République Algérienne Démocratique et Populaire

Ministère de l'enseignement Supérieure et de la Recherche Scientifique

Université Abderrahmane Mira, Bejaïa

Faculté des Sciences Exactes

Département d'Informatique

Mémoire De Fin d'Etude

En vue de l'obtention du diplôme de master professionnel en Informatique

Spécialité : Administration et Sécurité des Réseaux informatique

Thème

La Haute Disponibilité des Réseaux (HSRP)

Cas d'étude : Réseau LAN de CEVITAL Agro-industrie

Au sein du groupe CIVITAL

Réalisé par

Mlle KEMACHA Habiba & Mlle ALOUACHE Lynda

Soutenu le : 27 septembre 2022 devant le jury composé de :

Examinateur1	Dr K .AMROUN	U.A/Mira Bejaïa
Examinateur2	N.BATTAT	U.A/Mira Bejaïa
Encadreur	S.TIGHIDET & M.YAICI	U.A/Mira Bejaïa

Promotion 2021/2022

AVANT PROPOS

Le mémoire de fin d'étude est un prolongement naturel de l'immersion de l'étudiant dans le monde professionnel, qui comme de coutume, permet à celui-ci de couronner sa dernière année universitaire. Il met en exergue les qualités de réflexion de l'étudiant se souligne ses aptitudes d'analyse global à partir d'une expérience professionnelle.

La réalisation de ce mémoire répond à l'obligation pour tout étudiant en dernière année du cycle master administration et sécurité réseau de département d'informatique de l'université Abderrahmane MIRA de Bejaia de présenter un projet de fin d'étude en vue la validation de l'année académique.

Ce mémoire rend compte simultanément de la découverte du milieu professionnel et de la conduite d'une mission attribuée à l'étudiant.

Le thème sue lequel s'appuie ce document est **« la Haute Disponibilité des Réseaux (HSRP) cas d'étude Réseau Lan de Cevital Agro-industrie »**. Le choix de ce thème se justifie dans l'obligation d'avoir un réseau hautement disponible et continue en tous temps pour les entreprises.

REMERCIEMENTS

Pour commencer, nous remercions avant toute chose dieu le tout puissant de nous avoir donné la force, le courage et la patience pour réaliser ce modeste travail.

La réalisation de ce mémoire a été un parcours jalonné de nombreuses rencontres, sans lesquelles ce travail n'aurait pas pu aboutir. On n'aurait pas éprouvé autant de plaisir à réaliser ce travail sans ces personnes, qui par leur générosité, leur disponibilité, leur bonne humeur et l'intérêt manifesté à l'égard de notre recherche, ont grandement contribué à l'amélioration de notre travail.

Nous tenons à remercier notre encadreurs madame ALOUI SORYA et madame YAICI MALIKA d'avoir accepté de nous encadrer et de nous avoir orienté durant l'élaboration de ce travail.

Un grand merci pour l'organisme d'accueil de " Cevital " et on tient particulièrement à adresser nos remerciements pour Monsieur ARAB YOUNES et NORDDINE BENOUARET pour toute l'aide qu'ils ont pu nous procuré, et pour la transmission de son savoir-faire qui nous a était d'une aide précieuse.

Nous adressons, également, à remercier les membres du jury qui nous font honneur par leurs présences en acceptant d'évaluer notre modeste travail

Habiba & Lynda

Dédicace

Je dédie ce modeste travail :

A mes chers parents en témoignage de ma profonde affection, qui ont été souvent à mes côtés et le grand mérite revient à eux, ils m'ont ouvert les yeux et sans eux je ne serai jamais arrivé jusque-là

A mes deux chers frères Massinissa, Hani.

A mes chers sœurs Assia, Lamia, Hanane

A mes adorables neveux Dylan, Ilyas, Islam, Ayan, Nazim, Racim

A mes trésors nièces Liliane, Ilina

A mes grandes mères Zahra, Zineb

A ma précieuse binôme Lynda et sa famille

A tous mes amis et camarades

A ceux et celles QUI ont contribué de près ou de loin à la réalisation de ce travail.

A toute la famille KEMACHA

KEMACHA HABIBA

Dédicace

Je dédie ce modeste travail :

A mes chers parents en témoignage de ma profonde affection, qui ont été souvent à mes côtés et le grand mérite revient à eux, ils m'ont ouvert les yeux et sans eux je ne serai jamais arrivé jusque-là

A mes deux chers frères Lyes, Karim.

A ma chère sœur Asma.

A mes chers grands parents Larbi, Ouardia.

A ma chère adorable tante Djohra

A mes chers oncles Yacine, Toufik, Rafik, Lamine.

A mon cher mari Abdenour

A ma précieuse binôme Habiba et sa famille

A tous mes amis et camarades

A ceux et celles QUI ont contribué de près ou de loin à la réalisation de ce travail.

A toute la famille Alouache

ALOUACHE LYNDA

Table Des Matières

Chapitre 2 : La Haute Disponibilité d'un Réseau Informatique

Chapitre 03 : Conception et Réalisation

Table Des Figures

Liste Des Tableaux

Liste Des Abréviations

APPRO	**A**pprovisionnement
BPDU	**B**ridge **P**rotocol **D**ata **U**nit
Cdt	**C**onditionnement
CLI	**C**ommand **L**ine **I**nterface
DFC	**D**irection des **F**inances et de **C**omptabilité
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
DMZ	**D**e**M**ilitarized **Z**one
DNS	**D**omain **N**ame **S**ystem
DQMS	**D**irection **Q**ualité et **M**anagement **S**ystème
DRH	**D**irection des **R**essources **H**umaines
DSI	**D**irection des **S**ystèmes d'**I**nformation
EIGRP	**E**nhanced **I**nterior **G**ateway **R**outing **P**rotocol
GLBP	**G**ateway **L**oad **B**alancing **P**rotocol
GMAO	**G**estion de la **M**aintenance **A**ssistée par **O**rdinateur
GPAO	**G**estion de la **P**roduction **A**ssistée par **O**rdinateur
GSA	**G**eneral **S**ervices **A**dministration
HSE	**H**ygiène, **S**écurité et **E**nvironnement
HSRP	**H**ot **S**tandby **R**outer **P**rotocol
ID	**ID**entificateur
IEEE	**I**nstitute of **E**lectric and **E**lectronic **E**ngeneer
IGRP	**I**nterior **G**ateway **R**outing **P**rotocol
IT	**I**nformation **T**echnology
IP	**I**nternet **P**rotocol
LACP	**L**ink **A**ggregation **C**ontrol **P**rotocol

LAN	**L**ocal **A**rea **N**etwork
LLK	**L**a **L**a **K**hedija
MFG	**M**editerranean **F**loat **G**lass
MAC	**M**edia **A**ccess **C**ontrol
NAT	**N**etwork **A**ddress **T**ranslation
OSI	**O**pen **S**ystems **I**nterconnection
OSPF	**O**pen **S**hortest **P**ath **F**irst.
PAgP	**P**ort **A**ggregation **P**rotocol
PC	**P**ersonal **C**omputer
RJ45	**R**egistered **J**ack 45
RH	**R**essources **H**umaines
RIP	**R**outing **I**nformation **P**rotocol.
RPO	**R**ecovery **P**oint **O**bjectives
RTO	**R**ecovery **T**ime **O**bjective
RSI	**R**esponsable **S**ystèm**e** d'**I**nformation
SI	**S**ystème d'**I**nformation
SPA	**S**ociété **P**ar **A**ction
SSH	**S**ecure **SH**ell
STP	**S**panning **T**ree **P**rotocol
SVI	**S**witch **V**irtual **I**nterface
TCP	**T**ransmission **C**ontrol **P**rotocol
TTL	**T**ime **T**o **L**ive
UDP	**U**ser **D**atagram **P**rotocol
VLAN	**V**irtual **L**ocal **A**rea **N**etwork
VPN	**V**irtual **P**rivate **N**etwork
VRRP	**V**irtual **R**outer **R**edundancy **P**rotocol
VSAT	**V**ery **S**mall **A**perture **T**erminal**.**

VTP	**V**irtual **T**runking **P**rotocol
WAN	**W**ide **A**rea **N**etwork
WIFI	**WI**reless **FI**delity

Introduction générale

L'humanité a toujours su se développer au fils de temps, parmi l'un des basiques points de ce développement est la communication entre les être-humains.

Avec l'évolution de la technologie apparait la science de traitement de l'information basée sur les ordinateurs. C'est après cela que l'homme a su que c'était nécessaire de faire une communication entre les ordinateurs et d'être capable d'échanger des données et des ressources. Afin d'aboutir à ce but il a dû les relier entre eux, c'est ainsi qui venu l'idée et le concept des réseaux informatiques.

Au sein de toute entreprise il existe l'évidence d'avoir un réseau informatique. Ce dernier dépondra donc de la taille de ces entreprises et de leurs besoins pour leur permettre d'effectuer le partage des ressources et des données en les centralisant, ainsi que d'avoir une plateforme de travail collaboratif.

L'infrastructure réseau de l'entreprise joue un rôle important dans les développements de cette dernière. C'est pour cela qu'il est hautement indispensable d'avoir un bon degré de gestion, de sécurité mais surtout de continuité.

Cevital agro-industrie dispose d'un réseau local d'une taille importante auquel est ajouté des liaisons intersites du l'entreprise ainsi que l'accès à l'internet. Ceux qui rendent l'activité de son réseau informatique particulièrement haute mais surtout qui doit être en service en tout temps.

L'indisponibilité du réseau dû à un dysfonctionnement, ne serait-ce que pour quelque heure, mettrait l'entreprise dans une difficile position pour assumer les répercussions sur la productivité et par la même absorber les coûts financiers.

C'est dans cette initiative que vient l'obligation d'assurer et de garantir le bon fonctionnement de son réseau informatique en toute circonstance même dans le cas d'un dysfonctionnement ou d'une panne. Une question mérite d'être posé afin de remédier à ce problème, comment et avec quelle technologie pourrions-nous utiliser afin d'assurer la continuité de service et du fonctionnement optimale de réseau informatique de Cevital malgré la défaillance d'un ou plusieurs éléments matériels ou logiciels

Nous opterons pour une solution qui est d'utiliser une architecture hiérarchique redondante en utilisant le protocole HSRP (Hot Standby Router Protocol) afin de garantir la haute disponibilité.

Le présent mémoire comporte trois chapitres :

Le premier chapitre sera consacré à la présentation de l'organisme d'accueil (Direction de Systèmes d'information) et le contexte général du projet. Cependant nous critiquons le réseau LAN de « Cevital-Bejaia » tout en exposons la problématique de notre travail et quelques éventuelles solutions.

Au cours du deuxième chapitre, nous parlerons de la haute disponibilité ainsi quelques notions théoriques utiles pour une compréhension des éléments servant à résoudre notre problématique telle que HSRP, STP, VTP, Etherchannel.

Dans le dernier chapitre, nous abordons d'une part la conception du modèle dont la procédure de préparation, la schématisation, la nomination des équipements, la désignation des interfaces et les VLAN et d'autre part nous allons clôturer ce rapport par la réalisation de ce modèle type à travers le simulateur « Paquet Tracer », ainsi qu'un test pour validation de la configuration globale utilisé dans le souci de vérifier si vraiment les objectifs ont été atteints.

Nous allons conclure notre travail par une conclusion générale et quelques perspectives.

1 Chapitre 1 : Présentation De L'organisme D'accueil

1.1 Introduction

La clé de la réussite et de l'épanouissement de chaque entreprise est liée à son histoire, son organisation et aux différents acteurs qui la dirigent.

Dans ce chapitre nous allons présenter l'organisme d'accueil (Groupe CEVITAL), en citant les différents départements qui le constituent et donner quelques informations utiles dans notre travail, tout en posant la problématique autour de laquelle tournera notre mémoire.

1.2 Présentation de l'entreprise

Figure 1-1 : Logo CEVITAL **[1].**

Cevital agro-industrie est une des filiales du groupe Cevital, elle fait partie des entreprises algériennes qui ont vu le jour dès l'entrée de notre pays en économie de marché. Cevital est la troisième plus grande entreprise algérienne après Sonatrach et Naftal.

CEVITAL Agro-industrie offre des produits de qualité supérieure à des prix compétitifs, grâce à son savoir-faire, ses unités de production ultramodernes, son contrôle strict de qualité et son réseau de distribution. Elle couvre les besoins nationaux et a permis de faire passer l'Algérie du stade d'importateur à celui d'exportateur pour les huiles, les margarines et le sucre. Ses produits se vendent aujourd'hui dans plusieurs pays, notamment en Europe, au Moyen Orient et en Afrique de l'Ouest **[2].**

1.3 Historique et Evolution du Groupe CEVITAL

CEVITAL est un Groupe familial qui s'est bâti sur une histoire, un parcours et des valeurs qui ont fait sa réussite et sa renommée, c'est la première entreprise privée algérienne à avoir investi dans des secteurs d'activités diversifiés.

Le groupe CEVITAL s'est construit, au fil des investissements, autour de l'idée forte de constituer un ensemble économique. Ses produits se vendent aujourd'hui dans plusieurs pays, notamment en Europe, au Maghreb, au Moyen Orient et en Afrique de l'Ouest.

Aujourd'hui, CEVITAL agroalimentaire est le plus grand complexe privé en Algérie. Il est devenu le leader du secteur agroalimentaire en Afrique. CEVITAL a traversé d'importantes étapes historiques pour atteindre sa taille et sa notoriété actuelle. Ci-après, quelques dates qui ont marqué l'histoire de CEVITAL **[3].**

- **1975 :**
  Lancement dans la construction métallique
- **1986 :**
  Création de METAL SIDER (sidérurgie).
- **1991 :**
  Création du quotidien d'information liberté
- **1997 :**
  Création de Hyundai MOTORS ALGERIE : représentant officiel de Hyundai MOTOR COMPANY (Corée du sud).
- **1998 :**
  Création de CEVITAL SPA industries agro-alimentaires.
- **2006 :**
  Acquisition de COJEK, filiale d'ENAJUC : Jus et conserves.
  Création de NUMIDIS-UNO (GSA).
- **2007 :**
  Création de MFG (verre plat).
  Création de SAMHA : Assemblage et distribution de produits électroniques et électroménagers de marque SAMSUNG Électroniques en Algérie.
- **2008 :**
  Création de MFG Europe : Commercialisation de verre plat en Europe.
  Création de GOGETP : Engins de travaux publics VOLVO.
  Création de NUMILOG : Entreprise spécialisée dans logistique et la gestion de la chaîne logistique.
- **2010 :**
  Démarrage de l'exportation du sucre en Europe.
- **2013 :**
  CEVITAL rachète le Français OXXO, spécialisée dans la menuiserie PVC.
  Investi dans ALAS (Espagne) : Usine d'aluminium.
- **2014** :
  CEVITAL reprend les activités françaises du groupe FAGOR-Brandt : électroménager français. Investi dans AFFERPI (Italie) : usine de métal.
- **2014 → aujourd'hui**
  Le groupe a su marquer sa présence sur les trois continents (Afrique, Europe et Amérique latine) avec un volume d'export parmi les plus élevés en Algérie et en se positionnant parmi les fournisseurs majeurs des marchés européens, de l'Amérique
  Latine ainsi que les pays du Moyen-Orient. Aujourd'hui, le groupe CEVITAL réalise un chiffre d'affaire de 4 Milliards de dollars et vise à atteindre 25 Milliards de dollars à l'horizon 2025. Cette évolution est le résultat d'une vision moderne, ambitieuse et stratégiquement cohérente avec l'économie algérienne et internationale **[1].**

1.4 Valeurs du Groupe CEVITAL

Les quatre règles d'or (IRIS) à respecter **[4]** :

- **Initiative :** Le collaborateur anticipe les problèmes potentiels, et propose des solutions innovantes grâce à sa connaissance métier.
- **Respect :** Un principe prime entre collaborateurs, et avec les partenaires internes et externes.
- **Intégrité :** Une valeur fondamentale, les collaborateurs par leurs actes doivent adopter une éthique professionnelle irréprochable.
- **Solidarité :** Les collaborateurs doivent s'entraider mutuellement, et partager leur expérience et savoir.

1.5 Infrastructure de l'entreprise

CEVITAL Agro-industrie dispose de plusieurs unités de production ultramodernes se présente comme suit **[2]** :

- Deux raffineries de sucre.
- Une unité de sucre liquide.
- Une raffinerie d'huile.
- Une margarinerie.
- Une unité de conditionnement d'eau minérale (se situe à Tizi-Ouzou).
- Une unité de fabrication et de conditionnement de boissons rafraîchissantes (site EL-Kseur).
- Une conserverie.
- Silos portuaires.

1.6 Situation géographique

Le complexe CEVITAL agro-industrie s'étends sur une superficie de 45 000 M^2 (c'est le plus grand complexe privé en Algérie), il se situe au niveau du nouveau quai du port de Bejaia, à proximité de la route nationale N° 09 et N°26 ; Sur un terrain à l'origine inconstructible qui a été récupéré et viabilisé avec la dernière technologie de consolidation des sols par le système de colonnes ballastées (337 km de colonnes ballastées de 18M chacune ont été réalisées) ainsi qu'une partie à gagner sur la mer. L'entreprise a beaucoup profité de cette situation qui lui donne un avantage de proximité économique car se trouve proche du port et de l'aéroport.

Figure 1-2 : Vue satellitaire du complexe CEVITAL **[5].**

1.7 Organigramme de CEVITAL

L'organigramme suivant donne une vue générale sur les différents organes constituants le complexe CEVITAL .Il est composé de neuf directions principales dont le but de chaque direction est d'assurer le bon fonctionnement de ses tâches comme la figure suivante (figure 1-3) le montre :

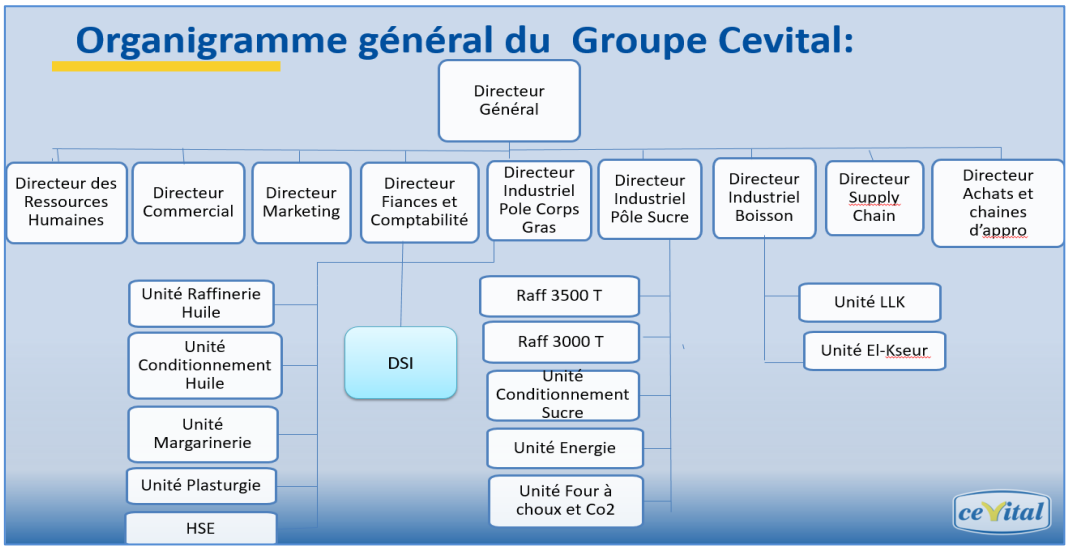


Figure 1-3 : Organigramme du Groupe CEVITAL **[6].**

1.8 Présentation du service informatique

Nous avons effectué notre stage au niveau de département Réseau et Télécom de la direction des systèmes d'information (DSI),cette dernière assure la mise en œuvre des moyens et des technologies de l'information nécessaire pour améliorer l'activité ,la stratégie et la performance de l'entreprise ,elle doit ainsi veiller à la cohérence des moyens informatiques et de la communication mises à la disposition des utilisateurs ,à leur maîtrise technique et à leur disponibilité et opérationnalité permanentes et ceux en toute sécurité . La figure ci-dessous (figure 1-4) montre l'organigramme du système d'information.

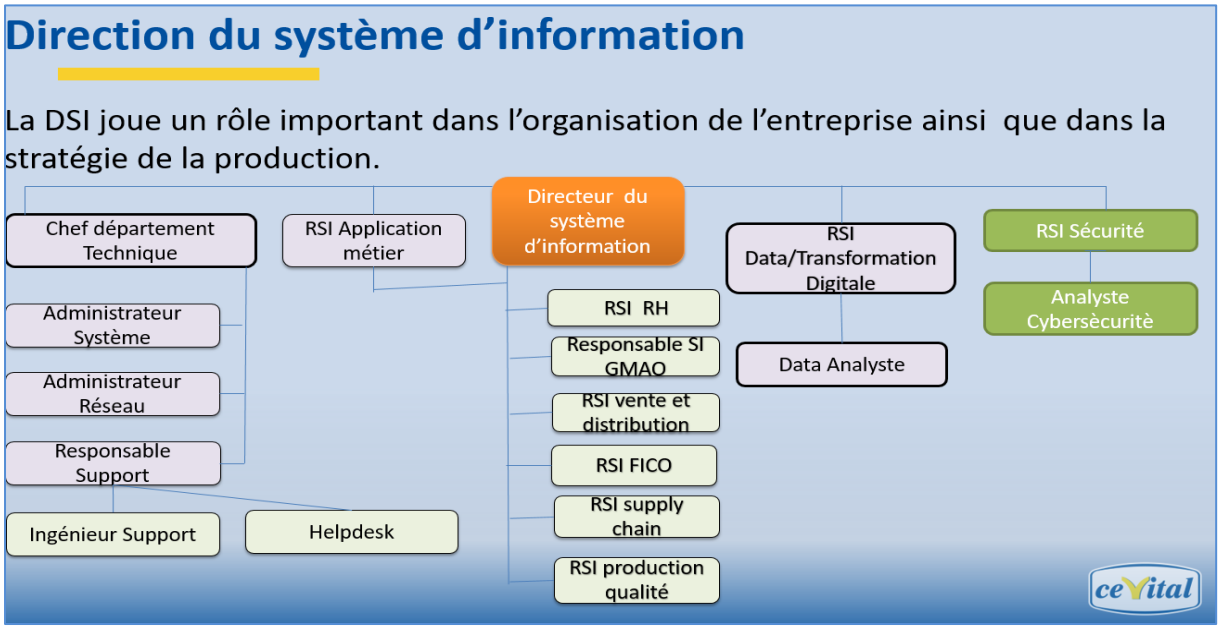


Figure 1-4 : Organigramme de la direction système d'information **[6].**

Le service informatique est suivi par des responsables spécialistes cités ci-dessous :

- **Directeur du système d'information :**

Il est chargé pour régler les problèmes à moindre coût et dans les plus brefs délais et opter des solutions informatiques améliorant la productivité de l'entreprise.

- **Administrateur système :**

Il conçoit, installe et veille au bon fonctionnement d'une infrastructure informatique et réseau d'une entreprise, il assume également la gestion et la maintenance de système opérant sur le rése²au

- **Administrateur réseau :**

Il permet d'administrer le réseau et d'assurer la bonne circulation de l'information dans l'entreprise en veillant à la qualité, continuité et la performance des équipements et du réseau, tous en répondant aux besoins des utilisateurs.

- **Responsable support :**

Il permet d'assurer un contrôle à distance des postes, apporter aux utilisateurs une aide pour la prise en main de leur équipement et assurer un support téléphonique interne.

1.9 Matériels utilisé dans l'architecture réseau

Le réseau est composé de plusieurs dispositifs dont la plupart sont de marque Cisco (Switch Catalyst, Routeur) interconnectés entre eux grâce à la fibre optique, ou paire de cuivre torsadée.

- **Distributeur (Backbone) de type Cisco Catalyst 4507R**

Il supporte le trafic de données le plus important du réseau CEVITAL avec une bande passante très large, sur lequel les commutateurs d'accès, le pare-feu, serveurs et routeurs de l'entreprise y sont connectés. Il s'occupe du routage inter-Vlan (Virtuel Lan). Il permet l'accès à internet via le pare-feu et c'est généralement un serveur DHCP. Il est appelé aussi un switch fédérateur.

Figure 1-5: Switch Distributeur Cisco Catalyst 4507R **[7].**

- **Switch d'accès et en cascade de type Cisco Catalyst 2960 et 2950**

Ils sont connectés au backbone et installés dans les différents bâtiments de l'entreprise.

Figure 1-6 : Switch Cisco Catalyst 2960 **[8].**

- **Routeur de type Cisco 2900 :**

Il permet de gérer le routage entre les différents sites de l'entreprise

Figure 1-7: Routeur Cisco 2900 **[9].**

- **Point d'accès WIFI :**

L'entreprise dispose de plusieurs points d'accès WIFI, créant ainsi une couverture réseau sans fil au niveau de certaines parties du complexe.

Figure 1-8 : Point d'accès WIFI Cisco **[10].**

- **Pare feu :**

Deux pare-feux sont reliés en redondance et permettant de sécuriser le réseau, d'isoler certaines parties de celui-ci, encadre et sécurise l'accès internet.

Figure 1-9 : Pare feu Palo Alto **[11].**

- **Data center**

Le data center est une pièce sécurisée, l'accès est restreint, seul les responsables et les techniciens de la DSI (Direction Système d'Information) y ont accès. En outre, une climatisation des équipements est aussi assurée grâce au contrôle de la température par un système d'air conditionné avec une alimentation électrique doublée pour veiller à son fonctionnement sans coupure. En fait, le data-center de CEVITAL est le noyau central du réseau de l'entreprise où on y trouve les serveurs de l'entreprise, Backbones, les pare-feu, les routeurs et le standard téléphonique.

Figure 1-10 : Data Center **[12]** .

1.10 Architecture du réseau CEVITAL

Dans le souci de faciliter le partage d'information entre les différents bâtiments, unité et direction, un réseau informatique local a été installé. Cevital dispose d'un réseau interne assez vaste permettant de relier les différents bâtiments, unités de production et directions du complexe. Nous pouvons le décomposer en plusieurs parties : Le backbone du réseau, un pare-feu, un DMZ (zone démilitarisée), une couverture WIFI, un routeur, Switches et un Datacenter (où sont placés les serveurs de l'entreprise).

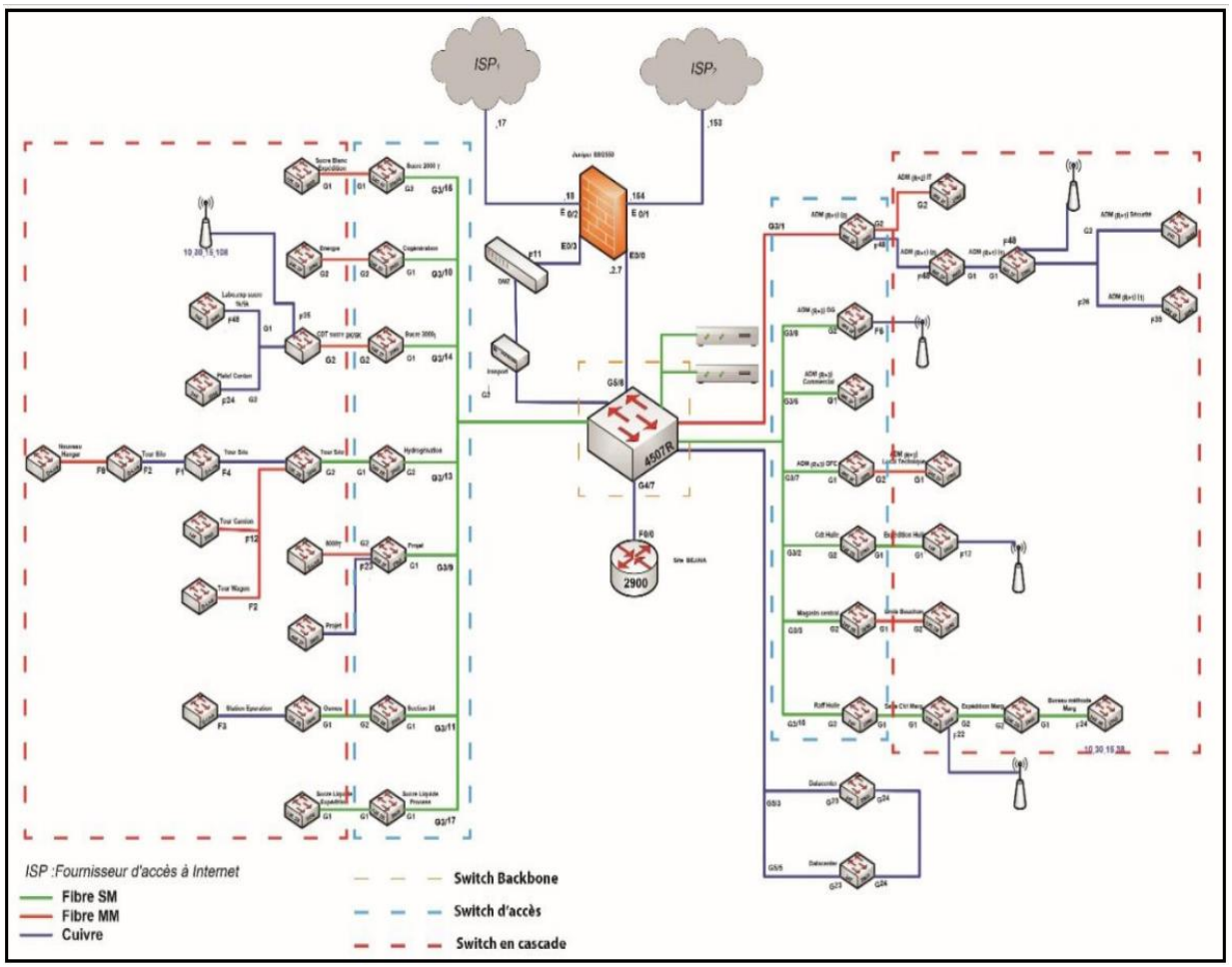


Figure 1-11 : Architecture du réseau informatique de CEVITAL **[6].**

Le réseau local de complexe se compose de trois couches, couche Core qui représente aussi la couche distribution (backbone), la couche accès et la couche en cascade.

- **Couche Core (Distribution) :**

  Le Backbone est composé d'un Switch Catalyst placé au data center du bâtiment, qui est relié aussi bien au pare feu et au routeur à l'aide des câble RJ45, qu'aux Switch d'accès à l'aide de la fibre optique offrant ainsi un meilleur débit aux différents postes. Cette partie est la plus sensible parce qu'elle est reliée à tous les équipements réseau.

- **Couche d'accès :**

  Cette couche se compose des switches qui sont distribués sur les différents sites locaux du bâtiment. Les responsables du réseau de CEVITAL utilisent des Vlans pour partager l'accès aux utilisateurs d'une façon que chaque site local (étage des bâtiments) comprend un ou plusieurs Vlans (plus de détails sur les Vlans sur l'Annexe **I**).

- **Couche en cascade :**

Dans cette couche les switches sont reliées entre eux et aux switches d'accès et fournissent un accès aux utilisateurs, au sein de ses switches des Vlans permettent de définir plusieurs sous-réseaux en fonctions des départements de l'entreprise.

1.11 Codification des équipements de CEVITAL

- CEVWKS 1XXX : Ordinateur de bureau
- CEVLAP 1XXX : Ordinateur portable
- CEVSRV 1XXX : Serveur
- CEVSWC 1XX : Switch
- CEVAP 1XXX : Point d'accès wifi
- CEVFW 1XXX : Pare feu
- CEVRTR 1XXX : Routeur

1.12 Environnement des logiciels de base

Les systèmes d'exploitation installés et les logiciels de base au niveau des différents postes de travail sont :

- Système d'exploitation (Microsoft office (2010), Windows Vista etc…).
- WinRAR.
- Firefox, Opera, IE.
- Norton Ghost 10.
- Adobe Acrobat, Foxit Reader.
- VMWare, Virtuel pc.

1.13 Câblage informatique

Le système de câblage informatique installé est conçu pour fonctionner de façon idéale pour permettre des améliorations futures. Tout dispositifs informatique existant dans l'entreprise sont interconnectés via le câblage de type fibre optique. Les boitiers des prises muraux sont repérés par des étiquettes portant un numéro unique sur le réseau et qui est repéré facilement dans le panneau de brassage pour l'interconnexion avec les commutateurs « prise Rj45 »

1.14 Utilisation du réseau informatique

CEVITAL compte environ mille utilisateurs du réseau informatique, ses différents collaborateurs utilisent chaque jour les différentes applications et services offerts par le réseau pour mener à bien leur travail. Nous pouvons citer les applications et services suivants :

- Applications de GPAO (Gestion de la production assistée par ordinateur).
- Le partage de document via un serveur dédié (cloud privé).
- Microsoft Exchange et Azure.
- Service Mail.
- Application comptabilité et gestion des stocks.
- Accès internet pour le collaborateur.

1.15 Liaison inter- sites (architectures WAN)

Afin de confirmer le partage des ressources et de la communication interne de l'entreprise, Cevital dispose des connexions qui permettent de relier le site Bejaïa aux différents annexes de l'entreprise tels que :

- Une liaison fibre optique point à point entre Bejaïa et Alger.
- Liaison par satellite (Vsat) entre Bejaïa et les sites d'El-kseur (Cojek), site de Tizi-Ouzou (Lala Khadija) et site El Kheroub (Constantine).

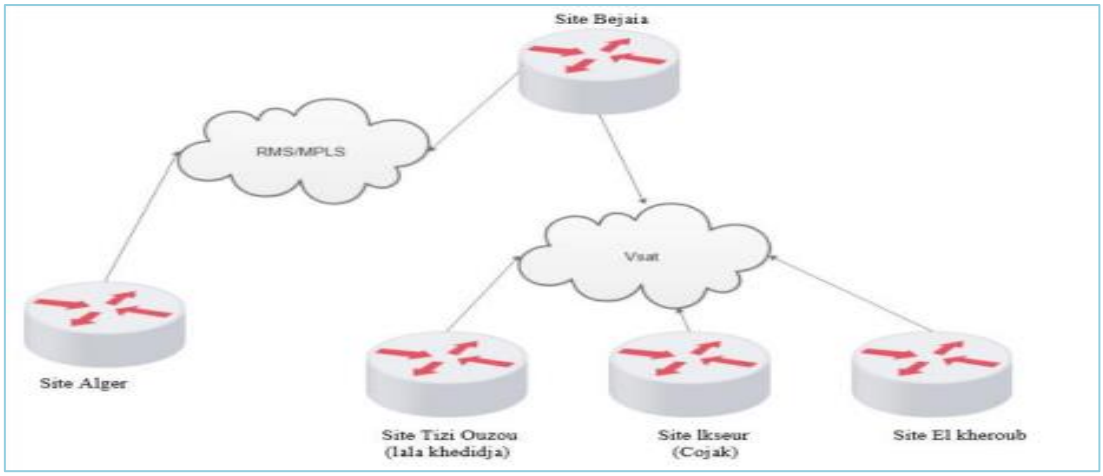


Figure 1-12 : Connexion inter sites du groupe CEVITAL **[6].**

1.16 Points forts du réseau

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

- Présence d'un firewall qui protège le réseau informatique interne de l'entreprise, analyse le trafic entrant en fonction de règles préétablies et filtre les données provenant de sources non sécurisées ou suspectes pour prévenir les attaques.
- Tenir compte de la protection contre les risques physiques (les dégâts d'eau, de feu ou d'électricité).
- Existence d'un système de gestion et de surveillance du réseau monitoring (recevoir des notifications en cas de panne du périphérique, et mettre des alertes par courrier électronique).

1.17 Critique du réseau

- Utilisation d'un seul domaine de diffusion ce qu'implique la surcharge de réseau.
- Une défaillance d'un des Switch raccordé au Switch cœur couperait du réseau à tous les utilisateurs qui sont connectés.
- La liaison des Switches en cascade limite la bande passante du réseau créant un ralentissement des applications et des ressources.
- Saturation de la bande passante diminue fortement les puissances de réseau et de son bon fonctionnement.
- Absence de serveurs en redondance pour assurer la tolérance aux pannes ainsi que la redondance des liens et des équipements causant ainsi des points de défaillance dans l'architecture de réseau.

1.18 Véritable problème

Il est fortement primordial d'assurer le bon fonctionnement et la continuité de réseau informatique de l'entreprise, car il est essentiel de collecter, stocker, traiter et communiquer les informations entre un grand nombre des collaborateurs répartis sur plusieurs sites. Dans le cas contraire cela entrainerai l'arrêt ou le ralentissement de son activité et nuit à la productivité de ces équipes.

L'infrastructure réseau de l'entreprise, c'est-à-dire l'ensemble des équipements interconnectés qui ont pour principale missions permettre l'échange, transport et la diffusion des différents flux de données, devient alors dominant pour Cevital, ceci dit, comment et avec quelle technologie pourrions-nous utilisés dans le souci de garantir la continuité des services et du fonctionnement optimal du réseau informatique malgré la défaillance d'un ou plusieurs éléments matérielles ou logicielles ?

1.19 Solutions

- Utilisation de plus de liens d'interconnexion entre les périphériques.
- Utilisation d'une redondance matérielle au niveau de la couche cœur et de la couche distribution afin de remédier aux pannes ainsi d'utiliser le protocole de haute disponibilité HSRP dans le but d'assurer la continuité de service ainsi que l'équilibre de charge.
- Investir dans un matériel haut de gamme avec une très grande fiabilité.
- Utilisation d'une réplication de données sensibles et leur placement aux endroits stratégiques.

1.20 Solution choisie

D'après les critiques précédentes et de la problématique, le réseau LAN de Cevital a hautement besoin d'utiliser une redondance Matérielle au niveau de la couche cœur et distribution ainsi d'utiliser le protocole HSRP.

Nous avons choisi cette solution car elle garantit une haute disponibilité dans l'utilisation de réseau dans le cas d'une panne matérielle.

Aussi bien que la solution optée présente les avantages suivants :

- Une architecture hiérarchique redondante qui assure la haute disponibilité du réseau.
- Intégrer des mécanismes de partage de la charge à l'architecture réseau qui permettront d'optimiser au mieux les équipements de même type.
- Avoir un mécanisme de basculement à la résilience du réseau de manière transparente pour les utilisateurs.

1.21 Conclusion

Dans ce chapitre nous avons vu l'organisme d'accueil de l'entreprise CEVITAL ainsi nous avons éclairci notre thème en mettant en avant une problématique bien précise qui déterminera les axes autour des quelles tournera notre mémoire, tous ce qui nous a conduit logiquement à la proposition d'une solution assure la haute disponibilité.

2 Chapitre 2 : La Haute Disponibilité d'un Réseau Informatique

2.1 Introduction

Après avoir présenté l'organisme de l'entreprise et les différents problèmes prisant sur leur réseau, nous allons à présent dans ce chapitre élaborer une étude descriptible de la haute disponibilité, ainsi qu'une présentation de différents protocoles assurant cette dernière.

2.2 Définition de la haute disponibilité

La haute disponibilité est un terme souvent utilisé en informatique concerne de plus en plus d'entreprises comme de particuliers. Elle fait référence à des systèmes durables et susceptibles de fonctionner en continu sans défaillance pendant une longue période. Ce terme implique que des parties d'un système ont été entièrement testées et dans de nombreux cas, qu'il existe des adaptations en cas de défaillance sous la forme de composants redondants. Elle s'agit de maintenir le réseau informatique en bon état de fonctionnement 24h/24h et 7j/7 en limitant la fréquence et la durée des interruptions **[13]**.

2.3 Évaluation des risques

La panne d'un système informatique peut causer une perte de productivité et d'argent, voire des pertes matérielles ou humaines dans certains cas critiques. Il est ainsi essentiel d'évaluer les risques liés à un dysfonctionnement d'une des composantes du système d'information et de prévoir des moyens et mesures permettant d'éviter ou de rétablir dans des temps acceptables tout incident. Comme chacun le sait, les risques de pannes d'un système informatique en réseau sont nombreux. L'origine des fautes peut être schématisée de la manière suivant **[14]** :

- **Origines physiques** :

Elles peuvent être d'origine naturelle ou humaine :

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

- **Origines humaines :**

Elles peuvent être soit intentionnelles soit fortuites :
• Erreur de conception (bogue logiciel, mauvais dimensionnement du réseau).
• Porte dérobée.
• Sabotage.
• Piratage.

- **Origines opérationnelles :**

Elles sont liées à un état du système à un moment donné :
•Bogue logiciel
•Dysfonctionnement logiciel.

2.4 Comment assurer la haute disponibilité d'une infrastructure informatique ?

2.4.1 La redondance

Ce que les entreprises de nos jours cherchent, c'est un réseau fiable et disponible à tout moment. Une telle solution n'est pas forcément très facile à mettre en place, de plus elle peut être relativement coûteuse pour l'entreprise. L'une des possibilités est d'avoir un réseau qui tient la charge sans pour autant avoir de coupure dans son utilisation, est la redondance. C'est-à-dire dupliquer de composants**,** d'éléments de liaisons ou de données essentielles d'un système**,** tout en étant au maximum transparent pour les utilisateurs. Grâce aux doublons, une entreprise peut garantir les fonctionnalités de son centre informatique dans l'éventualité où un dysfonctionnement **[15].**

2.4.2 Répartition de charge (Une architecture en Load Balancing)

La répartition de charge est un ensemble de techniques permettant de distribuer une charge de travail entre différents ordinateurs d'un groupe. Ces techniques permettent à la fois de répondre à une charge trop importante d'un service en la répartissant sur plusieurs serveurs d'une façon intelligente vers les équipements (serveurs) les moins chargés, et de réduire l'indisponibilité potentielle de ce service que pourrait provoquer la panne logicielle ou matérielle d'un unique serveur. Il est cependant nécessaire d'avoir une bande passante suffisamment élevée et puissante pour que cette architecture en load balancing fonctionne correctement **[16].**

La figure suivante (figure 2-1) montre que le flux entrant va être dirigé vers le serveur le moins chargé.

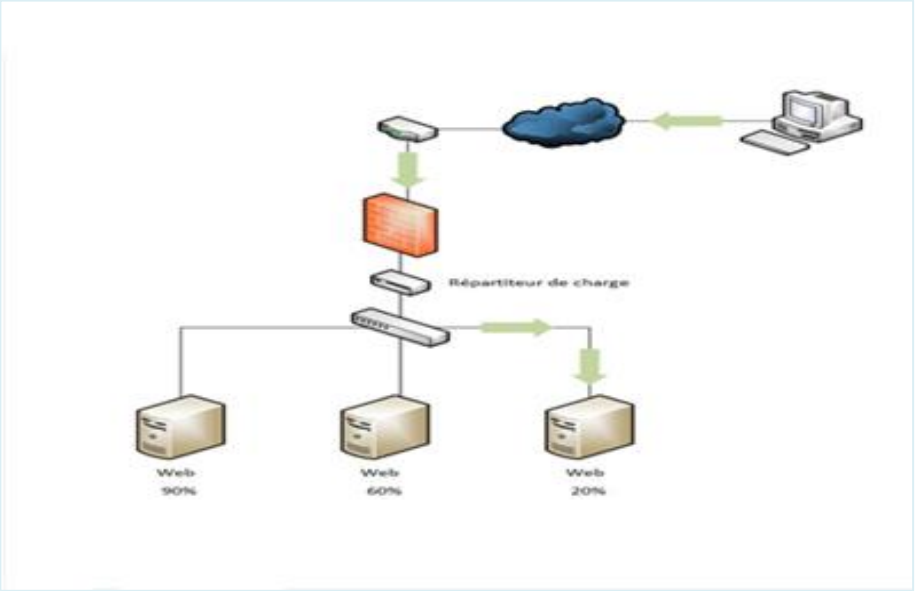


Figure 2-1 : Schéma illustre le principe de répartition de charge **[17].**

2.4.3 Tolérance aux pannes (le FailOver)

La tolérance aux pannes désigne une méthode de conception permettant à un système de continuer à fonctionner correctement même en cas de défaillance de certains de ses composants. En d'autres termes, la tolérance aux pannes signifie comment un système d'exploitation réagit et permet des dysfonctionnements et des défaillances matérielles ou logicielles. La capacité du système d'exploitation à récupérer et à tolérer les pannes peut être gérée par le biais d'un logiciel, d'un matériel ou d'une solution combinée qui exploite les équilibreurs de charge. Certains systèmes informatiques utilisent plusieurs systèmes de tolérance aux pannes en double pour gérer les pannes avec élégance, ce qu'on appelle un réseau tolérant aux pannes **[18].** La figure ci-dessous (figure 2-2) illustre qu'en fonctionnement normal, l'utilisateur sera dirigé vers le serveur disponible (en vert), les autres serveurs seront mis en attente (en jaune). Dans le cas où le serveur principal passe indisponible (en rouge), un des serveurs secondaires prend le relais (L'ordre de passage en mode actif est défini dans la configuration).

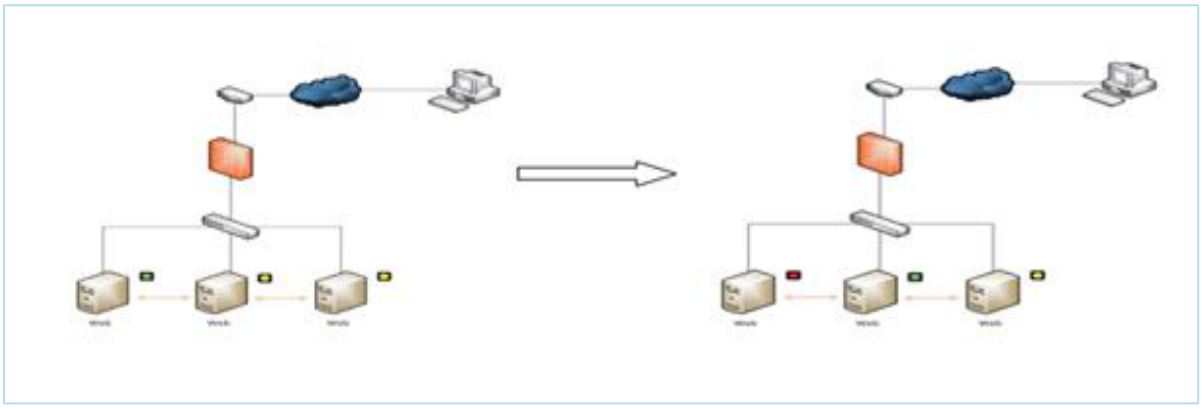


Figure 2-2 : Schéma illustratif sur le principe tolérance aux pannes **[17]**

2.4.4 La réplication des données

La combinaison des techniques de Load Balancing et le Failover permet de garantir la haute disponibilité d'une infrastructure informatique et le fonctionnement en continu des services. Cependant, il y a également des risques de perte de données lorsqu'une entreprise fait face à un incendie, une catastrophe naturelle, ou autres entrainant une perte d'équipements. La redondance seule ne suffit donc pas. C'est pourquoi il faut mettre en place un système de sauvegarde régulier pour pallier à ce risque.

La réplication permet de synchroniser une donnée entre plusieurs serveurs en sécurité. Cette synchronisation peut être unidirectionnelle, c'est-à-dire que la donnée est écrite et accessible mais ne peut être modifiée. Souvent utilisée pour faire de la sauvegarde, cette technique permet d'avoir plusieurs versions d'un même fichier. La seconde possibilité est d'avoir une synchronisation bidirectionnelle, ce qui signifie que la donnée sera clonée entre deux ou plusieurs serveurs mais également accessible et modifiable en temps réel. Pour éviter que deux clients écrivent en même temps sur le même fichier, des systèmes de verrous et de temporisations peuvent être mise en place **[19]**.

La figure suivante (figure 2-3) montre la synchronisation des données de serveur web dans un serveur web1 :

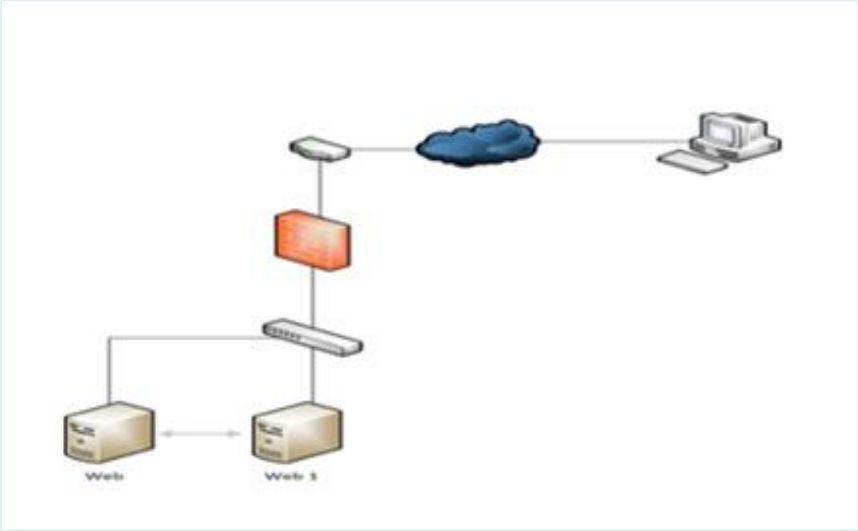


Figure 2-3 : Schéma illustratif sur le principe de réplication des données **[17].**

2.5 Critères de la haute disponibilité

- **Objectif de temps de reprise(RTO) :**

Le RTO (Recovery Time Objective) désigne le temps maximal acceptable pendant lequel une ressource informatique peut ne pas être fonctionnelle suite à une interruption majeure de service. Cette durée est définie à l'avance, et ce en fonction des besoins de production d'une entreprise vis-à-vis de la ressource informatique **[20]**.

- **Objectif de point de reprise(RPO) :**

Le RPO (Recovery Point Objective) représente la durée maximale d'enregistrement des données qu'il est acceptable de perdre lors d'une panne. Le fait de quantifier le RPO définit en fait les objectifs de sauvegarde, ce qui demande de connaître la volumétrie et les fenêtres de sauvegarde **[20]**.

- **Budget :**

Chaque solution à haute disponibilité implique un cout qui doit être comparé aux avantages qu'elle apporte à l'entreprise.

- **Les besoins en temps de disponibilité :**

Les besoins en temps de disponibilité indiquent la durée totale de disponibilité du système pour les applications des utilisateurs finaux.

- **Vérification de système de basculement :**

Le système de basculement doit être vérifié pour s'assurer qu'il est prêt à prendre le relais en cas de panne, une fois le système opérationnel.

- **Une vue d'ensemble des types d'indisponibilité :**

Tenir en compte des pannes, arrêts non prévus et les maintenances planifiées qui peuvent apparaitre est nécessaire pour choisir une solution à haute disponibilité.

- **Besoins de résilience :**

Identification des entités qui doivent être disponible même en cas de panne du système qui les héberge.

- **Performance du système :**

La solution de haute disponibilité choisie a souvent des implications sur les performances, c'est pour cela que l'entreprise doit choisir en fonction de ses besoins la technologie de résilience.

2.6 Les protocoles de redondance

Les protocoles réseaux transportent les données des applications à travers le réseau de l'entreprise. Ces protocoles comptent sur une architecture réseau qui fournit la hiérarchie, les adresses et les informations de la topologie aux machines clientes. Une passerelle ou un routeur multi protocole approvisionne toutes ces informations. Les stations de travail, routeurs, et serveurs de fichiers doivent communiquer entre eux, et c'est dans ce but que les protocoles ont implémenté des méthodes de recherche pour trouver et conserver l'adresse de la passerelle.

2.6.1 VRRP (Virtual Router Redundancy Protocol)

Le protocole de redondance pour le routeur virtuel (en anglais VRRP) élimine le seul point d'échec inhérent à un environnement routé par défaut et en statique. VRRP spécifie un protocole d'élection qui assigne dynamiquement les responsabilités pour un routeur virtuel à un concentrateur VPN provenant d'un réseau LAN. Le routeur VRRP, qui contrôle les adresses IP associées au routeur virtuel, est appelé maitre, et les transferts de paquets sont redirigés vers ses adresses IP. Quand le maitre est indisponible, un back up concentrateur VPN prend la place du maitre **[21].**

2.6.2 HSRP (Hot Standby Router Protocol)

Le HSRP est un protocole Cisco propriétaire de la haute disponibilité accrue de la passerelle d'un réseau, implémenté pour la gestion des liens de secours. Il peut être mis en place sur un routeur ou un switch de niveau 3 du modèle OSI. Le but est qu'une éventuelle panne du routeur ne perturbe pas le routage. Il se met en place par la mise en commun du fonctionnement des plusieurs routeurs physiques ou switches multicouche (au minimum 2) qui, de manière automatique assurons la relève entre eux, c'est-à-dire d'un routeur à un autre **[22]**.

- **Fonctionnement de protocole HSRP**

Le protocole HSRP permettra aux routeurs situés dans un même groupe de former un routeur virtuel qui sera l'unique passerelle des hôtes du réseau local, en se cachant derrière ce routeur virtuel aux yeux des hôtes. Les routeurs garantissent en fait qu'il y est toujours un routeur qui assure le travail de l'ensemble du groupe. Un routeur dans ce groupe est donc désigné comme actif et ce sera lui qui fera passer les requêtes d'un réseau à un autre.

Pendant que le routeur actif travail, il envoie également des messages aux autres routeurs indiquant qu'il est toujours vivant et opérationnel. Si le routeur principal (élu actif) vient à tomber, Il sera automatiquement remplacé par un routeur qui était alors jusque-là passif et lui aussi membre du groupe HSRP. Aux yeux des utilisateurs toutefois, cette réélection et ce changement de passerelle sera totalement invisible car ils auront toujours pour unique passerelle le routeur virtuel que forment les routeurs membres du groupe HSRP. Le routeur virtuel aura donc toujours la même IP et adresse MAC aux yeux des hôtes du réseau même si en réalité il y a un changement du chemin par lequel transitent les paquets **[23]**.

- Ce que voient les hôtes du réseau :

Un seul routeur qui fait office de passerelle toujours disponible sur la même IP

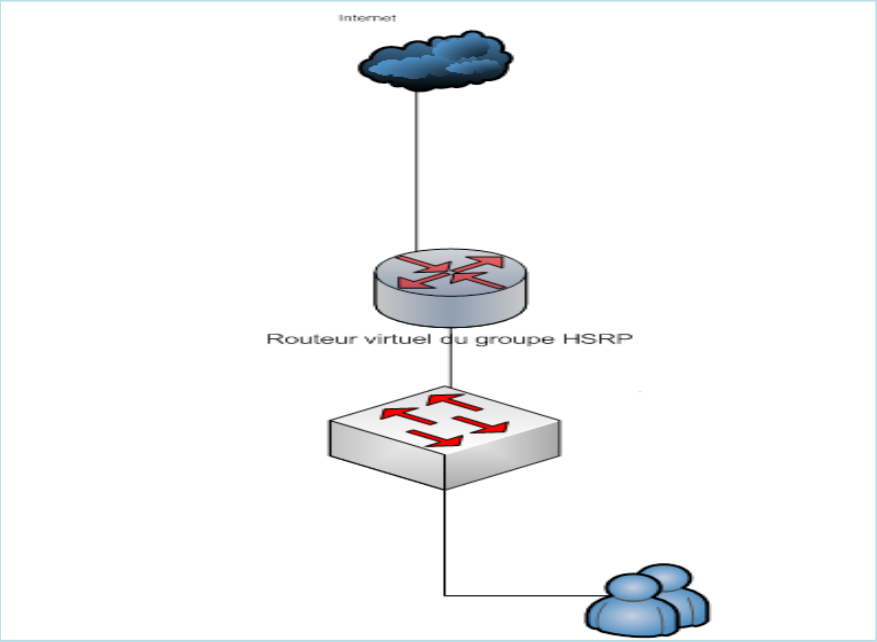


Figure 2-4 : Schéma illustre le protocole HSRP vue d'un hôte d'un réseau **[23].**

- L'état réel du réseau :

Les routeurs physiques forment un routeur virtuel. Un des routeurs est en état actif et transmet les échanges alors que l'autre est en passif et reste à l'écoute de l'état de routeur actif prêt à prendre la relève.

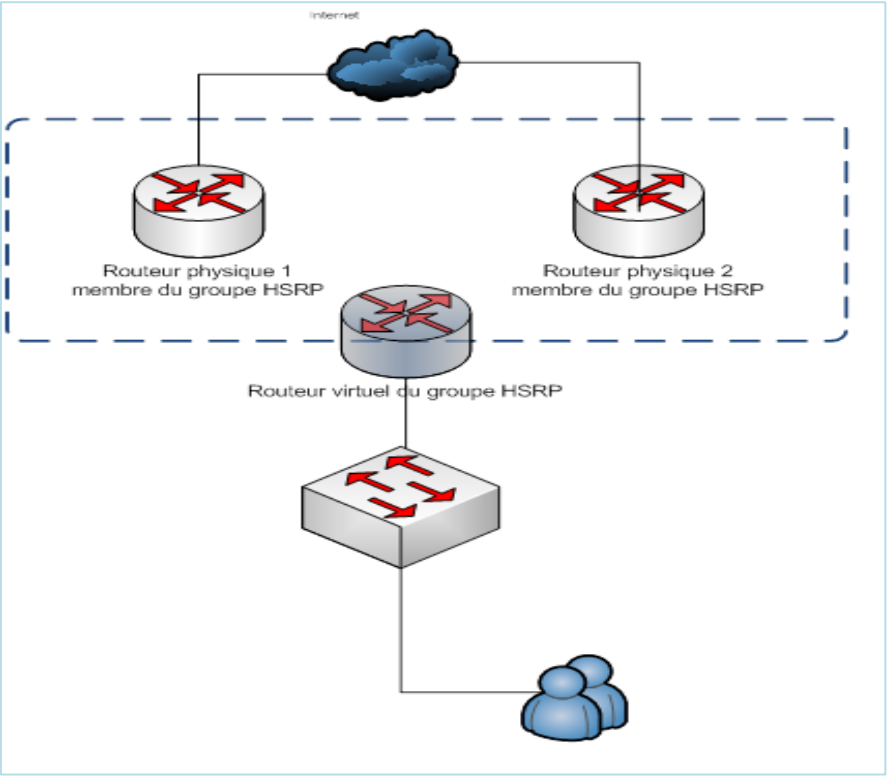


Figure 2-5 : Schéma physique et virtuel d'un réseau HSRP **[23].**

Avec HSRP, il existe trois types de messages multicast envoyés entre les appareils **[24]** :

- ✓ **Hello** : il est envoyé entre les appareils actifs et en veille (par défaut, toutes les 3 secondes). Si l'appareil de veille n'entend pas l'appareil actif (via un message d'accueil) dans environ 10 secondes, il assumera le rôle actif.
- ✓ **Démissionner** : il est envoyé par le périphérique HSRP actif lorsqu'il se prépare à se déconnecter ou à abandonner le rôle actif pour une autre raison. Ce message indique au routeur de secours d'être prêt et de reprendre le rôle actif.
- ✓ **Coup** : il est utilisé lorsqu'un routeur de secours veut assumer le rôle actif (préemption).

Après la configuration de HSRP, Chaque routeur HSRP passera par un certain nombre d'états avant de devenir un routeur actif ou de secours, voici ce qui se passera :

Initial	Indique un état de démarrage, le protocole n'est pas encore en cours d'exécution. Des interfaces sont disponibles.
Learn	Indique que le routeur ne sait encore rien. Attend les hello, pour apprendre Virtual IP.
Listen	Indique que le routeur connaît l'adresse IP virtuelle, il n'a pas été choisi comme veille ou actif.
Speak	Le routeur participe activement à l'élection Actif/Veille en envoyant des hello.
Standby	Agit en tant que sauvegarde. Surveille et envoie des hello.
Active	Acceptation et transfert du trafic utilisateur.

Tableau 2-1 : l'état d'un routeur actif ou de secours

2.6.3 GLBP (Gateway Load Blancing Protocol)

GLBP est un protocole propriétaire Cisco qui fournit une redondance ainsi que de la répartition de charge sur plusieurs routeurs utilisant une seule adresse IP virtuelle, mais plusieurs adresses MAC virtuelles**,** Il protège les données de toutes failles d'un routeur ou d'un circuit, à peu près comme le fait le VRRP et le HSRP, tout en permettant le partage de charge de paquets entre plusieurs routeurs redondants **[25].**

Le GLBP offre un service similaire mais plus que le HSRP et que le VRRP. Les deux derniers protocoles nommés permettent l'utilisation de plusieurs routeurs qui participent à faire un routeur virtuel configuré avec une adresse IP virtuelle. Le souci, quand on utilise HSRP ou VRRP, c'est qu'un seul des routeurs est sélectionné c'est lui qui gère tout le trafic, et les autres routeurs attendent que le principal lâche, les routeurs inactifs n'utilisent pas la bande passante qui leur est allouée. Tous les groupes de routeur servant, à faire un routeur virtuel, ne servent qu'à cela.

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

2.7 STP (Spanning-Tree Protocol)

Pour assurer la fiabilité des liaisons entre des commutateurs du réseau, la mise en œuvre d'une topologie redondance est primordiale. 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 :

2.7.1 Problèmes du Spanning-Tree :

2.7.1.1 Tempête de diffusion

Lorsque des trames de diffusion (broadcast) ou de multicast sont envoyées, les commutateurs les transfèrent par tous les ports. Les trames circulent en boucle et sont multipliées à chaque passage sur un commutateur tel que ses trames n'ayant pas de durée de vie elles vont tourner indéfiniment entre les commutateurs.
La figure ci-dessous montre une trame de diffusion multipliée en boucle sur tous les ports jusqu'à surcharger les liens et rendre le réseau indisponible.

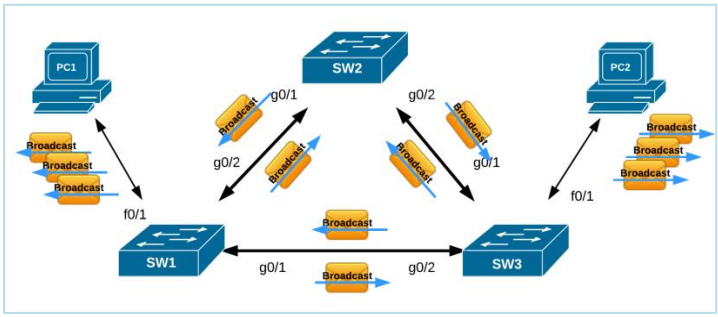


Figure 2.6: Représentation de Tempête de diffusion **[26]**.

Ce problème de bouclage dans un réseau commuté trouve sa solution avec la rupture de la boucle. Un seul chemin est possible d'une extrémité à l'autre du réseau comme la figure suivante le montre :

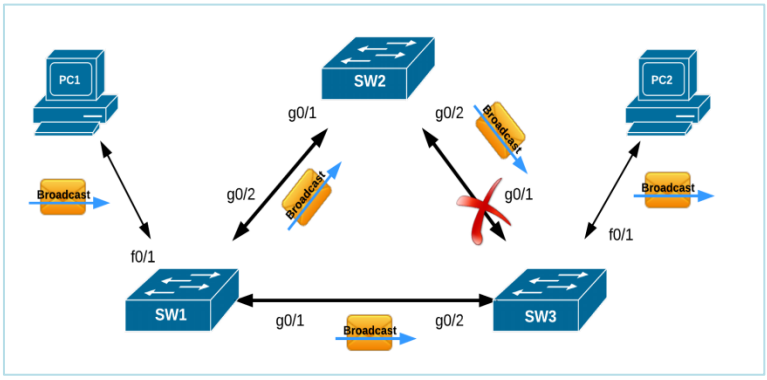


Figure 2.7: Représentation de coupure de la boucle de commutation **[26]**.

2.7.1.2 Trames dupliquées :

Les trames peuvent être dupliquées sur certaines topologies redondantes. Ce scenario on le retrouve rarement car une tempête de diffusion fera tomber le réseau bien avant. La figure 2-8 illustre que PC1 envoie une trame à PC2.elle arrive en double à sa destination.

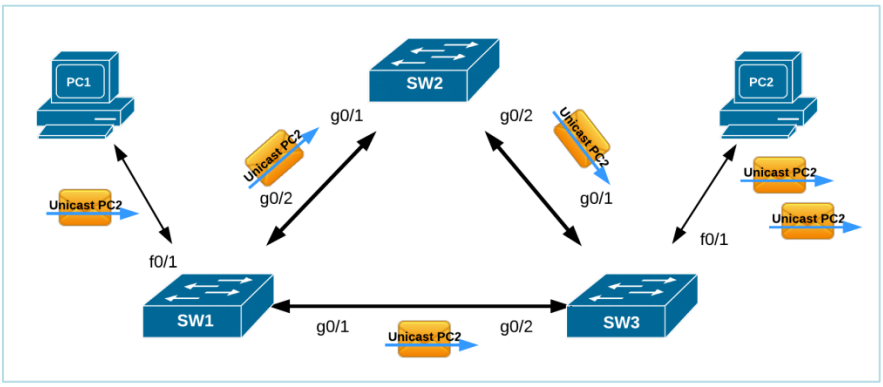


Figure 2-8 : Représentation de trame dupliquée **[26]**.

Le protocole de couche 2 du modèle OSI, STP conçu pour les commutateurs répond à la problématique de trames dupliquées dans un environnement de liaisons redondantes. Il détecte et désactive les boucles et fournit un mécanisme de liens de sauvegarde.

2.7.2 Fonctionnement de STP

Son fonctionnement est basé sur la sélection d'un commutateur Root (principal) et de calculs des chemins les plus courts vers ce commutateur. Les ports des commutateurs rencontrent cinq états dont le "Blocking" qui ne transfère pas de trames de donnée et le "Forwarding" qui transfère les trames de donnée. STP échange régulièrement des informations (appelées des BPDU - Bridge Protocol Data Unit) afin qu'une éventuelle modification de topologie puisse être adaptée sans boucle.STP est conçues pour empêcher les boucles, mais sur ces points de terminaisons, en théorie il ne peut pas y avoir de boucle. C'est

pourquoi Cisco a conçu les fonctionnalités PortFast et BPDU pour réduire le temps requis qu'un équipement en bout de chaine puisse avoir accès à l'état de forwarding **[27]**.

2.7.3 Fonctionnalité de STP :

2.7.3.1 Portfast :

La commande PortFast est une amélioration de Cisco qui permet à un switch de commencer la communication beaucoup plus rapidement. Il se configure uniquement sur des ports connectant des périphériques terminaux et dans une infrastructure VLAN uniquement sur des ports en mode Access (figure 2-9).

Lorsque la fonction PortFast est activée sur un port en mode accès, il contournera les différents états du spanning tree. En gros il passe directement de l'état de blocage à celui de forwarding dans le but d'éviter qu'il ne prenne 50 secondes avant de transférer le trafic. STP Portfast comporte aussi l'avantage de ne pas transférer de BPDUs inutiles.

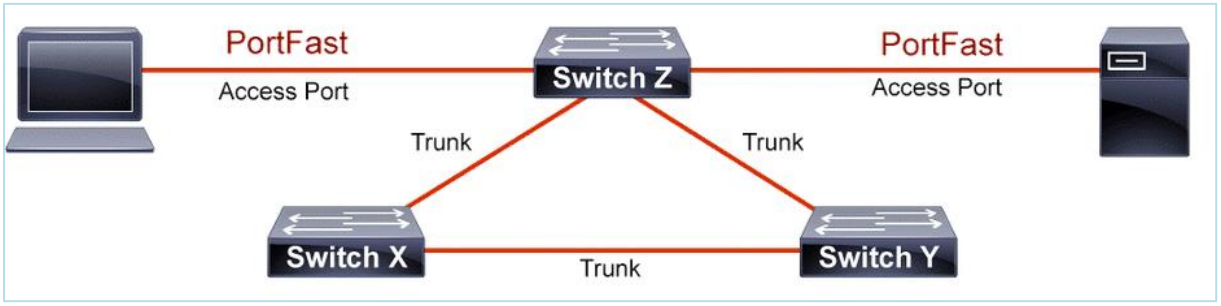


Figure 2-9 : Schéma illustre le fonctionnement de portfast **[27].**

✓ **Remarque** :

L'objectif de la fonction PortFast étant de minimiser le temps d'attente des ports d'accès avant la convergence Spanning Tree, elle doit être utilisée uniquement sur les ports d'accès. Si vous activez PortFast sur un port connecté à un autre commutateur, vous risquez de créer une boucle Spanning Tree.

2.7.3.2 BPDU Guard

BPDU est synonyme de Pont Protocol Data Unit, qui est un paquet de données, envoyé sur les réseaux locaux ou LAN, qui travaille pour détecter les boucles dans un réseau. Les boucles peuvent provoquer des paquets de données en double pour être envoyés, ce qui peut prendre de la bande passante sur un réseau. BPDU Guard protège les ordinateurs de la réception de paquets de données non autorisées qui pourraient contenir des virus.

La fonction BPDU Guard est utilisée pour protéger la topologie STP (Spanning Tree Protocol) contre les attaques liées à BPDU. La fonction BPDU Guard doit être activée sur un port qui ne doit jamais recevoir de BPDU de son appareil connecté. Si un port de commutateur est configuré avec la fonctionnalité PortFast du protocole STP (Spanning Tree Protocol), il doit être connecté à un périphérique d'extrémité (par exemple : poste de travail, serveur, imprimante, etc.). Le PortFast est activé uniquement sur les ports d'accès pour accélérer la transition du port d'accès à l'état de transfert STP. Les périphériques finaux ne sont pas censés générer de BPDU, car dans un environnement réseau normal, les messages BPDU sont échangés par des commutateurs réseau.

La fonction BPDU Guard peut être activée globalement en mode de configuration globale ou par interface en mode de configuration d'interface. Lorsqu'un port activé par BPDU Guard reçoit BPDU du périphérique connecté, BPDU Guard désactive le port et l'état du port passe à l'état errDisabled (down/down, même état qu'en cas de violation de Port-Security).

2.8 VTP (VLAN Trunking Protocol)

VTP 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). VTP permet ainsi d'éviter toute incohérence de configuration des VLAN sur l'ensemble d'un réseau local.VTP fonctionne sur les commutateurs Cisco dans un de ces 3 modes :

- ✓ **Serveur :**

Il est associé à un domaine VTP. La déclaration des VLANs s'effectue sur le serveur. Lorsque l'on modifie la configuration VLAN sur un serveur VTP, que ce soit un ajout, une suppression ou bien une simple modification, elle est propagée sur tous les switchs 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 est associé à aucun domaine VTP. Sa liste de VLAN est locale et n'est pas mis à jour lorsqu'il reçoit une trame VTP. Cependant il propage les listes de VLAN qu'il reçoit.

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 **[28].**

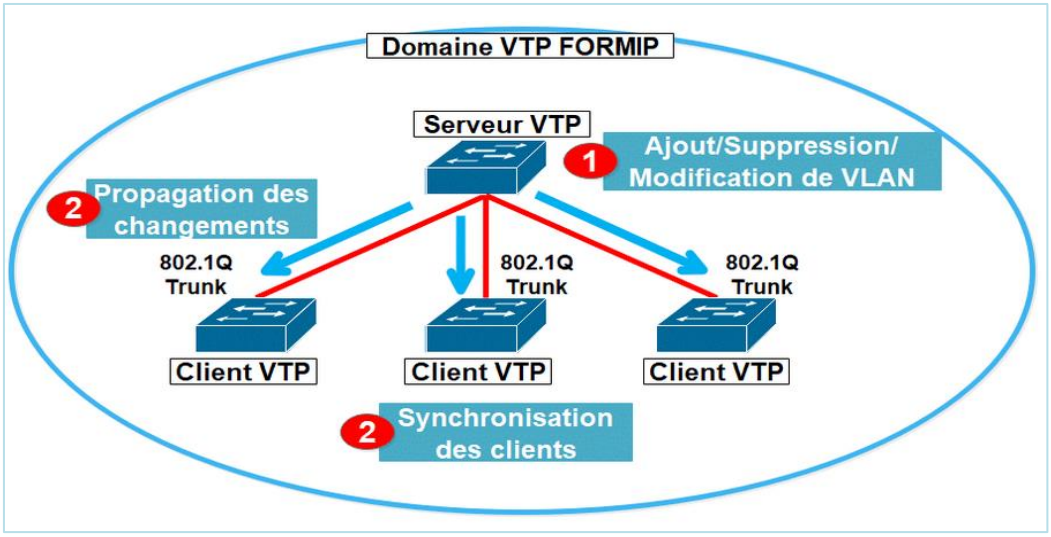


Figure 2-10: Représentation de fonctionnement de VTP **[29].**

2.9 EtherChannel

2.9.1 Définition Etherchannel :

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

2.9.2 Utilité de l'Ether Channel :

Comme nous venons de le dire, l'Etherchannel consiste en une agrégation de lien. Le principe est simple, il s'agit de combiner plusieurs liens pour avoir un lien virtuel de meilleure capacité **[19].**

Prenons l'exemple suivant (figure 2-11) :

Figure 2-11 : Schéma illustre l'interconnexion de deux switch sans Etherchannel **[30].**

Sur la figure ci-dessus, il existe un lien entre les deux switches. Ces derniers pourront donc communiquer à une vitesse de 100 Mbps. Pour bénéficier d'une meilleure bande passante, nous pouvons faire une agrégation de lien. Nous aurions alors une topologie représentée dans la figure suivante (figure 2-12) :

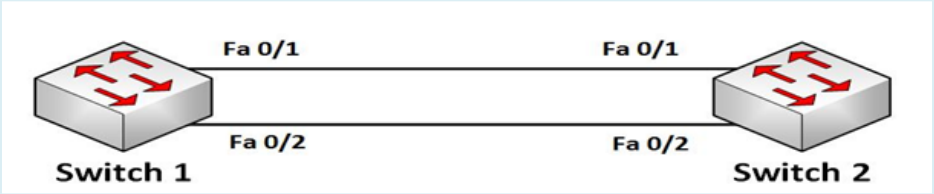


Figure 2-12 : Schéma illustre l'interconnexion de deux switch avec Etherchannel **[30].**

Sans aucune configuration, STP se chargerait de désactiver l'un des liens. En configurant l'Etherchannel, les deux switches ne verront plus qu'un seul lien virtuel. Ce lien virtuel aura une capacité de 200 Mbps.

2.9.3 Protocoles d'agrégation de canaux :

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

- **PAgP :** c'est un protocole propriétaire de Cisco .il facilite la création automatique de 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.

✓ **Remarque :**

PAgP et LACP ne fonctionnent pas ensemble. Le mode **ON** existe pour PAgP et LACP car il crée un Etherchannel de manière inconditionnelle, sans utiliser PAgP et LACP par défaut, aucun mode n'est configuré pour Etherchannel.

2.9.4 Avantages de l'Etherchannel :

Au moment où un Etherchannel est configuré, l'interface virtuelle résultante est appelée un canal de port. Les interfaces physiques sont regroupées dans une interface de canal de port. Etherchannel présente de nombreux avantages citant **[31]** :

- 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.
- 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.
- EtherChannel crée une agrégation que STP reconnaît comme une seule liaison logique.
- EtherChannel garante la redondance et la perte d'un lien physique ne génère pas de changement dans la topologie.

2.10 Les protocoles de routage

Le routage désigne le mécanisme par lequel les données d'un équipement expéditeur sont acheminées jusqu'à leur destinataire en examinant les informations situées au niveau 3 du modèle OSI, même si aucun des deux ne connaît le chemin complet que les données devront suivre. Avoir une procédure de routage efficace est particulièrement important pour les réseaux décentralisés sur un réseau.

2.10.1 RIP (Routing Information Protocol)

Le protocole RIP est un protocole de routage à vecteur de distance utilise le nombre de sauts pour calculer la valeur de la mesure qui déterminer le chemin le plus court de la source à la destination afin d'atteindre le réseau. Cela permet aux données d'être livrées à grande vitesse dans les plus brefs délais. Le RIP est utilisé à la fois dans les réseaux locaux et étendus et est généralement considéré comme étant facilement configuré et mis en œuvre **[32].**

2.10.2 EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP (Enhanced Interior Gatway Routing Protocol) est un protocole de routage propriétaire développé par Cisco à partir de leur protocole original IGRP. De ce fait, EIGRP ne pouvait être utilisé que sur des équipements Cisco, mais est devenu un protocole partiellement, EIGRP est un protocole de routage à vecteur de distance IP, avec une optimisation permettant de minimiser l'instabilité de routage due aussi bien au changement de topologie qu'à l'utilisation de la bande passante et la puissance du processeur du routeur.

2.10.3 OSPF (Open Shortest Path First)

OSPF est un protocole de routage à état de liens qui est massivement adopté dans les réseaux des grandes entreprises. Il recueille les informations sur l'état des liens des routeurs du réseau et détermine les informations de la table de routage pour transmettre les paquets. Cela se produit en créant une carte topologique pour le réseau. Il est plus performant que le protocole RIP (Routing Information Protocol) et commence donc à le remplacer petit à petit.

Contrairement à RIP, ce protocole n'envoie pas aux routeurs adjacents le nombre de saut qui les séparent, mais l'état de la liaison qui les sépare. De cette façon, chaque routeur est capable de dresser une carte de l'état du réseau et peut, par conséquent, choisir à tout moment la route la plus appropriée pour un message. De plus, ce protocole évite aux routeurs intermédiaires d'avoir à incrémenter le nombre de sauts, ce qui se traduit par une information beaucoup moins abondante, ce qui permet d'avoir une meilleure bande passante utile qu'avec RIP **[33]**.

2.11 Conclusion

Ce chapitre est consacré à la définition des différents protocoles dont certain on a utilisé durant notre projet et comprendre le fonctionnement de chacun ainsi que les avantages qu'ils présentent au réseau.

3 Chapitre 03 : Conception et Réalisation

3.1 Introduction

Dans le but d'éclaircir et de compléter ce qui a été traité auparavant, à travers ce chapitre nous allons présenter le simulateur Cisco Packet Tracer qui nous permettra d'effectuer les configurations nécessaires dans l'intention d'arriver à notre désir principal qui est l'obtention d'un réseau sous haute disponibilité.

Nous allons commencer par la configuration des VLANs, puis le VTP, le STP, l'Ether Channel, HSRP et enfin l'OSPF tout en expliquant et illustrant chaque étape, et à la fin nous allons tester la fiabilité de la solution optée.

3.2 Présentation du simulateur Cisco packet Tracer 8.1.1

Cisco Packet Tracer est un simulateur de matériel réseau très puissant 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 (voir annexe II).

Figure 3-1 : Capture de simulateur Cisco Packet Tracer 8.1.1

3.3 Amélioration de l'architecture :

Afin de tester notre solution choisie nous étions dans l'obligation de porter des modifications matérielles sur l'ancienne architecture et ceci en ajoutons deux backbones pour la partie Core celle qui reliera le réseau vers les autres sites et comprendra en elle avec la partie distribution le protocole de routage choisi (OSPF), nous avons aussi mis en œuvre deux backbones dans la partie distribution afin de configurer le protocole de la haute disponibilité HSRP sur ces deux backbones qui eux même sont relier en EtherChannel pour une meilleure connectivite et un débit plus haut. Afin que cette architecture soit hautement disponible, on doit aussi brancher tous les switches d'accès au premier backbone que nous avons nommé SWD1 ainsi qu'au deuxième que nous avons nommé SWD2.

3.4 Nouvelle architecture du réseau Cevital

Voici donc le modèle d'architecture adopté pour le réseau de Cevital, il se décompose en trois couches, une couche Core de deux switches niveau 3, une couche distribution avec deux switchs aussi niveau 3, une couche accès là ou tous les switch d'accès y sont, un protocole de haute disponibilité HSRP sera configurer à la partie distribution qui assure la continuité de service , un protocole OSPF sera configurer entre la partie Core et distribution qui vas assurer le bon routage du réseau, et tout ça sera un mi- travaille sans que les périphériques de la couche accès soient interconnecter au deux switches en redondance pour qu'ils assurent la haute disponibilité dans le cas où l'un des switches de distribution subit un disfonctionnement ou une coupure d'un des liens d'interconnexion.

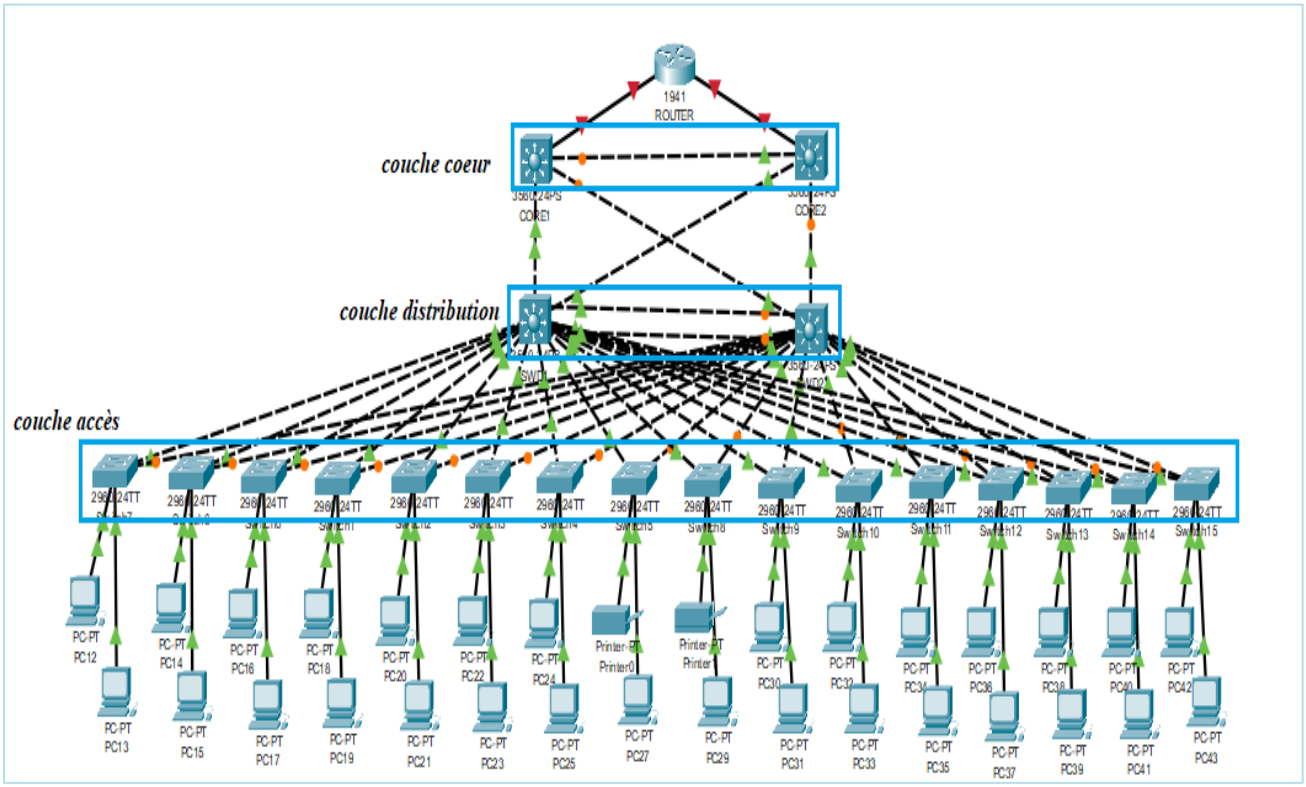


Figure 3-2 : Modèle d'architecture réseau Cevital.

3.4.1 Présentation des équipements utilisés

Au sein de Cevital les différents équipements utilisés sont tous de même marque, ce qui évite tout problème de compatibilité entre les protocoles propriétaires. Les équipements réseau sont illustrés dans le tableau 3-1 :

Equipement du modèle type	Nombre	Type et marque de Switch
Switch Core	02	Cisco Catalyst C6807-XL
Switch Distribution	02	Cisco Catalyst C3850-24S
Switch d'Accès	53	Cisco Catalyst C2960

Tableau 3-1:Représentation de la liste des équipements utilisés.

3.4.2 Nomination des équipements

On nomme les équipements par des termes significatifs pour simplifier la conception d'architecture et la gestion de réseau. Le tableau 3.2 indique les noms des différents équipements utilisés :

Couche Cœur	Couche Distribution	Couche Accès	Pcs	Imprimantes
Core1 Core2	SWD1 SWD2	SWAcces n n=1..16	Pc n n=0..36	Printer n n=0..2

Tableau 3-2: Représentation des noms des équipements

3.4.3 Désignation des interfaces

Le tableau suivant (tableau 3-3) indique la répartition des interfaces sur les différents équipements.

..

Appareil Local	Appareil distant	Interface(s) locale(s)	Interface(s) distante(s)
Router	Core1	Gig0/0	Fa0/4
Router	Core2	Gig0/1	Fa0/4
Core1	Core2	Fa0/3	Fa0/3
Core1	SWD1	Fa0/2	Fa0/20
Core1	SWD2	Fa0/1	Fa0/19
Core2	SWD1	Fa0/1	Fa0/19
Core2	SWD2	Fa0/2	Fa0/20
SWD1	Core1	F0/20	Fa0/2
SWD1	Core2	F0/19	Fa0/1
SWD1	SWD2	Fa0/17 - Fa0/18	Fa0/17 - Fa0/18
SWD1	Raff-Huile	Fa0/1	F0/3
SWD1	IT	F0/2	F0/3
SWD1	DFC	F0/3	F0/3
SWD1	DG	F0/4	F0/3
SWD1	Commercial	F0/5	F0/3
SWD1	Cdt-Huile	F0/6	F0/3
SWD1	Exp-Huile	F0/7	F0/3
SWD1	Tour-Silo	F0/8	F0/3
SWD1	Energie	F0/9	F0/3
SWD1	Projet	F0/10	F0/3
SWD1	Sucre3500T	F0/11	F0/3
SWD1	Cam-new-DC	F0/12	F0/3
SWD1	Tituration	F0/13	F0/3
SWD1	Sucre-roux	F0/14	F0/3

SWD1	Achat-Appro	F0/15	F0/3
SWD1	Exp-Sucre-Blan	F0/16	F0/3
SWD2	Raff-Huile	Fa0/1	F0/4
SWD2	IT	F0/2	F0/4
SWD2	DFC	F0/3	F0/4
SWD2	DG	F0/4	F0/4
SWD2	Commercial	F0/5	F0/4
SWD2	Cdt-Huile	F0/6	F0/4
SWD2	Exp-Huile	F0/7	F0/4
SWD2	Tour-Silo	F0/8	F0/4
SWD2	Energie	F0/9	F0/4
SWD2	Projet	F0/10	F0/4
SWD2	Sucre3500T	F0/11	F0/4
SWD2	Cam-new-DC	F0/12	F0/4
SWD2	Tituration	F0/13	F0/4
SWD2	Sucre-roux	F0/14	F0/4
SWD2	Achat-Appro	F0/15	F0/4
SWD2	Exp-Sucre-Blan	F0/16	F0/4

Tableau 3-3 : Désignation des interfaces des différents équipements

3.5 Vlan de l'entreprise

L'administrateur réseau à diviser le réseau en plusieurs VLANs en fonction des différents départements, L'adressage utilisé dans l'architecture est de classe à segmenter en plusieurs sous réseaux 10.30.0.0/24, chaque vlan a une adresse de sous réseau (plus de détails sur les adresses des Vlans voir Annexe **IV** et Annexe **V**).

VLAN		Description
ID	NOM	
10	DRH	Direction Ressource Humaine
H	Direction des Appro	Direction des Approvisionnement
12	DSI	Direction Systèmes Informatique
13	Raff Huile	Raffinerie Huile
14	Raff sucre 3000T	Raffinerie de sucre
15	Division utilités	/
16	Supply-chain	/
17	Unité margarinerie	/
18	Printer	Imprimantes
20	Téléphone	/
21	Voice	/
22	Direction R&D	/
23	Performance industriel	/
24	Unité Cdt Huile	Unité Conditionnement de Huile
25	Management switch	Switch Management
26	DFC	Direction Finances et Comptabilité
27	Commercial	Direction commercial
28	DG	Direction Générale
29	DQMS	Direction Qualité et Management Système
30	Raff sucre 3500T	Raffinerie de Sucre
31	Cdt sucre	Conditionnement sucre
32	Caméra	/
33	Projets	/
36	Trituration	/

Tableau 3-4 : Nomination des Vlans de l'entreprise **[6].**

- **Configuration des équipements utilisés**

Dans ce qui suit nous allons lancer une série de configuration sur tous les périphériques qui vont nous permettre de réaliser l'architecture, en montrant un exemple de chaque configuration.

3.6 Configuration de base

La même configuration de base sera effectuée pour le routeur, les Switches Cores , les Switches de distribution SWD1 et SWD2 ainsi que les Switches d'accès.

3.6.1 Configuration de Hostname

Comme premier pas dans notre travail nous allons changer le nom de chaque équipement en donnant des noms significatifs et facile à reconnaitre. Voici un exemple illustratif la nomination de l'un des Switches de distribution « SWD1 »

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SWD1
SWD1(config)#
```

Figure 3-3 : Exemple de configuration de Hostname.

3.6.2 Configuration de la ligne Console :

Pour sécuriser l'accès aux périphériques nous avons attribué un mot de passe « Cevital » pour la ligne console de chaque commutateur de niveau 2 et 3.

```
SWD1(config)#line con 0
SWD1(config-line)#password cevital
SWD1(config-line)#login
SWD1(config-line)#exit
SWD1(config)#
```

Figure 3-4 : Configuration de ligne console

3.6.3 Sécuriser le mode privilégié :

Nous avons attribué un mot de passe chiffré « Cevital » pour l'accès au mode privilégié

```
SWD1(config)#enable password Cevital
SWD1(config)#
```

Figure 3-5 : Sécurisation en mode privilégié.

3.6.4 Sécurisation des mots de passe :

Les mots de passe apparaissent en clair lors de l'affichage du fichier de configuration. Nous allons donc activer le service **password-encryption** afin de sécuriser les équipements.

```
SWD1(config)#service password-encryption
SWD1(config)#
```

Figure 3-6 : Exemple de sécurisation du « SWD1 »

3.6.5 Configuration d'une bannière

Nous avons utilisé une bannière de type « banner motd » qu'indique que cet accès est interdit aux utilisateurs non autorisé (Hackers).

```
SWD1(config)#
SWD1(config)#banner motd " Acces aux personnes autorisees "
SWD1(config)#
```

Figure 3-7 : Attribution d'une bannière au « SWD1 »

Pour Vérifier les configurations de base pratiquées on tapera la commande **show running-config,** la figure ci-dessous (Figure 3-14) apparaitre :

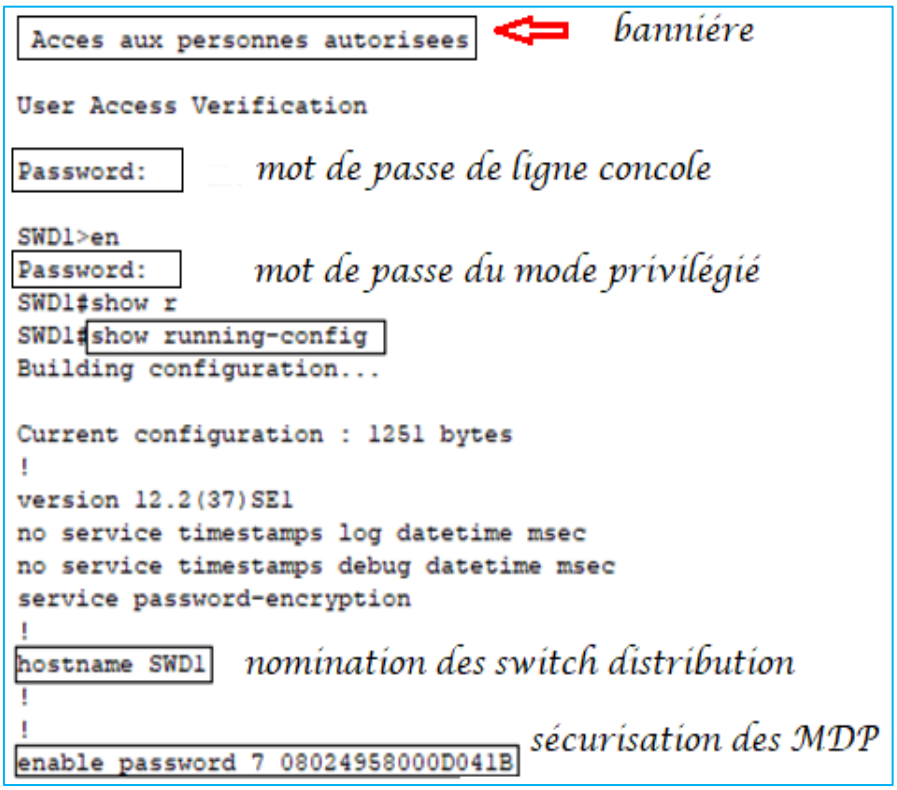


Figure 3-8 : Vérification des configurations de base sur SWD1

3.6.6 Sécurisation d'accès à distance avec SSH

SSH est largement utilisé par les administrateurs réseau pour gérer à distance les systèmes et les applications en toute sécurité, car il leur 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.

Nous allons activer le SSH sur les commutateurs de la couche Core et distribution. Voire un exemple des étapes de configuration sur le switch « SWD1 »

```
SWD1(config)#username Admin password cevitalAgro
SWD1(config)#ip domain-name cisco.com
SWD1(config)#crypto key generate rsa
The name for the keys will be: SWD1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

SWD1(config)#line vty 04
*Mar 1 0:4:12.236: %SSH-5-ENABLED: SSH 1.99 has been enabled
SWD1(config-line)#transport input ssh
SWD1(config-line)#login
```

Figure 3-9 : Exemple de configuration SSH sur « SWD1 »

3.7 Configuration des Liens trunks

Dans cette section nous allons configurer les liaisons entre les switches de distribution et les switches d'accès (Niveau 2) en mode trunk afin que ses derniers communiquent et transmettent entre eux les Vlans configurés dans les switches de distribution.

Les figures ci-dessous indiquent les commandes à saisir qui va nous permettre de configurer les différents commutateurs en mode trunk en utilisons la commande « **interface range »** qui va nous permettre de regrouper les interfaces en un seul coup.

✓ Sur le Switch distribution SWD1 :

```
SWD1(config)#Interface range fastEthernet 0/1-18
SWD1(config-if-range)#Switchport trunk encapsulation dot1q
SWD1(config-if-range)#Switchport mode trunk
```

Figure 3-10 : Exemple de configuration des liens trunk sur « SWD1»

✓ Sur le Switch distribution SWD2 :

```
SWD2(config)#Interface range fastEthernet 0/1-18
SWD2(config-if-range)#Switchport trunk encapsulation dot1q
SWD2(config-if-range)#Switchport mode trunk
```

Figure 3-11 : Exemple de configuration des liens trunk sur « SWD2»

✓ Sur les Switch niveau accès :

```
raff-huile(config)#Interface range fastEthernet 0/3-4
raff-huile(config-if-range)#Switchport mode trunk
raff-huile(config-if-range)#Exit
raff-huile(config)#
```

Figure 3-12 : Exemple de configuration des liens trunk sur « raff-huile »

Afin de vérifier cette configuration, on vérifie l'état des interfaces avec la commande **« Show running-config ».**

```
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/18
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/19
```

Figure 3-13 : Vérification des liens trunks sur « SWD1 »

3.8 Configuration des VLANs

3.8.1 Création des VLANs :

A présent nous allons créer les différents VLANs de l'entreprise sur le switch de distribution SWD1 en utilisant la commande « **vlan** » sur le mode configuration et ensuite le nommer avec la commande « **name »** sur le même mode comme suit :

```
SWD1(config)#Vlan 10
SWD1(config-vlan)#Name DRH
SWD1(config-vlan)#Vlan 11
SWD1(config-vlan)#Name Direction-appro
```

Figure 3-14 : Création des VLANs

Au-delà de création des 24 Vlans de l'entreprise nous allons ensuite vérifier leurs créations avec la commande « **show vlan brief »** :

```
SWD1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
10   DRH                              active
11   Direction-appro                  active
12   DSI                              active
13   Raff-huile                       active
14   Raff-sucre3000T                  active
15   Division-U                       active
16   supply-chain                     active
17   Unit-MARG                        active
18   printer                          active
20   telephone                        active
21   Voice                            active
22   Direction-R&D                    active
23   performance-industriel           active
24   unit-cdthuile                    active
25   management-sw                    active
26   DFC                              active
27   Commercial                       active
28   DG                               active
29   DQMS                             active
30   Raff-sucre3500T                  active
31   Cdt-sucre                        active
32   camera                           active
33   projet                           active
36   Tituration                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SWD1#
```

Figure 3-15 : Vérification de la création des VLANs.

3.8.2 Configuration du VTP (VLAN Trunking protocol)

Afin de profiter des services VTP (création, suppression, modification des Vlans), Nous allons donc configurer le switch de distribution « SWD1 » en mode **Serveur** et lui attribué un nom de domaine ainsi un mot de passe, et le reste des switches en mode **Client** afin que les Vlans se propagent du SDW1 vers les autres switches. Pour cela nous allons procéder comme suit :

- ✓ Configurer le SWD1 en VTP serveur :

```
SWD1(config)#Vtp mode server
Setting device to VTP SERVER mode.
SWD1(config)#Vtp domain cevital.com
Domain name already set to cevital.com.
SWD1(config)#Vtp password cevital
Password already set to cevital
SWD1(config)#Vtp version 2
```

Figure 3-16 : Configuration de VTP serveur

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

```
SWD1#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0050.0FE5.1910
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 10.30.10.252 on interface Vl10 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 29
Configuration Revision          : 97
MD5 digest                      : 0x50 0x24 0xDB 0x8C 0x99 0xF9 0x7D 0x8C
                                  0xE3 0x7A 0x20 0x5B 0x01 0xDC 0x87 0x36
```

Figure 3-17 : Vérification de configuration VTP serveur

- ✓ Configurer SWD2 en mode VTP client :

```
SWD1(config)#Vtp mode client
Setting device to VTP CLIENT mode.
SWD1(config)#Vtp domain cevital.com
Changing VTP domain name from NULL to cevital.com
SWD1(config)#Vtp password cevital
Setting device VLAN database password to cevital
SWD1(config)#Vtp version 2
Cannot modify version in VTP client mode
SWD1(config)#
```

Figure 3-18 : Configuration de VTP client

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

```
SWD2#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0060.2F8B.5600
Configuration last modified by 0.0.0.0 at 3-1-93 00:22:53

Feature VLAN :
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
Configuration Revision          : 1
MD5 digest                      : 0x1D 0xBD 0xEE 0x2C 0x43 0x8D 0x9B 0x3A
                                  0x9E 0xD1 0x3F 0x85 0x6A 0x50 0xA4 0x0A

SWD2#
```

Figure 3-19 : Vérification de la configuration VTP client.

✓ Configurer les autres Switches niveau accès en mode VTP client :

```
Raff-Huile(config)#Vtp mode client
Setting device to VTP CLIENT mode.
Raff-Huile(config)#Vtp domain cevital.com
Domain name already set to cevital.com.
Raff-Huile(config)#Vtp password cevital
Setting device VLAN database password to cevital
Raff-Huile(config)#Vtp version 2
Cannot modify version in VTP client mode
Raff-Huile(config)#exit
```

Figure 3-20 : Exemple de configuration VTP client sur le Switch accès « Raff-huile ».

On vérifie aussi cette configuration en tapant **show vtp status :**

```
Raff-Huile#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 00D0.FFC6.5000
Configuration last modified by 0.0.0.0 at 3-1-93 00:22:53

Feature VLAN :
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
Configuration Revision          : 1
MD5 digest                      : 0x1D 0xBD 0xEE 0x2C 0x43 0x8D 0x9B 0x3A
                                  0x9E 0xD1 0x3F 0x85 0x6A 0x50 0xA4 0x0A

Raff-Huile#
```

Figure 3-21 : Vérification de la configuration VTP client sur le Switch accès « Raff-huile »

3.8.3 Attribuer des ports aux différents VLANs

Dans cette étape nous allons assigner des ports aux Vlans au niveau des switches d'accès avec les commandes citées dans la figure ci-dessous (figure 3-22) :

```
Raff-Huile(config)#interface range fastethernet 0/1-2
Raff-Huile(config-if-range)#switchport mode access
Raff-Huile(config-if-range)#switchport access vlan 10
```

Figure 3-22 : Exemple d'attribution de port au Vlan 10

En utilisant la commande « show **running-config »** pour vérifier la configuration du mode accès sur le Switch Raff-huile par exemple (figure 3-23) :

```
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
```

Figure 3-23 : Vérification de la configuration du mode accès sur le switch « Raff-huile »

Nous allons maintenant vérifier si les ports sont bien attribués avec la commande

Show vlan brief.

```
Raff-huile#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, 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    Fa0/1, Fa0/2
11   Direction-appro                  active
12   DSI                              active
13   Raff-huile                       active
14   Raff-sucre3000T                  active
15   Division-U                       active
16   supply-chain                     active
17   Unit-MARG                        active
18   printer                          active
20   telephone                        active
21   Voice                            active
22   Direction-R&D                    active
23   performance-industriel           active
24   unit-cdthuile                    active
25   management-sw                    active
26   DFC                              active
27   Commercial                       active
28   DG                               active
29   DQMS                             active
30   Raff-sucre3500T                  active
31   Cdt-sucre                        active
32   camera                           active
33   projet                           active
36   Tituration                       active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure 3-24 : Vérification si les Vlans sont bien été propagés.

3.9 Configuration des liens EtherChannel

Dans l'architecture, nous avons opté pour une agrégation des liens FastEthernet entre les deux switchs de distribution SWD1 et SWD2, on a donc mis les deux ports fastEthernet dans un groupe en précisant le mode ON, puis on les a mis en mode trunk comme la figure ci-dessous (figure 3-25) le montre :

```
SWD1(config-if)#interface range f0/17-18
SWD1(config-if-range)#Channel-group 1 mode on
SWD1(config-if-range)#exit
SWD1(config)#interface port-channel 1
SWD1(config-if)#switchport trunk encapsulation dot1q
SWD1(config-if)#switchport mode trunk
SWD1(config-if)#exit
```

Figure 3-25 : Configuration de l'EtherChannel sur « SWD1 »

Pour vérifier la configuration en mode trunk sur l'un des switchs d'accès, en utilisant la commande **show interface trunk**

```
Raff-Huile#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/3       on           802.1q         trunking      1
Fa0/4       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/3       1-1005
Fa0/4       1-1005

Port        Vlans allowed and active in management domain
Fa0/3       1,10,11,12,13,14,15,16,17,18,20,21,22,23,24,25,26,27,28,29,30,31,32,33,36
Fa0/4       1,10,11,12,13,14,15,16,17,18,20,21,22,23,24,25,26,27,28,29,30,31,32,33,36

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/3       1,10,11,12,13,14,15,16,17,18,20,21,22
Fa0/4       23,24,25,26,27,28,29,30,31,32,33,36
```

Figure 3-26 : Vérification de la configuration du mode trunk sur « Switch accès »

3.10 Configurations du protocole STP

Pour faciliter la mise en place d'un chemin logique sans boucle sur l'ensemble du domaine de diffusion nous allons configurer le protocole STP.

3.10.1 La configuration du l'ID du pont

On commence par l'activation du rapid spanning-tree en tapant la commande « **spanning-tree mode rapid-pvst** » ensuite forcer le commutateur SWD1 d'être le root bridge de Vlan 10 jusqu'à vlan 22 et le root bridge de secours de Vlan 23 jusqu'à vlan 36.

```
SWD1(config)#Spanning-tree mode rapid-pvst
SWD1(config)#Spanning-tree vlan 10,11,12,13,14,15,16,17,18,20,21,22 root primary
SWD1(config)#Spanning-tree vlan 23,24,25,26,27,28,29,30,31,32,33,36 root secondary
SWD1(config)#
```

Figure 3-27 : Configuration du STP sur SWD1

Nous avons procédé la même chose pour le SWD2 qui est le root bridge de Vlan 23 jusqu'à vlan 36 et le root bridge de secours de vlan 10 jusqu'à vlan 22.

```
SWD2(config)#Spanning-tree mode rapid-pvst
SWD2(config)#Spanning-tree vlan 23,24,25,26,27,28,29,30,31,32,33,36 root primary
SWD2(config)#Spanning-tree vlan 10,11,12,13,14,15,16,17,18,20,21,22 root secondary
SWD2(config)#
```

Figure 3-28 : Configuration de STP sur SWD2

Et nous allons vérifier cette configuration avec la commande **Show running-config :**

```
!
!
spanning-tree mode rapid-pvst
spanning-tree vlan 10-18,20-22 priority 24576
spanning-tree vlan 23-33,36 priority 28672
!
!
```

Figure 3-29 : Vérification du STP sur SWD1

```
!
!
spanning-tree mode rapid-pvst
spanning-tree vlan 23-33,36 priority 24576
spanning-tree vlan 10-18,20-22 priority 28672
!
!
```

Figure 3-30: Vérification du STP sur SWD2

Pour voir la configuration de chaque instance Spanning-tree (c'est-à-dire pour chaque vlan) en tapant la commande **« show spanning-tree »**

```
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID     Priority    24586
              Address     0060.5C96.AD43
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24586  (priority 24576 sys-id-ext 10)
              Address     0060.5C96.AD43
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
```

Figure 3-31 : Instance STP (exemple Vlan 10).

3.10.2 Configurations de PortFast et BPDU

Lors du démarrage d'un Switch, la recherche de la meilleure topologie prend un peu de temps. Pour cela on utilise la commande « **Spanning-tree portfast** » qui fait passer directement le port de l'état blocking á l'état forwarding, le démarrage de l'interface est donc plus rapide et aussi on ajoute La commande « **Spanning-tree bpduguard enable** » pour sécuriser les ports des Switches de façon à empêcher tous intrus de brancher un Switch externe à l'un des Switches de l'entreprise (bloquer les ports non utilisé).ces commandes sont applicable uniquement sur les ports d'accès(couche d'accès) reliés à des machines terminales.

```
Raff-huile(config)#interface range f0/1-2
Raff-huile(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/2 but will only
have effect when the interface is in a non-trunking mode.
Raff-huile(config-if-range)#spanning-tree bpduguard enable
Raff-huile(config-if-range)#
```

Figure 3-32 : Configurations des Portfasts et BPDU

3.11 Configuration du DHCP

Afin de faciliter la gestion et l'attribution des adresses IP pour chaque hôte du réseau, nous allons utiliser le protocole DHCP, ce dernier permet de configurer les paramètres de chaque hôte et le laissera profiter d'un adressage dynamique (voir Annexe **III**). La configuration se fera au niveau des switches de distribution SWD1 et SWD2.

Afin de réussir ce protocole, et de permettre aux deux Switches de distribution d'attribuer des adresses au même temps sans conflit, nous allons exclure les adresses de 128 à 254 sur le SWD1, c'est-à-dire le SWD1 va attribuer les adresses allant de 1 jusqu'à 127.

```
SWD1(config)#Ip dhcp excluded-address 10.30.10.128 10.30.10.254
SWD1(config)#Ip dhcp excluded-address 10.30.11.128 10.30.11.254
SWD1(config)#Ip dhcp excluded-address 10.30.12.128 10.30.12.254
SWD1(config)#Ip dhcp excluded-address 10.30.13.128 10.30.13.254
SWD1(config)#Ip dhcp excluded-address 10.30.14.128 10.30.14.254
SWD1(config)#Ip dhcp excluded-address 10.30.15.128 10.30.15.254
SWD1(config)#Ip dhcp excluded-address 10.30.16.128 10.30.16.254
SWD1(config)#Ip dhcp excluded-address 10.30.17.128 10.30.17.254
SWD1(config)#Ip dhcp excluded-address 10.30.18.128 10.30.18.254
SWD1(config)#Ip dhcp excluded-address 10.30.20.128 10.30.20.254
SWD1(config)#Ip dhcp excluded-address 10.30.21.128 10.30.21.254
SWD1(config)#Ip dhcp excluded-address 10.30.22.128 10.30.22.254
SWD1(config)#Ip dhcp excluded-address 10.30.23.128 10.30.23.254
SWD1(config)#Ip dhcp excluded-address 10.30.24.128 10.30.24.254
SWD1(config)#Ip dhcp excluded-address 10.30.25.128 10.30.25.254
SWD1(config)#Ip dhcp excluded-address 10.30.26.128 10.30.26.254
SWD1(config)#Ip dhcp excluded-address 10.30.27.128 10.30.27.254
SWD1(config)#Ip dhcp excluded-address 10.30.28.128 10.30.28.254
SWD1(config)#Ip dhcp excluded-address 10.30.29.128 10.30.29.254
SWD1(config)#Ip dhcp excluded-address 10.30.30.128 10.30.30.254
SWD1(config)#Ip dhcp excluded-address 10.30.31.128 10.30.31.254
SWD1(config)#Ip dhcp excluded-address 10.30.32.128 10.30.32.254
SWD1(config)#Ip dhcp excluded-address 10.30.33.128 10.30.33.254
SWD1(config)#Ip dhcp excluded-address 10.30.36.128 10.30.36.254
```

Figure 3-33 : Les adresses exclues 128-254 sur SWD1

Aussi nous allons exclure les adresses 1 à 127 et 252 à 254 sur SWD2 c'est-à-dire le SWD2 va attribuer les adresses allant de 128 à 251.

```
SWD2(config)#Ip dhcp excluded-address 10.30.10.1 10.30.10.127
SWD2(config)#Ip dhcp excluded-address 10.30.11.1 10.30.11.127
SWD2(config)#Ip dhcp excluded-address 10.30.12.1 10.30.12.127
SWD2(config)#Ip dhcp excluded-address 10.30.13.1 10.30.13.127
SWD2(config)#Ip dhcp excluded-address 10.30.14.1 10.30.14.127
SWD2(config)#Ip dhcp excluded-address 10.30.15.1 10.30.15.127
SWD2(config)#Ip dhcp excluded-address 10.30.16.1 10.30.16.127
SWD2(config)#Ip dhcp excluded-address 10.30.17.1 10.30.17.127
SWD2(config)#Ip dhcp excluded-address 10.30.18.1 10.30.18.127
SWD2(config)#Ip dhcp excluded-address 10.30.20.1 10.30.20.127
SWD2(config)#Ip dhcp excluded-address 10.30.21.1 10.30.21.127
SWD2(config)#Ip dhcp excluded-address 10.30.22.1 10.30.22.127
SWD2(config)#Ip dhcp excluded-address 10.30.23.1 10.30.23.127
SWD2(config)#Ip dhcp excluded-address 10.30.24.1 10.30.24.127
SWD2(config)#Ip dhcp excluded-address 10.30.25.1 10.30.25.127
SWD2(config)#Ip dhcp excluded-address 10.30.26.1 10.30.26.127
SWD2(config)#Ip dhcp excluded-address 10.30.27.1 10.30.27.127
SWD2(config)#Ip dhcp excluded-address 10.30.28.1 10.30.28.127
SWD2(config)#Ip dhcp excluded-address 10.30.29.1 10.30.29.127
SWD2(config)#Ip dhcp excluded-address 10.30.30.1 10.30.30.127
SWD2(config)#Ip dhcp excluded-address 10.30.31.1 10.30.31.127
SWD2(config)#Ip dhcp excluded-address 10.30.32.1 10.30.32.127
SWD2(config)#Ip dhcp excluded-address 10.30.33.1 10.30.33.127
SWD2(config)#Ip dhcp excluded-address 10.30.36.1 10.30.36.127
```

Figure 3-34 : Les adresses exclues 1-127 sur SWD2

```
SWD2(config)#Ip dhcp excluded-address 10.30.10.252 10.30.10.254
SWD2(config)#Ip dhcp excluded-address 10.30.11.252 10.30.11.254
SWD2(config)#Ip dhcp excluded-address 10.30.12.252 10.30.12.254
SWD2(config)#Ip dhcp excluded-address 10.30.13.252 10.30.13.254
SWD2(config)#Ip dhcp excluded-address 10.30.14.252 10.30.14.254
SWD2(config)#Ip dhcp excluded-address 10.30.15.252 10.30.15.254
SWD2(config)#Ip dhcp excluded-address 10.30.16.252 10.30.16.254
SWD2(config)#Ip dhcp excluded-address 10.30.17.252 10.30.17.254
SWD2(config)#Ip dhcp excluded-address 10.30.18.252 10.30.18.254
SWD2(config)#Ip dhcp excluded-address 10.30.20.252 10.30.20.254
SWD2(config)#Ip dhcp excluded-address 10.30.21.252 10.30.21.254
SWD2(config)#Ip dhcp excluded-address 10.30.22.252 10.30.22.254
SWD2(config)#Ip dhcp excluded-address 10.30.23.252 10.30.23.254
SWD2(config)#Ip dhcp excluded-address 10.30.24.252 10.30.24.254
SWD2(config)#Ip dhcp excluded-address 10.30.25.252 10.30.25.254
SWD2(config)#Ip dhcp excluded-address 10.30.26.252 10.30.26.254
SWD2(config)#Ip dhcp excluded-address 10.30.27.252 10.30.27.254
SWD2(config)#Ip dhcp excluded-address 10.30.28.252 10.30.28.254
SWD2(config)#Ip dhcp excluded-address 10.30.29.252 10.30.29.254
SWD2(config)#Ip dhcp excluded-address 10.30.30.252 10.30.30.254
SWD2(config)#Ip dhcp excluded-address 10.30.31.252 10.30.31.254
SWD2(config)#Ip dhcp excluded-address 10.30.32.252 10.30.32.254
SWD2(config)#Ip dhcp excluded-address 10.30.33.252 10.30.33.254
SWD2(config)#Ip dhcp excluded-address 10.30.36.252 10.30.36.254
```

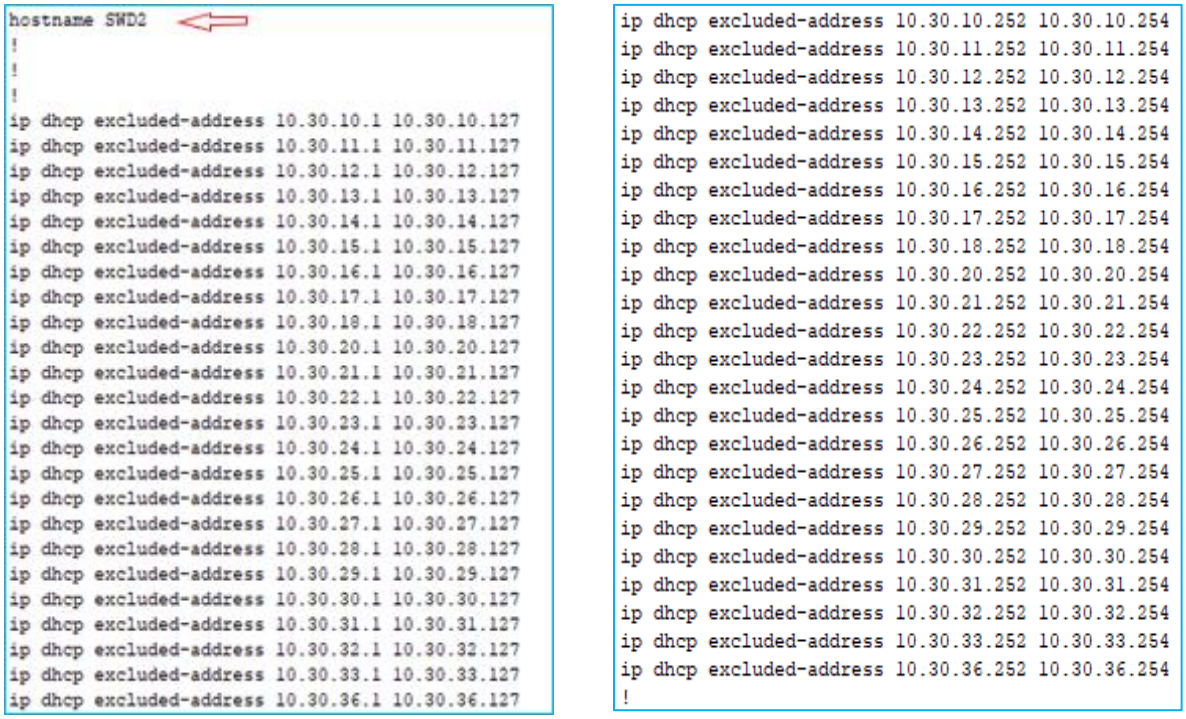
Figure 3-35 : Les adresses exclues 252-254 sur SWD2.

Avec la commande **show running-config** nous pouvons vérifier les adresses exclues sur le Switch SWD1 comme la figure 3-36 le montre :

```
hostname SWD1
!
!
!
ip dhcp excluded-address 10.30.10.128 10.30.10.254
ip dhcp excluded-address 10.30.11.128 10.30.11.254
ip dhcp excluded-address 10.30.12.128 10.30.12.254
ip dhcp excluded-address 10.30.13.128 10.30.13.254
ip dhcp excluded-address 10.30.14.128 10.30.14.254
ip dhcp excluded-address 10.30.15.128 10.30.15.254
ip dhcp excluded-address 10.30.16.128 10.30.16.254
ip dhcp excluded-address 10.30.17.128 10.30.17.254
ip dhcp excluded-address 10.30.18.128 10.30.18.254
ip dhcp excluded-address 10.30.20.128 10.30.20.254
ip dhcp excluded-address 10.30.21.128 10.30.21.254
ip dhcp excluded-address 10.30.22.128 10.30.22.254
ip dhcp excluded-address 10.30.23.128 10.30.23.254
ip dhcp excluded-address 10.30.24.128 10.30.24.254
ip dhcp excluded-address 10.30.25.128 10.30.25.254
ip dhcp excluded-address 10.30.26.128 10.30.26.254
ip dhcp excluded-address 10.30.27.128 10.30.27.254
ip dhcp excluded-address 10.30.28.128 10.30.28.254
ip dhcp excluded-address 10.30.29.128 10.30.29.254
ip dhcp excluded-address 10.30.30.128 10.30.30.254
ip dhcp excluded-address 10.30.31.128 10.30.31.254
ip dhcp excluded-address 10.30.32.128 10.30.32.254
ip dhcp excluded-address 10.30.33.128 10.30.33.254
ip dhcp excluded-address 10.30.36.128 10.30.36.254
!
```

Figure 3-36 : Vérification des adresses exclues sur SWD1

Avec la même commande nous vérifions aussi les adresses exclues sur le switch SWD2 comme la figure 3-37 le montre :



```
hostname SWD2
!
!
!
ip dhcp excluded-address 10.30.10.1 10.30.10.127
ip dhcp excluded-address 10.30.11.1 10.30.11.127
ip dhcp excluded-address 10.30.12.1 10.30.12.127
ip dhcp excluded-address 10.30.13.1 10.30.13.127
ip dhcp excluded-address 10.30.14.1 10.30.14.127
ip dhcp excluded-address 10.30.15.1 10.30.15.127
ip dhcp excluded-address 10.30.16.1 10.30.16.127
ip dhcp excluded-address 10.30.17.1 10.30.17.127
ip dhcp excluded-address 10.30.18.1 10.30.18.127
ip dhcp excluded-address 10.30.20.1 10.30.20.127
ip dhcp excluded-address 10.30.21.1 10.30.21.127
ip dhcp excluded-address 10.30.22.1 10.30.22.127
ip dhcp excluded-address 10.30.23.1 10.30.23.127
ip dhcp excluded-address 10.30.24.1 10.30.24.127
ip dhcp excluded-address 10.30.25.1 10.30.25.127
ip dhcp excluded-address 10.30.26.1 10.30.26.127
ip dhcp excluded-address 10.30.27.1 10.30.27.127
ip dhcp excluded-address 10.30.28.1 10.30.28.127
ip dhcp excluded-address 10.30.29.1 10.30.29.127
ip dhcp excluded-address 10.30.30.1 10.30.30.127
ip dhcp excluded-address 10.30.31.1 10.30.31.127
ip dhcp excluded-address 10.30.32.1 10.30.32.127
ip dhcp excluded-address 10.30.33.1 10.30.33.127
ip dhcp excluded-address 10.30.36.1 10.30.36.127
```

```
ip dhcp excluded-address 10.30.10.252 10.30.10.254
ip dhcp excluded-address 10.30.11.252 10.30.11.254
ip dhcp excluded-address 10.30.12.252 10.30.12.254
ip dhcp excluded-address 10.30.13.252 10.30.13.254
ip dhcp excluded-address 10.30.14.252 10.30.14.254
ip dhcp excluded-address 10.30.15.252 10.30.15.254
ip dhcp excluded-address 10.30.16.252 10.30.16.254
ip dhcp excluded-address 10.30.17.252 10.30.17.254
ip dhcp excluded-address 10.30.18.252 10.30.18.254
ip dhcp excluded-address 10.30.20.252 10.30.20.254
ip dhcp excluded-address 10.30.21.252 10.30.21.254
ip dhcp excluded-address 10.30.22.252 10.30.22.254
ip dhcp excluded-address 10.30.23.252 10.30.23.254
ip dhcp excluded-address 10.30.24.252 10.30.24.254
ip dhcp excluded-address 10.30.25.252 10.30.25.254
ip dhcp excluded-address 10.30.26.252 10.30.26.254
ip dhcp excluded-address 10.30.27.252 10.30.27.254
ip dhcp excluded-address 10.30.28.252 10.30.28.254
ip dhcp excluded-address 10.30.29.252 10.30.29.254
ip dhcp excluded-address 10.30.30.252 10.30.30.254
ip dhcp excluded-address 10.30.31.252 10.30.31.254
ip dhcp excluded-address 10.30.32.252 10.30.32.254
ip dhcp excluded-address 10.30.33.252 10.30.33.254
ip dhcp excluded-address 10.30.36.252 10.30.36.254
!
```

Figure 3-37 : Vérification des adresses exclues sur SWD2

Nous allons créer maintenant un pool d'adresse pour chaque vlan à l'exception du vlan 18 (printer), vlan 20 (téléphone) vlan 21(Voice), vlan 25 (Management), et vlan 32(Camera), par la suite on définira la passerelle par défaut du sous réseau.

```
SWD1(config)#Ip dhcp pool vlan10
SWD1(dhcp-config)#Network  10.30.10.0 255.255.255.0
SWD1(dhcp-config)#Default-router 10.30.10.254
SWD1(dhcp-config)#Exit
SWD1(config)#
```

Figure 3-38 : Exemple de création d'un pool pour le Vlan 10 sur le SWD1

Nous allons vérifier la création de nos pools DHCP avec la commande **show running-config**

```
ip dhcp pool vlan10
 network 10.30.10.0 255.255.255.0
 default-router 10.30.10.254
ip dhcp pool vlan11
 network 10.30.11.0 255.255.255.0
 default-router 10.30.11.254
ip dhcp pool vlan12
 network 10.30.12.0 255.255.255.0
 default-router 10.30.12.254
ip dhcp pool vlan13
 network 10.30.13.0 255.255.255.0
 default-router 10.30.13.254
ip dhcp pool vlan14
 network 10.30.14.0 255.255.255.0
 default-router 10.30.14.254
ip dhcp pool vlan15
 network 10.30.15.0 255.255.255.0
 default-router 10.30.15.254
ip dhcp pool vlan16
 network 10.30.16.0 255.255.255.0
 default-router 10.30.16.254
ip dhcp pool vlan17
 network 10.30.17.0 255.255.255.0
 default-router 10.30.17.254
ip dhcp pool vlan18
 network 10.30.18.0 255.255.255.0
 default-router 10.30.18.254
ip dhcp pool vlan20
 network 10.30.20.0 255.255.255.0
 default-router 10.30.20.254
ip dhcp pool vlan21
 network 10.30.21.0 255.255.255.0
 default-router 10.30.21.254
ip dhcp pool vlan22
 network 10.30.22.0 255.255.255.0
 default-router 10.30.22.254
```

```
ip dhcp pool vlan23
 network 10.30.23.0 255.255.255.0
 default-router 10.30.23.254
ip dhcp pool vlan24
 network 10.30.24.0 255.255.255.0
 default-router 10.30.24.254
ip dhcp pool vlan25
 network 10.30.25.0 255.255.255.0
 default-router 10.30.25.254
ip dhcp pool vlan26
 network 10.30.26.0 255.255.255.0
 default-router 10.30.26.254
ip dhcp pool vlan27
 network 10.30.27.0 255.255.255.0
 default-router 10.30.27.254
ip dhcp pool vlan28
 network 10.30.28.0 255.255.255.0
 default-router 10.30.28.254
ip dhcp pool vlan29
 network 10.30.29.0 255.255.255.0
 default-router 10.30.29.254
ip dhcp pool vlan30
 network 10.30.30.0 255.255.255.0
 default-router 10.30.30.254
ip dhcp pool vlan31
 network 10.30.31.0 255.255.255.0
 default-router 10.30.31.254
ip dhcp pool vlan32
 network 10.30.32.0 255.255.255.0
 default-router 10.30.32.254
ip dhcp pool vlan33
 network 10.30.33.0 255.255.255.0
 default-router 10.30.33.254
ip dhcp pool vlan36
 network 10.30.36.0 255.255.255.0
 default-router 10.30.36.254
```

Figure 3-39 : Vérification de la création des pools DHCP

Après la configuration du DHCP, nous allons configurer les PC en mode DHCP afin qu'ils reçoivent la configuration du réseau dynamiquement.

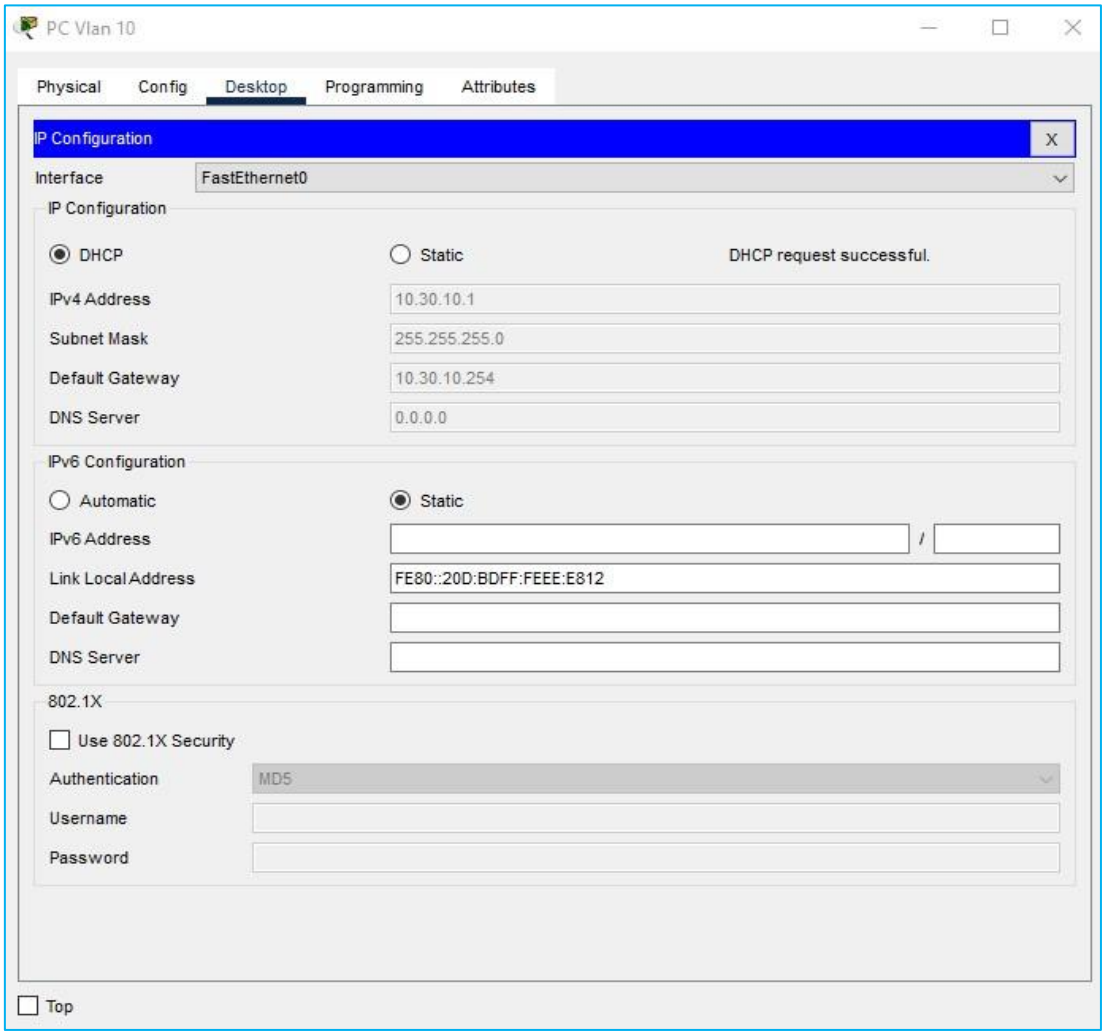


Figure 3-40 : Configurer le DHCP sur le pc et vérifier son fonctionnement.

3.12 Configuration de protocole de la haute disponibilité (HSRP)

3.12.1 Configuration des SVI (Switch Virtual Interface)

Durant cette étape nous allons configurer les SVI de chaque vlan, autrement dit, nous allons attribuer une adresses IP virtuel pour chaque vlan sur les deux switches de distribution SWD1 et SWD2, cela va nous permettre de faire un routage inter-vlan, mais ce dernier ne se fera pas sauf si on active la fonction de routage avec la commande **ip routing**.

```
SWD1>en
SWD1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1(config)#ip routing
SWD1(config)#
```

Figure 3-41: Configuration d'ip routing

Afin de configurer prochainement le protocole HSRP, à présent nous allons attribuer les adresses aux SVI avec **252** sur la partie machine de chaque vlan sur le SWD1, et sur le SWD2 nous allons faire **253** sur la partie machine de chaque vlan.

```
SWD1(config)#Int vlan 10
SWD1(config-if)#Ip address 10.30.10.252 255.255.255.0
SWD1(config-if)#No sh
SWD1(config-if)#Exit
```

Figure 3-42 : Configuration SVI sur SWD1

Après avoir configuré les SVI de chaque vlan nous allons vérifier avec la commande **show running-config.**

```
interface Vlan10
 mac-address 0030.a33c.3c01
 ip address 10.30.10.252 255.255.255.0
!
interface Vlan11
 mac-address 0030.a33c.3c02
 ip address 10.30.11.252 255.255.255.0
!
interface Vlan12
 mac-address 0030.a33c.3c03
 ip address 10.30.12.252 255.255.255.0
!
interface Vlan13
 mac-address 0030.a33c.3c04
 ip address 10.30.13.252 255.255.255.0
!
interface Vlan14
 mac-address 0030.a33c.3c05
 ip address 10.30.14.252 255.255.255.0
!
interface Vlan15
 mac-address 0030.a33c.3c06
 ip address 10.30.15.252 255.255.255.0
!
interface Vlan16
 mac-address 0030.a33c.3c07
 ip address 10.30.16.252 255.255.255.0
!
interface Vlan17
 mac-address 0030.a33c.3c08
 ip address 10.30.17.252 255.255.255.0
!
interface Vlan18
 mac-address 0030.a33c.3c09
 ip address 10.30.18.252 255.255.255.0
```

```
interface Vlan20
 mac-address 0030.a33c.3c0a
 ip address 10.30.20.252 255.255.255.0
!
interface Vlan21
 mac-address 0030.a33c.3c0b
 ip address 10.30.21.252 255.255.255.0
!
interface Vlan22
 mac-address 0030.a33c.3c0c
 ip address 10.30.22.252 255.255.255.0
!
interface Vlan23
 mac-address 0030.a33c.3c0d
 ip address 10.30.23.252 255.255.255.0
!
interface Vlan24
 mac-address 0030.a33c.3c0e
 ip address 10.30.24.252 255.255.255.0
!
interface Vlan25
 mac-address 0030.a33c.3c0f
 ip address 10.30.25.252 255.255.255.0
!
interface Vlan26
 mac-address 0030.a33c.3c10
 ip address 10.30.26.252 255.255.255.0
!
interface Vlan27
 mac-address 0030.a33c.3c11
 ip address 10.30.27.252 255.255.255.0
!
interface Vlan28
 mac-address 0030.a33c.3c12
 ip address 10.30.28.252 255.255.255.0
```

```
interface Vlan29
 mac-address 0030.a33c.3c13
 ip address 10.30.29.252 255.255.255.0
!
interface Vlan30
 mac-address 0030.a33c.3c14
 ip address 10.30.30.252 255.255.255.0
!
interface Vlan31
 mac-address 0030.a33c.3c15
 ip address 10.30.31.252 255.255.255.0
!
interface Vlan32
 mac-address 0030.a33c.3c16
 ip address 10.30.32.252 255.255.255.0
!
interface Vlan33
 mac-address 0030.a33c.3c17
 ip address 10.30.33.252 255.255.255.0
!
interface Vlan36
 mac-address 0030.a33c.3c18
 ip address 10.30.36.252 255.255.255.0
```

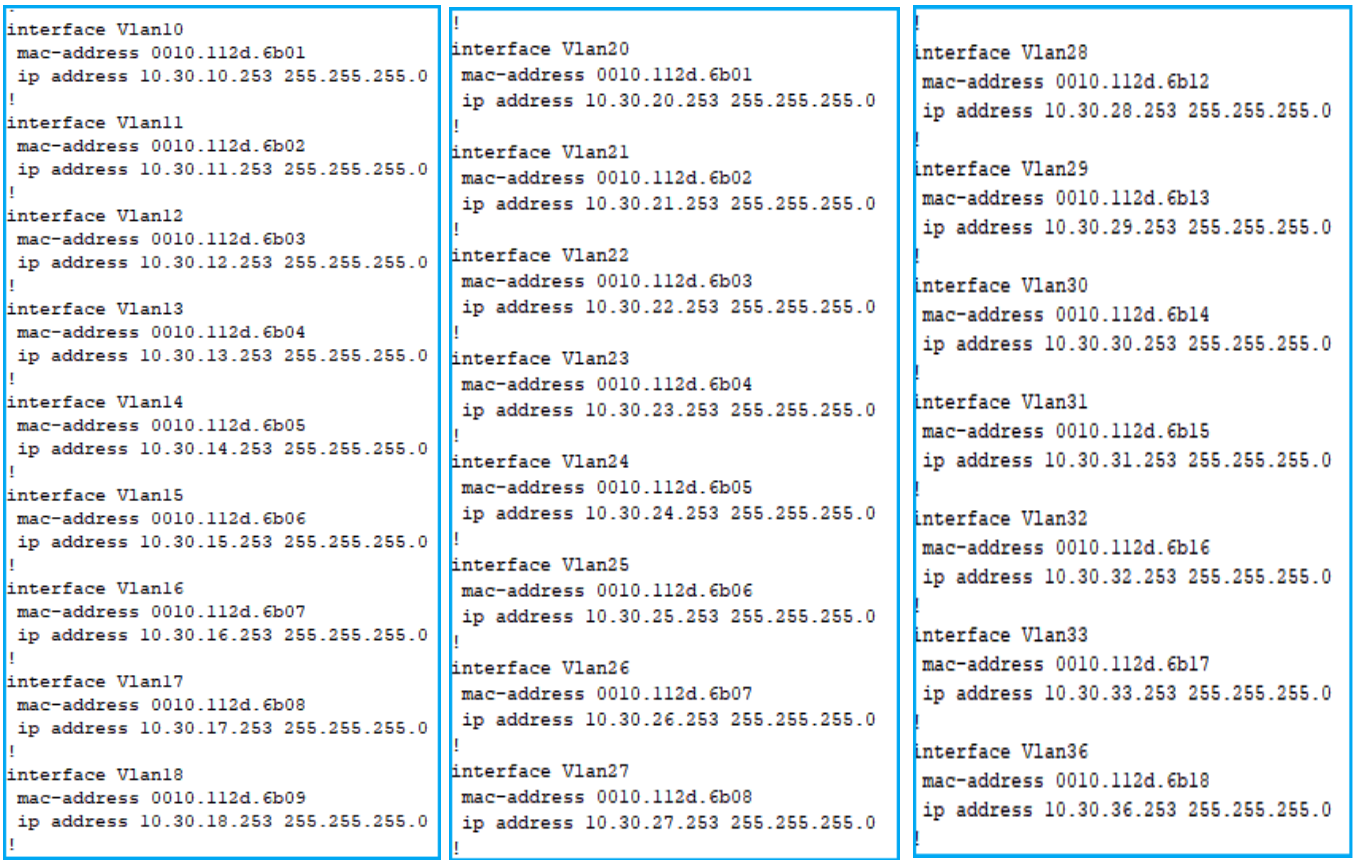
Figure 3-43 : Vérification SVI sur SWD1

Nous allons procéder la même chose sur SWD2 mais avec un 253 sur la partie machine.

```
SWD2(config)#Int vlan 10
SWD2(config-if)#Ip address 10.30.10.253 255.255.255.0
SWD2(config-if)#No sh
SWD2(config-if)#Exit
```

Figure 3-44 : Configuration SVI sur SWD2

Nous allons aussi vérifier la configuration SVI sur chaque Vlan avec la commande « **show running-config ».**



```
interface Vlan10
 mac-address 0010.112d.6b01
 ip address 10.30.10.253 255.255.255.0
!
interface Vlan11
 mac-address 0010.112d.6b02
 ip address 10.30.11.253 255.255.255.0
!
interface Vlan12
 mac-address 0010.112d.6b03
 ip address 10.30.12.253 255.255.255.0
!
interface Vlan13
 mac-address 0010.112d.6b04
 ip address 10.30.13.253 255.255.255.0
!
interface Vlan14
 mac-address 0010.112d.6b05
 ip address 10.30.14.253 255.255.255.0
!
interface Vlan15
 mac-address 0010.112d.6b06
 ip address 10.30.15.253 255.255.255.0
!
interface Vlan16
 mac-address 0010.112d.6b07
 ip address 10.30.16.253 255.255.255.0
!
interface Vlan17
 mac-address 0010.112d.6b08
 ip address 10.30.17.253 255.255.255.0
!
interface Vlan18
 mac-address 0010.112d.6b09
 ip address 10.30.18.253 255.255.255.0
!
```

```
!
interface Vlan20
 mac-address 0010.112d.6b01
 ip address 10.30.20.253 255.255.255.0
!
interface Vlan21
 mac-address 0010.112d.6b02
 ip address 10.30.21.253 255.255.255.0
!
interface Vlan22
 mac-address 0010.112d.6b03
 ip address 10.30.22.253 255.255.255.0
!
interface Vlan23
 mac-address 0010.112d.6b04
 ip address 10.30.23.253 255.255.255.0
!
interface Vlan24
 mac-address 0010.112d.6b05
 ip address 10.30.24.253 255.255.255.0
!
interface Vlan25
 mac-address 0010.112d.6b06
 ip address 10.30.25.253 255.255.255.0
!
interface Vlan26
 mac-address 0010.112d.6b07
 ip address 10.30.26.253 255.255.255.0
!
interface Vlan27
 mac-address 0010.112d.6b08
 ip address 10.30.27.253 255.255.255.0
!
```

```
!
interface Vlan28
 mac-address 0010.112d.6b12
 ip address 10.30.28.253 255.255.255.0
!
interface Vlan29
 mac-address 0010.112d.6b13
 ip address 10.30.29.253 255.255.255.0
!
interface Vlan30
 mac-address 0010.112d.6b14
 ip address 10.30.30.253 255.255.255.0
!
interface Vlan31
 mac-address 0010.112d.6b15
 ip address 10.30.31.253 255.255.255.0
!
interface Vlan32
 mac-address 0010.112d.6b16
 ip address 10.30.32.253 255.255.255.0
!
interface Vlan33
 mac-address 0010.112d.6b17
 ip address 10.30.33.253 255.255.255.0
!
interface Vlan36
 mac-address 0010.112d.6b18
 ip address 10.30.36.253 255.255.255.0
!
```

Figure 3-45 : Vérification SVI sur SWD2.

3.12.2 Configuration de protocole HSRP

Maintenant nous allons configurer le protocole HSRP au niveau des deux switches de distribution SWD1 et SWD2, on définit un groupe HSRP, une priorité « **standbay priority** » la plus élevée qui décide le commutateur “active”, et de la préemption « **standby preempt** » comme suite :

✓ Sur SWD1 pour les Vlans 10 à 22 :

```
SWD1(config)#Int vlan10
SWD1(config-if)#Standby 10 ip 10.30.10.254
SWD1(config-if)#Standby 10 priority 200
SWD1(config-if)#Standby 10 preempt
SWD1(config-if)#exit
```

Figure 3-46 : Configuration du HSRP (Vlan 10 à 22).

✓ Sur SWD1 pour les Vlans 23 à 36 :

```
SWD1(config)#Int vlan23
SWD1(config-if)#Standby 23 ip 10.30.23.254
SWD1(config-if)#Standby 23 priority 100
SWD1(config-if)#Standby 23 preempt
SWD1(config-if)#exit
```

Figure 3-47 : Configuration du HSRP (Vlan 23 à 36).

On procédera de même pour le SWD2 :

✓ Pour les Vlans 23 à 36 :

```
SWD2(config)#Int vlan10
SWD2(config-if)#Standby 10 ip 10.30.10.254
SWD2(config-if)#Standby 10 priority 100
SWD2(config-if)#Standby 10 preempt
SWD2(config-if)#exit
```

Figure 3-48 : Configuration du HSRP (Vlan 23 à 36).

✓ Pour les Vlans 10 à 22 :

```
SWD2(config)#Int vlan23
SWD2(config-if)#Standby 23 ip 10.30.23.254
SWD2(config-if)#Standby 23 priority 200
SWD2(config-if)#Standby 23 preempt
SWD2(config-if)#exit
```

Figure 3-49 : Configuration du HSRP (Vlan 10 à 22).

Nous allons vérifier cette configuration avec la commande **show standby brief.**

✓ Sur SWD1 :

```
SWD1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   200 P Active   local           10.30.10.253    10.30.10.254
Vl11        11   200 P Active   local           10.30.11.253    10.30.11.254
Vl12        12   200 P Active   local           10.30.12.253    10.30.12.254
Vl13        13   200 P Active   local           10.30.13.253    10.30.13.254
Vl14        14   200 P Active   local           10.30.14.253    10.30.14.254
Vl15        15   200 P Active   local           10.30.15.253    10.30.15.254
Vl16        16   200 P Active   local           10.30.16.253    10.30.16.254
Vl17        17   200 P Active   local           10.30.17.253    10.30.17.254
Vl18        18   200 P Active   local           10.30.18.253    10.30.18.254
Vl20        20   200 P Active   local           10.30.20.253    10.30.20.254
Vl21        21   200 P Active   local           10.30.21.253    10.30.21.254
Vl22        22   200 P Active   local           10.30.22.253    10.30.22.254
Vl23        23   100 P Standby  10.30.23.253    local           10.30.23.254
Vl24        24   100 P Standby  10.30.24.253    local           10.30.24.254
Vl25        25   100 P Standby  10.30.25.253    local           10.30.25.254
Vl26        26   100 P Standby  10.30.26.253    local           10.30.26.254
Vl27        27   100 P Standby  10.30.27.253    local           10.30.27.254
Vl28        28   100 P Standby  10.30.28.253    local           10.30.28.254
Vl29        29   100 P Standby  10.30.29.253    local           10.30.29.254
Vl30        30   100 P Standby  10.30.30.253    local           10.30.30.254
Vl31        31   100 P Standby  10.30.31.253    local           10.30.31.254
Vl32        32   100 P Standby  10.30.32.253    local           10.30.32.254
Vl33        33   100 P Standby  10.30.33.253    local           10.30.33.254
Vl36        36   100 P Standby  10.30.36.253    local           10.30.36.254
SWD1#
```

Figure 3-50 : Vérification du HSRP sur SWD1

✓ Sur SWD2 :

```
SWD2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   100 P Standby  10.30.10.252    local           10.30.10.254
Vl11        11   100 P Standby  10.30.11.252    local           10.30.11.254
Vl12        12   100 P Standby  10.30.12.252    local           10.30.12.254
Vl13        13   100 P Standby  10.30.13.252    local           10.30.13.254
Vl14        14   100 P Standby  10.30.14.252    local           10.30.14.254
Vl15        15   100 P Standby  10.30.15.252    local           10.30.15.254
Vl16        16   100 P Standby  10.30.16.252    local           10.30.16.254
Vl17        17   100 P Standby  10.30.17.252    local           10.30.17.254
Vl18        18   100 P Standby  10.30.18.252    local           10.30.18.254
Vl20        20   100 P Standby  10.30.20.252    local           10.30.20.254
Vl21        21   100 P Standby  10.30.21.252    local           10.30.21.254
Vl22        22   100 P Standby  10.30.22.252    local           10.30.22.254
Vl23        23   200 P Active   local           10.30.23.252    10.30.23.254
Vl24        24   200 P Active   local           10.30.24.252    10.30.24.254
Vl25        25   200 P Active   local           10.30.25.252    10.30.25.254
Vl26        26   200 P Active   local           10.30.26.252    10.30.26.254
Vl27        27   200 P Active   local           10.30.27.252    10.30.27.254
Vl28        28   200 P Active   local           10.30.28.252    10.30.28.254
Vl29        29   200 P Active   local           10.30.29.252    10.30.29.254
Vl30        30   200 P Active   local           10.30.30.252    10.30.30.254
Vl31        31   200 P Active   local           10.30.31.252    10.30.31.254
Vl32        32   200 P Active   local           10.30.32.252    10.30.32.254
Vl33        33   200 P Active   local           10.30.33.252    10.30.33.254
Vl36        36   200 P Active   local           10.30.36.252    10.30.36.254
SWD2#
```

Figure 3-51 : Vérification du HSRP sur SWD2

3.13 Configurations de Protocole OSPF :

Ici pour l'OSPF, nous allons configurer ce Protocol au niveau des switches de distribution et ceux du Core. Nous allons tout d'abord convertir les ports de couche 2 en des ports de couche 3 et les faire fonctionner comme des interfaces de routeur plutôt que comme des ports de commutateur en utilisant la commande **« no switchport »,** puis on attribue une adresse IP et un masque de réseau pour chacun des ports routés.

Les figures ci-dessous montrent la configuration des ports routés :

✓ Sur le SWD1 :

```
SWD1(config)#interface f0/19
SWD1(config-if)#no switchport
SWD1(config-if)#ip address 172.16.2.1 255.255.255.252
SWD1(config-if)#no shutdown
SWD1(config-if)#interface f0/20
SWD1(config-if)#no shutdown
SWD1(config-if)#ip address 172.16.1.1 255.255.255.252
SWD1(config-if)#no shutdown
SWD1(config-if)#exit
```

Figure 3-52 : Configuration des ports routés sur SWD1.

✓ Sur le SWD2 :

```
SWD2(config)#interface f0/19
SWD2(config-if)#no switchport
SWD2(config-if)#ip address 172.16.3.1 255.255.255.252
SWD2(config-if)#no shutdown
SWD2(config-if)#exit
SWD2(config)#interface f0/20
SWD2(config-if)#no switchport
SWD2(config-if)#ip address 172.16.4.1 255.255.255.252
SWD2(config-if)#no shutdown
SWD2(config-if)#exit
```

Figure 3-53 : Configuration des ports routés sur SWD2.

✓ Sur le switch Core1 :

```
Core1(config)#Interface f0/1
Core1(config-if)#No switchport
Core1(config-if)#Ip address 172.16.3.2 255.255.255.252
Core1(config-if)#No sh
Core1(config-if)#exit
Core1(config)#Interface f0/2
Core1(config-if)#No switchport
Core1(config-if)#Ip address 172.16.1.2 255.255.255.252
Core1(config-if)#No sh
Core1(config-if)#Exit
Core1(config)#Interface f0/3
Core1(config-if)#No switchport
Core1(config-if)#Ip address 172.16.5.1 255.255.255.252
Core1(config-if)#No sh
Core1(config-if)#exit
Core1(config)#Interface f0/4
Core1(config-if)#No switchport
Core1(config-if)#Ip address 172.16.6.1 255.255.255.252
Core1(config-if)#No sh
Core1(config-if)#Exit
```

Figure 3-54 : Configuration des ports routés sur Core1.

✓ Sur le switch Core2 :

```
Core2(config)#Interface f0/1
Core2(config-if)#No switchport
Core2(config-if)#Ip address 172.16.2.2 255.255.255.252
Core2(config-if)#No sh
Core2(config-if)#exit
Core2(config)#Interface f0/2
Core2(config-if)#No switchport
Core2(config-if)#Ip address 172.16.4.2 255.255.255.252
Core2(config-if)#No sh
Core2(config-if)#Exit
Core2(config)#Interface f0/3
Core2(config-if)#No switchport
Core2(config-if)#Ip address 172.16.5.2 255.255.255.252
Core2(config-if)#No sh
Core2(config-if)#exit
Core2(config)#Interface f0/4
Core2(config-if)#No switchport
Core2(config-if)#Ip address 172.16.7.1 255.255.255.252
Core2(config-if)#No sh
Core2(config-if)#Exit
```

Figure 3-55 : Configuration des ports routés sur Core2.

✓ Sur le routeur Router :

```
Router(config)#Interface g0/0
Router(config-if)#Ip address 172.16.6.2 255.255.255.252
Router(config-if)#No sh

Router(config-if)#exit
Router(config)#Interface g0/1
Router(config-if)#Ip address 172.16.7.2 255.255.255.252
Router(config-if)#No sh

Router(config-if)#Exit
```

Figure 3-56 : Configuration des ports routés sur Router.

Ensuite nous allons activer le routage OSPF on attribue un groupe 1 par exemple et nous allons saisir tous les réseaux directement connectés dans chaque switch.

Pour les Vlans, nous allons saisir le réseau 10.30.X.0 avec un masque inversé 0.0.0.255 comme suit :

✓ Sur SWD1 :

```
SWD1(config)#Ip routing
SWD1(config)#Router ospf 1
SWD1(config-router)#Network 172.16.1.0  0.0.0.3 area 0
SWD1(config-router)#Network 172.16.2.0  0.0.0.3 area 0
SWD1(config-router)#Network 10.30.10.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.11.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.12.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.13.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.14.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.15.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.16.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.17.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.18.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.20.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.21.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.22.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.23.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.24.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.25.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.26.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.27.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.28.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.29.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.30.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.31.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.32.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.33.0  0.0.0.255 area 0
SWD1(config-router)#Network 10.30.36.0  0.0.0.255 area 0
SWD1(config-router)#exit
SWD1(config)#
```

Figure 3-57:Configuration de l'OSPF sur SWD1

✓ Sur SWD2 :

```
SWD2(config)#Ip routing
SWD2(config)#Router ospf 1
SWD2(config-router)#Network 172.16.3.0  0.0.0.3 area 0
SWD2(config-router)#Network 172.16.4.0  0.0.0.3 area 0
SWD2(config-router)#Network 10.30.10.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.11.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.12.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.13.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.14.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.15.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.16.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.17.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.18.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.20.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.21.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.22.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.23.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.24.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.25.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.26.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.27.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.28.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.29.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.30.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.31.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.32.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.33.0  0.0.0.255 area 0
SWD2(config-router)#Network 10.30.36.0  0.0.0.255 area 0
```

Figure 3-58 : Configuration de l'OSPF sur SWD2

Nous allons procéder la même chose :

- ✓ Sur le Switch Core1

```
Core1(config)#Ip routing
Core1(config)#Router ospf 1
Core1(config-router)#Network 172.16.1.0  0.0.0.3 area 0
Core1(config-router)#Network 172.16.3.0  0.0.0.3 area 0
Core1(config-router)#Network 172.16.5.0  0.0.0.3 area 0
Core1(config-router)#Network 172.16.6.0  0.0.0.3 area 0
Core1(config-router)#exit
```

Figure 3-59:Configuration de l'OSPF sur Core1

- ✓ Sur le switch Core2 :

```
Core2(config)#Ip routing
Core2(config)#Router ospf 1
Core2(config-router)#Network 172.16.2.0  0.0.0.3 area 0
Core2(config-router)#Network 172.16.4.0  0.0.0.3 area 0
Core2(config-router)#Network 172.16.5.0  0.0.0.3 area 0
Core2(config-router)#Network 172.16.7.0  0.0.0.3 area 0
Core2(config-router)#exit
Core2(config)#
```

Figure 3-60:Configuration de l'OSPF sur Core2

- ✓ Sur le routeur Router :

```
Router(config)#
Router(config)#Ip routing
Router(config)#Router ospf 1
Router(config-router)#Network 172.16.6.0  0.0.0.3 area 0
Router(config-router)#Network 172.16.7.0  0.0.0.3 area 0
Router(config-router)#exit
```

Figure 3-61:Configuration de l'OSPF sur Router

Et nous pouvons vérifier avec la commande **Show IP route**

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

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 24 subnets
O       10.30.10.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.11.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.12.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.13.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.14.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.15.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.16.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.17.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.18.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.20.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.21.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.22.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.23.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
```

```
O       10.30.24.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.25.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.26.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.27.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.28.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.29.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.30.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.31.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.32.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.33.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       10.30.36.0/24 [110/3] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/3] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
    172.16.0.0/16 is variably subnetted, 9 subnets, 2 masks
O       172.16.1.0/30 [110/2] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
O       172.16.2.0/30 [110/2] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       172.16.3.0/30 [110/2] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
O       172.16.4.0/30 [110/2] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
O       172.16.5.0/30 [110/2] via 172.16.6.1, 01:27:00, GigabitEthernet0/0
                      [110/2] via 172.16.7.1, 01:27:00, GigabitEthernet0/1
C       172.16.6.0/30 is directly connected, GigabitEthernet0/0
L       172.16.6.2/32 is directly connected, GigabitEthernet0/0
C       172.16.7.0/30 is directly connected, GigabitEthernet0/1
L       172.16.7.2/32 is directly connected, GigabitEthernet0/1
```

Figure 3-62 : Vérification de l'OSPF

3.14 La nouvelle architecture sous haute disponibilité :

Voici la nouvelle architecture avec les protocoles configurés sur elle afin qu'il s'assure son fonctionnement ainsi que l'acheminement des paquets entre le périphériques d'interconnexion. Nous avons ajouté un routeur qui est interconnecté à deux switches Cores afin de tester la fiabilité niveau 2 et niveau 3.

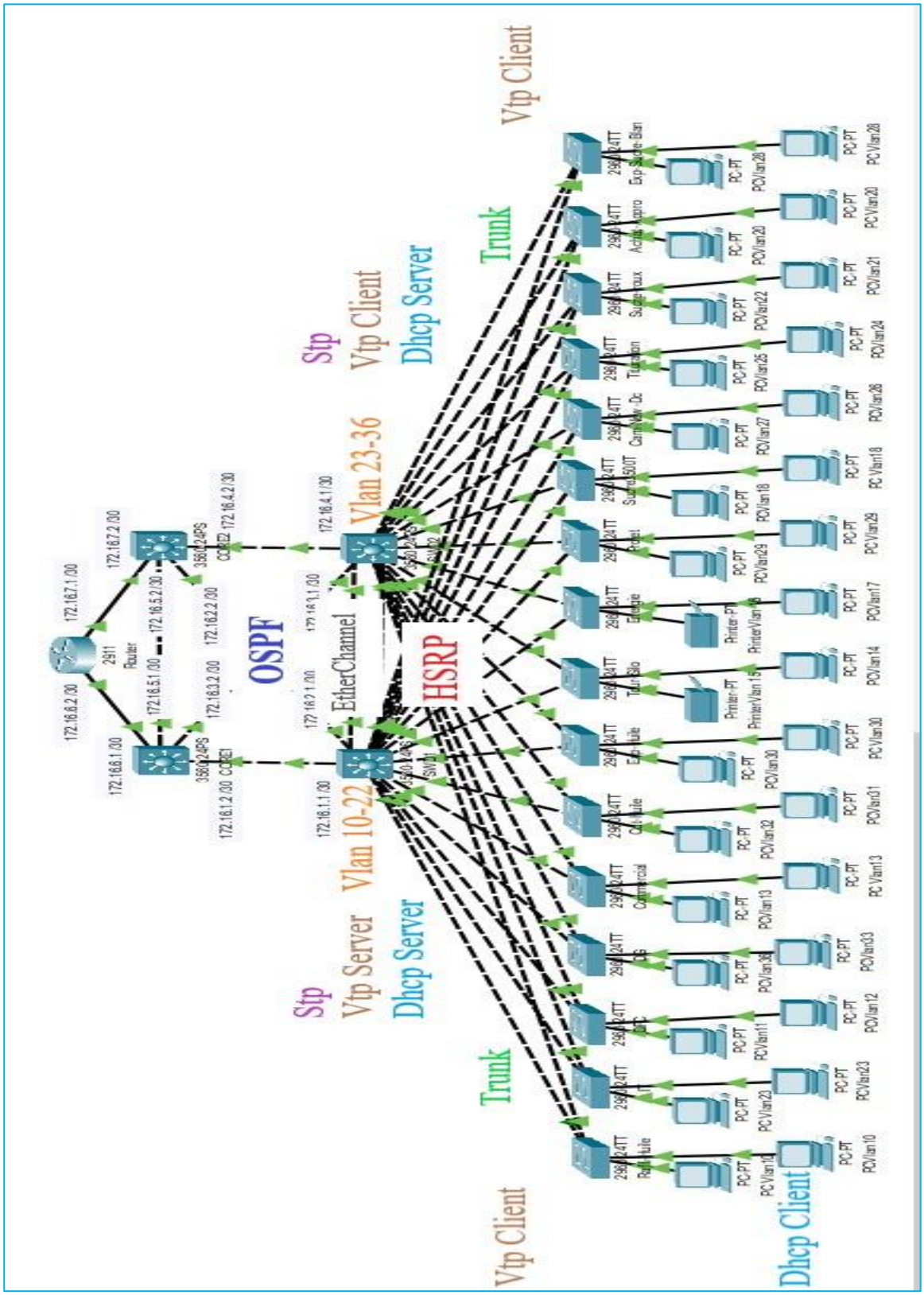


Figure 3-63 : La nouvelle architecture sous haute disponibilité

3.15 Tester la haute disponibilité du réseau

Afin de tester le bon fonctionnement de notre réseau LAN et de s'assurer qu'il est opérationnel, nous allons simuler un ping continu d'un des Vlans vers une autre interface, nous allons simuler une panne en mettant la route principale en « **shutdown** », nous allons vérifier si le ping change facilement de route, et ensuite nous allons à nouveau rallumer la route principale afin de vérifier le « **preempt** » du HSRP et qui vas à nouveau reprendre sa route principale.

- **Test entre pc de différents Vlans au niveau de la couche distribution :**

Premièrement nous avons pris un PC du VLAN 10 (**10.30.10.1**) et nous allons faire un ping continue vers VLAN 23 (**10.30.23.128),** En premier lieu nous avons constaté que le ping fonctionne parfaitement et sans problème, comme la figure 3-64 l'explique :

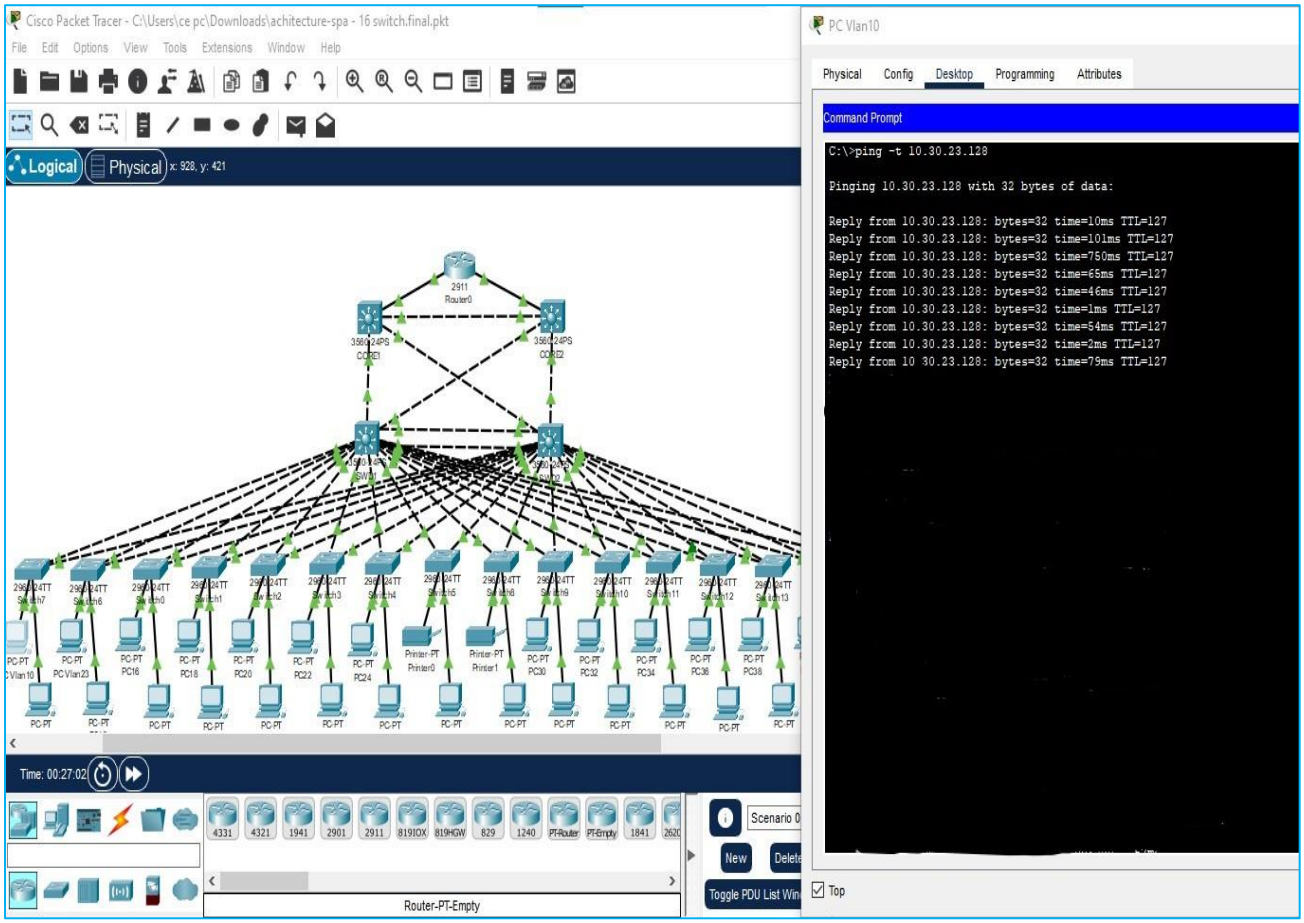


Figure 3-64 : Capture explicative du ping au niveau de la couche distribution

Ensuite nous allons simuler une panne, celle d'éteindre la route principale de ce vlan (la ligne rouge sur la figure 3-65), nous allons constater directement que le ping s'arrête, Juste après 5 ou 6 arrêts le protocole HSRP discute avec le SWD2 et active automatiquement la route qu'est standby en active, nous allons constater directement que le ping reprend, ce qui prouve que la route a bien été basculé vers le SWD2, comme est visible sur la figure 3- 65 :

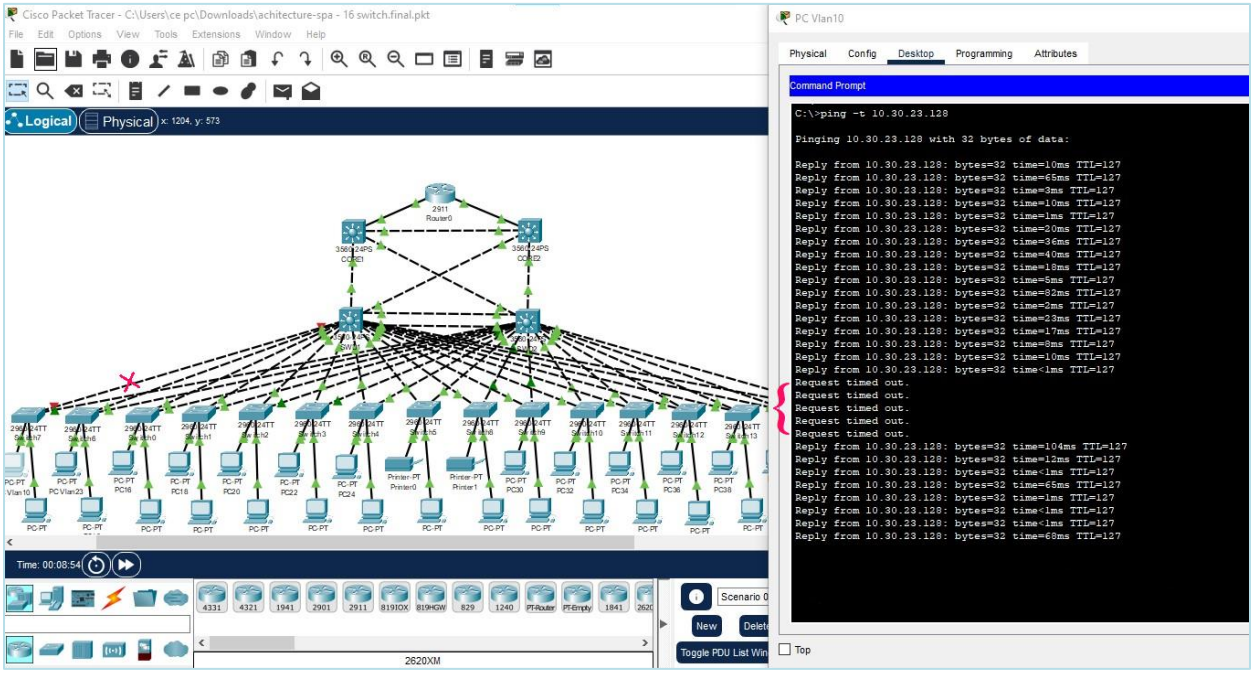


Figure 3-65 : Capture explicative du ping au niveau de la couche distribution

Maintenant, nous allons réactiver l'interface principale sur le SDW1 afin de s'assurer qu'il va reprendre sa route principale et vérifier que le preempt du HSRP fonctionne parfaitement.
Dès qu'on active l'interface, on constate qu'il y a encore un arrêt dans le ping et aussi environ 4 ou 5 arrêts le temps que les deux switches discutent les priorités il reprend facilement sa route et le ping reprend comme si rien n'était (la figure 3-66) :

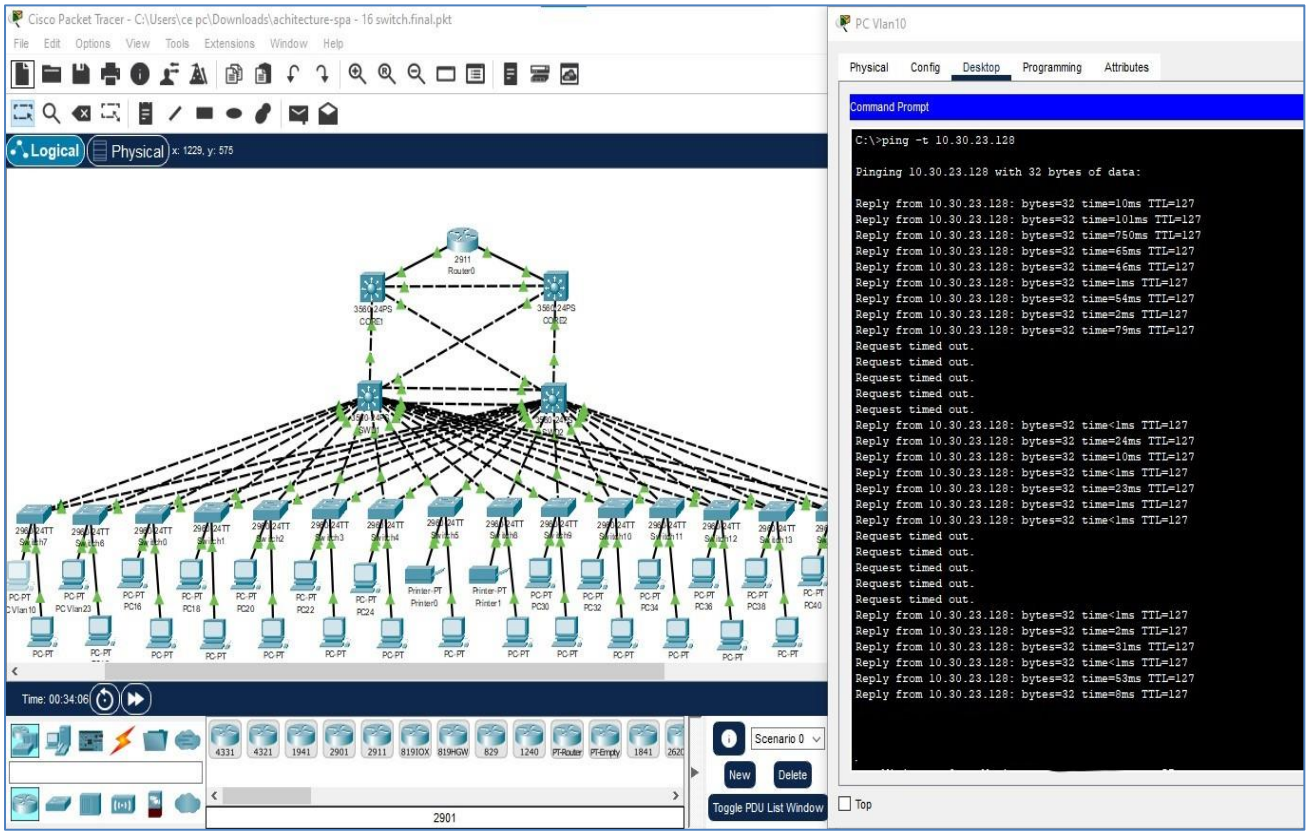


Figure 3-66: Capture explicative du Ping au niveau de la couche distribution

A présent, Nous allons simuler une panne lorsque l'un des switches de distribution est défectueux, l'autre switch prendra le relai (celui qui aura la deuxième priorité la plus haute). Lorsque le changement de Switch s'effectue, les clients vont subir une courte interruption de service due au temps de latence. Ce temps de latence sera plus court lors des prochaines interruptions de service car les Switches seront connus.

Dans l'exemple suivant, on a simulé une panne au niveau de Switch distribution SWD2. On constate qu'il y a un arrêt dans le ping et aussi environ 4 ou 5 arrêts le temps que les deux switches discutent les priorités il reprend facilement sa route et le ping reprend comme si de rien n'était, comme la figure 3-67 le montre :

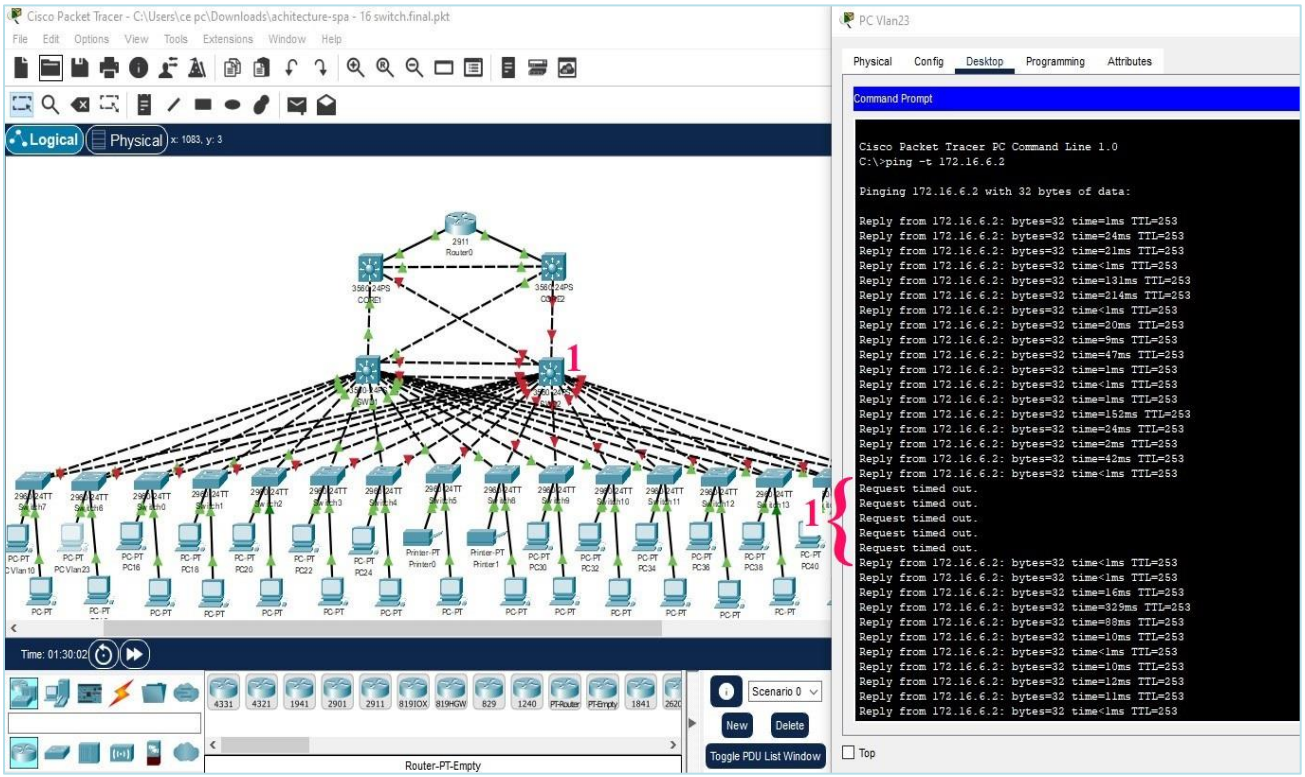


Figure 3-67 : Capture explicative du Ping au niveau de la couche distribution

- **Test de haute disponibilité du Réseau LAN de Cevital (niveau2 et niveau3) :**

Suivant la même méthode nous allons tester la haute disponibilité de tout le réseau local de Cevital. Nous avons simulé ici la défaillance de l'un des switches de distribution et les interfaces amenant au routeur.

Donc Nous avons pris un PC du VLAN 23 (10.30.23.128) et nous allons faire un ping continue vers l'adresse 172.16.6.2. Puis on a simulé une panne au niveau de Switch de distribution SWD2 (root bridge de Vlan 23) et aussi au niveau l'un des liens de Switch SWD1 (interface Fa0/20) et Core2 (interface Fa0/4) afin de vérifier non seulement le HSRP mais aussi l'OSPF comme (la figure 3-68) l'explique :

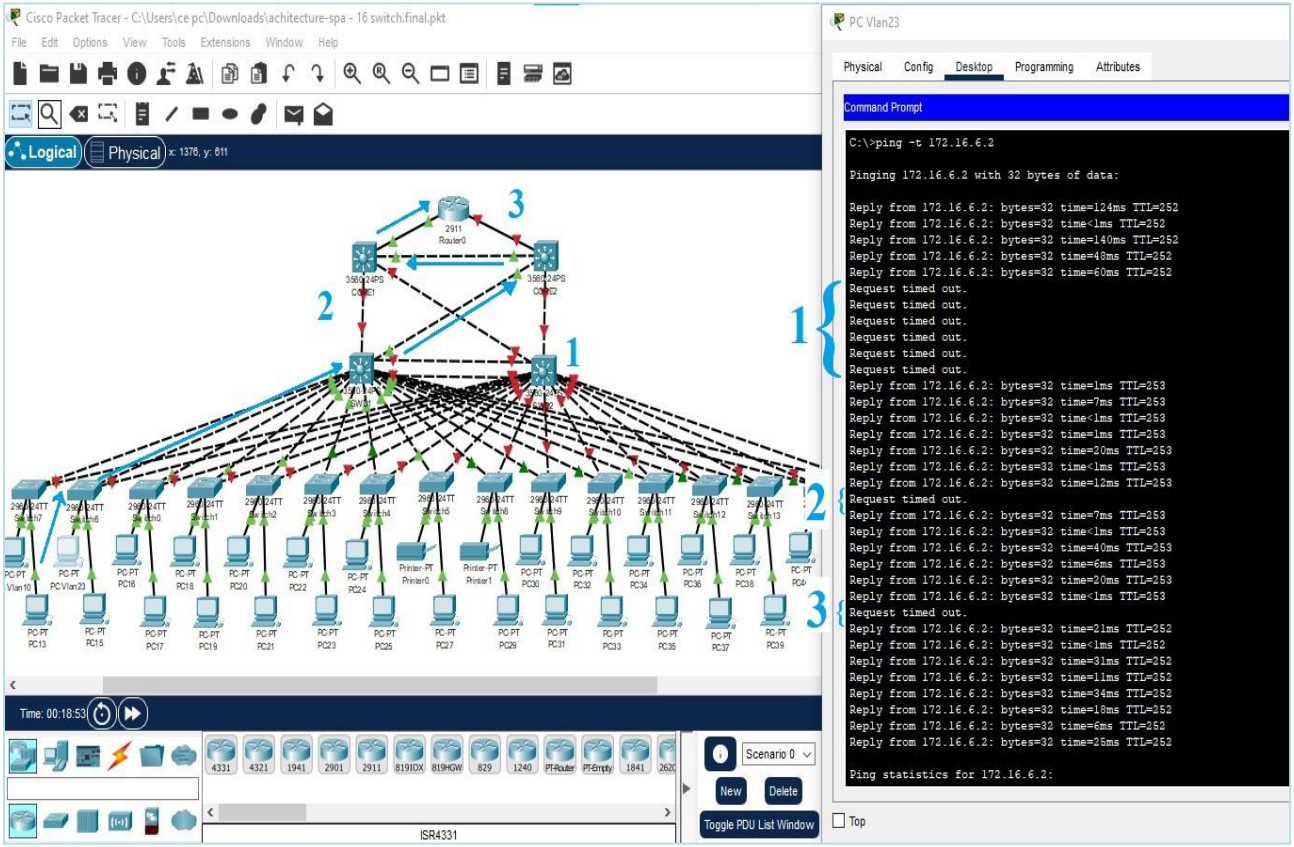


Figure 3-68 : Capture explicative de test de la haute disponibilité LAN

Désormais le protocole HSRP que nous avons configuré, ainsi que le protocole de routage OSPF fonctionnent parfaitement et ne signalent aucun problème.

3.16 Conclusion

Dans ce chapitre nous avons présenté les différentes étapes de configuration qui nous a aidés à réaliser un réseau hautement disponible. Enfin nous avons effectué un ensemble de tests de validation et de vérification afin de prouver l'efficacité des solutions.

Conclusion générale

Pour conclure, Aujourd'hui la haute disponibilité est un investissement essentiel pour qu'une entreprise quelle que soit sa taille puisse accroitre et fonctionner parfaitement. Si un système d'information disponible et fiable n'est pas mis en place, il y a un risque de pertes de productivité, de matériels, mais également de coûts supplémentaires (liées aux pannes, aux ressources à déployer, etc.)

Ce mémoire nous a permis de capter beaucoup d'information sur la situation de réseau LAN de complexe Cevital ainsi de pratiquer de nos nouvelles acquisitions théoriques et comprendre au mieux le fonctionnement de ce réseau durant notre période de stage.

Le thème qui nous a été proposé à cet effet à savoir la haute disponibilité d'un Réseau Local(HSRP) au sein de groupe Cevital-Bejaïa, nous a permis d'appréhender et de cerner les différents critiques et problèmes de son système informatique. Nous avons proposé des solutions afin d'avoir une infrastructure réseau opérationnelle et idéal, en s'appuyant sur la redondance des matériels et des liaisons tout en assurant la continuité de service.

Afin de mettre en œuvre ce projet, nous avons commencé par les configurations niveau 2 tous en configurant les liens trunks, les VLANs, le VTP, le STP et l'agrégation des liens. Par la suite nous avons approfondi les fonctionnalités des commutateurs niveau 3 tels que HSRP, DHCP et l'OSPF.

Afin d'atteindre le résultat escompté, nous avons choisi de simuler notre réseau physique virtuel en utilisant Cisco Packet Tracer 8.1.1 pour les divers avantages qu'il présente notamment la simplicité de la configuration des équipements et protocoles dont mon a besoin.

Ce projet a été pour nous une occasion et une formidable opportunité de découvrir un nouvel environnement informatique, complexe et vaste, Cela nous a permis d'acquérir de précieuses connaissances techniques, notamment pour assurer un service 24h/24 et 7j/7 et obtenir les bons retours que tout réseau informatique devrait avoir.

Pour d'autres apprentis nous vous concieux d'aller au niveau de Cevital afin d'assister et de prendre part à migration de son parc informatique vers les solutions :

- Utiliser le protocole GLBP, qui non seulement permet de gérer la gestion de passerelles redondantes, mais en plus il permet d'équilibrer le trafic entre elles, là où HSRP et VRRP se contentent d'en utiliser une et de laisser les autres en standby
- Une nouvelle installation qui va se faire de toute la fibre optique vers le nouveau data center où se placé les switches Cores en enlevons la couche distribution afin de permettre d'optimiser au maximum sa nouvelle architecture réseau.

Bibliographie

[1] Https://www.cevital.com/cevital-agro-industrie/,consulté le 14 Mai 2022.

[2] Https://www.cevital-agro-industrie.com/fr/page/cevital-agro-industrie-p6, consulté le 14 Mai 2022.

[3] Https://www.cevital-agro-industrie.com/fr/page/groupe-cevital-p15,consulté le 15 Mai 2022.

[4] Https://cevital-recrute.com/index.php/nos-valeurs,consulté 15Mai 2022.

[5] Https://www.google.com/maps/place/Cevital+Agroindustrie/,consulté 17 Mai 2022.

[6] Document délivré par l'organisme d'accueil Cevital Agro-industrie de l'entreprise.

[7] Https://www.router-switch.com/ws-c4507r-e-p-516.html, consulté 30 Mai 2022.

[8] Https://www.solostocks.ma/vente-produits/reseaux-communications/switches/switch-administrable-cisco-catalyst-2960-24-ports-10-100-2t-sfp-avec-lan-11912433,consulté 30 Mai 2022.

[9] Https://itandoffice.com/products/cisco-2901-k9-v02-2900-series-router-cisco2901-k9-v02, consulté 30 Mai 2022.

[10] Https://www.ldlc.com/fr-lu/fiche/PB00149647.html , consulté le 30 Mai 2022.

[11] Https://www.ade24.de/Palo-Alto-PA-3020-Next-Generation-Firewall-System/en, consulté le 30 Mai 2022.

[12] Https://datacenter.legrand.com/fr, consulté le 30 Mai 2022.

[13] Https://fr.theastrologypage.com/high-availability, consulté le 31 Mai 2022.

[14] Jean-François Pillou, Jean-Philippe Bay, Tout sur la sécurité informatique, Dunod, 2016, consulté le 2 Juin 2022.

[15] Https://www.netexplorer.fr/blog/redondance-des-systemes-informatiques-la-meilleure-solution /consulté le 17 Juin 2022.

[16] Https://www.reseaucerta.org/sites/default/files/repartitionCharge-V1.1_sansCorrection/, consulté le 15 Juin 2022.

[17] Https://www.sekurigi.com/2016/06/introduction-aux-principaux-de-haute-disponibilite, consulté le15 Juin 2022.

[18] Https://www.bitwarsoft.com/fr/a-brief-introduction-to-fault-tolerance.html. consulté le 16 Juin 2022.

[19] Https://cisco.goffinet.org/ccna/redondance-de-liens/spanning-tree-rapid-stp-pvst-cisco, consulté le 18 Juin 2022.

[20] Https://www.access-group.fr/parole-expert/quelle-est-la-difference-entre-rpo-rto/, consulté le 18 Juin 2022.

[21] Https://support.huawei.com/enterprise/en/doc/EDOC1100055104/a5b057b1/overview-of-vrrp,consulté le 25 Juin 2022.

[22] Https://study-ccna.com/cisco-hsrp-explained/,consulté le 26 juin 2022.

[23] Https://www.it-connect.fr/mise-en-place-du-protocole-hsrp/,consulté le 29 juin 2022.

[24] Https://www.pearsonitcertification.com/articles/article.aspx?p=2141271, consulté le 02 Juillet 2022

[25] Https://fr.acervolima.com/protocole-d-equilibrage-de-charge-de-passerelle-glbp/, consulté le 5 Juillet 2022.

[26] Https://cisco.goffinet.org/ccna/redondance-de-liens/spanning-tree-rapid-stp-pvst-cisco/, consulté le 5 Juillet 2022.

[27] Https://formip.com/portfast-bpdu-guard/, consulté le 15 Juillet 2022.

[28]Http://wwwigm.univmlv.fr/~dr/XPOSE2007/vlanparlegrandquinapascomprislesconsignes/vtp.html , consulté le 18 Juillet 2022.

[29] Https://formip.com/dtp/ consulté le 18 Juillet 2022.

[30] Https://mondiluca.files.wordpress.com/2018/03/ppe4.pdf**,** consulté le 24/06/2022.

[31] Https://fr.slideshare.net/ELAMRIELHASSAN/cours-etherchannel, consulté le 28 Juillet 2022.

[32] Https://fr.theastrologypage.com/routing-information-protocol, consulté le 28 Juillet 2022.

[33] Https://community.fs.com/fr/blog/rip-vs-ospf-what-is-the-difference.html, consulté le 29 Juillet 2022.

❖ Définition

Un réseau local virtuel (VLAN) est un réseau logique de niveau 2. Il permet de se connecter à un groupe logique de poste de travail, serveurs et périphériques réseau même si ces derniers ne sont pas géographiquement proches les uns des autres. Par exemple, un logiciel développé pour le service finance ne concerne pas les personnes du département ressources humaine. De la même façon, les ressources disponibles ne doivent pas forcement être accessibles par toutes personne de l'entreprise. Les VLAN ont été uniformisés conformément à la spécification IEEE 802.1Q. Il subsiste cependant des variantes d'implémentation d'un constructeur à l'autre.

❖ Agrégation de VLAN

Une agrégation est une liaison point à point entre deux périphériques réseau qui porte plusieurs VLANs à l'ensemble d'un réseau. Une agrégation de VLAN n'appartient pas à un VLAN spécifique, mais constitue plutôt un conduit pour les VLANs entre les commutateurs et les routeurs.

❖ Types de VLAN

Il existe différents types de VLAN utilisés dans les réseaux on y trouve **[3]** :

- **VLAN de données :**

Un VLAN de données (peut être nommé en tant que VLAN utilisateur) est configuré pour ne transporter que le trafic généré par l'utilisateur. L'importance de la séparation des données utilisateur à partir de tout autre type de VLAN est la gestion du commutateur et un contrôle adéquat. Un VLAN acheminant du trafic de gestion ne peut pas faire partie d'un VLAN de données

- **VLAN par défaut :**

Tous les ports de commutateur font partie du VLAN par défaut après le démarrage initial d'un commutateur chargeant la configuration par défaut. Les ports de commutateur qui participent au VLAN par défaut appartiennent au même domaine de diffusion. Cela permet à n'importe quel périphérique connecté à n'importe quel port du commutateur de communiquer avec d'autres périphériques sur d'autres ports du commutateur. Le VLAN par défaut pour les commutateurs Cisco est VLAN 1. Dans la figure 3-15 (chapitre 03), la commande **show vlan brief** a été émise sur un commutateur utilisant la configuration par défaut. Notez que tous les ports sont assignés au VLAN 1 par défaut. Le VLAN 1 dispose de toutes les fonctions de n'importe quel VLAN, à l'exception du fait qu'il ne peut pas être renommé ni supprimé. Par défaut, tout le trafic de contrôle de couche 2 est associé au VLAN 1.

- **VLAN natif :**

Un réseau local virtuel natif est affecté à un port trunk 802.1Q. Les ports trunk sont les liaisons entre les commutateurs qui prennent en charge la transmission du trafic associée à plusieurs VLAN. Un port trunk 802.1Q prend en charge le trafic provenant de nombreux VLAN (trafic étiqueté ou « tagged traffic »), ainsi que le trafic qui ne provient pas d'un VLAN (trafic non étiqueté ou « untagged traffic »).

Les VLAN natifs sont définis dans la spécification IEEE 802.1Q pour assurer la compatibilité descendante avec le trafic non étiqueté qui est commun aux scénarios LAN existants. Un VLAN natif sert d'identificateur commun aux extrémités d'une liaison trunk. Il est généralement recommandé de configurer le VLAN natif en tant que VLAN inutilisé, distinct du VLAN 1 et des autres VLAN. En fait, il n'est pas rare de dédier un VLAN fixe jouant le rôle de VLAN natif pour tous les ports trunk du domaine commuté.

- **VLAN de management :**

Le VLAN de management utilisé par les matériels réseaux pour échanger leurs trames de contrôle et de management (OSPF, RIP, Spanning-Tree, VTP). C'est aussi le VLAN par lequel les administrateurs peuvent se connecter sur les équipements afin de les administrer. Généralement le VLAN de management par défaut est le VLAN 1 donc le " VLAN par défaut". Il est fortement conseiller de le modifier car les Hackers voulant accéder ou porter atteinte aux matériels réseaux tenteront dans un premier temps des attaques sur ce VLAN **[3]**.

- **Les avantages des VLANs :**

Ce nouveau mode de segmentation des réseaux locaux modifie radicalement la manière dont les réseaux sont conçus, administrés et maintenus. La technologie de VLAN comporte ainsi de nombreux avantages.

Parmi les avantages liés à la mise en œuvre d'un VLAN, on retiendra notamment **[4]** :

La flexibilité de segmentation du réseau : Les utilisateurs et les ressources entre lesquels les communications sont fréquentes peuvent être regroupés sans devoir prendre en considération leur localisation physique. Il est aussi envisageable qu'une station appartienne à plusieurs VLAN en même temps.

La simplification de la gestion : L'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement et simplement sans devoir manipuler les connexions physiques dans le local technique.

L'augmentation considérable des performances du réseau : Comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du VLAN qui lui est associé, de la bande passante est libérée, ce qui augmente les performances du réseau.

Une meilleure utilisation des serveurs réseaux : Lorsqu'un serveur possède une interface réseau compatible avec le VLAN, l'administrateur a l'opportunité de faire appartenir ce serveur à plusieurs VLAN en même temps. Cette appartenance à de multiples VLAN permet de réduire le trafic qui doit être routé (traité au niveau du protocole de niveau supérieur, par exemple IP) de et vers ce serveur et donc d'optimiser ce trafic. Tout comme le découpage d'un disque dur en plusieurs partitions permet d'augmenter les performances (la fragmentation peut être diminuée) de son ordinateur, le VLAN améliore considérablement l'utilisation du réseau.

Le renforcement de la sécurité du réseau : Les frontières virtuelles créées par les VLANs ne pouvant être franchies que par le biais de fonctionnalités de routk2age, la sécurité des communications est renforcée.

La technologie évolutive et à faible coût : La simplicité de la méthode d'accès et la facilité de l'interconnexion avec les autres technologies ont fait d'Ethernet une technologie évolutive à faible coût quelles que soient les catégories d'utilisateurs.

La régulation de la bande passante : Un des concepts fondamentaux des réseaux Ethernet est la notion d'émission d'un message réseau vers l'ensemble (broadcast ou multicast) des éléments connectés au même commutateur (hub/Switch). Malheureusement, ce type d'émission augmente sérieusement le trafic réseau au sein du composant de connexion. Même si les vitesses de transmission ne cessent d'augmenter, il est important de pouvoir contrôler ce gaspillage de capacité de trafic (bande passante). Ici encore, le VLAN offre à l'administrateur les moyens de réguler l'utilisation de la capacité de trafic disponible au sein de l'infrastructure.

❖ Fenêtre générale de Packet Tracer

Une fois nous ouvrons Cisco Packet tracer, l'interface ci-dessous va être affiché d'où y' on trouve : La zone (1) indique l'espace de travail dans lequel on construira notre réseau, regardera des simulations et affichera de nombreux types d'informations et de statistiques. 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 (9) signifie la barre de menu, la zone (8) indique la barre d'outils principale et 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 : pour placer des notes sur le réseau – Delete : pour supprimer un équipement ou une note – Inspect : permet d'ouvrir une fenêtre d'inspection sur un équipement (table ARP, routage). La zone (5) permet d'ajouter des indications dans le réseau. La zone (4) permet de passer du mode temps réel au mode simulation, et enfin la zone (7) permet la gestion des paquets dans les scénarios de simulation.

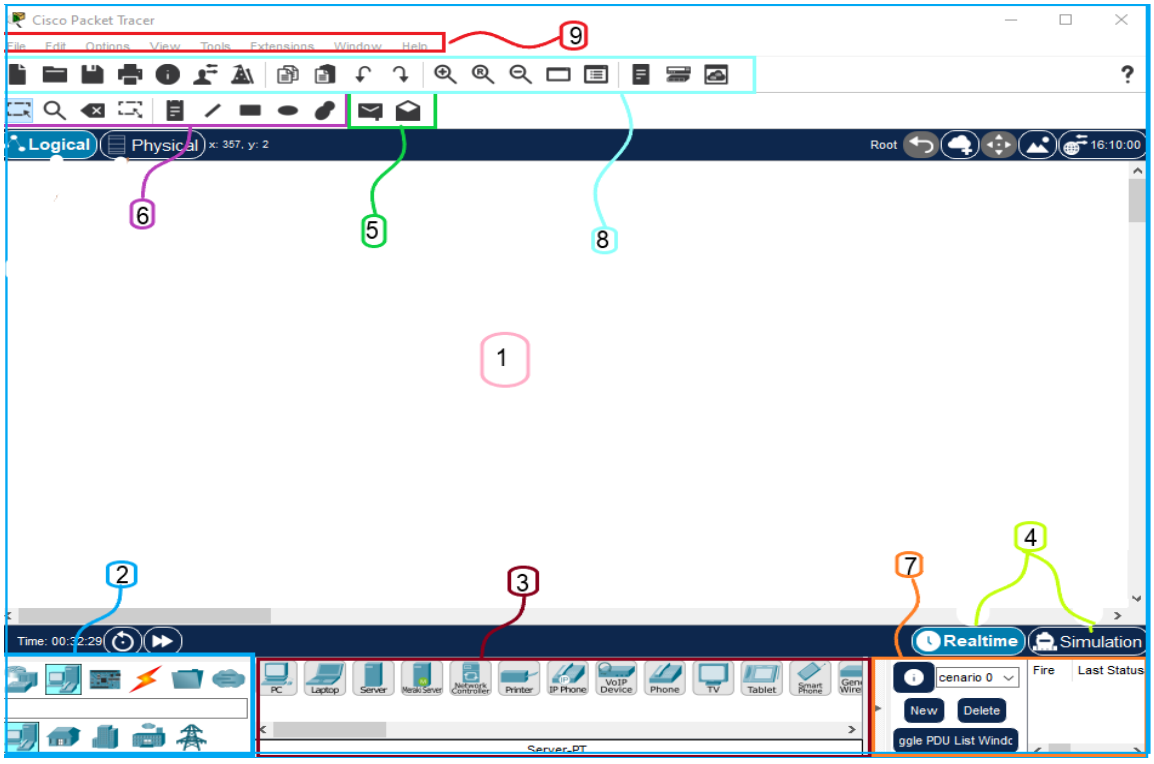


Figure 1 : Capture de l'interface Cisco Packet Tracer 8.1.1.

❖ Ajout d'un équipement

Pour ajouter un équipement l'utilisateur doit sélectionner un type d'équipement parmi les catégories proposées par ce simulateur y'on trouve : les routeurs, les commutateurs, les hubs, les équipements sans-fil, les connexions, les équipements dit terminaux (ordinateur, serveur), des équipements personnalisées et connexion multiutilisateur. Lorsqu'une catégorie est sélectionnée l'utilisateur a le choix entre plusieurs équipements différents .il suffit donc de cliquer dessus puis de cliquer à l'endroit choisi et en fin cliquer sur l'espace de travail.

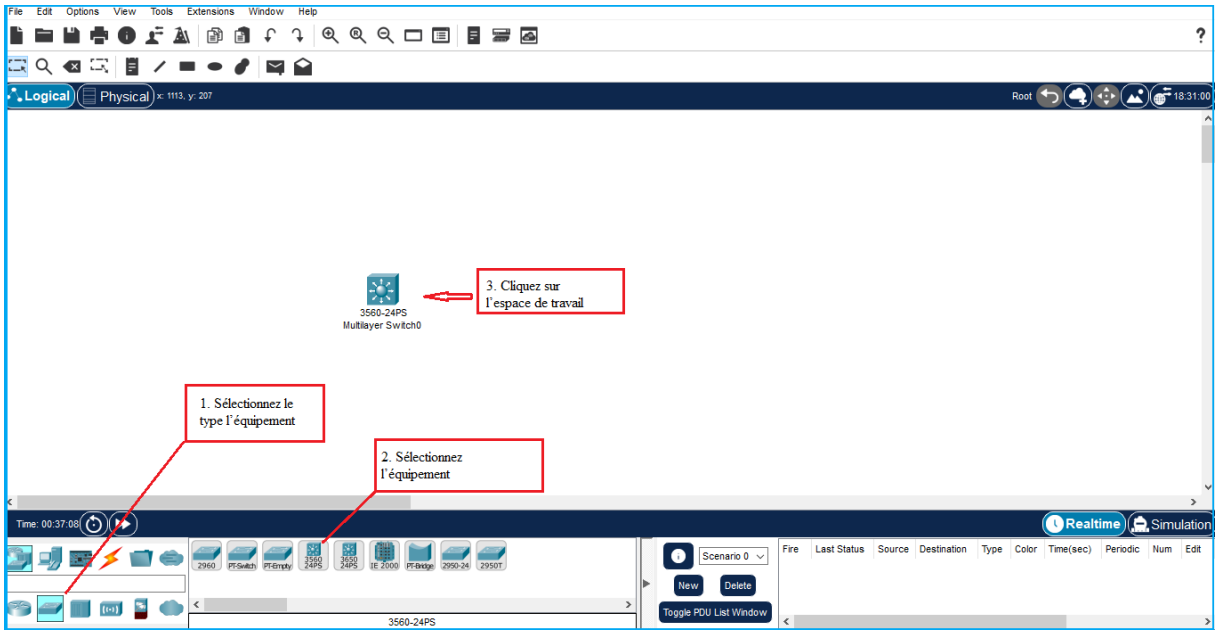


Figure 2 : Capture d'ajout d'un équipement

❖ **Création d'une connexion**

Pour relier deux équipements il faut choisir la catégorie connexion et cliquer sur la connexion souhaitée, puis choisir l'interface désirée sur le premier équipement et enfin cliquer sur le deuxième équipement et choisir l'interface désirée aussi. La connexion est visible sur la capture suivante :

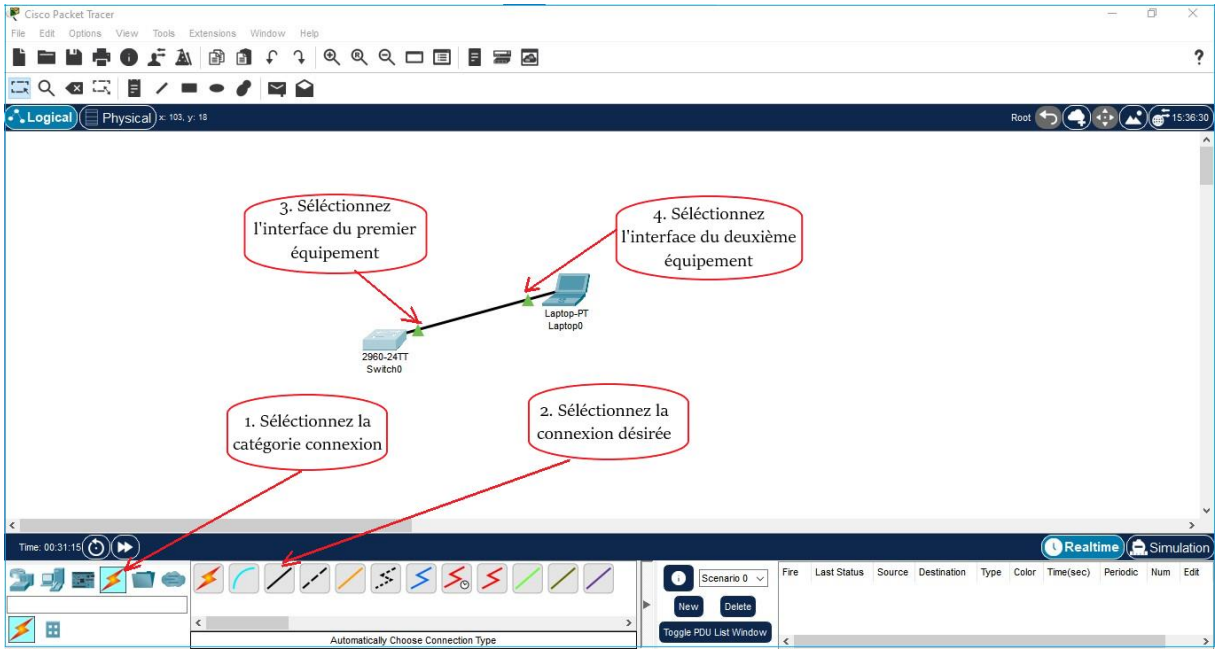


Figure 3 : Capture création d'une connexion entre deux équipements

❖ Configuration d'un équipement

Lorsqu'un équipement est ajouté, il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau. Une nouvelle fenêtre s'ouvre comportant différents onglets : **Physical, config, desktop, CLI** … etc. Généralement pour les ordinateurs on utilise l'onglet config pour configurer l'adresse IP et le DNS et tout le nécessaire du PC.

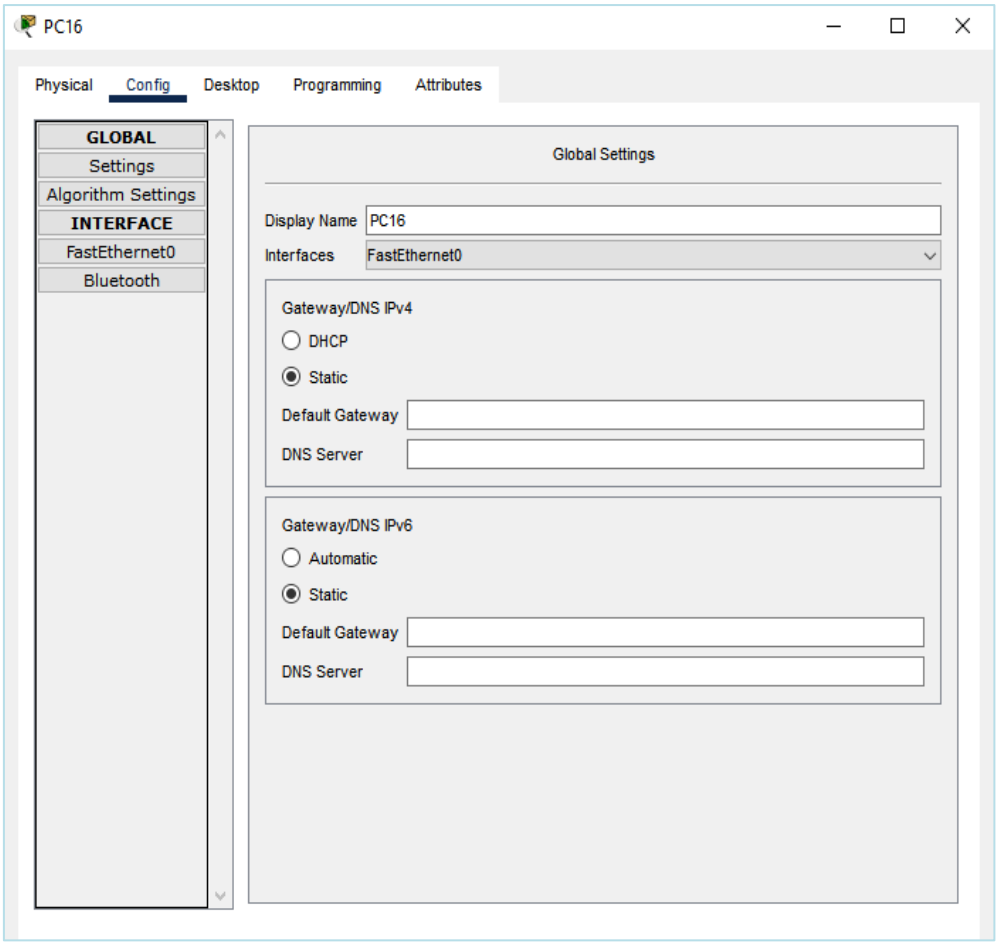


Figure 4 : Fenêtre de configuration d'un PC

Pour les switches on utilise l'onglet CLI afin de les configurer avec les commandes nécessaires.

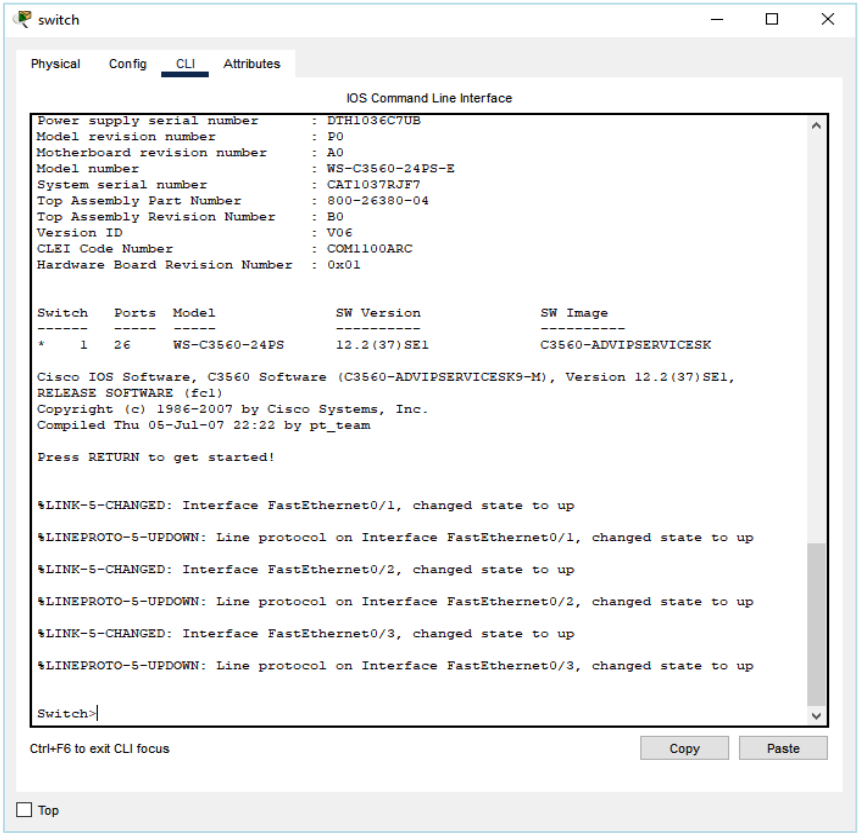


Figure 5 : Fenêtre de configuration d'un Switch

❖ **Les différents modes de configuration**

On se base sur l'invite CLI pour se situer dans un mode. Afin d'exécuter les tâches de diagnostic ou de gestion, il faut les droits d'administration (mode privilège). Toutes les commandes de configuration de la machine s'exécutent en mode de configuration globale et toutes les commandes spécifiques pour les interfaces, le routage, des services (DHCP, NAT, Firewall, …) ont leur mode configuration particulier. Une fois que l'utilisateur fini de taper les commandes dans le mode dans lequel il se trouve, il peut à tout moment basculer vers un mode supérieur via les commandes citées ci-dessus (figure 1-7) ou alors revenir vers un mode inférieur via des commandes (exit, end) comme illustre la figure ci-dessous :

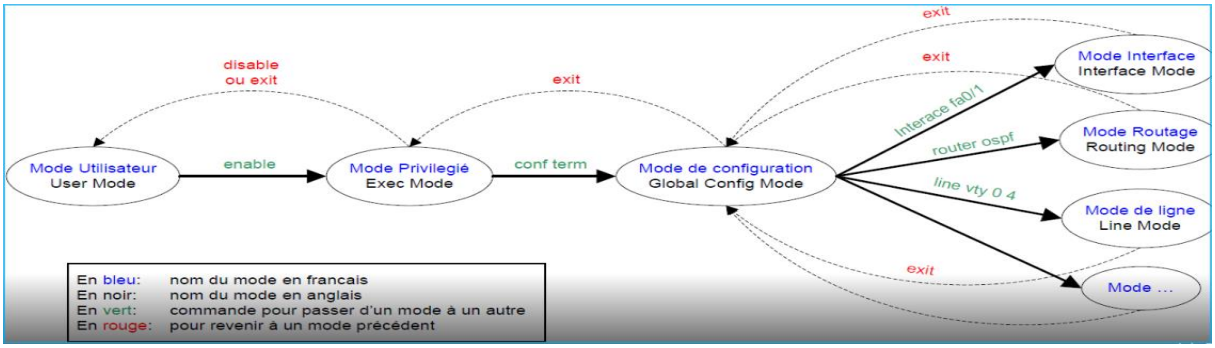


Figure 6 : Schéma illustre les modes de configuration **[5]**

❖ **Mode simulation**

Une fois le réseau créé et prêt à fonctionner, il est possible de passer en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau. En mode simulation, la fenêtre principale est scindée en deux, la partie de droite permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulation, protocoles visibles. La partie gauche de la figure montre la partie simulation et sa partie droite montre les détails obtenus en cliquant sur un message.

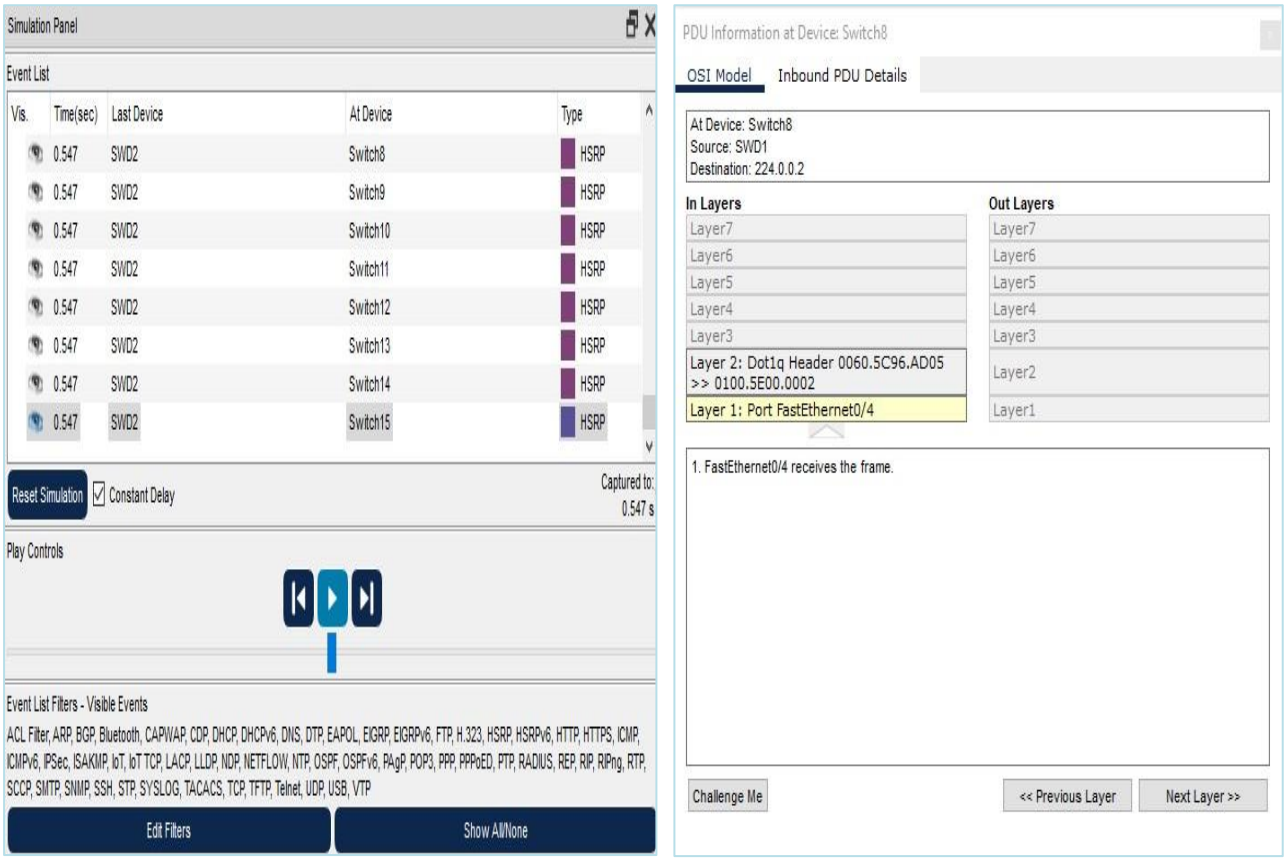


Figure 7 : Capture du mode simulation

❖ **Définition**

Un serveur DHCP, est un serveur qui attribue une configuration IP (adresse IP, masque, passerelle, serveur de noms), aux ordinateurs configurés en adressage dynamique. Avec un serveur DHCP, l'utilisateur n'a plus besoin de rentrer les informations lui-même. La configuration est attribuée pour une durée déterminée, on appelle ce temps : le bail. Le protocole DHCP se diffuse par broadcast, ce qui signifie que la demande du client ne peut pas traverser un routeur (sauf commande explicite). La configuration du service DHCP se fait en 4 étapes :

- Exclusion d'adresses IP
- Création d'un pool DHCP
- Indication du réseau à écouter
- Définition des options du pool

❖ **Fonctionnement de DHCP**

Il faut dans le premier temps un serveur DHCP qui distribue des adresses IP. Cette machine va servir de base pour toutes les requêtes DHCP, aussi elle doit avoir une adresse IP fixe. Dans un réseau, on peut donc n'avoir qu'une seule machine avec adresse IP fixe, le serveur DHCP. Le mécanisme de base de la communication est BOOTP (avec trame UDP). Quand une machine est démarrée, elle n'a aucune information sur sa configuration réseau, et surtout, l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP. Pour faire ça, la technique utilisée est le broadcast : pour trouver et dialoguer avec un serveur DHCP, la machine va simplement émettre un paquet spécial de broadcast (broadcast sur 255.255.255.255) avec d'autres informations comme le type de requête, les ports de connexion sur le réseau local. Lorsque le serveur DHCP recevra le paquet de broadcast contenant toutes les informations requises pour le client.

❖ Avantage de protocole DHCP

Parmi les avantages de Dynamic Host Contrôle Protocol on cite **[3]**:

- Évite les conflits d'adresse IP et permet de contrôler l'utilisation des adresses IP de Façon centralisée. Ainsi, si un paramètre change au niveau du réseau, comme, par exemple l'adresse de la passerelle par défaut, il suffit de changer la valeur du paramètre au niveau du serveur DHCP, pour que toutes les stations aient une prise en compte du nouveau paramètre dès que le bail sera renouvelé. Dans le cas de l'adressage statique, il faudrait manuellement reconfigurer toutes les machines.

- Plus le réseau est grand, plus c'est pratique à maintenir

- Economie d'adresse : ce protocole est presque toujours utilisé par les fournisseurs d'accès Internet qui disposent d'un nombre d'adresses limité. Ainsi grâce à DHCP, seules les machines connectées en ligne ont une adresse IP. En effet, imaginons un fournisseur d'accès qui a plus de 1000 clients. Il lui faudrait 5 réseaux de classe C, s'il voulait donner à chaque client une adresse IP particulière. S'il se dit que chaque client utilise en moyenne un temps de connexion de 10 mn par jour, il peut s'en sortir avec une seule classe C, en attribuant, ce que l'on pourrait appeler des "jetons d'accès" en fonction des besoins des clients.

- Le changement de plan d'adressage se trouve facilité par le dynamisme d'attribution.

- Avec DHCP, il suffit d'attribuer une adresse au serveur. Lorsqu'un ordinateur client DHCP demande l'accès au réseau en TCP-IP son adresse est allouée dynamiquement à l'intérieur d'une plage d'adresses définie sur le serveur.

- L'administrateur de réseau contrôle le mode d'attribution des adresses IP en spécifiant une durée de bail qui indique combien de temps l'hôte peut utiliser une configuration IP attribuée, avant de devoir solliciter le renouvellement du bail auprès du serveur DHCP.

- L'adresse IP est libérée automatiquement, à l'expiration du bail, pour un ordinateur client DHCP retiré d'un sous-réseau, et une nouvelle adresse est automatiquement définie pour ce dernier, lorsque cet ordinateur est reconnecté à un autre sous-réseau. Ni l'utilisateur ni l'administrateur de réseau n'ont besoin de fournir de nouvelles informations relatives à la configuration. Cette fonctionnalité est non négligeable, tant pour les utilisateurs de portables fixés ou non à différentes stations d'accueil que pour les ordinateurs fréquemment déplacés.

- Il est possible de fixer une Adresse IP pour des serveurs à volonté en fonction de l'adresse MAC.

L'adresse du réseau est 10.30.0.0/24 avec une possibilité de création de 255 sous-réseaux, avec un masque 255.255.255.0. L'adressage du réseau local et de toutes les stations, se basera sur une adresse privée et c'est à partir de cette dernière que l'affectation des adresses IP pour l'ensemble des équipements et des VLANs va être accomplie. Les machines affiliées à un VLAN, vont prendre toute les adresses IP d'une même adresses sous-réseau. Le tableau suivant montre le plan d'adressage des VLANs.

Vlan		Adressage		
Id	Nom	Type	Réseau	Défault Gateway
10	DRH	DHCP	10.30.10.0/24	10.30.10.254
11	Direction-appro	DHCP	10.30.11.0/24	10.30.11.254
12	DSI	DHCP	10.30.12.0/24	10.30.12.254
13	Raff-huile	DHCP	10.30.13.0/24	10.30.13.254
14	Raff-Sucre3000T	DHCP	10.30.14.0/24	10.30.14.254
15	Division-U	DHCP	10.30.15.0/24	10.30.15.254
16	Supply-Chain	DHCP	10.30.16.0/24	10.30.16.254
17	Unit-MARG	DHCP	10.30.17.0/24	10.30.17.254
18	Printer	Statique	10.30.18.0/24	10.30.18.254
20	Téléphone	Statique	10.30.20.0/24	10.30.20.254
21	Voice	Statique	10.30.21.0/24	10.30.21.254
22	Direction-R&D	DHCP	10.30.22.0/24	10.30.22.254
23	Performance-Industriel	DHCP	10.30.23.0/24	10.30.23.254
24	Unit-cdthuile	DHCP	10.30.24.0/24	10.30.24.254
25	Management	Statique	10.30.25.0/24	10.30.25.254
26	DFC	DHCP	10.30.26.0/24	10.30.26.254
27	Commercial	DHCP	10.30.27.0/24	10.30.27.254
28	DG	DHCP	10.30.28.0/24	10.30.28.254
29	DQMS	DHCP	10.30.29.0/24	10.30.29.254
30	Raff-sucre3500T	DHCP	10.30.30.0/24	10.30.30.254
31	Cdt-sucre	DHCP	10.30.31.0/24	10.30.31.254
32	Camera	Statique	10.30.32.0/24	10.30.32.254
33	Projet	DHCP	10.30.33.0/24	10.30.33.254
36	Tituration	DHCP	10.30.36.0/24	10.30.36.254

Un nouveau plan d'adressage des VLANs de Cevital avec les SVI des VLANs aux niveaux de la couche distribution (SWD1, SWD2) :

Vlan		**Adressage**				
Id	Nom	Type	Réseau	SVI sur SWD1	SVI sur SWD2	Passerelle
10	DRH	DHCP	10.30.10.0/24	10.30.10.252	10.30.10.253	10.30.10.254
11	Direction-appro	DHCP	10.30.11.0/24	10.30.11.252	10.30.11.253	10.30.11.254
12	DSI	DHCP	10.30.12.0/24	10.30.12.252	10.30.12.253	10.30.12.254
13	Raff-huile	DHCP	10.30.13.0/24	10.30.13.252	10.30.13.253	10.30.13.254
14	Raff-Sucre3000T	DHCP	10.30.14.0/24	10.30.14.252	10.30.14.253	10.30.14.254
15	Division-U	DHCP	10.30.15.0/24	10.30.15.252	10.30.15.253	10.30.15.254
16	Supply-Chain	DHCP	10.30.16.0/24	10.30.16.252	10.30.16.253	10.30.16.254
17	Unit-MARG	DHCP	10.30.17.0/24	10.30.17.252	10.30.17.253	10.30.17.254
18	Printer	Statique	10.30.18.0/24	10.30.18.252	10.30.18.253	10.30.18.254
20	Téléphone	Statique	10.30.20.0/24	10.30.20.252	10.30.20.253	10.30.20.254
21	Voice	Statique	10.30.21.0/24	10.30.21.252	10.30.21.253	10.30.21.254
22	Direction-R&D	DHCP	10.30.22.0/24	10.30.22.252	10.30.22.253	10.30.22.254
23	Performance-Industriel	DHCP	10.30.23.0/24	10.30.23.252	10.30.23.253	10.30.23.254
24	Unit-cdthuile	DHCP	10.30.24.0/24	10.30.24.252	10.30.24.253	10.30.24.254
25	Management-sw	Statique	10.30.25.0/24	10.30.25.252	10.30.25.253	10.30.25.254
26	DFC	DHCP	10.30.26.0/24	10.30.26.252	10.30.26.253	10.30.26.254
27	Commercial	DHCP	10.30.27.0/24	10.30.27.252	10.30.27.253	10.30.27.254
28	DG	DHCP	10.30.28.0/24	10.30.28.252	10.30.28.253	10.30.28.254
29	DQMS	DHCP	10.30.29.0/24	10.30.29.252	10.30.29.253	10.30.29.254
30	Raff-sucre3500T	DHCP	10.30.30.0/24	10.30.30.252	10.30.30.253	10.30.30.254
31	Cdt-sucre	DHCP	10.30.31.0/24	10.30.31.252	10.30.31.253	10.30.31.254
32	Camera	Statique	10.30.32.0/24	10.30.32.252	10.30.32.253	10.30.32.254
33	Projet	DHCP	10.30.33.0/24	10.30.33.252	10.30.33.253	10.30.33.254

36	Tituration	DHCP	10.30.36.0/24	10.30.36.252	10.30.36.253	10.30.36.254

Références

[1] http://cisco.ofppt.info/ccna2/course/module3/3.1.1.3/3.1.1.3.html,consulté le 31/08/2022.

[2] Toussaint KOUASSI, Etude et optimisation du réseau local de innova si, mémoire Master, option Informatique et Télécommunications, consulté le 31/08/2022.

[3] http://mariepascal.delamare.free.fr/IMG/pdf/1_coursVlan_11.pdf, consulté le 31/08/2022.

[4]https://www.developpez.net/forums/d869384/systemes/linux/reseau/avantage-inconvenient-dhcp-dns/,consulté le 5 Août 2022.

[5]Http://reussirsonccna.fr/wp-content/uploads/2012/10/IOS_Mode-3.png, consulté le 31 Juillet 2022.

Résumé :

De nos jours, la haute disponibilité est quasi-indispensable pour le bon fonctionnement de n'importe quel réseau informatique. Pour cela, la présente étude consiste à désigner une solution de haute disponibilité et d'équilibre des charges au niveau du réseau local de cevital-béjaia en utilisant le protocole HSRP, cette solution consiste à mettre en place une redondance (liens et équipements) dans le réseau. A l'aide du simulateur Packet Tracer, une architecture hiérarchique interconnectant différent VLANs est proposée assurant ainsi la haute disponibilité afin de faciliter la communication entre les stations.

Mots clés : réseau local, haute disponibilité, Cevital , VLAN's, HSRP .

Abstract :

Nowadays, high availability is almost essential for the proper functioning of any computer network. For this, the present study consists in designating a solution of high availability and load balancing at the level of the local network of cevital-béjaia using the HSRP protocol, this solution consists in setting a redundancy (links and equipment) in the network. Using the Packet Tracer simulator, a hierarchical architecture interconnecting different VLANs is proposed, thus ensuring high availability in order to facilitate communication between stations.

Keywords : Local Area Network, high availability, Cevital, VLAN's, HSRP .