(config-if)#standby 70 preempt
sw-secours(config-if)#ex
sw-secours(config)#int vlan80
sw-secours(config-if)#ip add 172.16.80.252 255.255.255.0
sw-secours(config-if)#standby 80 ip 172.16.80.254
sw-secours(config-if)#standby 80 priority 150
sw-secours(config-if)#standby 80 preempt
sw-secours(config-if)#ex
```

Figure 3.36 – Configuration du hsrp vlan sur les switchs de secours.

➢ **Vérification de la configuration du protocole HSRP sur tous les siwtchs :**

- Au niveau LAN :

```
swc#sh standby br
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   150 P Active   local           172.16.10.252   172.16.10.254
Vl20        20   150 P Active   local           172.16.20.252   172.16.20.254
Vl70        70   100 P Standby  172.16.70.252   local           172.16.70.254
Vl80        80   100 P Standby  172.16.80.252   local           172.16.80.254
swc#
```

Figure 3.37 – La commande show standby brief LAN.

- Au niveau de la topologie secours :

```
sw-secours#sh standby br
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   100 P Standby  172.16.10.252   local           172.16.10.254
Vl20        20   100 P Standby  172.16.20.252   local           172.16.20.254
Vl70        70   150 P Active   local           172.16.70.252   172.16.70.254
Vl80        80   150 P Active   local           172.16.80.252   172.16.80.254
sw-secours#
```

Figure 3.38 – La commande show standby brief secours.

3.2.6 Test et validation

Nous avons simulé des pings continus entre deux PCs du même VLAN, entre les PCs des différents VLANs puis entre un PC du réseau LAN et un PC de la topologie de secours pour tester la connectivité et le bon fonctionnement de notre réseau.

3.2.6.1 Test de connectivité entre les PCs du même VLAN

- ping entre PC0 et PC1 :

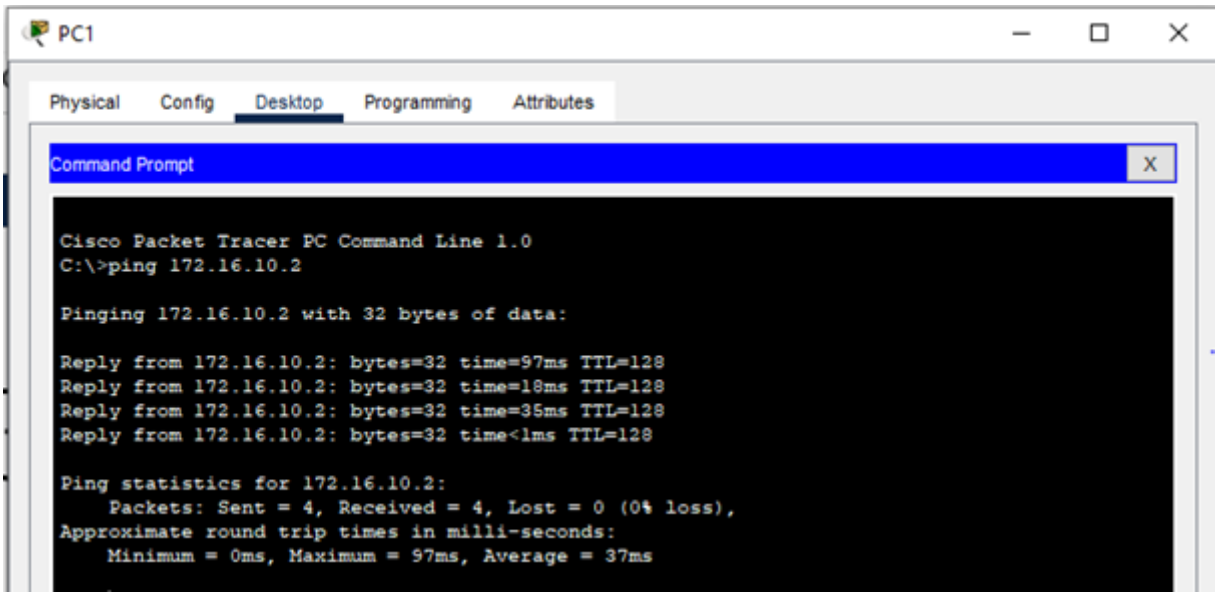

Figure 3.39 – ping entre PCs du VLAN10.

- ping entre PC4 et PC5 :

  PC4 ping avec le PC5 du même VLAN qui est 30 :

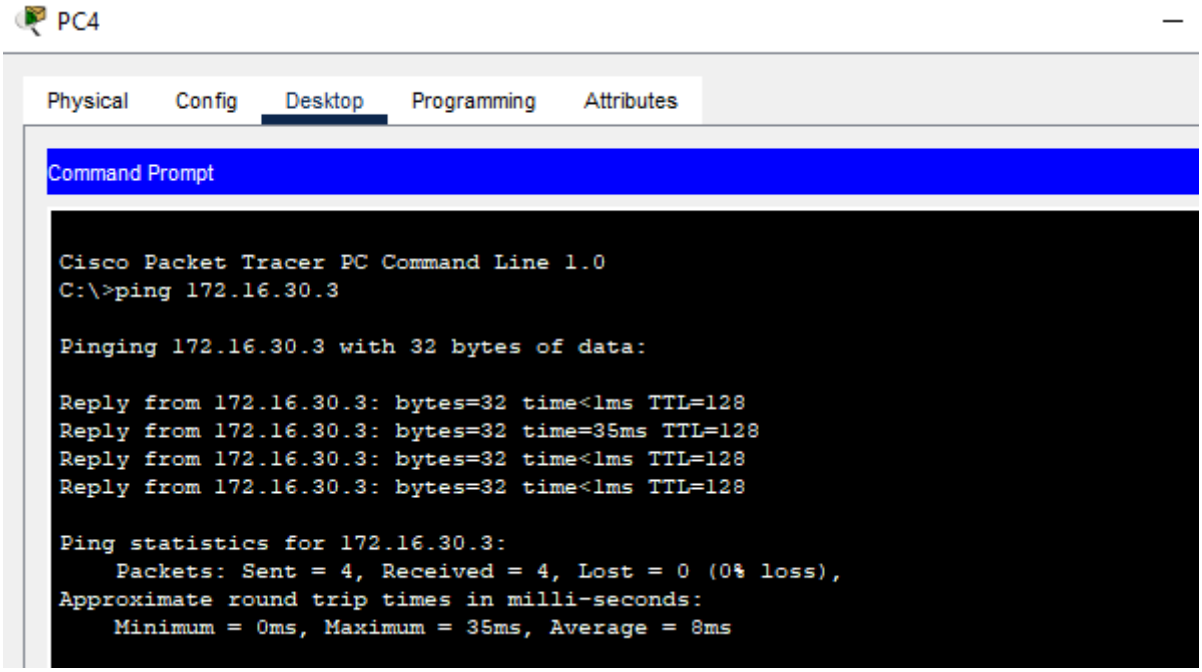

Figure 3.40 – ping entre PCs du VLAN30.

3.2.6.2 Test de connectivité entre les PCs des différents VLANs

On teste la connectivité entre le PC0 qui se trouve dans le VLAN 10 avec tous les autres VLANs qui restent.

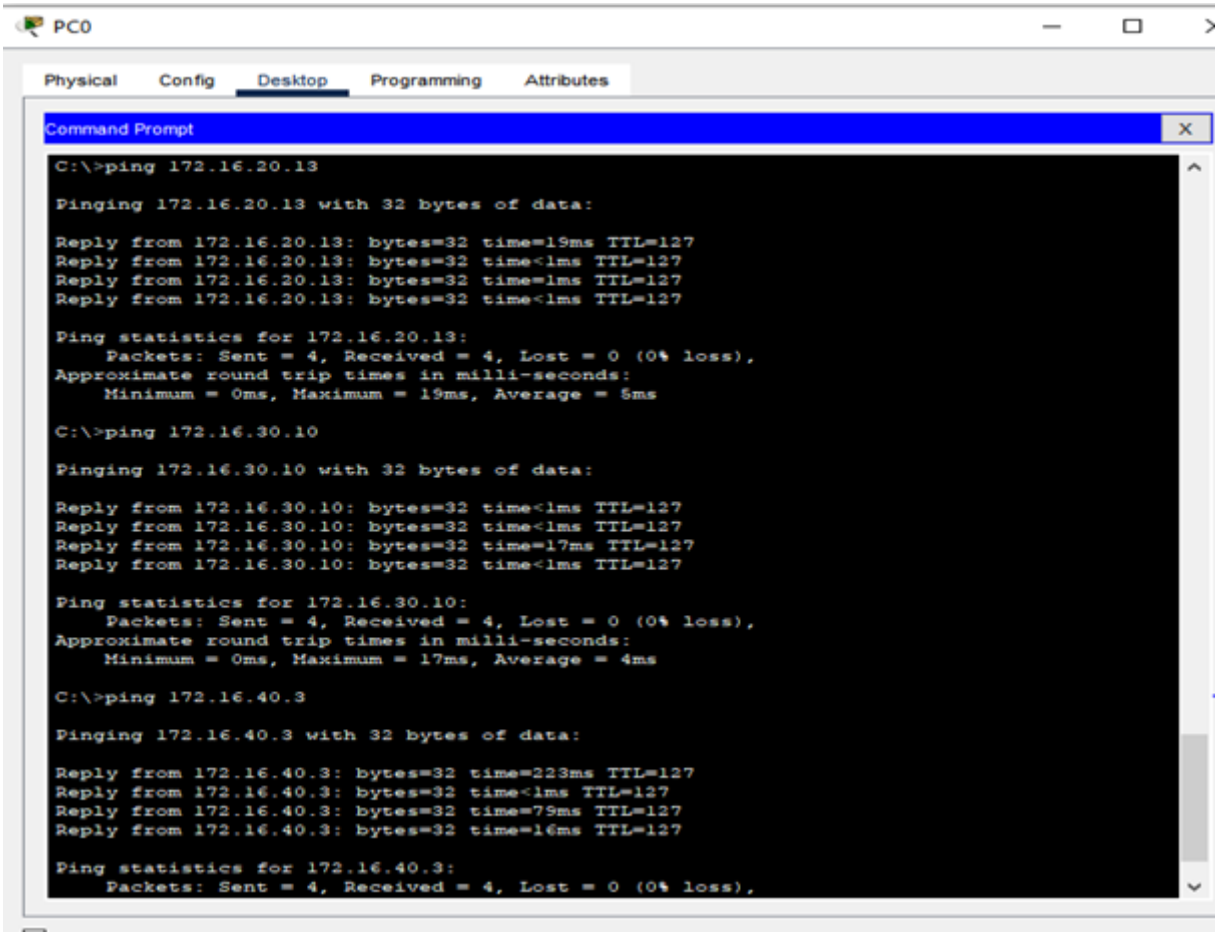

Figure 3.41 – ping entre PC du VLAN 10 et PCs des VLANs 20-30-40.

3.2.6.3 Test de connectivité entre un PC de LAN et un PC de secours

Le PC0 de vlan 10 au niveau de LAN ping avec le PC12 de vlan 70 au niveau de la topologie de secours

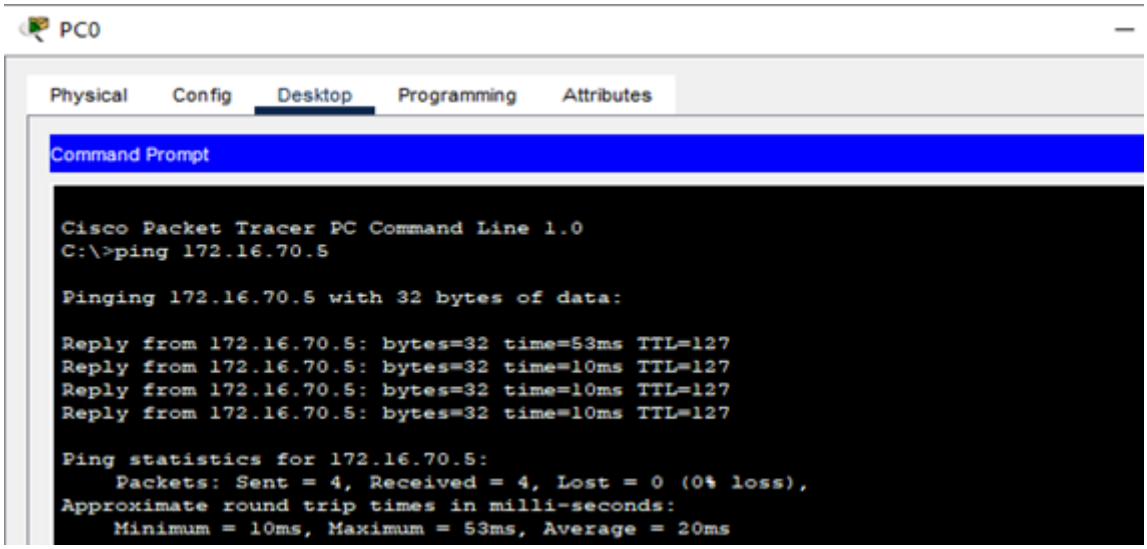

Figure 3.42 – ping entre un PC LAN et un PC de secours.

3.2.6.4 Test le bon fonctionnement de HSRP

Dans cette partie, nous avons simulé une panne et désactivé les interfaces principales et vérifié si les VLANs de secours, 70 et 80, prennent le relais sans interruption. Ce test confirme la redondance et l'efficacité de notre configuration HSRP pour assurer la continuité des services critiques en cas de défaillance.

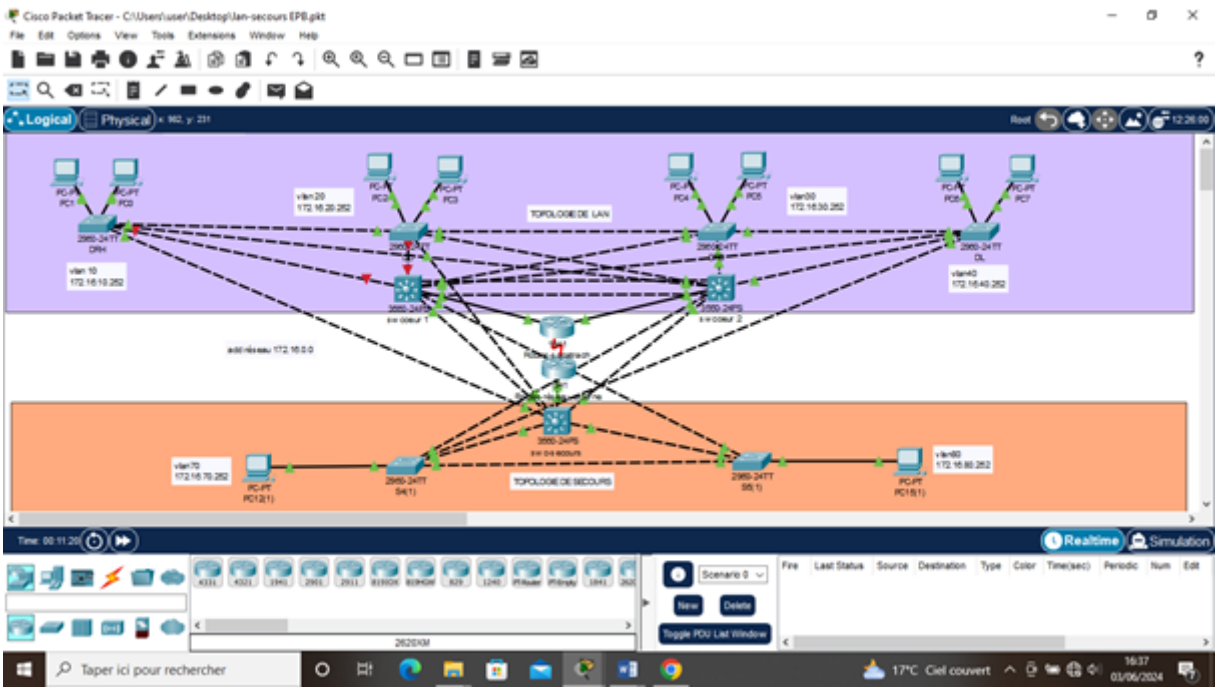

Figure 3.43 – Création d'une panne au niveau de LAN.

Cette figure montre que le ping envoyé en continu, démontre la connectivité entre le réseau LAN et la topologie de secours grâce au protocole HSRP. Lorsqu'une panne survient sur l'interface du VLAN 10, la connectivité s'interrompt brièvement. Après quelques secondes, le switch principal communique avec le switch de secours pour activer la route secondaire, et le ping reprend normalement. De même, en cas de panne sur l'interface du VLAN 20, le VLAN 80, situé sur la topologie de secours, assure la continuité.

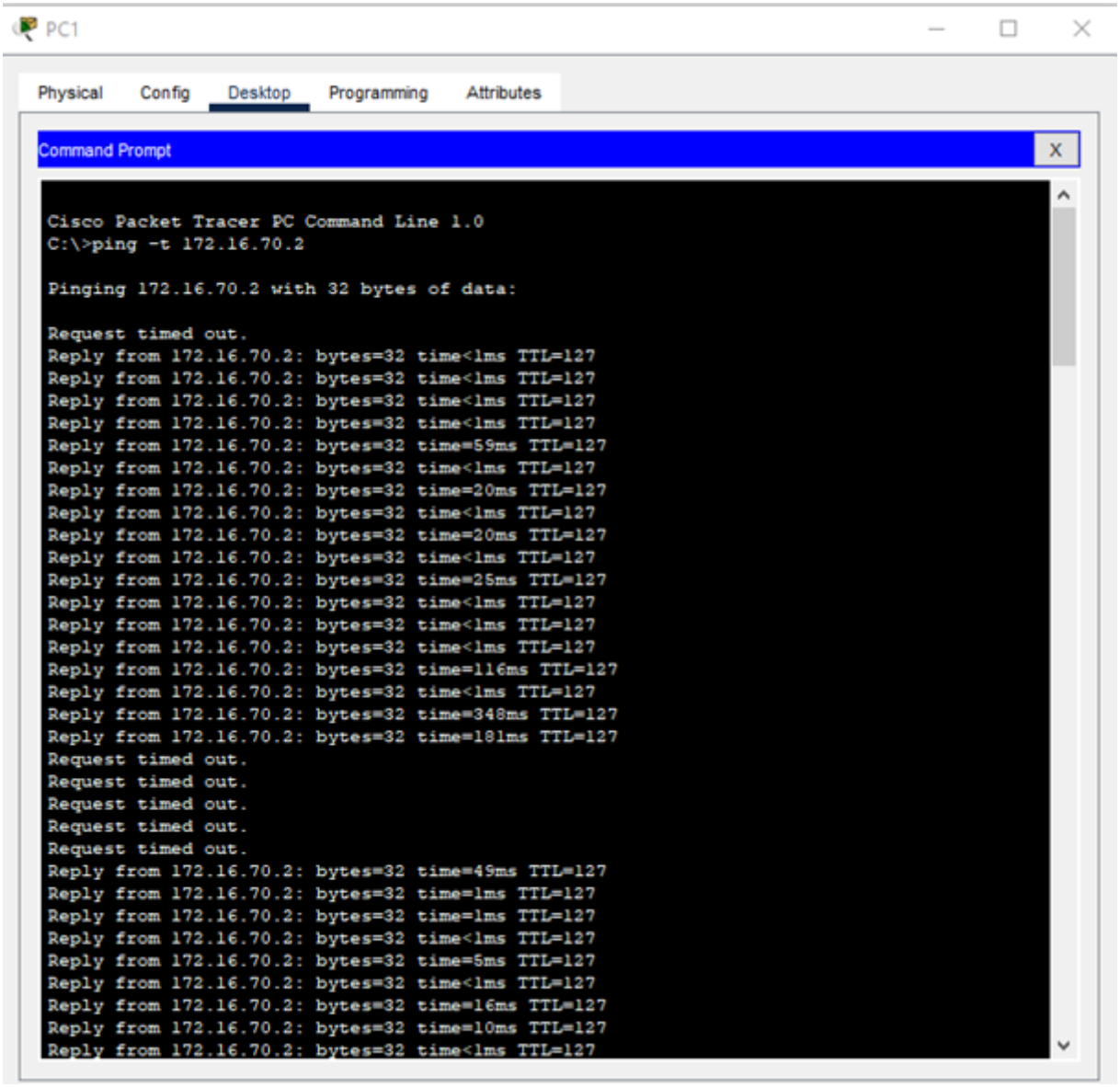

Figure 3.44 – Test sur le fonctionnement de HSRP entre les deux réseaux (LAN-secours).

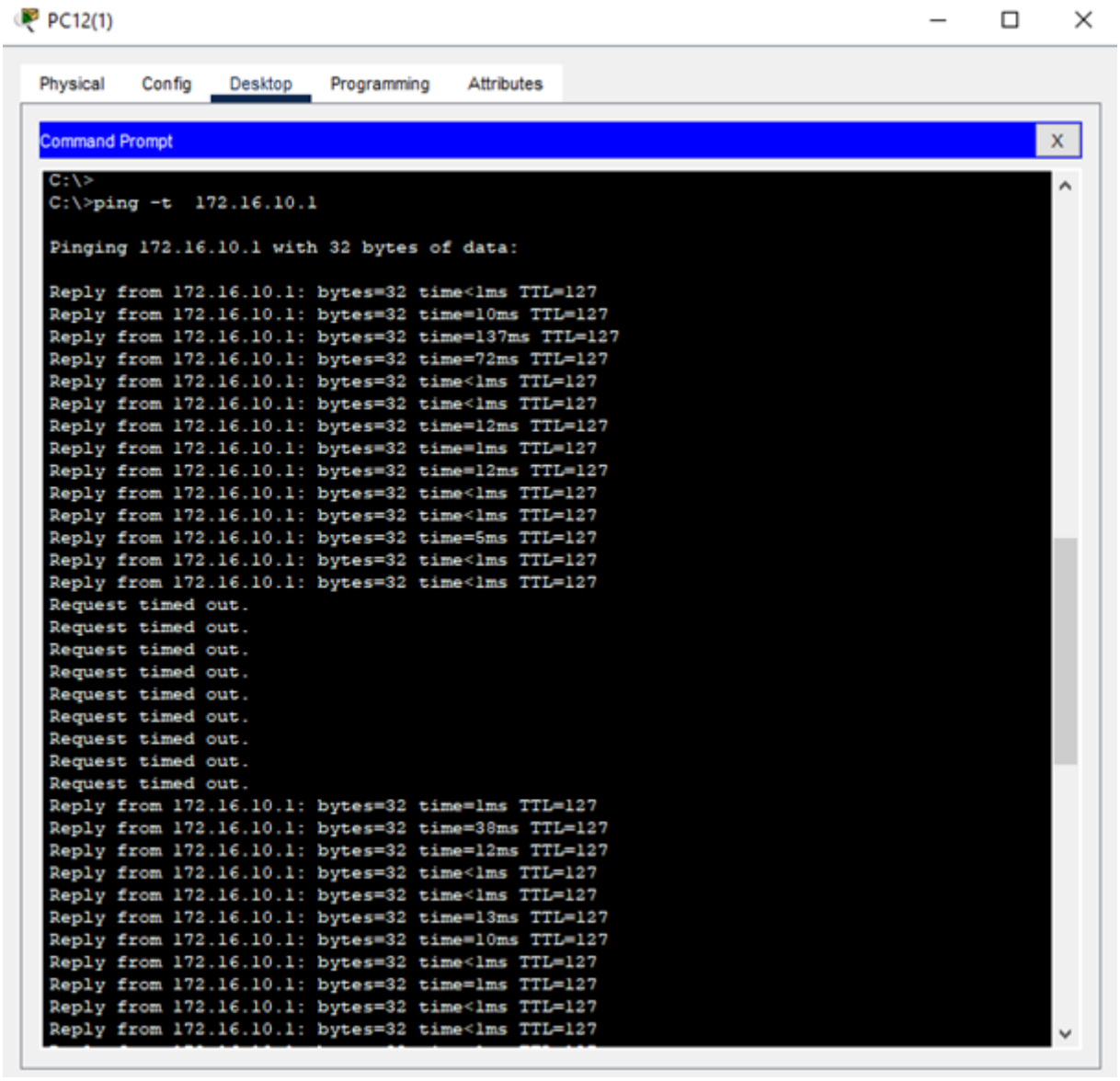

Figure 3.45 – Test sur le fonctionnement de HSRP entre les deux réseaux (secours-LAN).

3.2.7 Discussion

Avec la mise en place de la topologie de secours ainsi que la configuration des équipements avec des protocoles de redondance, l'EPB garantira la continuité de ses opérations. La topologie de secours utilise des chemins redondants pour équilibrer la charge réseau et pour permettre une reprise immédiate en cas de panne.

L'intégration de HSRP assure une redondance des routeurs où un routeur de secours prend automatiquement le relai sans interruption de service.

Cette configuration garantit que le réseau reste opérationnel même en situation de crise, démontrant ainsi son efficacité et sa robustesse.

Conclusion

Dans ce chapitre, nous avons présenté l'entreprise, ses activités et décrit une initiative de mise en place d'un PCA au seins de l'EPB suivant les concepts théoriques tels que la sensibilisation et la formation, le BIA et l'identification des risques.

Ensuite, nous avons mis en place une architecture de secours pour le réseau LAN de l'EPB en configurant des protocoles comme HSRP, STP, et EtherChannel, ainsi que des VLAN de secours pour les logiciels critiques. Cette configuration assure la haute disponibilité et la continuité des activités de l'EPB en cas de défaillances majeures. Les tests de validation ont confirmé l'efficacité de cette architecture pour garantir la résilience des systèmes informatiques de l'entreprise.

Conclusion générale

L'objectif de ce mémoire a été d'explorer la mise en place d'un Plan de Continuité d'Activité (PCA) pour l'entreprise portuaire de Béjaïa (EPB), en mettant particulièrement l'accent sur la résilience des systèmes informatiques .

À travers la conception et la configuration d'une architecture de secours, nous avons intégré des protocoles de redondance tels que HSRP, STP et EtherChannel, et mis en place des VLAN de secours pour les logiciels critiques. Cette architecture a été conçue pour maintenir les opérations essentielles de l'EPB même en cas de défaillances majeures. En d'autres termes, la mise en place d'un PCA vise à garantir que, même face à des pannes matérielles, des attaques cybernétiques ou des catastrophes naturelles, les activités critiques de l'entreprise puissent continuer sans interruption significative.

Les tests effectués ont permis de valider l'efficacité de cette configuration en termes de haute disponibilité et de continuité des activités. Les résultats montrent que la topologie de secours et les protocoles de redondance mis en place sont capables de prendre le relais immédiatement en cas de défaillance des systèmes primaires.

Ce travail souligne que l'implémentation d'une architecture de secours ne se limite pas seulement à l'aspect technique, mais doit également inclure une formation adéquate du personnel, des procédures de maintenance régulières et une évaluation continue des risques. La pérennité des opérations critiques de l'EPB dépend de ces facteurs combinés, qui ensemble, assurent une réponse efficace et rapide en cas de crise.

Enfin, ce mémoire a démontré que la préparation proactive et la mise en place d'un PCA robuste sont essentielles pour la résilience et la continuité des opérations dans un environnement de plus en plus dépendant des technologies informatiques. La méthodologie et les solutions présentées peuvent servir de référence pour d'autres entreprises désireuses de renforcer leur propre PCA et de protéger leurs opérations critiques contre les diverses menaces.

Webographie

[W1] https ://www.ccohs.ca/publications/PDF/businesscontinuity.pdf [consulté le 20/03/2024].

[W2] https ://fr.smartsheet.com/content/writing-business-continuity-plan [consulté le 22/03/2024].

[W3] https ://www.cnpp.com/etre-accompagne/gestion-des-risques/le-plan-de-continuite-activites-veritable-outil-strategique-au-service-de-la-gestion-des-risques-et-des-crises [consulté le 25/03/2024].

[W4] https ://www.rubrik.com/fr/insights/rto-rpo-whats-the-difference# [consulté le 28/03/2024].

[W5] https ://www.federated.ca/wp-content/uploads/2020/03/3778-001-Business-Continuity-Planning-Guide-v07F.pdf [consulté le 29/03/2024].

[W6] https ://openclassrooms.com/fr/courses/6227526-mettez-en-place-un-plan-de-continuite-dactivite-pca [consulté le 02/04/2024].

[W7] https ://www.criseetresilience-magazine.com/ [consulté le 02/04/2024].

[W8] https ://www.migso-pcubed.com/fr/blog/gestion-des-risques/etapes-du-management-des-risques/ [consulté le 09/04/2024].

[W9] https ://www.cyberuniversity.com/post/systeme-informatique-definition-structure-et-classification [consulté le 09/04/2024].

[W10] https ://www.oracle.com/fr/security/#database-security [consulté le 13/04/2024].

[W11] https ://docplayer.fr/34585202-Faire-face-a-un-sinistre-informatique.html [consulté le 21/04/2024].

[W12] https ://www.ionos.fr/digitalguide/serveur/securite/redondance/ [consulté le 05/05/2024].

[W13] https ://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html [consulté le 05/05/2024].

[W14] https ://datascientest.com/vlan-tout-savoir [consulté le 09/05/2024].

[W15] https ://cr10.fr/le-protocole-vtp-tout-savoir-sur-le-virtual-trunk-protocol/ [consulté le 22/04/2024].

[W16] https ://www.cloudflare.com/fr-fr/learning/network-layer/what-is-routing/ [consulté le 28/05/2024].

[W17] https ://www.portdebejaia.dz [consulté le 01/06/2024].

Bibliographie

[1] Bennasar, Matthieu. Plan de continuité d'activité et système d'information-2e éd. : Vers l'entreprise résiliente. Dunod, 2010.

[2] BERKANI Djedjiga et BOUZERIA Massylia(2022). Etude et mise en place d'une infrastructure réseau sécurisée (mémoire de master). Université de Bejaia.

[3] Planché, A. & Del Duca, J. La sécurité informatique en mode projet : Organisez la sécurité du SI de votre entreprise (2e édition). Nantes, France : Éditions ENI, 2017.

[4] Eddy Meylan, « Bases de données : Réplication des données » Support de cours. Haute Ecole spécialisée de Suisse Occidentale, Informatique de Gestion, (Février 2005).

[5] BENLALA Riane et BELHADDAD Sara(2023). Mise en place d'un réseau LAN/WAN redondant (Haute disponibilité) - Cas CEVITAL. (Mémoire de Master). Université de Bejaia.

[6] Li, T., Cole, B., Morton, P., & Li, D. (1998). Cisco hot standby router protocol (HSRP) (No. rfc2281).

[7] OUCHIHA Asma et MERSEL Nadjet(2023). Étude et mise en place de protocoles de haute disponibilité HSRP et GLBP-cas CEVITAL. (Mémoire de master). Université de Béjaia.

[8] Noida and U.Pradesh. Review of first hop redundancy protocol and their functionalities, International Journal of Engineering Trends and Technology (IJETT), 4, 2013.

[9] Zhang, M., Wen, H., & Hu, J. (2016). Spanning tree protocol (STP) application of the inter-chassis communication protocol (ICCP) (No. rfc7727).

[10] Savage, D., Ng, J., Moore, S., Slice, D., Paluch, P., & White, R. Cisco's enhanced interior gateway routing protocol (EIGRP) (No. rfc7868), 2016.

[11] Brochure-epb

[12] kaddouh Adada et Belhocine Faycal(2021). Mise en place d'un Serveur d'authentification RADIUS Sous Gns3 Cas-EPB. (Mémoire de master). Université de Bejaïa.

Résumé

Ce mémoire aborde le thème de l'élaboration d'un plan de continuité d'activité (PCA) visant à assurer la résilience des systèmes informatiques de l'entreprise portuaire de Bejaia l'EPB. Le PCA permet de garantir la continuité des opérations, de minimiser les interruptions coûteuses et de fournir une expérience utilisateur fiable.

L'étude propose de créer une topologie de secours pour la topologie principale, en configurant sur les équipements des protocoles de redondance tels que HSRP et STP. Cette solution vise à assurer la continuité des opérations de l'entreprise, dont les activités se basent principalement sur des logiciels critiques. À l'aide du simulateur Packet Tracer, une architecture hiérarchique interconnectant différents VLANs a été développée pour garantir la haute disponibilité. Cette architecture permet de maintenir une communication fluide entre les stations, même en cas de défaillance d'un équipement, grâce à la redondance intégrée. La simulation démontre comment un PCA efficace peut être mis en œuvre pour garantir la continuité des services informatiques dans un environnement d'entreprise.

Mots clés : PCA, LAN, topologie de secours, HSRP.

Abstract

This thesis addresses the theme of the development of a business continuity plan (PCA) to ensure the resilience of the computer systems of the port company of Bejaia the EPB.PCA ensures business continuity, minimizes costly downtime and provides a reliable user experience.

The study proposes to create a backup topology for the main topology, by configuring redundancy protocols such as HSRP and STP on the equipment. This solution aims to ensure the continuity of the company's operations, whose activities are based mainly on critical software. Using the Packet Tracer simulator, a hierarchical architecture interconnecting different VLANs was developed to ensure high availability. This architecture allows seamless communication between stations, even in the event of equipment failure, thanks to built-in redundancy. The simulation demonstrates how effective BCP can be implemented to ensure continuity of IT services in an enterprise environment.

Keywords : PCA, LAN, emergency topology, HSRP.