République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. MIRA-BEJAIA

Faculté des Sciences Exactes

Département d'Informatique

MÈMOIRE

EN VUE DE L'OBTENTION DU DIPLÔME DE MASTER PROFESSIONNEL

Domaine : Mathématiques et Informatique **Filière :** Informatique

Spécialité : Administration et sécurité des réseaux

Présenté par

Mlle.ADJED NOURIA

Mlle.KISRI TASSADIT

Thème

Optimisation du fonctionnement du réseau informatique de l'entreprise Candia

Soutenu le 24 Septembre devant le jury composé de :

M.	KACIMI Farid	MAB	Univ.de Béjaia	Président
M.	YAZID Mohand	MCA	Univ.de Béjaia	Rapporteur
M.	MOKTEFI Mohand	MAA	Univ.de Béjaia	Rapporteur
M.	AISSANI Sofiane	MCA	Univ.de Béjaia	Examinateur

Année Universitaire : 2019/2020

⁂ *Remerciements* ⁂

Nous tenons à remercier en premier lieu DIEU le Tout Puissant, qui nous a donné la force, la volonté et surtout le courage afin d'accomplir ce modeste mémoire.

Nous adressons nos remerciments les plus chaleureux à notre Co-encadrant MOHAND Yazid, pour son aide et son soutien.
Nos vifs remerciements à Monsieur MEKETFI MEHEND, notre encadreur, pour nous avoir fait l'honneur de nous encadrer, et nous guider par ses conseils avisés et son aide très précieuse.

Nous remercions également les membres du jury qui ont pris la peine de juger ce modeste travail.

Nous tenons à remercier sincèrement Monsieur MERABET de nous avoir donné l'opportunité et l'occasion de suivre un stage pratique au sien de l'entreprise Condia de Bejaia.

Par la même occasion, nous tenons à remercier Monsieur BAROUTDJI RIAD pour sa générosité et la grande patience dont il fait preuve.

Un grand remerciement a nos enseignants et enseignantes qui ont contribués à notre formation, depuis le cycle primaire au cursus universitaire.

On remercie tous ceux qui ont contribués de prés ou de loin à l'aboutissement de notre travail. Pour tous, merci infiniment.

⁂ *Dédicaces* ⁂

Je dédie ce travail

A ***mes chers parents*** symbole de sacrifice, de tendresse, et qui m'ont donnés un magnifique modèle de labeur et de persévérance.

J'espère qu'ils trouveront dans ce travail toute ma reconnaissance et tout mon amour.

A mes ***chères sœurs*** et ***mon cher frère.***

Aux êtres chers auxquels je ne saurais exprimer ma gratitude et ma reconnaissance.

Au reste de toute la famille ainsi que mes proches amis qui n'ont cessés de m'encourager.

A ma camararde et amie ***KISRI TASSADIT*** qui a été un binôme très compétent lors de la réalisation du présent mémoire.

NOURIA.

⁕ *Dédicaces* ⁕

Je dédie ce travail

A ***mon très cher père et ma très chère mère*** qui n'ont pas cessés de m'encourager et de se sacrifier pour que je puisse franchir tout obstacle durant toutes mes années d'étude que Dieu me les garde en très bonne santé .
Aucune dédicace ne pourra compenser les sacrifices de mes parents.

A mon cher frère qui ma toujours soutenue dans la vie et auquel je ne saurais exprimer ma gratitude et ma reconnaissance

Au reste de toute la famille ainsi que mes proches amis qui n'ont cessés de m'encourager.

A ma camarade et amie ***ADJED NOURIA*** qui a été un binôme très compétent lors de la réalisation du présent mémoire.

TASSADIT.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS

Abréviations	Significations
ADSL	Asymetric Digital Subscriber Line
BNC	Bayonet Neill–Concelman
CLI	Commande Langage Interface
CSMA/CD	Carrier Sense Multiple Access-Collision Detection
DAP	Delivery at Place
DNS	Domain Name System
DSLAM	Digital Subscriber Line Access Multiplexer
ERP	Enterprise Resource Planning
FAI	Fournisseurs d'accès à Internet
IEEE	Institute of Electronic and Electronics Engineers
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LER	Label Edge Router
LS	ligne Spécialisé
LSP	Label Switch Path
MAC	Media Access Control
MAN	Metropolitan Area Network
MMF	Multi-mode Optical Fiber
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
OSI	Open Systems Interconnection

RJ45	Registered Jack
SC	Simplex Préchargés
SD WAN	Software Defined Wide Area Network
SMF	Single Mode Fiber
TCP/IP	Transmission Control Protocol/Internet Protocol
VDSL	Very high-bit-rate Digital Subscriber Line
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
Wifi	Wireless Fidelity
Wi max	Worldwide Interoperability for Microwave Access

Introduction générale

Nul doute que l'informatique a envahi tous les aspects de notre vie quotidienne, avec l'explosion d'internet, les réseaux sociaux , et tous les services que nous propose ce formidable outil.Donc tout naturellement tous les organismes qu'ils soient gouvernementaux, commerciaux ou privés se voient presque obligés de se doter d'un réseau informatique, qui est en passe de devenir un outil incontournable dans tous les domaines, aussi bien pour booster l'économie, que pour rester aussi performant que les autres, dans un monde où la concurrence est féroce , ou la planète n'est plus qu'un petit village ou l'information circule instantanément.C'est dans cette optique, que nous avons été accueillie par l'entreprise Candia, ou il nous a été demande de proposer une architecture réseau conforme, dans le but d'assurer l'interconnexion de l'ensemble des utilisateurs, sans qu'elle soit interrompu et optimiser son réseau tout en garantissant la cohérence de sa configuration.

Afin de résoudre notre problématique, nous allons présenter le moyen le plus adéquat et le plus efficace Pour optimiser ce réseau qui consiste à la mise en place de la redondance au sein du réseau étudie, en multipliant les chemins entre les différents sites de l'entreprise pour éviter le dysfonctionnement du réseau,et proposer des solutions de supervision afin que l'administrateur soit alerté d'éventuelles pannes et être en mesure de les régler le plus rapidement possible.

Ce présent mémoire est subdivisé en quatre chapitres, le premier chapitre sera consacré à donner quelques notions de base et généralités sur les réseaux informatiques d'entreprises et leurs utilités, ainsi que des concepts de gestion et de sécurité de réseau.

Le second chapitre sera divisé en deux parties ; la première, porte sur la présentation de l'organisme d'accueil, et la deuxième partie concerne l'étude du réseau local existant

dans le but de proposer d'éventuelles améliorations.

Concernant le troisième chapitre , il sera consacré à l'amélioration de l'architectur réseau de l'entreprise.

Enfin, nous allons clôturer ce rapport par la réalisation d'un modèle type à travers le simulateur « **Graphical Network Simulator** », ainsi qu'un test de validation de la configuration globale utilisé pour une optimisation des processus de sécurisation de l'ensemble des réseaux locaux.

CHAPITRE 1

Définitions et Géneralités sur les réseaux informatique

1.1 Réseau informatique d'entreprise

À travers ce chapitre, nous souhaitons faire un rappel des notions de base sur les réseaux informatiques d'entreprises et leur utilité, ainsi que des concepts de gestion et de sécurité de réseau.

1.1.1 Définition

Un réseau informatique est l'interconnexion d'au moins deux ou plusieurs ordinateurs en vue de partager des données, des ressources ou des informations. En d'autres termes, c'est une infrastructure de communication reliant des équipements informatiques qui permettent de partager des ressources communes. Il est caractérisé par un aspect physique (câble véhiculant des signaux électriques) et un aspect logique (les logiciels qui réalisent les protocoles).

1.1.2 Intérêt

Les réseaux informatiques permettent :[14]

— Le partage de ressources

— Le partage d'applications

— La garantie de l'unicité de l'information

— Réduire ses charges et mutualiser les coûts

— Le partage des fichiers

— Partage de ressources matérielles

— L'interaction avec les utilisateurs connectés

1.2 Différents type de reseaux

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

— **Réseaux locaux (Local Area Network)**

Correspondant par leur taille aux réseaux intra-entreprises. Ils servent au transport de toutes les informations numériques de l'entreprise. En règle générale, les bâtiments à câbler s'étendent sur plusieurs centaines de mètres [17]

— Parmi les technologies qui sont utilisées dans les réseaux locaux (LAN) :

- **Ethernet**

Ethernet est une technologie câblée utilisée dans les réseaux locaux (LAN). Elle permet aux appareils connectés de communiquer entre eux via un protocole, qui est une norme développée pour faciliter les échanges réseaux. Le réseau Ethernet

d'origine a été développé par DEC Triumvirate, Intel et Xerox au début des années 1980 puis par un grand nombre de fabricants d'ordinateurs. Aujourd'hui il s'agit d'un protocole de réseau local avec une fonction de communication par paquets et est souvent utilisé sur des câbles à paires torsadées. Ethernet fonctionne selon deux modes distincts mais entièrement compatibles, le mode partagé et le mode de commuté. Ethernet peut facilement étendre l'interconnexion de divers appareils. Ses principales caractéristiques sont :[13]

— Débit de 10 Mbit/s à 10 Gbit/s

— Transmission en bande de base, codage Manchester

— Topologie en étoile (en bus sur les anciens réseaux)

— Méthode d'accès suivant la norme IEEE 802.3 (CSMA/CD)

— Longueur des trames comprises entre 64 et 1 518 octets

— Gestion des couches 1 et partiellement 2 du modèle OSI (sous-couches Physique et MAC

- **Wifi**

Il s'agit d'un ensemble de protocoles de communication sans fil soumis aux normes du groupe IEEE 802.11 (ISO / CEI 8802-11). Les réseaux Wi-Fi permettent aux ondes radio d'un réseau informatique de connecter plusieurs périphériques informatiques (ordinateurs, routeurs, smartphones, modems Internet, etc.) pour permettre la transmission de données entre eux.[16]

— **Réseaux métropolitains (Métropolitain Area Network)**

Permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole. Ils doivent être capables d'interconnecter les réseaux locaux des différentes entreprises pour leur donner la possibilité de dialoguer avec l'extérieur [17].

— Parmi les technologies qui sont utilisées dans les réseaux man :

- **Wi max (Worldwide Interoperability for Microwave Access)**

WiMax signifie « Interopérabilité globale de l'accès micro-ondes ». Il s'agit d'un ensemble de normes techniques basées sur la norme de transmission radio 802.16, permettant la transmission de données IP à haut débit par voie hertzienne. La vitesse théorique maximale supportée par WiMax est de 70 Mbits / s à une distance de plusieurs dizaines de kilomètres. WiMax peut prendre en charge des solutions à très haut débit [17].

— **Réseaux étendus (Wide Area Network)**

Sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et il utilise dans ce cas des infrastructures au niveau du sol, essentiellement de grands réseaux de fibre optique, soit hertzien, comme les réseaux satellites [17].

— Parmi les technologies qui sont utiliées dans les réseaux étendus (wan) :

- **xDSL**

Le terme xDSL est utilisé de façon générique pour décrire l'ensemble des technologies DSL (Digital Subscriber Line ou ligne numérique d'abonné) disponibles actuellement sur le marché (ADSL, VDSL, DSLAM, . . .).[10]

- **ADSL**

ADSL est l'une des technologies xDSL les plus prometteuses, elles offrent une transmission asymétrique avec une bande passante différente depuis et vers le client. C'est la technologie dominante dans les applications commerciales. Les débits de transfert de données pouvant atteindre 8 Mbit/s et pour atteindre ces débits, l'ADSL tire parti des bandes de fréquences non utilisées sur les lignes reliant les

abonnés au réseau téléphonique commuté (RTC), afin de transmettre des données. Alors que la voix utilise traditionnellement les fréquences de 300 à 3 100Hz, ADSL accapare les fréquences hautes non utilisées de 30KHz à 1,1MHz, d'où le terme parfois utilisé de technologie « Broadband » (large bande).[15]

- **VDSL**

Le déploiement de la fibre optique demande beaucoup de temps car il faut poser les câbles et l'augmentation des accès optiques . Le VDSL est une solution courante qui a l'avantage d'utiliser un câble déjà en place, deux générations se sont succédées VDSL et le VDSL2. Les modems VDSL permetent d'atteindre des débits beaucoup plus élevés que les modems ADSL mais sur quelques dizaines de mètres seulement, leurs capacités est de plusieurs dizaines de mégabits par seconde.[15]

- **DSLAM**

un dispositif de distribution de réseau qui regroupe des lignes d'abonné individuelles en une liaison montante haute capacité. Ces liaisons montantes haute capacité, soit ATM ou Gigabit Ethernet, connectent les abonnés à leurs fournisseurs d'accès Internet (FAI). Les unités DSLAM sont généralement situées dans des centraux téléphoniques ou des points de distribution. Ils permettent la transmission à haut débit de la technologie DSL en utilisant des lignes de cuivre existantes. En utilisant des techniques de multiplexage avancées, ces unités récupèrent l'utilité des millions de lignes de cuivre qui ont été initialement déployées pour l'utilisation du téléphone dans les années 1950. Les DSLAM sont également fournis avec de nombreuses fonctionnalités avancées de gestion du trafic pour séparer et hiérarchiser le trafic voix, vidéo et données.[3]

- **MPLS (Multiprotocol Label Switching) :**

MPLS est l'aboutissement logique de toutes les propositions qui ont été faites dans les années 1990. L'idée de l'IETF a été de proposer une norme commune pour

transporter des paquets IP sur des sous-réseaux travaillant en mode commuté. Les nœuds sont des routeurs-commutateurs capables de remonter soit au niveau IP pour effectuer un routage, soit au niveau trame pour effectuer une commutation.

Les nœuds de transfert spécifiques utilisés dans MPLS sont appelés LSR (Label Switch Router). Les LSR se comportent comme des commutateurs pour les flots de données utilisateur et comme des routeurs pour la signalisation. Pour acheminer les trames utilisateur, on utilise des références, ou labels. À une référence d'entrée correspond une référence de sortie. La succession des références définit le chemin suivi par l'ensemble des trames contenant les paquets du flot IP

Les caractéristiques les plus importantes de la norme MPLS sont les suivantes :[18]

— Spécification des mécanismes pour transporter des flots de paquets IP avec diverses granularités des flots entre deux points, deux machines ou deux applications. La granularité désigne la grosseur du flot, qui peut intégrer plus au moins de flots utilisateur.

— Indépendance du niveau trame et du niveau paquet, bien que seul le transport de paquets IP soit réellement pris en compte.

— Mise en relation de l'adresse IP du destinataire avec une référence d'entrée dans le réseau.

— Reconnaissance par les routeurs de bord des protocoles de routage de type OSPF et de signalisation comme RSVP.

— Utilisation de différents types de trames

- **SD-WAN**

c'est un acronyme qui signifie Software Defined Wide Area network. son objectif est de simplifier le management et l'opérabilité du WAN, ou Réseau Privé Etendu, par un mécanisme d'identification et de priorisation intelligente et dynamique des flux. Le SD-WAN représente la troisième génération de réseau, après IPsec (Inter-

net Protocol Security) et MPLS (Multi Protocol Label Switching). Cette avancée technologique permet, en toute simplicité, de créer ou faire évoluer son réseau d'entreprise à travers le monde entier, avec ses établissements distants, ses partenaires, des Cloud providers, en utilisant n'importe quel Fournisseur d'Accès à Internet local et n'importe quelle technologie, filaires ou sans fil.

Un SD-WAN utilise une fonction de contrôle centralisée pour diriger le trafic sur le WAN en toute sécurité et de manière judicieuse. Ainsi, la performance des applications est accrue, ce qui se solde par une meilleure expérience des utilisateurs, une meilleure productivité de l'entreprise et des coûts informatique réduits.

En règle générale, les WAN basés sur des routeurs classiques ne sont pas compatibles avec le cloud. Ils exigent habituellement un retour du trafic, y compris le trafic destiné au cloud, depuis les filiales à un centre ou au data center du siège, où les services d'inspection avancés de sécurité sont applicables. Le retard occasionné par ce retour entrave la performance des applications, ce qui se solde par une expérience médiocre des utilisateurs et une perte de productivité. Contrairement à l'architecture classique du WAN axée sur le routeur, le modèle SD-WAN a été conçu pour prendre entièrement en charge les applications hébergées dans des data centers sur site, des clouds publics ou privés, et des solutions SaaS, comme Salesfore.com, Workday, Office365 et Dropbox, tout en garantissant des niveaux optimaux de performance des applications.[2]

- **VPN**

Un VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers de réseaux peu sûrs comme peut l'être le réseau Internet. Cette technologie, de plus en plus utilisée dans les entreprises, permet de créer une liaison virtuelle entre deux réseaux physiques distants de manière transparente pour les utilisateurs concernés. Les données envoyées au travers de ces liaisons virtuelles sont chiffrées, ceci garantit aux utilisateurs d'un VPN l'illisibilité des donnés en cas d'interception malveillante.

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunnelisation,

c'est-à dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.

Le terme de tunnel est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées et donc incompréhensibles pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN (ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du côté de l'organisation.[12]

- **Ligne spécialisée :**

Une LS est un terme générique pour désigner une liaison point à point entre deux sites. Pour l'utilisateur, une LS consiste en deux ou quatre fils de cuivre reliant deux de ses sites.[18]

1.2.1 Protocoles LAN (protocole de niveau 2)

a) Virtual LAN (VLAn)

- **Définition**

Un réseau local virtuel est un réseau logique de niveau 2. Il permet de se connecter à un groupe logique de stations de travail, même si ces dernières ne sont pas géographiquement proches les unes 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 pour toutes les personnes de l'entreprise. Les VLANs ont été uniformisés conformément à la spécification IEEE 802.1Q. Il subsiste cependant des variantes d'implémentation d'un constructeur à l'autre.[10]

b) Spanning-Tree Protocol (STP)

La redondance améliore la disponibilité de la topologie du réseau en supprimant

le risque de points de défaillance uniques dans un réseau, par exemple, une panne d'un commutateur ou d'un câble du réseau. Lorsqu'une architecture redondante est introduite dans une conception de couche 2, des boucles et des trames en double peuvent apparaître, les conséquences peuvent être dramatiques pour le réseau. Le protocole STP a été conçu afin de résoudre ces problèmes.[15]

- **Définition**

Le STP est un protocole de couche 2 (liaison de données) conçu pour les commutateurs. Le standard STP est défini dans le document 802.1D-2004. Il permet de créer un chemin sans boucle dans un environnement commuté et physiquement redondant. STP détecte et désactive ces boucles et fournit un mécanisme de liens de sauvegarde.[15]

1.3 Système de câblage

1.3.1 Types de câbles

Le câble à fibre optique, le câble à paire torsadée et le câble coaxial sont les trois types principaux de câbles réseau utilisés dans les systèmes de communication.

- **Paire torsadée**

C'est le moyen de transmission le plus simple. Il peut être blindé ou non blindé, utilisé pour les communications téléphoniques et la plupart des Ethernet. Il se compose d'un ou plusieurs mécanismes en spirale de fil. Ce type de support convient à la transmission analogique et numérique [13].

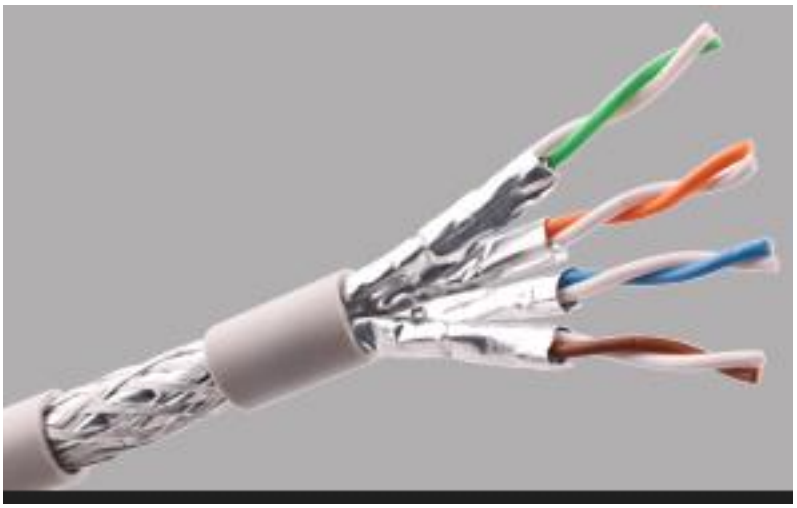

FIGURE 1.1 – Paire torsadée .

- **Câble coaxial**

Les câbles coaxiaux sont exigés pour transmettre des signaux hautes fréquences. Il se compose d'un conducteur rond en cuivre et de trois couches d'isolation et de blindage pour éviter les interférences, ce qui peut limiter les interférences réalisées par le bruit externe [13].

FIGURE 1.2 – Câble coaxial .

- **Fibre optique**

C'est un type de câble Ethernet utilisés pour la transmission de données sous forme d'impulsions de lumière qui passent à travers de minuscules tubes de verre. Elle est utilisée la ou un très haut débit est demandé, mais généralement dans les environnements de

mauvaise qualité ,la fibre peut être divisée en fibres monomode (SMF) et multimode (MMF) [9].

FIGURE 1.3 – Fibre optique .

1.3.2 Type de prise

- **RJ45 (Registered Jack)**

RJ45 est utilisée pour les câbles à paires torsadées, ce qui permet de connecter divers appareils de communication entre eux. RJ45 existe principalement dans la connexion Ethernet.[13]

- **Prise SC (simplex préchargés)**

Le SC pour fibre optique est conçu pour amener la fibre optique dans les bureaux et est déployé dans les immeubles de grande hauteur. Ces prises peuvent fournir jusqu'à 4 ports d'adaptateurs LC, SC, ST, FC, ces adaptateurs sont préinstallés dans la prise murale.[13]

- **BNC (Bayonet Neill–Concelman)**

Utilisé pour la terminaison de câbles coaxiaux, en particulier dans le domaine des radio-fréquences. Facile à utiliser et rapide à installer. Pour plus de simplicité, le même type de prises est installé dans le bureau et la local technique.[13]

1.3.3 Equipements de base d'un réseau informatique

- **Unités hôte**

Les hôtes sont des unités directement connectées à un segment de réseau, nous pouvons les retrouver sous forme d'ordinateurs, de serveurs, de scanners ou d'imprimantes.[16]

- **Routeur**

Un routeur est un élément intermédiaire qui permet de relier deux réseaux. Il assure le routage des paquets d'une interface à l'autre. Il opère au niveau de La troisième couche du modèle OSI (couche réseau). La plupart des routeurs sont capables de déterminer automatiquement l'itinéraire le plus adapté entre le départ et la destination à l'aide des adresses. Ce qui permet d'acheminer le paquet avec le meilleur itinéraire. Pour diriger les informations, le routeur doit comprendre le protocole utilisé, qui est un langage que les ordinateurs utilisent pour communiquer, comme par exemple : TCP/IP, TCP, IP. [16]

- **Commutateur**

Un commutateur réseau est un équipement qui relie plusieurs câbles ou fibres dans un réseau informatique ou un réseau de télécommunication. Les commutateurs permettent de crée des circuits virtuels et de diriger les informations vers une destination précise sur le réseau, l'utilisation de Switch permet de sécuriser les informations transmises sur le réseau : A la différence des concentrateurs qui envoient les informations sur tous les ordinateurs, les Switch envoient les données uniquement aux destinataires qui doivent les recevoir. La commutation est un mode de transport de trame au sein d'un réseau informatique et de communication. [16]

1.3.4 Baie de brassage

La baie de brassage est une armoire technique et métallique permettant la centralisation des équipements réseau d'une entreprise en un seul endroit, facilitant l'accès au réseau intranet et internet. Elle sert à connecter les ports de matériels de réseau et de té-

léphonie aux arrivées des câbles réseau. Son installation est nécessaire pour les structures possédant un certain nombre d'équipements informatiques et/ou téléphoniques qui sont connectés au réseau.Son principal avantage est de faciliter l'organisation et l'utilisation du câblage [1].

- **Panneau de brassage**

Sert à lier les câbles partant des ports du switch ou du panneau de brassage téléphonique, et les câbles reliés aux prises murales situés dans les étages du bâtiment de l'entreprise, où est branché soit un câble téléphonique, soit un câble réseau.[19]

- **Panneau de brassage téléphonique**

Sert à relier les ports du premier panneau de distribution où arrivent le téléphone ainsi qu'un appareil nommé autocom, lequel est branché à la ligne téléphonique et permet la création de plusieurs lignes téléphoniques internes à l'entreprise à partir d'une ligne unique.[19]

- **Connectiques**

Comme connectique, la baie de brassage comporte des prises RJ45, au niveau switch, panneau de distribution, boîtier mural et routeur. Cela permet d'utiliser le câble RJ45 ainsi que les connecteurs RJ45 aux deux bouts du câble s'insérant dans les prises correspondantes.[11]

1.4 Administration et sécurité des réseaux

L'administration et la sécurité des réseaux est une fonction indispensable dont il faut tenir compte lorsqu'on décide de s'investir dans la conception d'un réseau.

1.4.1 Administration des réseaux

L'administration désigne plus spécifiquement les opérations de contrôle du réseau avec la gestion des configurations et de sécurité. De façon générale, une administration de réseaux a pour objectifs d'englober un ensemble de techniques de gestion mises en œuvre pour :[19]

— Offrir aux utilisateurs une certaine qualité de service

— Permettre l'évolution du système en incluant de nouvelles fonctionnalités

— Rendre opérationnel un système

1.4.2 Techniques d'administration

a) Métrologie

Désigne la science des mesures. Dans le cadre des réseaux, son objectif est de connaître et comprendre le réseau afin de pouvoir, non seulement intervenir dans l'urgence en cas de problème, mais aussi anticiper l'évolution du réseau, planifier l'introduction de nouvelles applications et améliorer les performances pour les utilisateurs [11].

b) Supervision

La supervision comprend la surveillance du système et la récupération d'informations sur l'état et le comportement du système, ce qui peut être fait par interrogation périodique ou par remontée non sollicitée du périphérique réseau lui-même. Le plus gros souci de l'établissement est l'échec. En effet, il doit être en mesure de réagir le plus rapidement possible pour effectuer les réparations nécessaires. Il doit être capable de surveiller en permanence l'état du réseau pour éviter de couper le réseau pendant une longue période.[11]

d) Annuaires

— **Active Directory**

Active Directory est le nom du service d'annuaire de Microsoft. Il a été créé et présenté en 1996, mais il n'a été vraiment utilisé que dans la version Windows Server 2000 en 1999. Le service d'annuaire Active Directory est basé sur les normes TCP/IP, DN et LDAP. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels et l'installation de mises à jour critiques par les administrateurs.

Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés et les imprimantes. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées [19].

— **LDAP**

LDAP (Lightweight Directory Access Protocol), est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP. Le protocole LDAP définit la méthode d'accès aux données sur le serveur au niveau du client, et non la manière par laquelle les informations sont stockées. LDAP fournit à l'utilisateur des méthodes lui permettant de se connecter et de se déconnecter, rechercher des informations. etc. [19]

1.4.3 La sécurité

L'objectif principale de la sécurité informatique est de contrôler l'accès aux réseaux, de protéger le flux d'informations sensible et de prévenir les attaques malveillantes visant les systèmes de télécommunication, le transport de l'information et le contenue de l'information.

1) Cloud

Le Cloud est un paradigme né vers 2005 qui propose de positionner les équipements et les logiciels d'une entreprise à l'extérieure de l'entreprise elle-même, c'est-à-dire dans le cloud. Les Avantages de cette solution sont nombreux pour l'entreprise, premièrement il permet d'augmenter ou diminuer les ressources à volonté.

L'entreprise n'est obligée de surdimensionner son système puis'quelle ajoute de nouvelles ressources dès que nécessaire, De plus l'utilisateur ne paie que ce qu'il consomme. Entreprise n'a pas à gérer du personnel pour prendre en charge la gestion des équipements. Du côté du fournisseur de service cloud, les avantages du cloud sont également nombreux et parmi ces avantages on trouve : le partage de ressources entre les clients, virtualisation de serveurs, de systèmes, de logiciels, de réseaux, etc.

Type de cloud

• **IaaS (infrastructure as a service) :** L'IaaS fournit aux utilisateurs l'accès aux ressources informatiques élémentaires telles que capacité de traitement, capacité de stockage de données et mise en réseau, dans l'environnement d'un centre de données sécurisé.

• **PaaS (Platform as a service) :** Destinées aux équipes de développement logiciel, les offres PaaS fournissent des infrastructures informatiques de traitement et de stockage, ainsi qu'une couche de plate-forme de développement équipée de composants tels que serveurs Web, systèmes de gestion de base de données et kits de développement logiciel (SDK) avec prise en charge de plusieurs langages de programmation.

• **SaaS (software as a service) :** Les fournisseurs de SaaS offrent des services applicatifs adaptés aux besoins variés des entreprises tels que la gestion de la relation client (CRM), l'automatisation du marketing ou l'analyse de valeur et de rentabilité.

La supervision doit permettre d'anticiper les problèmes et de faire remonter les informations sur l'état des équipements et des logiciels. Plus le système est important et complexe, plus la supervision devient compliquée sans les outils adéquats. Une grande

majorité des logiciels de supervision sont basés sur le protocole SNMP qui existe depuis de nombreuses années. La plupart de ces outils permettent de nombreuses fonctions dont voici les principales [11] :

— Surveiller le système d'information

— Visualiser l'architecture du système

— Analyse des problèmes

— Déclencher des alertes en cas de problèmes

— Effectuer des actions en fonction des alertes

— Réduire les attaques entrantes

2) Défenses Matérielle

Les défenses matérielles interviennent au niveau de l'architecture du réseau, directement sur le support sur lequel est stockée l'information à protéger (protection d'une base de données centralisée sur le disque dur d'un serveur par exemple), sur les médias servants à transporter cette information (sécurisation du réseau Wi-Fi) et sur les équipements intermédiaires traversés lors du transport (utilisation d'un firewall installé sur le routeur d'accès).

- **Pare-feu**

Un pare-feu (firewall) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets).

Un pare-feu est un appareil de protection du réseau qui surveille le trafic entrant et sortant et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies.

Un pare-feu peut être un équipement physique, un logiciel ou une combinaison des deux. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :[6]

— La machine soit suffisamment puissante

— Le système soit sécurisé

— Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur [14].

- **NAT (Network Address Translator)**

NAT (Network Address Translation), la traduction d'adresses IP, est une technologie plus récente que le proxy. On considère généralement que l'un des objectifs de cette technologie est d'adapter des réponses au problème des adresses IP insuffisantes sur Internet. Par conséquent, la technologie de traduction doit permettre à un groupe de machines d'utiliser une seule adresse IP pour accéder à Internet.

Des passerelles NAT sont souvent installées entre deux réseaux ; le réseau interne et le réseau externe. Les systèmes installés sur le réseau interne se voient généralement attribuer des adresses IP incompatibles avec un acheminement vers les réseaux externes [14].

- **Proxys**

Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges. Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement Internet. Par extension, on appelle aussi « proxy » un matériel comme un serveur mis en place pour assurer le fonctionnement de tels services. Attention : le proxy se situe au niveau de la couche application (HTTP, FTP, SSH, etc. de niveau 7). Une erreur commune est d'utiliser la commande traceroute (ou tracert sous Windows) pour tenter de voir le proxy. Il n'apparaît pas, car cette commande, qui utilise le protocole réseau IP de niveau 3, ne peut pas connaître le proxy.[5]

3) Défenses Logicielles

Tous les systèmes de défense utilisent des programmes ou des algorithmes pour gérer essentiellement l'authentification, le cryptage des données et la détection de malwares. Ces défenses logicielles sont mises en place sur des architectures matérielles, par exemple.

L'authentification sur une liaison point à point pour se connecter à son FAI, le cryptage sur un tunnel VPN ou l'antivirus sur les postes de travail. Les paragraphes suivants décrivent les principes de base utilisés dans le cryptage et l'authentification.

- **Cryptage**

Le but de la cryptographie est de garantir la confidentialité, l'authenticité et l'intégrité des données échangées. Il existe à l'heure actuelle deux grands principes de chiffrement ou cryptage : le cryptage symétrique qui utilise une même clé partagée et le cryptage asymétrique qui utilise deux clés distinctes.[11]

- **Authentification**

L'authentification pour un système informatique est un processus permettant au système de s'assurer de la légitimité de la demande d'accès faite par une entité (être humain ou un autre système...) afin d'autoriser l'accès de cette entité à des ressources du système (systèmes, réseaux, applications...)conformément au paramétrage du contrôle d'accès. L'authentification permet donc, pour le système, de valider la légitimité de l'accès de l'entité, ensuite le système attribue à cette entité les données d'identité pour cette session (ces attributs sont détenus par le système ou peuvent être fournis par l'entité lors du processus d'authentification). C'est à partir des éléments issus de ces deux processus que l'accès aux ressources du système pourra être paramétré (contrôle d'accès).[4]

- **ANTI-VIRUS**

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique ne sont qu'une catégorie). Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés

sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).

Un logiciel antivirus vérifie les fichiers et courriers électroniques, les secteurs de démarrage (afin de détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.), les données qui transitent sur les éventuels réseaux (dont internet), etc.[7]

1.5 Conclusion

Cette partie nous a permis d'acquérir les notions de bases du réseau d'entreprise ainsi les techniques d'administration et les outils de sécurité. Le chapitre suivant sera consacré à la présentation de l'entreprise et à l'étude approfondie de son réseau.

CHAPITRE 2

Présentation de l'organisme d'accueil

2.1 Introduction

Ce chapitre sera réservé à l'études du réseau Candia. Nous donnerons un bref aperçu de l'entreprise ,les différents départements qui la composent , puis continuerons à étudier les composants existants.

2.2 Présentation de l'unité Tchin-Lait / Candia

2.2.1 La marque Candia en Algérie

La marque Candia est présente en Algérie depuis plusieurs années, grâce à son exportation de lait liquide.Au fil des années, le lait en poudre Candia, en particulier ses campagnes publicitaires, a été bien accueilli par le peuple algérien, qui a largement valorisé la notoriété de la marque sur le territoire national.[8]

2.2.2 Historique de l'entreprise

Tchin lait est une laiterie privée de droit Algérien structurée en SARL (Société A responsabilité Limitée) créée et fondée par MR BERKATI en 1999. Les origines de la société Tchin lait se trouvent dans la wilaya de Bejaia, Tchin lait était spécialisée dans le conditionnement des boissons gazeuses depuis 1945. Lors de l'arrivée des grandes firmes multinationales des boissons gazeuses en Algérie, Tchin lait s'est converti vers le lait UHT (Ultra Haute Température) ce qui a donné la naissance à cette dernière.

En 1999 la franchise CANDIA est née en Algérie, devenue opérationnelle en 2001,cette laiterie moderne avec des équipements high tech s'étend sur une superficie de 3000 m2 à BIR SLEM, l'entrée ouest de la ville de Bejaia au bord de la route nationale 26.

Candia 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, grâce à la créativité et l'innovation de l'entreprise qui offre toute une gamme de marques : Candia Viva, Candy'choco, jus, Préparation Culinaire Liquide, etc.

2.3 Présentation de l'entreprise

Candia est caractérisée par sa conception qu'elle a mise en place pour délimiter les différents secteurs qui la forment, dans ce qui suit on va présenter les directions essentielles de cette entreprise :

— **Direction des Finances et comptabilité**

Cette direction a pour mission l'animation, la coordination et le contrôle de l'ensemble des activités financières et comptable de l'entreprise [8].

— **Direction marketing et vente**

Le role de cette direction est de regrouper l'ensemble des activités et processus permettant à une entreprise clients de comprendre les attentes des consommateurs et la situation du marché sur lequel elle évolue et d'essayer d'influencer le comportement des consommateurs dans le sens de ses objectifs [8].

— **Direction des Finances et comptabilité**

Dirige une organisation, des services, des structures informatiques, télécoms et fixe les évolutions des systèmes d'information et de télécommunications, selon les besoins fonctionnels et la stratégie de l'entreprise. Supervise la conception, la mise en oeuvre et le maintien opérationnel (qualité, sécurité, fiabilité, coûts, délais) des prestations informatiques produites et des systèmes d'information et télécoms. Supervise et pilote des projets en systèmes d'information. [8].

— **Direction Système d'informations**

Assure la mise en place des moyens des technologies de l'information nécessaires pour supporter et améliorer l'activité, la stratégie et la performance de l'entreprise.

Elle doit ainsi veiller à ce que l'ensemble du système d'information en parfaite adéquation avec les objectifs métiers l'entreprise au sien de laquelle il évolue.[8]

2.4 Organigramme Tchin-Lait / Candia

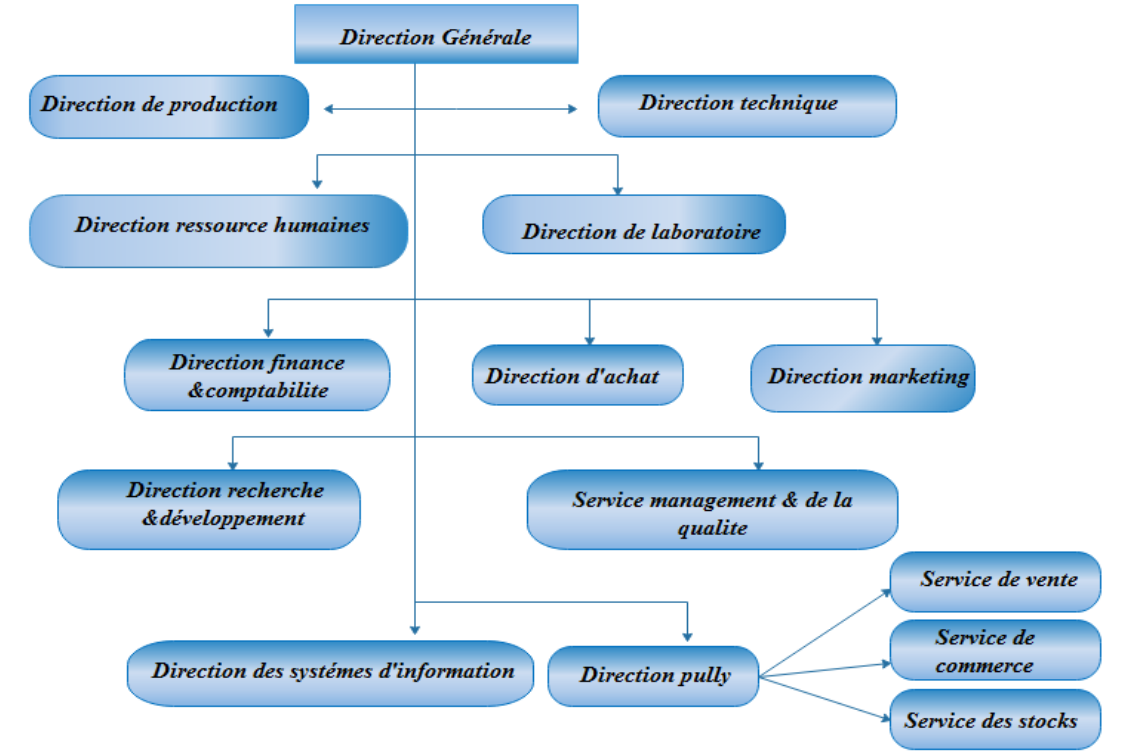

FIGURE 2.1 – Organigramme général de Tchin-Lait.

2.5 Présentation du réseau d'entreprise Candia

De manière générale,les réseaux d'entreprise sont un ensemble d'entreprises indépendantes qui entretiennent des relations formelles. Ce sont des réseaux professionnels qui ont pour vocation de permettre à leurs adhèrents de réaliser des objectifs dans l'intérêt commun de tous.[8]

Dans ce qui suit on va présenter l'architectur réseau de l'entreprise Candia et ses diffirents sites.

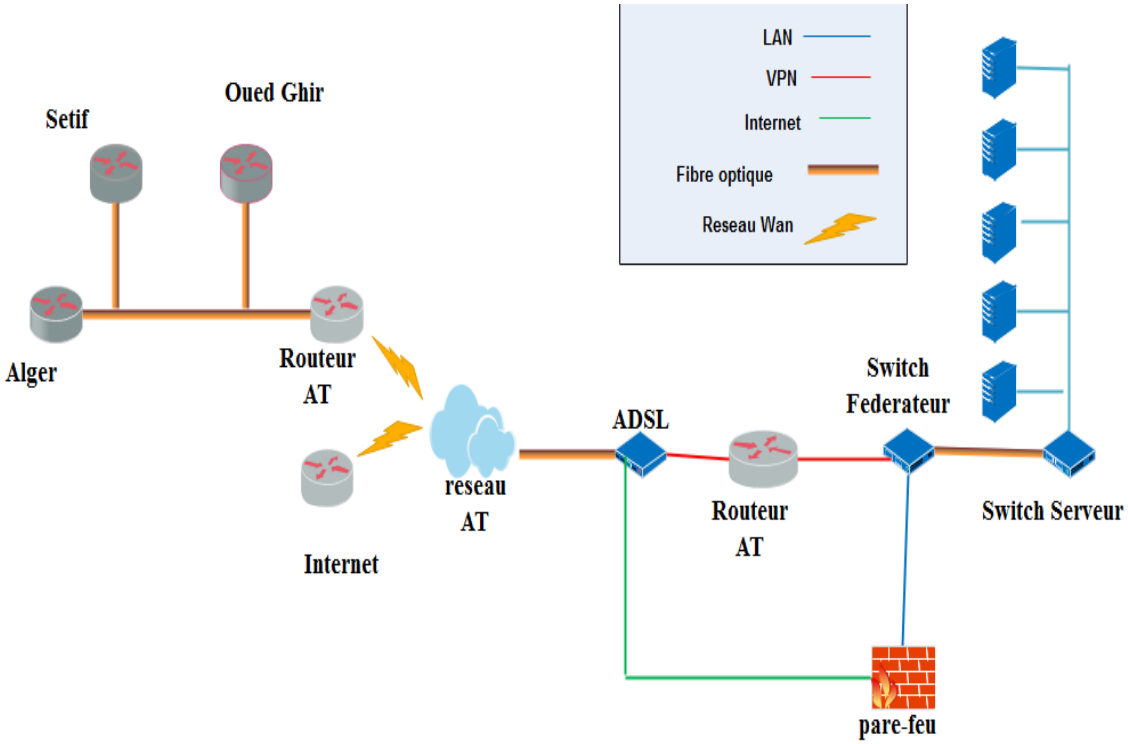

FIGURE 2.2 – L'Architectures du réseau de Tchin-Lait.

2.6 Problématique et hypothèse

2.6.1 Problématique

A l'Aube du 21 -ème siècle, la technologie a connu et connaît un essor extraordinaire et de plus en plus fascinant dans plusieurs domaines, notamment celui de l'informatique, domaine sur lequel les entreprises quelques soient leurs tailles sont obligées de se reposer notamment sur les systèmes informatiques pour le développement et la modernisation de leurs activités afin de répondre aux attentes des clients et pouvoir faire face aux nombreuses concurrences.

Les performances du réseau, la disponibilité et la rapidité d'accès à divers services d'applications sont primordiales et constituent un vrai avantage pour les entreprises

Après une analyse détaillée de l'architecture du réseau de l'entreprise Candia nous dégageons les problématiques suivantes :

- **Sécurité faible du réseau**

Cela est dû à l'absence d'un système de signature numérique utilisant des méthodes de cryptage pour garantir l'authenticité et l'intégrité des messages.

- **Aucune solution de supervision n'est mise en place**

En l'absence d'une surveillance du système d'informatique, il y a de fortes chances qu'il y ait des dysfonctionnements et des pannes de réseaux ce qui va engendrer des pertes d'argents et du temps sur les réparations.

- **Risque d'arrêt du réseau**

Actuellement la seule liaison entre les sites est celle d'Algérie télécom, si elle s'arrête les sites distants seront paralysés.

2.6.2 Hypothèses

La prise en compte des problèmes évoqués précédemment a abouti à l'élaboration des hypothèses d'administration suivantes :

— Mettre en place un système de signature numérique pour empêcher la divulgation des informations.

— Mettre en place une solution de supervision pour permettre d'anticiper les problèmes et de faire remonter les informations sur l'état des équipements et des logiciels.

— Une nouvelle topologie de l'architecture du réseau en la développant en une architecture hiérarchique .

— Une solution de redondance qui réduit le taux de risque d'un arrêt total du réseau

.

— La configuration du réseau est la démarche essentielle à entreprendre pour améliorer ce dernier et éviter tous dysfonctionnements.

2.7 Conclusion

Dans ce chapitre nous avons pris connaissance de l'architecture réseau associée à l'entreprise Candia ce qui nous a mené à déduire les principales faiblesses de ce réseau, et de proposer des solutions pour y remédier et cela dans le but d'améliorer et d'optimiser le réseau de cette entreprise.

CHAPITRE 3

Planification du déploiement

3.1 Introduction

Ce chapitre offre un aperçu du processus de conception du modèle type de configuration, Ou on va proposer des améliorations aux faiblesses cité précédament ,afin d'assurer la rapidité et la stabilité du réseau

3.2 Présentation de l'architecture étudiée

3.2.1 Présentation des équipements réseau

Le tableau suivant représente la liste des équipements réseau et leurs adresses IP du site Candia -Bejaia :

Equipement	**Marque**	**Modèle**	**IP**	**Nombre de ports**	**Emplacement**
Switch	Cisco	WS-C3750G-48TS-S	10.10.1.1	48	Data Center
Switch	Cisco	WS-C2960X-24PS-L	10.10.1.2	24	Data Center

Switch	Cisco	WS-C2960-48TC-S	10.10.1.3	48	DRH
Switch	NetGear	GS724T	10.10.1.4	24	DG
Switch	Cisco	WS-C3560E-48TD-S	10.10.1.5	48	Technique
Switch	Cisco	WS-C3560E-48TD-S	10.10.1.5	48	Technique
Switch	NetGear	GS724T	10.10.1.7	24	Salle d'Archive
Switch	Cisco	WS-C3560E-48TD-S	10.10.1.8	48	C.D.B
Switch	NetGear	GS724T	10.10.1.9	24	Dépôt pf
Switch	HP		10.10.1.10	24	Nouveau Labo
Routeur	Cisco	C892FSP-K9	192.168.19.198	2	Data Center
Routeur	Cisco	CISCO1941/K9	10.10.99.254	2	Data Center
Routeur	Cisco	CISCO1921/K9	10.10.98.254	2	Data Center
Contrôleur Wifi	Aruba	Aruba7030	10.10.1.20		
Pare Feu	Sophos	XG330	10.10.97.254		

Tableau 3.1 – Liste des équipements réseau

3.3 Architectuers étudiée

1. Comme on l'a déjà constaté dans la Figure2.2 (Architecturs du réseau de Tchin-Lait) actuellement la seule liaison entre les sites est celle d'Algérie télécom,
2. Le second problème est que l'architecture réseau de l'enterprise Candia est une architecture non-hiérarchique
3. Le dernier problème détecté est l'absence d'une solution de supervision

Cette figure ci-dessous représente l'interconnexion des Switch du réseau LAN de Candia :

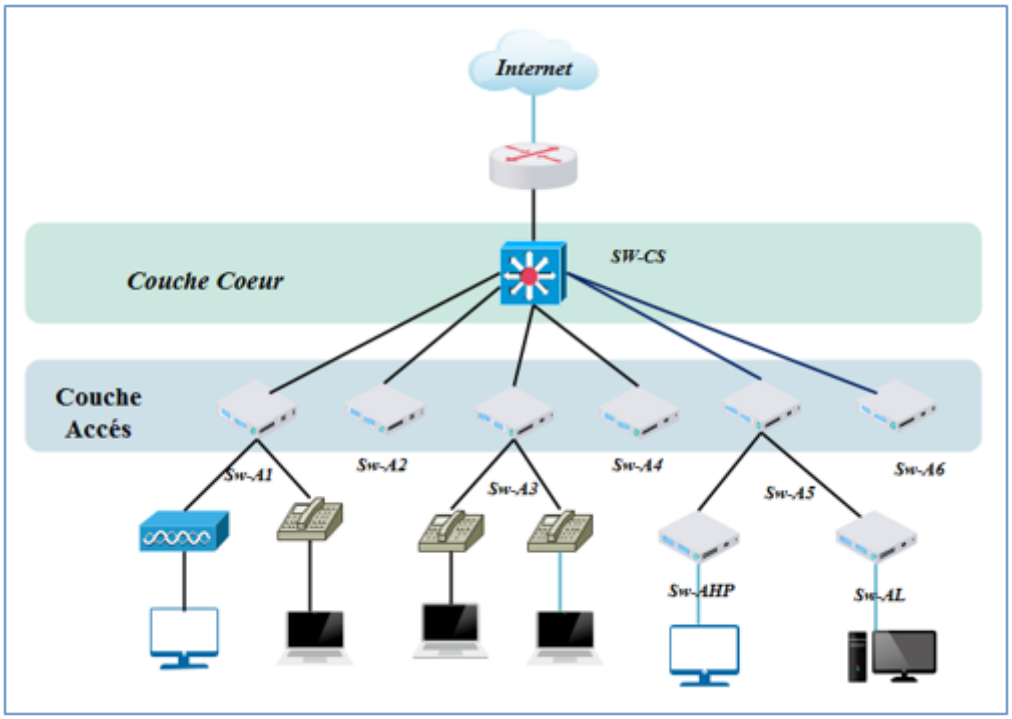

FIGURE 3.1 – Topologie du réseau étudié

3.3.1 Critique de l'existant

Comme on l'a déjà évoqué précédemment, il existe une seule liaison entre les différents sites de cette entreprise, et si elle s'arrête les sites distants seront paralysés.

Pour cela il est indispensable de mettre en place une nouvelle liaison entre les déférents sites pour éviter la perte du temps et d'argent en cas de dysfonctionnement du réseau de cette entreprise.

Apres l'étude du réseau de l'entreprise et le schéma d'interconnexion des switches, nous avons constaté l'absence de la couche de distribution, en effet ce réseau ne comprend Que deux couches : la couche d'accès et la couche cœur et cette dernière n'est dotée que d'un seul Switch, la défaillance de ce Switch engendrera le dysfonctionnement de tout le réseau.

3.3.2 Améliorations

D'après les études effectuées sur l'ensemble du réseau de l'entreprise de Candia on a constaté que ce dernier est exposé à un grand risque de pannes.

1) Etude des Différentes liaisons d'interconnexion entre sites

Avant de choisir la seconde liaison qui va relier les différents sites de l'entreprise on a dû les présenter en exposant les avantages de chaqu'une afin de choisir la bonne liaison.

MPLS	**SD-Wan**	**VPN**
Permet la gestion de Qos	Réduire les couts de déploiement et d'exploitation	Rend la connexion privée, anonyme et protégée
Basé sur le matériel.	Préparer l'intégration du Cloud.	Masquer les adresses IP sur internet.
Interconnectivité sans contraintes.	Garantir la sécurité de ses accès	Le faible coût de l'accès à Internet.
Contrats de niveau de service (contrats SLA) avec garanties de prestation.	Améliorer et automatiser la gestion du réseau WAN.	Les données circulant sur un réseau sécurisé et crypté.
Est idéal pour gérer des applications métiers lourdes nécessitant à la fois une sécurité accrue, une Qualité de Service irréprochable et une large bande passante.	Dispose d'une infrastructure virtualisée. Simplifier l'évolutivité de l'infrastructure réseau. Éviter les limitations en bande passante	Solution économique en termes de coût de mise en place.

Tableau 3.2 – Comparaison entre VPN, MPLS et SD-Wan

- **Les inconvénients de MPLS, SD-WAN et VPN**

MPLS	**SD-Wan**	**VPN**
Coût élevé.	En effet, bien qu'ils soient sécurisés, les liens SD WAN passent par Internet et sont donc soumis aux aléas de ce dernier.	Une connexion internet plus lenteUn blocage de l'accès par certains services
Les offres MPLS ne sont pas toujours disponibles chez votre opérateur.	Le SD WAN peut reporter le trafic d'un lien saturé vers le meilleur lien disponible.	Ne pas savoir si le cryptage fournit par votre VPN est fort
Un seul lien disponible à la fois.		La journalisation et potentiellement la revente de vos données à des tiers

Tableau 3.3 – Les inconvénients de MPLS, SD-WAN et VPN

- **Choix de la liaison**

L'un des objectifs de notre projet est de garantir une bonne qualité de service, et après avoir présenté les trois liaisons d'interconnexion possible entres les Différentes sites de l'entreprise, on a décédé de choisir MPLS. Car c'est la liaison qui permet d'assurer une QoS excellente, sans perte de paquets. Contrairement au Sd-wan et VPN qui reste soumis aux aléas d'Internet (congestion, trafic saturé) malgré que ce soit une solution simple à mettre en œuvre et moins coûteuse qu'une architecture MPLS.

Nous tenons a précisé qu'il y a une autre solution qui est MPLS/VPN, Il s'agit d'une méthode permettant d'utiliser la commutation d'étiquettes multiprotocoles (MPLS) pour créer des réseaux privés virtuels (VPN). MPLS VPN est une méthode flexible pour transporter et acheminer plusieurs types de trafic réseau, il fournit une connectivité point à point de couche 2 entre deux sites.

La figure suivante représente l'architectur réseau de l'entreprise après avoir rajouté la nouvelle liaison MPLS :

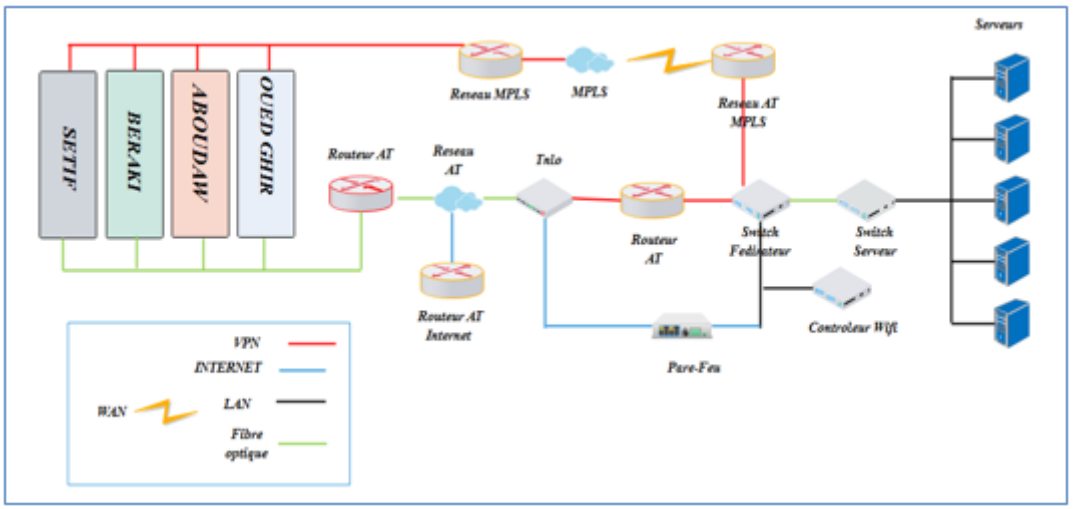

FIGURE 3.2 – Architecture reseau avec une seconde liaison

2) Principes d'un modèle de réseau hiérarchique

Pour optimiser la bande passante d'un réseau d'entreprise, celui-ci doit être organisé afin que le trafic reste local et ne soit pas propagé inutilement vers d'autres portions du réseau. L'utilisation d'un modèle de conception hiérarchique à trois couches permet d'organiser le réseau.

- **Division du réseau en couches distinctes**

La conception de réseau hiérarchique implique la division du réseau en couches distinctes : couche cœur, couche distribution et couche d'accès. Chaque couche fournit des fonctions spécifiques qui définissent son rôle dans le réseau global.

- **Diamètre du réseau**

Le premier élément dont il faut tenir compte lors de la conception d'une topologie de réseau hiérarchique est le diamètre du réseau. Le diamètre de réseau correspond au nombre de périphériques que doit traverser un paquet avant d'atteindre sa destination. Lorsque vous maintenez un faible diamètre de réseau, cela garantit une latence faible et prévisible entre les périphériques.

- **Redondance**

La redondance au niveau des couches principales et de distribution garantit la disponibilité de chemins d'accès. La redondance peut se présenter sous différentes formes : doubler les connexions réseau entre les périphériques, ou bien doubler les périphériques eux-mêmes. L'implémentation de liaisons redondantes peut être coûteuse. Il serait improbable d'implémenter une redondance sur la couche d'accès, en raison du coût et des fonctionnalités limitées des périphériques finaux. Cependant, la redondance sera implémentée au niveau des couches de distribution et cœur du réseau.

3) Solution de supervision

Un réseau informatique est aussi critique que le système nerveux chez l'être humain. Garantir sa disponibilité et sa sécurité est donc primordial. Les logiciels de supervision réseau permettent de répondre à cette problématique en fournissant les outils de surveillance, d'analyse, d'alerte et d'assistance dont les décideurs informatiques ont besoin. Parmi ces logiciels on propose :

- **Nagios**

Nagios est la référence incontournable de la supervision depuis 2000. Il permet de couvrir l'intégralité des besoins du système d'information (plus étendu que la supervision réseau) et dispose de fonctionnalités très utiles dans la gestion de son infrastructure réseau comme les notifications à plusieurs niveaux ou la gestion du support des surveillances.

- **CACTI**

CACTI est un logiciel Open Source rarement utilisé seul. Il est la plupart du temps utilisé conjointement avec une solution de supervision plus complète comme Nagios. La force de CACTI est de permettre la visualisation n'importe quel type de données structurées ce qui rend la lecture de son infrastructure réseau très facile au sein d'une interface Web.

- **OpManager**

OpManager est une solution de supervision qui permet d'avoir un contrôle et une visibilité total sur la gestion du réseau. OpManager est particulièrement pointu et com-

plet dans ce domaine précis. Il bénéficie d'une interface très ergonomique et permet une utilisation optimale des ressources.

3.4 Planification du déploiement

3.4.1 Présentation des équipements utilisés

Les équipements réseau sont illustrés dans le tableau 1 :

Switch	**Type et Marque de Switch**
Switch Cœur	Cisco C3560
Switch distribution	NetGear GS724T
Switch d'accès	Cisco C2960

Tableau 3.4 – Liste des équipements utilisés

3.4.2 Nomination des équipements et désignations des interfaces

a) Nominations des équipements

On intitule les équipements par des termes significatifs pour simplifier la conception de l'architecture.le tableau ci-dessous indiquent les noms des équipements utilisés :

Couche Cœur	**Couche Distribution**	**Couche Accès**
Sw-CS1	Sw-D1	Sw-AN
Sw-CS2	Sw-D2	N=1...6
	Sw-G1	SW-AL
	Sw-G2	SW-AHP

Tableau 3.5 – Nom des équipements

b) Désignations des interfaces

Les interfaces sur les équipements seront comme indiquées dans le tableau suivant :

Local Device	**Remote Device**	**Local Interface(s)**
Sw-CS1	Sw-CS2	F0/1
Sw-CS2	Sw-CS1	F0/1
Sw-CS1	Sw-D1	F0/2
Sw-CS1	Sw-D2	F0/3
Sw-CS1	Sw-G1	F0/4
Sw-CS1	Sw-G2	F0/5
Sw-CS2	Sw-D1	F0/2
Sw-CS2	Sw-D2	F0/3
Sw-CS2	Sw-G2	F0/4
Sw-CS2	Sw-G1	F0/5
Sw-G1	Sw-CS1	F0/1
Sw-G1	Sw-CS2	F0/2
Sw-G1	Sw-D1	Gig0/1, Gig0/2
Sw-G1	Sw-A1	F0/4
Sw-G1	Sw-A2	F0/5
Sw-G1	Sw-A3	F0/6
Sw-G2	Sw-CS1	F0/1
Sw-G2	Sw-CS2	F0/2
Sw-G2	Sw-D2	Gig0/1, Gig0/2
Sw-G2	Sw-A1	F0/3
Sw-G2	Sw-A2	F0/4
Sw-G2	Sw-A3	F0/5
Sw-D1	Sw-CS1	F0/1
Sw-D1	Sw-CS2	F0/2
Sw-D1	Sw-G1	Gig0/1, Gig0/2
Sw-D1	Sw-A5	F0/3
Sw-D1	Sw-A6	F0/4
Sw-D1	Sw-A4	F0/5
Sw-D2	Sw-CS1	F0/1

Sw-D2	Sw-CS2	F0/2
Sw-D2	Sw-G1	Gig0/1, Gig0/2
Sw-D2	Sw-A5	F0/3
Sw-D2	Sw-A6	F0/4
Sw-D2	Sw-A4	F0/5
Sw-A1	Sw-G1	F 0/1
Sw-A2	Sw-G1	F 0/2
Sw-A3	Sw-G1	F 0/3
Sw-A4	Sw-D1	F 0/4
Sw-A1	Sw-G2	F 0/2
Sw-A2	Sw-G2	F 0/1
Sw-A3	Sw-G2	F 0/1
Sw-A4	Sw-D2	F 0/1
Sw-A6	Sw-D2	F 0/1
Sw-A5	Sw-D12	F 0/2
Sw-A6	Sw-D1	F 0/2

Tableau 3.6 – Désignation des interfaces

3.4.3 Présentation de l'architecture améliorée

En s'appuyant sur les principes d'un modèle hiérarchique, nous avons apporté des modifications sur les deux couches existantes dans le réseau de l'entreprise (la couche cœur et la couche d'accès), comme nous avons créé une couche distribution.

1) Division du réseau en couches distinctes et redondance des équipements

a) Couche cœur

Au niveau de cette couche on a rajouté un autre switch cœur Sw-CS1, qui va partager le trafic avec le Sw-CS2, pour éviter le risque de dysfonctionnement du réseau c'est -à -dire en cas de panne de l'un des deux Switch, le trafic sera acheminé par l'autre.

b) Création de la couche distribution

A propos de la couche distribution on a rajouté deux switches entre la couche cœur et la couche Accès, pour rendre le réseau plus efficace, et avec la redondance, ou on a doublé les équipements (switch), ainsi les chemins entre les différents équipements.

c) Couche accès

Au niveau de cette couche, on a repris les switchs qui sont reliés en série afin de maintenir un faible diamètre du réseau.

2) Redondance des liaisons

On a doublé les liaisons comme suit :

a) Entre la couche cœur et la couche distribution

Le trafic est acheminé sur deux liaisons entre tous les switchs de la couche cœur avec tous les switchs de la couche distribution.

b) Au niveau de la couche distribution

Dans la couche de distribution le trafic est acheminé avec une double liaison entre deux Switch (Sw-D1 et Sw-G1) et (Sw-D2 et Sw-G2).

c) Entre la couche distribution et la couche d'accès

Le trafic est acheminé sur deux liaisons entre tous les Switchs de la couche distribution avec tous les Switchs de la couche d'accès.

La figure ci-dessous illustre l'architecture après les améliorations effectuées.

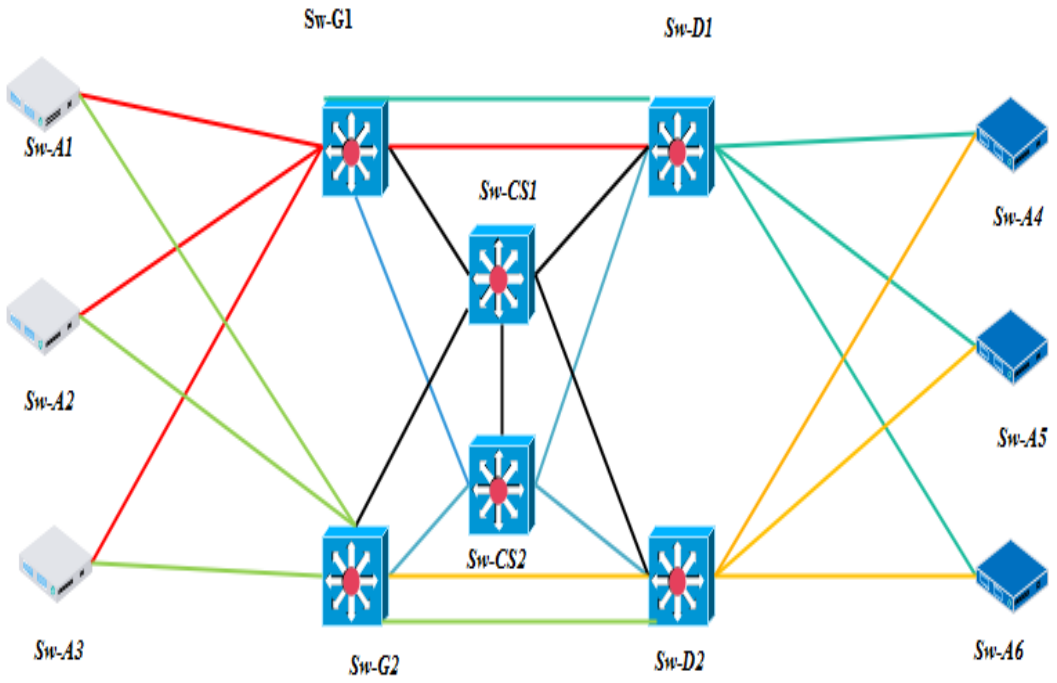

FIGURE 3.3 – Architecture réseau améliorée

3.4.4 Nomination des VLAN

Le tableau suivant représente la liste des VLAN

Nom de Vlan	ID Vlan	Default Gateway	Adresse IP	Masque
Default	1	192.168.1.254	192.168.1.0	255.255.255.0
Management	5	10.10.5.254	10.10.5.0	255.255.255.0
Wifi	10	10.10.10.254	10.10.10.0	255.255.255.0
Wifi-invité	11	10.10.11.254	10.10.11.0	255.255.255.0
User/Data	30	10.10.30.254	10.10.30.0	255.255.255.0
VoIP	100	10.10.100.254	10.10.100.0	255.255.255.0

Tableau 3.7 – Liste des VLANs

3.5 Conclusion

Apres avoir présente le cadre général du projet, une étude préalable s'impose afin d'étudier le domaine de plus près et de repérer la procédure de fonctionnement actuelle, et de planifié un déploiement adéquat a notre sujet.

CHAPITRE 4

Mise en œuvre

4.1 Introduction

Dans ce chapitre nous allons présenter les différentes configurations de notre modèle avec l'utilisation du simulateur « (Graphical Network Simulator)», ainsi que les tests de validation de ces configurations.

4.2 1. Présentation du simulateur (Graphical Network Simulator)

GNS3 est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques, qui permet de réaliser des configurations réseau arbitraires tant que le matériel (hardware) des équipements réseau impliqués est supporté par GNS3.il est utilisé par les professionnels, notamment ISP pour le design de leurs réseaux.[3]

De plus, GNS3 peut être interfacé avec VirtualBox pour que de vraies machines puissent être inclues dans le réseau.

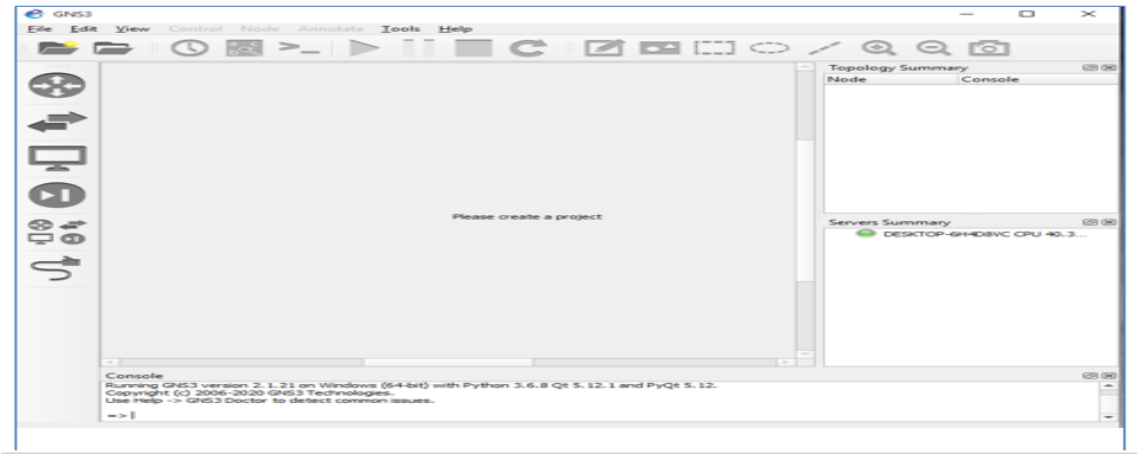

FIGURE 4.1 – Interface GNS3

4.3 Architecture de configuration

Afin de bien présenté les configurations que nous avons effectués, nous nous sommes évertués à configurer une partie de notre architecture améliorée.

La figure ci-dessous représente une branche de l'architecture améliorée.

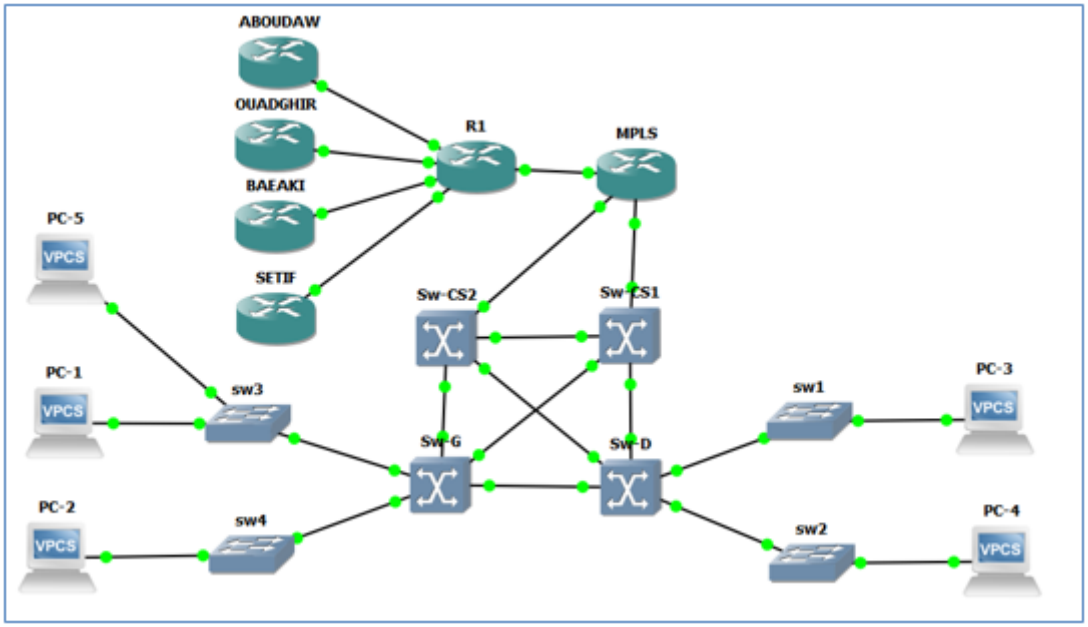

FIGURE 4.2 – Architecture amélioré

4.4 Configuration des équipements

Nous allons commencer par la gestion des VLANs en les divisant en deux parties une sera affectée pour le switch Sw-D1 et l'autre partie pour le Sw-G1.

Le tableau suivant présente les différents VLAN que nous utiliserons dans notre configuration

Name of Vlan	**ID VLAN**	**Difault Gateway**	**Subnet mask**
Labo	10	10.10.10.254	255.255.255.0
Lait	20	10.10.20.254	255.255.255.0
Jus	30	10.10.30.254	255.255.255.0
Voice	9	10.10.9.254	255.255.255.0
Production	8	10.10.8.254	255.255.255.0
DG	7	10.10.7.254	255.255.255.0

Tableau 4.1 – Vlan pour la configuration

Switch Distribution SW-D1	**Switch Distribution SW-G1**
Switch>	Switch>
Switch>enable	Switch>enable
Switch # configure terminal	Switch # configure terminal
Switch (config)#vlan 10	Switch # configure terminal
Switch (config-vlan) # name Labo	Switch (config-vlan) # name Voice
Switch>	Switch>
Switch>enable	Switch>enable
Switch # configure terminal	Switch # configure terminal
Switch (config)#vlan 20	Switch (config)#vlan 8
Switch (config-vlan) # name Lait	Switch (config-vlan) # name production
Switch>	Switch>
Switch>enable	Switch>enable
Switch # configure terminal	Switch # configure terminal

Switch (config)# vlan 30	Switch (config)#vlan
Switch (config-vlan) # name jus	Switch (config-vlan) # name DG

Exemple de configuration :

a) Configuration de Hostname

Nous allons affecter un nom pour chaque commutateur dans chaque couche de la topologie en utilisant la commande **hostname nom du commutateur**

```
Switch>
Switch>enable
Switch # configure terminal
Switch (config) # hostname SW- D1
SW- D1 (config) #
```

b) Configuration des Vlan

```
SW- D1 (config)#interface vlan 10
SW- D1 (config-if) #ip address 10.10.10.254 255.255.255.0
SW- D1 (config-if) # exit
SW- D1 (config)#interface vlan 20
SW- D1 (config-if) #ip address 10.10.20.254 255.255.255.0
SW- D1 (config-if) # exit
SW- D1 (config)#interface vlan 30
SW- D1 (config-if) #ip address 10.10.30.254 255.255.255.0
SW- D1 (config-if) # exit
```

c) Configuration des interfaces

- **Mode TRUNK**

Nous allons associer un port à un VLAN en **mode Trunk** :

```
SW- D1 (config)# interface FastEthernet0/0
SW- D1 (config-if) #switchport trunk encapsulation dot1q
SW- D1 (config-if) #switchport mode trunk
```

- **Mode ACCESS**

Nous allons associer un port à un VLAN en mode Access :

```
SW- D1 #configure terminal
SW- D1 (config)#interface fastEthernet0/0
SW- D1 (config-if) #switchport mode access
SW- D1 #switchport access vlan 10
SW- D1 #exit
```

- **Configuration de Spanning-Tree**

La configuration du protocole STP est réalisée pour la redondance entre la couche distribution et la couche d'accès.

```
SW- D1 (config)#spanning-tree mode rapid-pvst
SW- D1 (config)#spanning-tree vlan 10, 20,30 root primary
SW- D1 (config)#spanning-tree vlan 7, 8,9 root secondary
```

d) Configuration d'etherchannel

C'est une technologie d'agrégation de liens utilisé principalement sur les commutateurs de Cisco. Elle permet d'assembler plusieurs liens physiques Ethernet en un lien logique. Le but est d'augmenter la vitesse et la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs.

Le channel-group nous permet de regrouper plusieurs ports d'un commutateur, à titre d'exemple, l'interface **Gigabithethernet0/1** du switch **SW-D1** est configurée comme suit :

```
SW- D1 (conf-if) #interface Gigabithethernet0/1
SW- D1 (conf-if) #channel-group 2 mode on
```

e) Configuration de la connectivité IP d'un Switch

```
SW- D1#configure terminal
SW- D1 (config)#interface vlan 30
SW- D1 (config-if) #ip address 10.1.30.1 255.255.255.0
SW- D1 (config-if) #no shutdown
SW- D1 (config-if) #end
SW- D1#configure terminal
SW- 1 (config)#interface fastethernet 0/2
SW- D1 (config-if) #switchport mode access
SW- Dt-G1 (config-if) #switchport acces vlan 30
SW- Dt-G1 (config-if) #end
SW- Dt-G1#configure terminal
SW- Dt-G1 (config)#interface vlan 7
SW- Dist-G1 (config-if) #ip address 10.10.7.1 255.255.255.0
SW- Dt-G1 (config-if) #no shutdown
SW- Dt-G1 (config-if) #end
SW- Dt-G1#configure terminal
SW- Dt-G1 (config)#interface fastethernet 0/3
```

```
SW- Dt-G1 (config-if) #switchport mode access
SW- Dt-G1 (config-if) #switchport acces vlan 7
SW- Dt-G1 (config-if) #end
SW- Dt-G1#copy running-config startup-config
```

f) Configuration d'accès à distance (Telnet)

```
SW- Dist-G1 #configure terminal
SW- Dist-G1 (config)#line console 0
SW- Dist-G1 (config-line) #password Candia
SW- Dist-G1 (config-line) #login
SW- Dist-G1 (config-line) #end
SW- Dist-G1 #line vty 0 4
```

g) Configuration niveau 3

- **Configuration de réseau MPLS**

Configuration MPLS
Router>enable
Router# configure terminal
Router (config)#hostname MPLS
MPLS (config)#ip cef
MPLS (config)#interface FastEthernet 0/0
MPLS (config-if) #mpls IP
MPLS (config-if) #mpls label protocol ldp
MPLS (config-if) #exit

- **Configuration Dynamic Host Configuration Protocol, DHCP**

```
SW- D1#configure terminal
SW- D1 (config)# ip dhcp pool poo1cev10
SW- D1 (config)# Network 10.10.10.0 255.255.255.0
SW- D1 (config)# Default-router 10.10.10.1
SW- Dt-G1#configure terminal
SW- Dt-G1 (config)# ip dhcp pool poo1cev20
SW- Dt-G1 (config)# Network 10.10.20.0 255.255.255.0
SW- Dt-G1 (config)# Default-router 10.10.20.1
SW- Dt-G1#configure terminal
SW- Dt-G1 (config)# ip dhcp pool poo1cev30
SW- Dt-G1 (config)# Network 10.10.30.0 255.255.255.0
SW- Dt-G1 (config)# Default-router 10.10.30.1
```

h) Configurations des PC

Dans notre modèle nous avons utilisé 4 PCs, dont les adresses IPs, les masques sous réseaux et les passerelles seront configurés en mode **DHCP**.

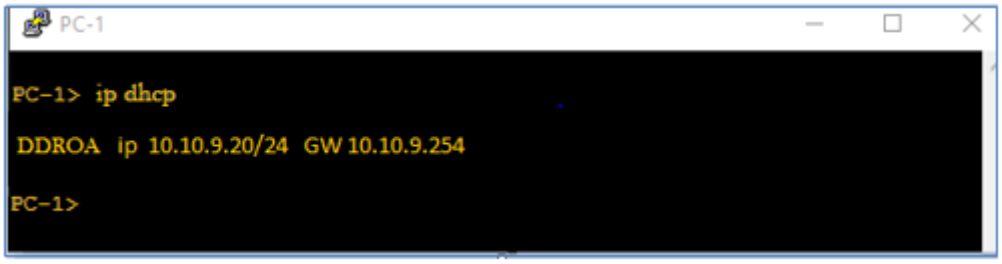

FIGURE 4.3 – Configuration IP en mode DHCP

i) Test et validation de la configuration

Dans cette partie nous allons entamer la vérification de la connectivité entre les différents équipements de l'architectur améliorée. Cette vérification est effectuée grâce à la commande « **ping** » .

- **Test inter-VLAN**

Exemple : vérifier la connectivité entre pc-1(10.10.9.20) et pc-5(10.10.9.21) du même **Vlan9**.

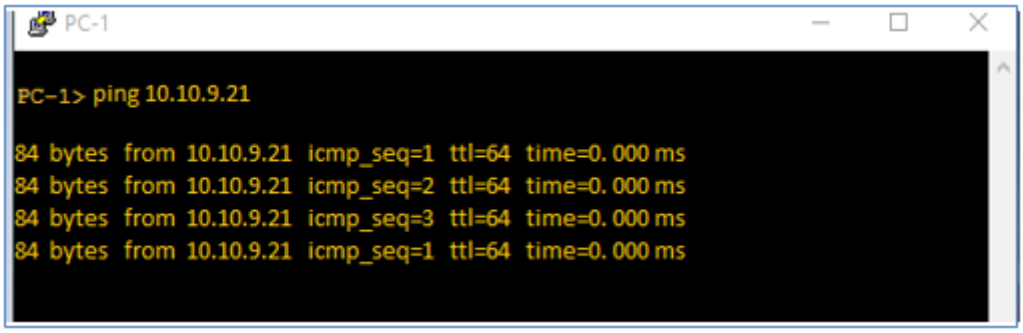

FIGURE 4.4 – Test de connectivité inter-VLAN

- **Test intra-VLAN**

Exemple : vérifier la connectivité entre pc-1**(Vlan9)** et pc-3**(Vlan 30)**

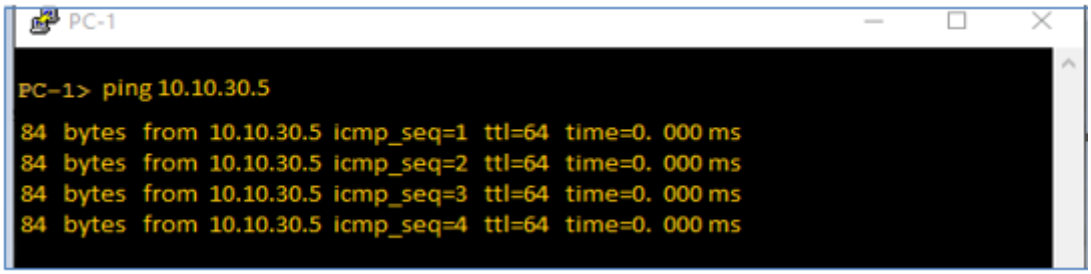

FIGURE 4.5 – Test de connectivité intra -VLAN

- **Test de la liaison MPL**

Dans cette partie nous allons tester la connectivité entre le routeur avec l'un des sites de l'entreprise a titre d'exemple Sétif.

Exemple : entre MPLS (IP :172.19.51.12) et Sétif (172.19.27.21)

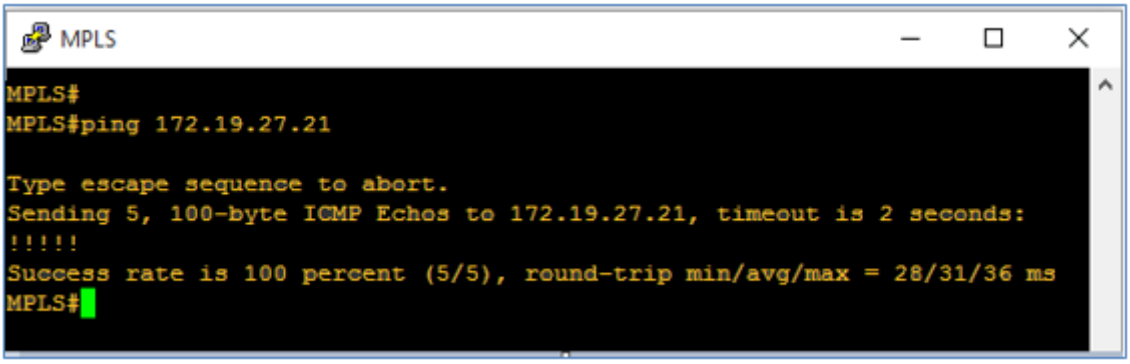

FIGURE 4.6 – Test de connectivité entre Router MPLS et Sétif

Exemple : entre Sétif (IP :172.19.27.21) et MPLS (IP :172.19.51.12)

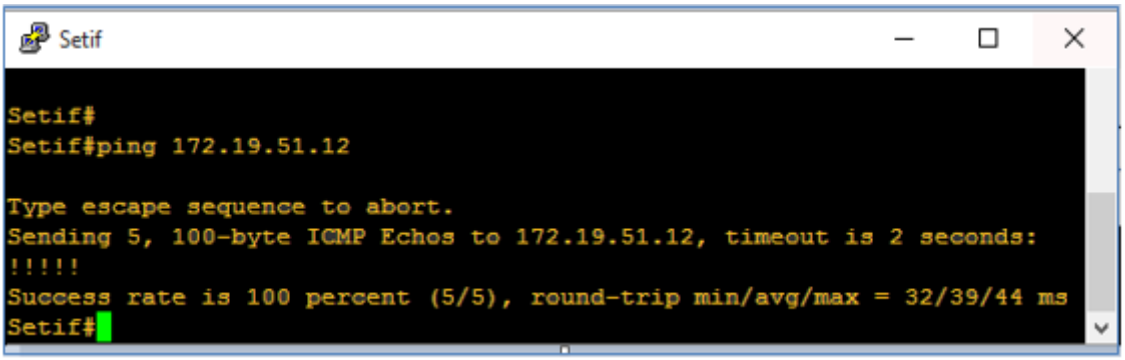

FIGURE 4.7 – Test de connectivité entre Router Sétif et MPLS

4.5 Conclusion

Dans ce chapitre nous avons réaliser l'ensemble de configuration des équipements réseau, et Lors de la simulation de notre topologie des résultats satisfaisant ont été constaté. Cependant nous n'avons pas pu procéder à tous les essais nécessaires.

Conclusion générale

Le présent mémoire est centré sur l'optimisation du fonctionnement du réseau informatique de l'entreprise Candia. Ou nous avons essayé de garantir les principaux objectifs de ce projet qui sont : l'offre d'une bonne qualité de service, la gestion des pannes, la gestion de la performance, etc.

En réalisant ce projet, nous avons consacré du temps pour l'étude de l'architecture réseau de cette entreprise. Cette étude était menée dans les détails et nous a permis de soulever différentes lacunes et faiblesses de ce réseau.

Face à toutes les faiblesses, nous avons formulé des hypothèses selon lesquelles, l'implantation d'un modèle hiérarchique et l'ajout d'une liaison d'interconnexion entre les différents sites de l'entreprise, seront les moyens efficient et efficaces pour remédier aux différents problèmes.

Notre travail a été subdivisé en quatre chapitres. Le premier a porté sur des généralités sur le réseau informatique de l'entreprise, le second est consacré à une brève présentation de l'organisme d'accueil et dans le troisième chapitre, on s'est penché sur le présentation, conception et d'optimisation d'un réseau local. Dans le premier point, on a pu schématiser l'architecture et la topologie du réseau étudié. A partir de là, certains manques quant à ce qui concerne cette architecture sont apparus, ce qui nous a conduit directement à optimiser ce dernier.Le dernier chapitre Concerne la partie réservée à la mise en œuvre d'un model type de réseau en utilisant un simulateur **GNS3**.

Certes, il peut y avoir des petits manquements à notre mémoire, qui peuvent être dû à l'impossibilité de l'entreprise à nous communiquer certaines informations sensibles de leurs domaine informatique ou bien à des informations qui ont pu nous échapper.

Enfin, comme suite à ce travail, on propose l'implémentation des améliorations présentée dans ce mémoire dans le but de vérifier les résultats en pratique, et suite a ça plusieurs points restent à développer et à améliorer parmi lesquelles citions :

— Mise en place d'une solution de supervision.
— Mise en place d'un système de cryptage.
— Implémentation d'une autre liaison entre les différents sites de l'entreprise qui est MPLS/VPN, cette dernière est une solution d'interconnexion sécurisée permet de faire transiter les données reseau prive et nos pas par l'Internet public.

Bibliographie

[1] https://www.mixconcept.fr/a-quoi-sert-une-baie-de-brassage.

[2] https://fr.silver-peak.com/sd-wan/sd-wan-explained.

[3] https://www.versatek.com/www.GNS3.COM/what-is-dslam.

[4] https://fr.wikipedia.org/wiki/Authentification.

[5] https://fr.wikipedia.org/wiki/Proxy.

[6] https://fr.m.wikipedia.org/wiki/Pare-feu_(informatique).

[7] https://fr.m.wikipedia.org/wiki/Logiciel_antivirus.

[8] Source interne de l'entreprise (candia).

[9] Vaucamps A. « cisco ccna ». ENI éditions, 2010.

[10] ROHAUT S. CHAMILLARD G. création, configuration et gestion d'un réseau local d'entreprise. ENI édition, 2013.

[11] Cahier de l'Admin . « linux sécuriser un réseau ». 3-édition.

[12] J.ARCHIER. Les vpn : fonctionnement, mise en oeuvre et maintenance des réseaux privés virtuels. Edition ENI, 2010.

[13] Jean-Luc Montagnier. réseau d'entreprise par la pratique. Novembre 2010.

[14] Jean-François Pillou. Tout sur les réseaux et internet. 4e-edition .2015.

[15] G. PUJOLL. les réseaux. 8e-edition Septembre .2014.

[16] G. PUJOLL. les réseaux. Eyrolles éditions, 2008.

[17] G. PUJOLLE. Les réseaux. 5e-edition Septembre .2004.

[18] Claude Servin. Réseaux et télecoms 2. 4-édition.

[19] William R. STANECK. Guide de l'administrateur windows server 2013. Edition DUNOD.2013.

ANNEXE A

Questionnaire d'entreprise de Candia (tchin-lait)

A.1 Informations générales

1. Votre entreprise utilise-t-elle un réseau local d'entreprise de type LAN (réseau filaire) ?

   ☒ Oui

   ☐ Non

2. Votre entreprise utilise-t-elle un réseau d'entreprise de type Wan ?

   ☒ Oui

   ☐ Non

3. Votre entreprise dispose-t-elle d'un Intranet ?

   ☒ Oui

   ☐ Non

4. Est-ce que tous les services de votre entreprise utilisent le réseau ?

   ☒ Oui

   ☐ Non

5. Quel est l'intérêt(s) d'utilisé le réseau dans votre entreprise ?

— **Utilisation d'internet, Envoie de mail, partage de fichier ,travail collaboratif.**

— **Utilisation des logiciels de gestion**

A.2 Accès et utilisation d'internet

1. Votre entreprise utilise-t-elle un type quelconque de connexion par ligne fixe à internet (Par exemple : ADSL, la fibre optique (FTTP), le câble, etc.) ?

   ☒ Oui

   ☐ Non

2. La vitesse de votre (vos) connexion(s) fixe(s) à internet suffit-elle généralement aux besoins réels de votre entreprise ?

☒ Oui

☐ Non

3. Votre entreprise possède-t-elle un site web ?

☒ Oui

☐ Non

a) Description des services, information sur les produits et leur prix ?

☒ Oui

☐ Non

b) Possibilité de faire des achats en ligne ?

☐ Oui

☒ Non

c) Liens ou références renvoyant aux profils de l'entreprise sur les médias sociaux ?

☒ Oui

☐ Non

A.3 Transmision et traitement de l'internet

1. Votre entreprise échange-t-elle des informations avec le monde extérieur par voie électronique ?

   ☒ Oui

   ☐ Non

2. La transmission électronique et le traitement automatique sont-ils utilisés pour les opérations suivantes ?

   ☒ Oui

   ☐ Non

   a) Recevoir les commandes des clients ?

   ☒ Oui

   ☐ Non

   b) Passer une commande auprès d'un fournisseur ?

   ☒ Oui

   ☐ Non

   c) Envoyer ou recevoir des documents liés au transport de marchandises ?

☒ Oui

☐ Non

d) Envoyer et recevoir des factures électroniques ?

☒ Oui

☐ Non

3. Quels sont les systèmes utilises dans l'entreprise pour l'échange des données informatisés ?

— **Email(Outlook)**

A.4 Administration réseau

1. Quelles sont les technologie réseau utilisées dans votre entreprise ?

— **Ethernet, wifi**

2. Quelles sont les techniques utilisées pour prévenir et gérer les pannes réseaux ?

— **Monitoring(centtreon)**

3. Quelles sont les techniques utilisées pour la détection des anomalies ?

— **Monitoring**

— **Consultation des log et Journaux des événements**

A.5 Sécurité réseau

1. Tous les ordinateurs disposent-ils d'un antivirus à jour ? les systèmes d'exploitation (Windows) sont-ils régulièrement mis à jour ?

   ☒ Oui

   ☐ Non

2. Les utilisateurs doivent-ils demander l'autorisation avant d'installer des logiciels sur leurs ordinateurs ?

   ☒ Oui

   ☐ Non

3. Disposez-vous d'un système de protection réseau (firewall) et d'une console d'administration de l'antivirus sur les postes de travail ? Ces systèmes sont-ils consultés régulièrement ?

   ☒ Oui

   ☐ Non

4. Le serveur ,les sauvegardes, les équipements réseau sont-ils protégés dans un local fermé, climatisé ?

☒ Oui

☐ Non

5. Les utilisateurs ont-ils tous un mot de passe fort (difficile à deviner) ?

   ☒ Oui

   ☐ Non

6. La fiabilité des sauvegardes est-elle vérifiée régulièrement ?

   ☒ Oui

   ☐ Non

7. Votre entreprise utilise-t-elle un système de signature numérisée utilisant des méthodes de cryptage assurant l'authenticité et l'intégrité des messages ?

   ☐ Oui

   ☒ Non

ANNEXE B

Procédure d'installation et d'utilisation GNS3

GNS3 est une solution open source qui permet de simuler des équipements informatiques (routeurs, commutateurs, PC, etc.) et de simuler son fonctionnement. Cet outil est très utile pour la modélisation avant la mise en production en vue du déploiement.

B.1 Les étapes d'instalation de GNS3

1. Téléchargez l'installeur Windows depuis le lien fourni **(www.GNS3.com).**

FIGURE B.1 – Téléchargement du logiciel GNS3.

2. Lancer l'exécution de linstallateur

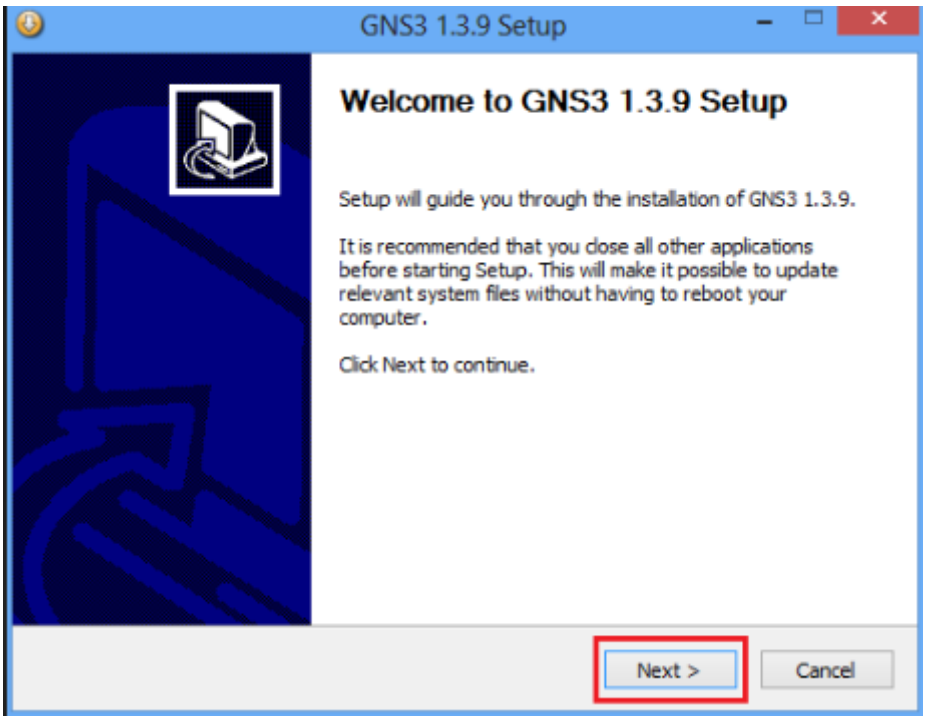

FIGURE B.2 – Instalation du logiciel GNS3.

3. Lorsque la fenêtre de bienvenue s'affiche, appuyez sur « next ».

4. Acceptez les termes de la licence.

5. Ne modifiez pas le répertoire du menu démarrer au travers duquel GNS3 est accessible.

6. Laissez la liste des composants à installer inchangée

7. A l'apparition de l'écran de bienvenue de Wireshark, appuyez sur « next »

8. Acceptez les termes de la licence.

9. Laissez la liste des composants à installer inchangée et validez.

10. Laissez la liste des taches additionnelles inchangée et validez.

11. Ne modifiez pas le répertoire dans lequel Wireshark sera installé et validez.

12. A l'apparition de l'écran de bienvenue de Winpcap, appuyez sur « OK ».

13. Acceptez les termes de la licence.

14. Autorisez le module winpcap à s'exécute au démarrage.

15. Lorsque l'installation se termine, cliquez sur « Finish ».

16. Après l'installation de GNS3, cliquez sur « Next ».

17. A la demande d'inscription à la mailing-list de GNS3,, cliquez sur « next » puis sur « No » à la fenêtre demandant de confirmer.

18. Décochez « Start GNS3 » et cliquez sur « Finish ».

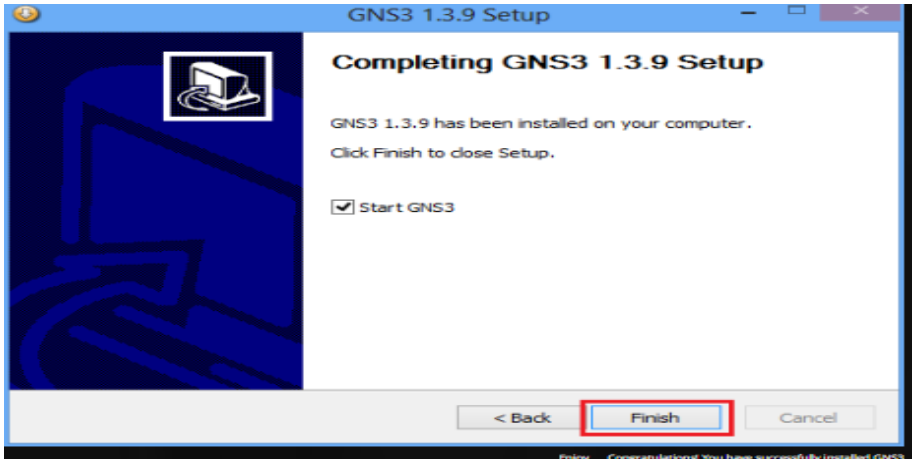

FIGURE B.3 – Instalation terminée du logiciel GNS3.

19. L'installation est terminée.

B.2 Manipulations de base sous GNS3

B.2.1 Les projets

GNS3 travaille en utilisant la notion de projet. Un projet est une configuration de réseau dans laquelle on conserve :

— Quels sont les équipements utilisés.

— Comment ces équipements sont connectés les uns aux autres (topologie).

— La configuration de chaque équipement.

B.2.2 Créer un nouveau projet

Lors du démarrage de GNS3, taper un nom de projet dans la ligne « project name », puis cliquez sur « OK ».

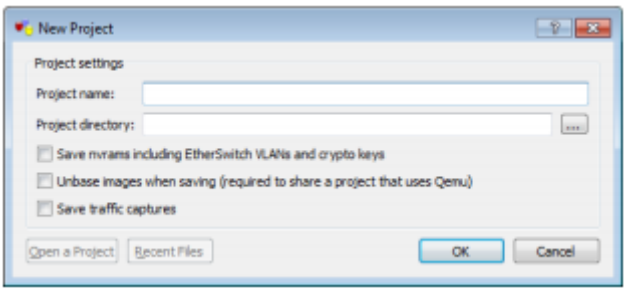

FIGURE B.4 – La création d'un nouveau projet.

B.2.3 Ajouter un équipement sur la feuille GNS3

1.Dans GNS3 faire glisser et déposer un routeur à partir du menu de gauche, puis un nuage.

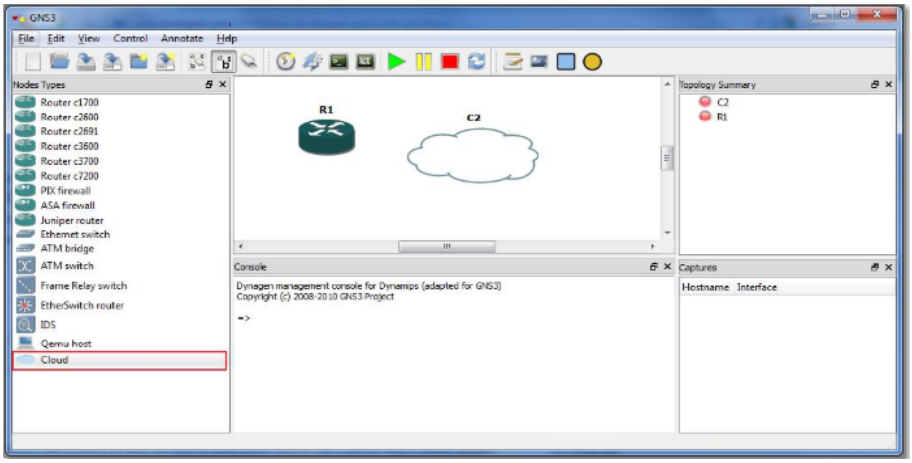

FIGURE B.5 – Glisser les équipements sur la Fenêtre de GNS3.

B.2.4 Interconnecter deux équipements

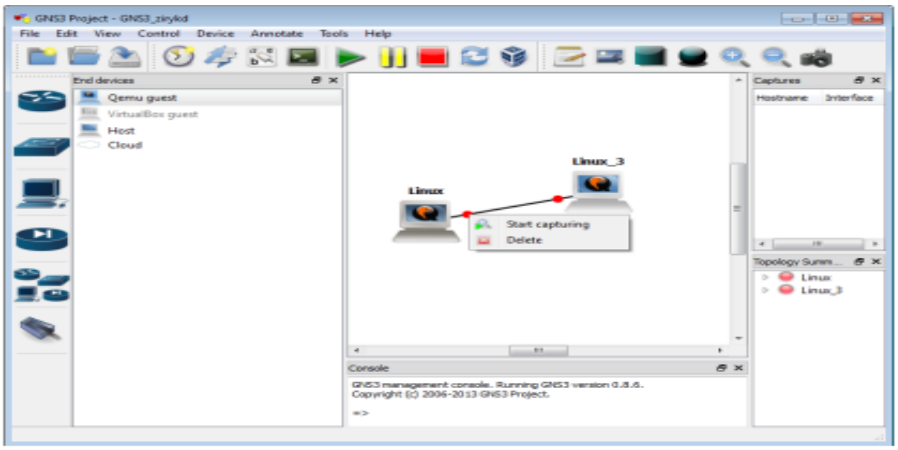

FIGURE B.6 – Interconnecter deux pc.

RÉSUMÉ

Face au développement des technologies informatiques, les réseaux locaux des entreprises présentent des infrastructures complexes qui doivent répondre à un certain nombre de normes spécifiques aux équipements à interconnecter et aux applications à supporter. C'est pourquoi la technologie de l'implémentation du réseau local offre plusieurs solutions qui doivent être adaptées tout particulièrement à l'architecture de l'organisme concerné et d'accompagner sa croissance tout en sécurisant ses services des attaques qui proviennent de l'intérieure ou de l'extérieure de l'entreprise. Dans ce mémoire nous nous sommes intéressées à l'optimisation du fonctionnement du réseau informatique de l'entreprise Candia, Où nous avons essayé de proposer des solutions adéquates aux nombreux problèmes tirés durant l'étude de l'architectur du réseau de cette entreprise, dont l'implémentation d'un modèle reseau hiérarchique, et la mise en place d'une nouvelle interconnexion entre les différents sites de l'entreprise, plus précisément MPLS.

Mots clés : Réseaux locaux des entreprises, sécurité, ,modèle réseau hiérarchique

ABSTRACT

Faced with the development of computer technologies, the local networks of companies present complex infrastructures which must meet a certain number of standards specific to the equipment to be interconnected and the applications to be supported. This is why the technology of the implementation of the local network offers several solutions that must be particularly adapted to the architecture of the organization concerned and to support its growth while securing its services from attacks originating from within. or from outside the company. In this thesis we are interested in the optimization of the operation of the computer network of the company Candia, where we have tried to propose adequate solutions to the many problems drawn during the study of the network architect of this company, of which the implementation of a hierarchical network model, and the establishment of a new interconnection between the various sites of the company, more precisely MPLS.

Key words : Local business networks, Security, hierarchical network model.