

CHERCHEUR-ENTREPRENEUR

* **KOUASSI KOUAME JEAN MICHAEL**
* **N’GORAN NIAMIEN THIERRY MICHAEL**
* **KOFFI KOFFI DESIRE**

**Option : RESEAUX ET SECURITE INFORMATIQUE**

**Mr KOUASSI ADINGRA PAUL ARSENE**

***En vue de l’obtention du diplôme de Licence en***

***Informatique et Sciences du Numérique***

TUTEUR ENCADREUR :

PRESENTÉ PAR :

**Année académique : 2019 - 2020**

**ETUDE DE LA MISE EN PLACE D’UNE INFRASTRUCTURE RESEAU POUR LE DEVELOPPEMENT D’UN COMMERCE EN LIGNE**

**PROJET COLLECTIF TUTORÉ**

**TABLES DES MATIERES**

**Introduction générale**……………………………………………………………………….1

* Première partie

**Chapitre I : présentation général de la structure**………………………………. 2

**I-Fonctionnement de la structure**…………………………………………………………..2

1. Contexte……………………………………………………………………………….2
2. Présentation……………………………………………………………………………2
3. Objectif et missions…………………………………………………………………….2
4. Structuration de la structure……………………………………………………………2
5. Organigramme………………………………………………………………………….3

**II-Le système informatique de la structure**………………………………………………...3

1. Le matériel……………………………………………………………………………..3
2. coté logiciel…………………………………………………………………………3
3. le parc informatique de la structure……………………………………………........3
4. Le logiciel…………………………………………………………………………........4
5. Objectifs d’un système d’exploitation………………………………………………4
6. Objectif d’une application…………………………………………………………...4
7. Critique de l’existant……………………………………………………………………4
8. Spécification des besoins……………………………………………………………….5
9. Besoins en services…………………………………………………………………..5
10. Besoins en sécurité…………………………………………………………………..5

**III-Les équipements nécessaires pour un réseau d’entreprise fonctionnel** ………………6

1. Les composants matériels pour un réseau d’entreprise fonctionnel……………….......6
2. Périphériques finaux…………………………………………………………………6
3. Les équipements d’interconnexion…………………………………………………..6
4. Les supports de transmission…………………………………………………………6

**Chapitre II : Etude de l’infrastructure du réseau informatique…………………………..7**

**I-Etude et choix des matériels**………………………………………………………………..7

1. Le routeur………………………………………………………………………………7
2. Les différents types de routeur…………………………………………………......7
3. Choix du routeur en fonction des besoins de la structure …………………………8
4. Commutateur (Switch)…………………………………………………………………8
5. Les différents types de commutateur………………………………………………….8
6. Choix du commutateur en fonction des besoins de la structure ……………………...9
7. Serveur…………………………………………………………………………………….9
8. Les différents types de serveur informatique …………………………………………9
9. Choix du serveur ……………………………………………………………………..10
10. Les câbles…………………………………………………………………………………10
11. Les différents types de câble………………………………………………………….10
12. Choix du câble………………………………………………………………………..10
13. Répéteur…………………………………………………………………………………..10
14. Les différents types de répéteur………………………………………………………10
15. Choix du répéteur……………………………………………………………………..11
16. Récapitulatif des matériels choisis pour l’entreprise ……………………………………..11

**II-Etude des différents logiciels disponibles sur le marché et choix des meilleurs**…………..11

1. Etude des différents logiciels disponibles sur le marché………………………………….12
2. Au niveau du système d’exploitation ………………………………………………...12
3. Au niveau du logiciel d’implémentation de la VoIP………………………………….13
4. Au niveau du logiciel de gestion des commandes ……………………………………13
5. Au niveau du logiciel de sécurité (antivirus) …………………………………………14
6. Choix du logiciel le plus adapté…………………………………………………………..14

* Deuxième partie

**Chapitre I : Mise en place d’une politique de sécurité**………………………………15

**I-Etablir une politique de sécurité**………………………………………………………………15

1. Définition d’une politique de sécurité……………………………………………………...15
2. Principaux point de cette politique de sécurité……………………………………………..15
3. Etape d’établissement d’une politique de sécurité………………………………………….15

**II-Les meilleurs pratiques et avantages de la mise en place d’une politique de sécurité**……..16

1. Les meilleurs pratiques ……………………………………………………………………..16
2. Avantages …………………………………………………………………………………..16

**Chapitre II : Etude de la sécurité**…………………………………………………………..17

I-Etude de la sécurité physique ……………………………………………………………………17

1. Sécurisation des locaux et leurs contenus…………………………………………………..17
2. Sécurisation des terminaux et des liaisons…………………………………………………18

II-Sécurisation des accès et des échanges………………………………………………………….19

1. Mise en place d’un vlan……………………………………………………………………19
2. La sécurité wifi …………………………………………………………………………….19

* Troisième partie

**Chapitre I : Conception de l’architecture,**

**gestion de l’adressage et création des différents vlan** ………………………………..20

**I-Conception de l’architecture** …………………………………………………………………..20

1. Inventaire du matériel………………………………………………………………......20
2. Présentation du modèle type ………………………………………………………….21

**II-Gestion de l’adressage** ………………………………………………………………………....21

**III-Création des différents VLAN** ……………………………………………………………….22

1. Création des VLAN………………………………………………………………………...22
2. Explication des répartitions des vlan ………………………………………………………22

**Chapitre II : Réalisation**……………………………………………………………………..23

**I-Présentation du logiciel utilisé et les méthodes de configuration**…………………………….23

1. Présentation de simulateur « Cisco Packet Tracer »……………………………………….23
2. Méthode de configuration des équipements ……………………………………………….23

**II-Configuration des équipements**………………………………………………………………..23

1. Configuration des commutateurs …………………………………………………………..23
2. Création des vlan………………………………………………………………………..23
3. Configuration des interfaces Vlan………………………………………………………23
4. Configuration du vlan voix sur le Switch S5……………………………………………24
5. Configuration du routeur PFsense 2 LAN ………………………………………………….24
6. Sur le simulateur…………………………………………………………………………24
7. Configuration sur des ordinateurs réels………………………………………………….25
8. Configuration du serveur et des PCs ………………………………………………………..25
9. Serveur …………………………………………………………………………………..25
10. PCs……………………………………………………………………………………….26
11. Configuration des téléphones VoIP …………………………………………………………26
12. Implémentation de la téléphonie sur cisco packet tracer………………………………...26
13. De façon réel : installation 3CX Phone Système ………………………………………..26

**Chapitre II : Test et validation de configuration** ………………………………………27

**I-Test inter-vlan**………………………………………………………………………………….....27

**II-Test entre vlan**…………………………………………………………………………………...27

**III-Test entre ordinateur et le serveur**…………………………………………………………....27

**Chapitre III : Critique et observations**…………………………………………………...29

**I-Critique** …………………………………………………………………………………………..29

**II-observation**………………………………………………………………………………………29

**Conclusion général** ………………………………………………………………………………..30

**ABREVIATIONS………………………………………………………..1**

**BIBLIOGRAPHIE………………………………………………………2**

**WEBOGRAPHIE……………………………………………….2**

**Introduction Générale**

La mondialisation et la globalisation ont fait émerger diverses formes d’entreprises (planétaires, multinationales) qui viennent se greffer aux entreprises locales préexistantes. Dans le même cas, on note une évolution indéniable dans le domaine des Technologies de l’Information et de la Communication. Ces mutations substantielles obligent la plupart des entreprises à intégrer des applications de systèmes distribués dans leurs environnements respectifs pour une gestion optimale de l’information et des tâches. Dès lors, les préoccupations suivantes surgissent : Est-il possible pour les employés d’une entreprise de se partager les données en temps réel sans faire de déplacement ? La sécurité ne serait-elle pas compromise ? Existe-t-il une possibilité de faire transiter la voie et les données sur ce même réseau ?

Pour répondre à ces épineuses préoccupations, le thème suivant : « Etude de la mise en place d’une infrastructure réseau pour le développement d’un commerce en ligne », nous été soumis en étude.

Notre travail est organisé en trois parties principales :

la première partie (chapitres 1 et 2) fait état de la présentation de la structure, de l’étude et du choix des équipements les plus adapter afin de répondre le mieux possible aux besoin énoncer par celui-ci.

La deuxième partie (chapitres 1et 2) passe en revue les principales solutions de sécurité. Cette étude définit les besoins et les caractéristiques des solutions de sécurité en particulier l’emplacement des équipements qui est décisive pour faire face à tous les problèmes éventuels.

La troisième partie (chapitres 1, 2,3) met en exergue les solutions que nous souhaitons apporter à la structure après nos différentes études, c’est-à-dire la conceptionde l’architecture, la gestion de l’adressage et la création des différents vlan .Dans ce même chapitre nous effectuerons les différents tests de simulation afin de prouver que les solutions trouver fonctionnent vraiment de façon réel.

Enfin, dans le chapitre 4, nous concluons sur l’intérêt de notre travail et ses perspectives

Une liste des publications associées à cette thèse est présentée à la fin de cet ouvrage.

* **PREMIERE PARTIE**

**CHAPITRE I : PRÉSENTATION GÉNÉRALE DE LA STRUCTURE (Ressource : utilisation du texte support et des ressources sur internet).**

1. **Fonctionnement de la structure**
2. **Contexte**

Dans le cadre de ces activités de prestation de services divers, la structure FORTIC GROUP SARL est sollicitée par un puissant groupement de coopératives de femmes ivoiriennes, spécialisé dans la production et la commercialisation en ligne de vivriers tant sur le plan national qu’international, pour l’étude et la mise en place de l’infrastructure réseau de son siège.

Ce siège est un bâtiment, composé d’un rez-de-chaussée et de trois étages. Il est situé à FAYA dans la commune de Cocody, à 500 mètres à droite du feu du carrefour FAYA dans le sens Riviera 2 - Bingerville.

1. **Présentation**

La structure étudiée est celui d’un puissant groupement de coopératives de femmes Ivoiriennes, spécialisé dans la production et la commercialisation en ligne de vivriers tant sur le plan national que vers l’international.

1. **Objectif et missions**

L’objectif principal de cette étude est d’assurer une grande fiabilité en ce qui concerne l’échange de données dans un environnement sécurisé.

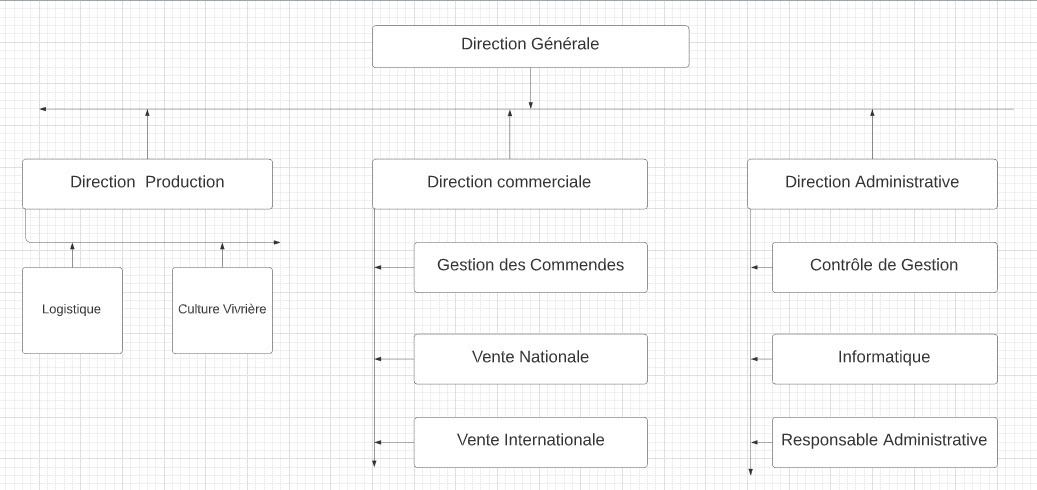
Dans la réussite de notre objectif nous nous somme fixer comme missions :

* la mise en place d’une architecture réseau LAN fiable supportant
* le système de VOIP ;
* le choix des équipements afin de
* Assurer la sécurité du réseau
* le déploiement des services nécessaires pouvant favoriser
* Le partager de fichiers, application et ressources en temps réel ;
* favoriser la communication entre personnelle administratif;
* favoriser l'accès aux données en temps réel ;

1. **Structuration de la structure**

Notre structure est constituée de :   
- Une Direction Générale qui gère toute les autres directions de la structure.  
- Une Direction Production qui se charge des unités de productions et d’approvisionnements, du stock et des moyens logistiques de la structure.  
- Une Direction Commerciale chargée du marketing, du management et de la commercialisation aussi bien sur le territoire national qu’à l’international.  
-Une Direction Administrative qui a la charge des services intégrés (finances, ressources humaines, informatiques, …)

1. **Organigramme (voir image)**

****

1. **Le système informatique de la structure**

Le système informatique est la partie informatique du système d’information

* L’objectif d’un système informatique est d’automatiser le traitement de l’information.
* Un système informatique est constitué de deux entités: le matériel et le logiciel.

1. **Le matériel**
2. **Côté matériel, un ordinateur est composé de:**

* L’Unité Centrale (UC) pour les traitements
* La Mémoire Centrale (MC) pour le stockage
* Les Périphériques: disque dur, clavier, souris, carte réseau...

1. **Le parc informatique de la structure**

En menant un inventaire aux différents services et départements du groupement de coopératives de femmes ivoiriennes dont le siège est un bâtiment composé d’un rez-de-chaussée accompagner de trois étages on a pu avoir les résultats suivants:

* Un ensemble de **90 ordinateurs** dédiés uniquement à la gestion des commandes dont la répartition est faite de la manière suivante :
* 10 postes situées au 1er étage
* 30 au 3ème étage
* 50 au rez-de-chaussée
* 3 grandes salles de type Open Space composer **75 ordinateurs** répartie en groupe de 25 box par salle, tous dédié à la gestion administrative de l’agence
* **5 bureaux** pour les responsables administratifs
* Un hangar d’une capacité de **100 places** assises équipé d’un wifi dédié aux visiteurs et leurs permettant de naviguer à l'aide de leur téléphone portable.

Vu tout cela on peut dire que le nombre totale d’ordinateur est de **170**, en fonction de cela nous ferons une architecture qui sera adapté aux différents besoin de l’entreprise en se chargeant d’acheter les autres équipements nécessaires pour un bon fonctionnement du réseau et répondant à tous les normes de sécurité en vigueur.

1. **Le logiciel**

Côté logiciel, un système informatique est composé de deux niveaux bien distincts:

Le système d’exploitation et les applications.

* + - * 1. **Objectifs d’un système d’exploitation**

Les deux objectifs majeurs d’un système d’exploitation sont:

* Transformer le matériel en une machine utilisable, c.-à-d. fournir des outils adaptés aux besoins des utilisateurs indépendamment des caractéristiques physiques,
* Optimiser l’utilisation des ressources (matérielles et logicielles).

Ces deux objectifs doivent être atteints en garantissant un bon niveau en Sécurité ; Fiabilité et Performance du système informatique.

* + - * 1. **Objectif d’une application**
* Améliorer l’offre de service au client
* Améliorer les processus de traitement des demandes des clients
* Amplifier l’intensité relationnelle avec le client

1. **Critique de l’existant**

Apres étude les limites suivantes sont à signales

* On constate que le groupement de coopératives de femmes ivoiriennes ne dispose pas encore de serveurs, pourtant la structure en a forcément besoin pour héberger un certain nombre de logiciels partagés.
* On constate aussi qu’il y’a manque d’équipement d’interconnexion hors Les équipements d'interconnexion représentent le cœur du réseau dans une architecture. S'ils sont mal dimensionnés, ils pourront avoir des effets négatifs sur le trafic du réseau, pouvant entrainer la détérioration de celui-ci.
* Et il n’y a pas encore de politique de sécurité.
* En gros le réseau doit être monté de A à Z

1. **Spécification des besoins**

Pendant cette phase nous allons étudier les besoins fonctionnels ainsi que les besoins en sécurité de l’infrastructure réseau.

Pour répondre au mieux aux besoins de l’entreprise nous nous sommes mis l’écoute du client qui est le groupement de coopératives de femmes ivoiriennes

Après analyse quelques besoins ont été relevés,

1. **Besoins en services**

Les services résultants de cette enquête se présentent comme suit :

* Service de transfert des fichiers et stockage de données;
* Service de téléphonie sur VoIP ;
* Service de gestion d’inventaire et maintenance
* Segmenter le réseau câblé en vlan ou en sous-réseau
* Installation d’un réseau WIFI dans le Hangar
* Mise en place d’une architecture réseau fiable

1. **Besoins en sécurité**

La sécurité informatique, c’est l’ensemble des moyens mis en œuvre pour réduire la vulnérabilité d’un système contre les menaces accidentelles ou intentionnelles.

C’est ce à quoi attendent les utilisateurs de systèmes informatiques en regard de la sécurité :

**Disponibilité :** Les données doivent rester accessibles aux utilisateurs.

**Confidentialité :** Les données ne doivent être visibles que des personnes habilitées.

**Intégrité :** Il faut pouvoir garantir que les données protégées n’ont pas été modifiées par une personne non autorisée.

**La non-répudiation et l'imputation :** Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

**L'authentification :** L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

La sécurité de notre réseau ainsi que de l’infrastructure peut être subdivisée en deux volet la sécurité contre les attaques et les menaces réseau ainsi que la sécurité contre les défaillances matérielles et supports de communications d’où la nécessité d’avoir les systèmes suivants :

Pare-feu (Firewall) ; Prévention des intrusions ; Supervision de la disponibilité.

* Les besoins résultants de notre étude sont :

*Gestion de la haute disponibilité ; Gestion de la monté en charge des serveurs ; Segmentation du réseau ; Créer une politique de sécurité*

**Les équipements nécessaires pour un réseau d’entreprise fonctionnel**

1. **Les composants matériels pour un réseau d’entreprise fonctionnel**
2. **Périphériques ﬁnaux**

Certains périphériques restent incontournables dans la conception d’un réseau d’entreprise. Ces périphériques forment l’interface entre les utilisateurs et le réseau de communication sous-jacent. Voici quelques exemples :

*Ordinateurs; Imprimantes réseau; Téléphones VoIP ; Terminal TelePresence; Caméras de surveillance; Appareils mobiles (tels que les Smartphones, tablettes) ; Serveur (physique ou virtuel).*

1. **Les équipements d’interconnexion**

Les équipements d’interconnexion ont pour but d’aiguiller les communications, les réorganiser afin que les informations transmises par les périphériques hôtes parviennent à la destination souhaitée. Ils sont utilisés dans le réseau selon le niveau d’action souhaité et les tâches à accomplir.

Nous trouvons dans cette catégorie les équipements suivant : *Répéteurs; Pont ; Routeur; Passerelle; Concentrateur ; Commutateur ; Adaptateur ; La carte réseau ; Le modem (modulateur démodulateur).*

1. **Les supports de transmission**

Ce sont les canaux utilisés pour véhiculer les informations dans le réseau. Nous avons:

* Les cables réseaux : UTP (Unshielded Twisted Pairs) ; FTP (Foiled Twisted Pairs) ; STP (Shielded Twisted Pairs) ; SFTP (Shielded Foiled Twisted Pairs) ; SSTP (Shielded Shielded Twisted Pairs)
* Fibre optique : Fibre optique monomode ; Fibre optique multimode
* Les supports sans fil : Appareil Wifi ; Carte Wifi ; Clé Wifi.

**CHAPITRE II : ETUDE DE L’INFRASTRUCTURE DU RÉSEAU INFORMATIQUE**

**Etude et choix des composants de l’infrastructure**

Apres avoir mené les différentes enquête sur les besoins de l’entreprise nous pouvons dire que notre infrastructure réseau sera composer :

|  |  |
| --- | --- |
| **Au niveau Matériel** | **Au niveau Logiciel** |
| Routeur**;** Switch**;** Serveur**;** Postes de travail**;** Câbles**;** Répéteur**;** Téléphonie IP**;** Imprimante réseau. | **Système d’exploitation (**machine client et serveur**) ; logiciel d'implémentation de la VoIP** ; **Les systèmes de gestion commerciale (**logiciels qui permettent laGestion et l'Administration des Ventes) ; **logiciel de sécurité (**antivirus**)** |

**I- Etude et choix des matériels**

1. **Le routeur**
2. **les différents types de routeur**

Il existe différents types de routeur, ces routeurs sont fabriqués par différents entreprises néanmoins il existe des normes internationaux qui permet à ce que ces routeurs fonctionnent ensemble même s’il ne vienne pas du même fabricant. Voici quelques un que nous citons:

|  |  |  |
| --- | --- | --- |
| ***Nom du routeur*** | ***Caractéristiques*** | ***Autres caractéristiques*** |
| **Le routeur TP-Link AC3200** | Antennes : 6 Vitesse : jusqu’à 3,2 Gbps  Ports : quatre ports lan Ethernet Gigabit  Routeur sans fil  Protocole : 802.11ac  Bande : une bande de 2,4 GHz et deux bandes de 5GHz | Prise en charge QoS, VPN intégré, Application mobile, Technologie Smart Connect. |
| **Le routeur Linksys AC5400** | Antennes : 8  Vitesse : jusqu’à 5,3 Gbps  Ports: huit ports Ethernet Gigabit  Protocole : 802.11ac  Bande : une bande de 2,4 GHz et deux bandes de 5 GHz | Fonctions de sécurité avancées, Pare-feu intégré, Technologie de formation de faisceau. |
| **Le routeur firewall Pfsense** | Open Source  Interface Web ergonomique  Nombreuses fonctionnalités  Packages gratuits (antivirus, scanner mail, Proxy…) | Utilisé dans les datacenters ou des fournisseurs de Streaming. |

1. **Choix du routeur en fonction des besoins de la structure**

Après énumération de quelque routeur présent ci-dessus nous nous somme basé sur les critères suivant pour effectuer le choix le plus adapter:

*Le type d'utilisation; La vitesse maximale; Le mode de sécurisation; La facilité dans l'installation et la manipulation; La question du prix vs. les performances*.

En fonction de tous ces critères et vue les besoins de cette entreprise notre choix se porte sur **Les routeurs firewall Pfsense**, plus précisément le [Parefeu PFSense 2 Lan 256Mo 2Go CF](http://www.itx-france.com/catalog/parefeu-pfsense-2-lan-256mo-2go-cf.html?osCsid=aoove2ffl249c7vtmp8mnvu7s5) car en plus d’avoir un prix abordable et une très bonne performance il est adaptée pour une utilisation comme Pare-feu et Routeur. Cela va nous éviter de dépenser encore de l’argent pour acheter un firewall.

1. **Commutateur (Switch)**

A pour fonction de démultiplier les prises informatiques pour accéder au serveur. Il permet de relier plusieurs équipements au réseau et ainsi de diffuser les informations à l’ensemble des ordinateurs.

1. **Les différents types de commutateur (Switch)**

Les commutateurs dans le monde du réseau sont nombreux, étudions certain afin de faire un choix :

|  |  |
| --- | --- |
| ***Nom du commutateur*** | ***Caractéristiques*** |
| **WS-C2960X-48LPS-L** | Type de produit : Commutateur Cisco  Modèle : WS-C2960X-48PS-L  Base LAN : Interfaces de liaison montante : 4 x 1G SFP  Les ports : 48 ports Ethernet 10/100/1000 Gigabit  Puissance PoE disponible : 370W  Nombre maximum d'empilement : 8  Pile bande passante : 80G  Largeur de bande de transmission : 108 Gbps  Bande passante de commutation : 216Gbps  RAM : 512 Mo  Mémoire flash : 128 Mo |
| **D-Link Switch D-Link 24 Ports** | 24 ports 10/100Mbps.  Full/half duplex supporté sur chaque port.  Auto-apprentissage de la configuration du réseau  Contrôle de flux en mode full duplex contre la perte de données  Back pressure en mode half duplex |

1. **Choix du Switch en fonction des besoins de la structure**

Le choix de notre Switch va se baser sur la performance de ses caractéristiques comme par exemple :

*Le nombre de port, sa ram, sa mémoire flash, sa puissance PoE.*

De ce fait pour notre étude notre choix se porte sur le WS-C2960X-48LPS-L car nous voulons ce qu’il y a de mieux pour l’entreprise. Les commutateurs Cisco Catalyst gamme 2960 prennent en charge les communications voix, vidéo et données et garantissent un accès hautement sécurisé.

1. **Serveur**

Un serveur informatique offre des services accessibles via un réseau.

Il peut être matériel ou logiciel, c’est un ordinateur qui exécute des opérations suivant les requêtes effectuées par un autre ordinateur appelé « client ».

* 1. **Les différents types de serveurs informatiques**

Un serveur offre plusieurs services, ainsi il existe plusieurs types de serveurs informatiques

|  |  |
| --- | --- |
| **Web** | c’est ce qui permet à un navigateur web d’afficher un site internet |
| **Fichiers** | il permet de stocker tous les documents et de les rendre accessibles depuis n’importe quel ordinateur |
| **Applicatifs métiers** | il permet de stocker toutes les données commerciales, clients, comptabilité et d’en extraire que les données nécessaires |
| **Messagerie** | il permet de gérer la distribution des mails et d’y avoir accès à distance |

Trois formats de serveur physique existent:

|  |  |
| --- | --- |
| **Serveur Tour** | similaire aux unités centrales d’un PC fixe. Ils peuvent être installés n’importe où, mais nécessitent tout de même une arrivée électrique adaptée. |
| **Serveur Rack** | ils ont un format aplati et sont destinés à être installés dans une baie. Les configurations sont plus performantes que sur les serveurs Tour. L’accès est facilité car ils sont généralement rangés dans des armoires dans des salles dédiées. |
| **Serveur Lame** | c’est le format le plus récent, ces serveurs ne peuvent fonctionner seuls, ils se glissent dans un châssis intégrant d’autres serveurs lames. La différence avec ce format de serveur, c’est que c’est le châssis qui est relié aux connexions réseau et alimentations électriques. |

* 1. **choix du serveur**

Pour notre étude nous aurons besoin de 3 types de serveurs qui sont : serveur web, serveur de fichier et serveur applicatifs métiers, néanmoins tout ces serveurs seront compilé en service dans un seul serveur administré à l’aide de Windows server 2016.

Au niveau du format nous nous pencherons sur le format de serveur Rack

1. **Les câbles**
   1. **Les différents types de câble**

Il existe Trois types de câbles qui sont :

* le câble coaxial (RG58) en voie de disparition
* le câble à paires torsadées (FTP, UTP, SFTP…) le plus répandu actuellement
* la fibre optique utilisée pour l'interconnexion de réseaux locaux
  1. **choix du câble**

Pour notre étude notre choix se portera sur les câbles pairs torsadés

1. **répéteur**

Le répéteur est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau. Il régénère un signal affaibli pendant le transport afin d’allonger le réseau**.**

* 1. **Les différents types de répéteur**

|  |  |
| --- | --- |
| ***Nom du répéteur*** | ***Caractéristiques*** |
| **Netgear Nighthawk EX7300** | Rapide, fiable et facile à installer  Technologie MU-MIMO  Technologie BEAMFORMING  Compatible avec toutes les normes Wi-Fi 802.11b/g/n et 802.11ac  Technologie Dual Band et inclut un port Ethernet  Jusqu’à 1733 Mbps sur une bande de 5 GHz  Couverture maximale de 930 m² |
| **TP-Link RE200 (AC750)** | Portée extensible, installation facile  Design discret et débit respectable  Compatible avec toutes les normes Wi-Fi 802.11b/g/n et 802.11ac  Technologie Dual Band et inclut un port Ethernet  Combine un signal 2,4 GHz et un signal 5 GHz  Vitesse allant de 300 Mbps à 750 Mbps  Vitesse maximale en mode “High Speed” |

* 1. **choix du répéteur**

Pour nous, le meilleur répéteur Wifi est sans conteste le Netgear Nighthawk EX7300 C’est l’un des répéteurs les plus rapides et les plus fiables du marché. Il couvre une surface très étendue. De plus, il est intuitif et facile à installer.

1. **Récapitulatif des matériels choisis pour l’entreprise**

|  |  |
| --- | --- |
| **Le routeur** | routeurs firewall Pfsense |
| **Commutateur (Switch)** | WS-C2960X-48LPS-L |
| **Serveur** | Windows server 2016 |
| **câbles** | paires torsadées |
| **répéteur** | Netgear Nighthawk EX7300 |

**II- Etude des différents logiciels disponibles sur le marché et choix des meilleurs**

Nous avonsplusieurs logiciels qui interviennent dans la composition d’un réseau informatique d’une entreprise de vente en ligne :

|  |  |
| --- | --- |
| **Système d’exploitation** | Un système d'exploitation est un ensemble de programmes qui dirige l'utilisation des ressources d'un ordinateur |
| **Logiciel d'implémentation de la VoIP** | La VoIP signifie Voice over Internet Protocol ou Voix sur IP (IP = Protocole Internet). Comme son nom l'indique, **la voix sur IP (VoIP)** désigne la technique d'acheminement des appels téléphoniques sur un réseau de données IP, qu'il s'agisse d'Internet ou du réseau IP interne propre à une entreprise. |
| **Logiciel de gestion des commandes** | Un système de gestion des stocks doit couvrir les fonctions suivantes  **Structuration des achats; Structuration des ventes; Entrée des marchandises; Sorties des marchandises; Gestion de stocks** |
| **Logiciel de sécurité (antivirus)** | Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Il vérifie aussi les fichiers et courriers électroniques, les secteurs de démarrage (afin de détecter les virus 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. |

1. **Etude des différents logiciels disponibles sur le marché**
   1. **Au niveau du système d’exploitation**

En informatique, les 3 principaux systèmes d’exploitation sont : **Windows**, **OS X** et **Linux.** Ces systèmes d’exploitation ont évolué avec le temps, il en existe donc plusieurs versions.

* **présentation de quelques logiciels**

|  |  |
| --- | --- |
| **Windows** | a été créé par Microsoft, il est actuellement le plus répandu des 3. La version vendue actuellement est Windows 10 mais il existe encore d’anciennes versions: Windows 8, 7, Vista ou encore Windows XP. Ce système est vendu sur différentes marques d’ordinateurs (Dell, HP etc.) |
| **MacOs** | (anciennement OS X) a été développé par la société Apple. Ce système d’exploitation n’est présent que sur les ordinateurs de la marque Apple (Macintosh).  Ceux-ci sont facilement reconnaissables grâce au logo représentant une pomme |
| **Linux** | est le moins connu des 3 systèmes d’exploitation. Il est rarement installé par défaut sur un ordinateur. Gratuit et libre, il est surtout utilisé par ceux qui ont de bonnes connaissances en informatique. |

* 1. **Au niveau du logiciel d'implémentation de la VoIP**

Il existe plusieurs logiciels qui permettent d'implémenter une solution VoIP dans une entreprise, que ça soit dans le monde libre, ou dans le monde des logiciels propriétaires (3CX Phone System).

* **présentation de quelques logiciels**

|  |  |
| --- | --- |
| **Asterisk** | est un autocommutateur téléphonique privé (PABX) open source pour systèmes UNIX. Il permet, entre autres, la messagerie vocale, les files d'attente, les agents d'appels, les musiques d’attente, les mises en garde d'appels, la distribution des appels et la gestion de conférences.  Asterisk peut également jouer le rôle de registrar et de passerelle avec les réseaux publics. Il est utilisé par certains opérateurs comme cœur de réseau téléphonique.  Dans son utilisation classique comme plateforme de téléphonie IP, Asterisk est généralement associé à Freepbx, une IHM permettant de piloter l'ensemble de ses fonctionnalités. |
| **3CX PHONE SYSTEM16** | est un IPBX logiciel qui tourne sur les systèmes d’exploitation les plus courants (Debian, Windows, Windows serveur) et se combine avec les téléphones IP, les trunks SIP et les passerelles VoIP compatibles SIP pour fournir une solution de téléphonie fixe complète, sans les soucis de gestion et les coûts importants liés à un PABX traditionnel. 3CX est reconnu pour son innovation et sa technologie de pointe. Il peut être facilement installé sans avoir besoin de connaissances télécoms spécifiques. 3CX est préconfiguré pour fonctionner avec les téléphones IP, les passerelles VoIP et les trunks SIP les plus courants, ce qui vous évite d’avoir à configurer ces appareils manuellement. |

* 1. **Au niveau du logiciel de gestion des commandes**

Ils font le lien entre les achats, les ventes et les stocks

* **présentation de quelques logiciels**

|  |  |
| --- | --- |
| **Le logiciel Ciel e-commerce** | Simplification des commandes clients  Mise à jour du catalogue de vente des produits et services  Bonne visibilité sur les conditions tarifaires des clients  Suivi des commandes en ligne et récupération automatiquement des commandes |
| **Le logiciel EBP** | Logiciel gratuit avec des fonctionnalités simplifiées  Interface rapide et simple d’utilisation  Facturation des clients, impression du livre d’achats-recettes et visualisation des charges sociales et les impôts |
| **Le logiciel Opensi,** | Grâce aux différentes options proposées par ce logiciel de vente et gestion de stock gratuit, nous aurons la possibilité d’assurer la gestion commerciale et la comptabilité de notre e-commerce. |

* 1. **Au niveau du logiciel de sécurité (antivirus)**

Les années passent et la menace de virus venue d’internet grandit de manière exponentielle. Les différents éditeurs de logiciels antivirus bloquent plusieurs millions de cyber-attaques de différents types : virus, exploit zero-day, ransomware, crypto-jacking et autres piratages très sensibles.

Vue tout cela l’installation d’un antivirus est plus qu'indispensable pour assurer une bonne sécurité des ordinateurs et ainsi se protéger plus efficacement contre les différentes attaques.

Il existe plusieurs antivirus disponibles sur le marché : **bit defender, Eset nod 32, Kaspersky, Avast business antivirus, Norton** etc...

1. **choix du logiciel le plus adapté**

|  |  |
| --- | --- |
| **système d’exploitation** | Windows 10 professionnel |
| **logiciel d'implémentation de la VoIP** | 3CX Phone System |
| **logiciel de gestion des commandes** | ciel e-commerce |
| **antivirus** | avast business antivirus |

* **DEUXIÈME PARTIE :**

**CHAPITRE I : MISE EN PLACE D’UNE POLITIQUE DE SECURITE**

Parce que les risques en matière de sécurité n’ont cessé d’augmenter ces dernières années, il est important pour notre entreprise de mettre en place une stratégie qui permet d’être **préparé en cas** **d’incident** et de **réduire l’occurrence de ces** **éventuels incidents**.

1. **Etablir une politique de sécurité**
2. **Définition de la politique de sécurité informatique**

Une politique de sécurité informatique est une*stratégie* visant à *maximiser la sécurité informatique**d’une entreprise*. Elle est matérialisée dans un *document* qui reprend l’ensemble des *enjeux,**objectifs, analyses, actions et procédures* faisant parti de cette stratégie.

* à distinguer de la *charte informatique*, qui est un document de recommandations concernant la bonne utilisation des technologies informatiques, et qui est destiné aux employés de l’entreprise
* ce document est *unique* et *personnalisé*, car établi en tenant compte du *fonctionnement*, de *l’environnement*, de la *composition du système d’information* de l’entreprise et des *enjeux*et des*risques* informatiques qui lui sont propres

1. **les principaux points de cette politique de sécurité**

La procédure de sécurité tournera autour de 4 points principaux :

* L’évaluation de ce qu'on veut sécuriser ici c’est tout le réseau
* La protection du serveur, et de tout les équipements
* La détection des erreurs, virus etc…
* Réponse (ou reprise d'activité)

1. **Étapes d'établissement d'une politique de sécurité**

L'établissement d'une politique de sécurité se fait selon différentes étapes.

**Etape 1 :** Identifier ce qu'il faut protéger

**Etape 2 :** Analyser les risques

**Etape 3** : Évaluer les contraintes

**Etape 4 :** Choisir les moyens

Il existe plusieurs techniques de base pour assurer la sécurité. Il faut faire un choix cohérent de ces techniques. Ces techniques se subdivisent en deux catégories :

-Les moyens de sécurisation (Les techniques cryptographiques ; La sécurisation des serveurs et des postes de travail ; L'authentification des utilisateurs; Les pare-feu ; Les VPN ; Les antivirus).

-Les moyens de détection d'intrusion (Tous les moyens logiciels et matériels permettant de détecter toute intrusion dans le système).

**Etape 5 :** Adopter la politique de sécurité

**Etape 6 :** Tester

Après avoir adopté et mis en place la politique de sécurité, on s'assurera par un audit externe si celle-ci répond au cahier des charges.

1. **Les meilleures pratiques et avantages de la mise en place d’une politique de sécurité informatique**
   1. **Les meilleures pratiques**

Quelques-unes des meilleures pratiques à observer lors de l’élaboration de notre politique de sécurité informatique :

**Désigner un responsable informatique**

**Définir le périmètre et les objectifs** de la politique de sécurité informatique

**Effectuer une analyse de l’existant**, matériel et logiciel, et tenir à jour un registre de l’ensemble des éléments qui composent le système d’information.

**Effectuer une analyse des risques informatiques**,

**Déterminer les moyens nécessaires** pour la réduction des risques et la prise en charge des incidents.

**Définir les procédures adaptées**, notamment en matière de gestion des incidents

**Rédiger une charte informatique**, à l’attention des collaborateurs

**Communiquer sur la politique de sécurité informatique** auprès de l’ensemble de l’entreprise

* 1. **Avantage**

Une politique de sécurité d'entreprise apporte les avantages suivants:

* Un cadre fonctionnel permettant d'implémenter des Procédures de sécurité dans l'infrastructure du réseau
* Un processus permettant l'audit de la sécurité
* Une sécurité globale
* Une base pour toute action juridique éventuelle
* un processus permettant l'audit de la sécurité actuelle du réseau

**CHAPITRE II : ETUDE DE LA SECURITE**

En vue de trouver le meilleur emplacement pour chaque équipement une étude sera au préalablement mené dans les locaux de l’entreprise

1. **Etude la sécurité physique**

Les locaux techniques sont des points essentiels du réseau local, sans lesquels il ne peut fonctionner correctement. Ils présentent un point de vulnérabilité important dans la mesure où ils abritent un nombre important d'appareils sensibles et sur lesquels pèsent des menaces importantes.

Les risques sont aussi physiques et sont davantage liés aux événements imprévisibles comme les pannes, les accidents ou encore les atteintes intentionnelles aux matériels.

Deux types de mesures existent pour se prémunir de ces risques :

Les mesures préventives: elles doivent éviter qu'un sinistre ne survienne (empêcher un départ de feu)

Les mesures protectrices: elles doivent protéger le patrimoine si un sinistre survient malgré tout (ex: protéger son serveur du feu en cas d'incendie)

1. **Sécurisation des locaux et leurs contenus**

Elle concerne tous les dispositifs déjà mis en place pour assurer le bon fonctionnement et la protection des équipements

* **Protection électrique des équipements**

Un onduleur est un dispositif permettant de protéger des matériels électroniques contre les aléas électrique. Il s’agit d’un boîtier placé en interface entre le réseau électrique et les matériels à protéger afin d’éviter des pertes de données et des interruptions de service, voire des dégâts matériels.

* **Protection Mécanique des équipements**

Les nœuds tels que les Switch, AP, Routeur seront installés dans des coffrets sécurisés (panneaux de brassage) pour éviter tout désagrément. Les équipements du réseau cœur seront par ailleurs centralisés dans la salle serveur qui est mieux protégée.

* **Système de refroidissement**

Les locaux informatiques (salle serveur, salle d'équipements) seront équipés d’un split fonctionnant à une température abordable afin de protéger les composants électroniques.

Le tableau ci-dessous nous cite quelque exemple de problème qui pourrait survenir et nous montre comment les éviter

|  |  |  |
| --- | --- | --- |
| **Type de Menace** | **Conséquences** | **Riposte** |
| **Incendie** | Indisponibilité des équipements du local  Destruction des équipements  Indisponibilité partielle ou  totale du réseau | mécanisme d'extinction des feux ne détériorant pas le matériel informatique |
| **les dégâts des eaux** | court-circuit entraînant la rupture de service des équipements ; danger d'électrocution ; détérioration du serveur corrosion des câbles et connecteur | installation des tubes hermétiques pour le câblage d'alimentation et le câblage réseau... |
| **les dégâts liés à l’électricité** | perte de données  panne d’équipement  risque d’incendie  électrocution du personnel | paratonnerre, groupe électrogène ou équivalent... |
| **la température ambiante** | vieillissement prématuré des composants informatiques  destruction du serveur si la température dépasse 35° | système de ventilation correctement dimensionné dans la pièce du serveur |
| **les intrusions physiques** | perte financière directes (perte de données cruciales, système d’information hors service  perte de crédibilité en cas de divulgation de données confidentiel  perte de temps (effort pour rétablir les données perdu | vidéosurveillance, porte blindée... |

1. **sécurisation des terminaux et des liaisons**

L'élément terminal du réseau local est le plus souvent un micro-ordinateur raccordé au réseau local mais il conviendra d'attacher la même importance aux autres équipements tels que (imprimantes, fax, téléphones portables, etc.)

* **Localisation du serveur**

L'emplacement du serveur est déterminant dans sa sécurité, il va donc être choisi avec soin.

* Choix d’un emplacement idéal

-On va éviter d'installer le serveur dans le rez-de-chaussée et le dernier étage du bâtiment à cause des risques plus importants d'infiltration d'eau donc l’emplacement idéal sera le deuxième étage.

-Pour le sol, on évitera la moquette au profit d’un revêtement antistatique.

-La pièce comportera très peu d'ouvertures, voire aucune autre que la porte (risque d'intrusion physique) et il sera aussi loin d'un lieu de passage (ex : entrée)

-Les serveurs sont prévus pour fonctionner entre 10° et 35° en moyenne (certains supportent une température plus élevée) donc vue cela on va prévoir un système de climatisation

-On Installera aussi un onduleur en cas de coupure de courant prolongée

* Ci-dessous, tableau relatent les types de menace, les conséquences et les parades pour avoir une sécurité optimal

|  |  |  |
| --- | --- | --- |
| **Type de Menace** | **Conséquences** | **Parades** |
| Piratage   Par écoute.     Par utilisation illicite | • Perte de confidentialité.    • Altération des informations, détournement, fraude, etc | • Orienter les matériels de façon à ce que personne ne puisse observer ceux-ci à partir d'un couloir ou d'une fenêtre par exemple  • Utiliser des économiseurs  d'écrans avec mots de passe.  • Sensibiliser les utilisateurs..  • Protéger l'accès aux données /matériels par des mots de passe.  • Prévoir un contrôle d'accès  physique aux locaux.  • Sensibiliser les utilisateurs. |
| Utilisation d'un élément terminal pour l'introduction d'un virus. | • Indisponibilité.  • Perte d'intégrité /confidentialité. | • Introduire dans la politique de protection contre les virus une procédure de validation des disquettes et autres supports.  Exemple: Zone neutre avec  un point de passage unique et  obligatoire des entrées /  sorties.  • Verrouiller les lecteurs de  supports externes voire les  supprimer. |

1. **Sécurisation des accès et des échanges**
   * 1. **Mise en place d’un vlan**

Pour réduire les domaines de diffusion et pour ne permettre que les communications autorisées, des VLAN et un routage Inter-VLAN sera définis.

Parmi les avantages liés à la mise en œuvre d’un VLAN, on retiendra notamment:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| La flexibilité de segmentation du réseau | La simplification de la gestion | L’augmentation des performances du réseau | Une meilleure utilisation des serveurs réseaux. | Le renforcement de la sécurité du réseau. |

* + 1. **la sécurité wifi**

Pour sécuriser notre réseau Wi-Fi, nous utiliserons la certification WPA2.

Nous avons donc :

* Une sécurité et une mobilité plus efficaces grâce à l’authentification du client indépendamment du lieu où il se trouve.
* Une intégrité et une confidentialité fortes garanties par un mécanisme de distribution dynamique de clés.
* Une flexibilité grâce à une réauthentification rapide et sécurisée.
* **TROISIÈME PARTIE :**

**CHAPITRE I**: **CONCEPTION DE L’ARCHITECTURE**, **GESTION DE L’ADRESSAGE ET CREATION DES DIFFERENTS VLAN**

1. **Conception de l’architecture**

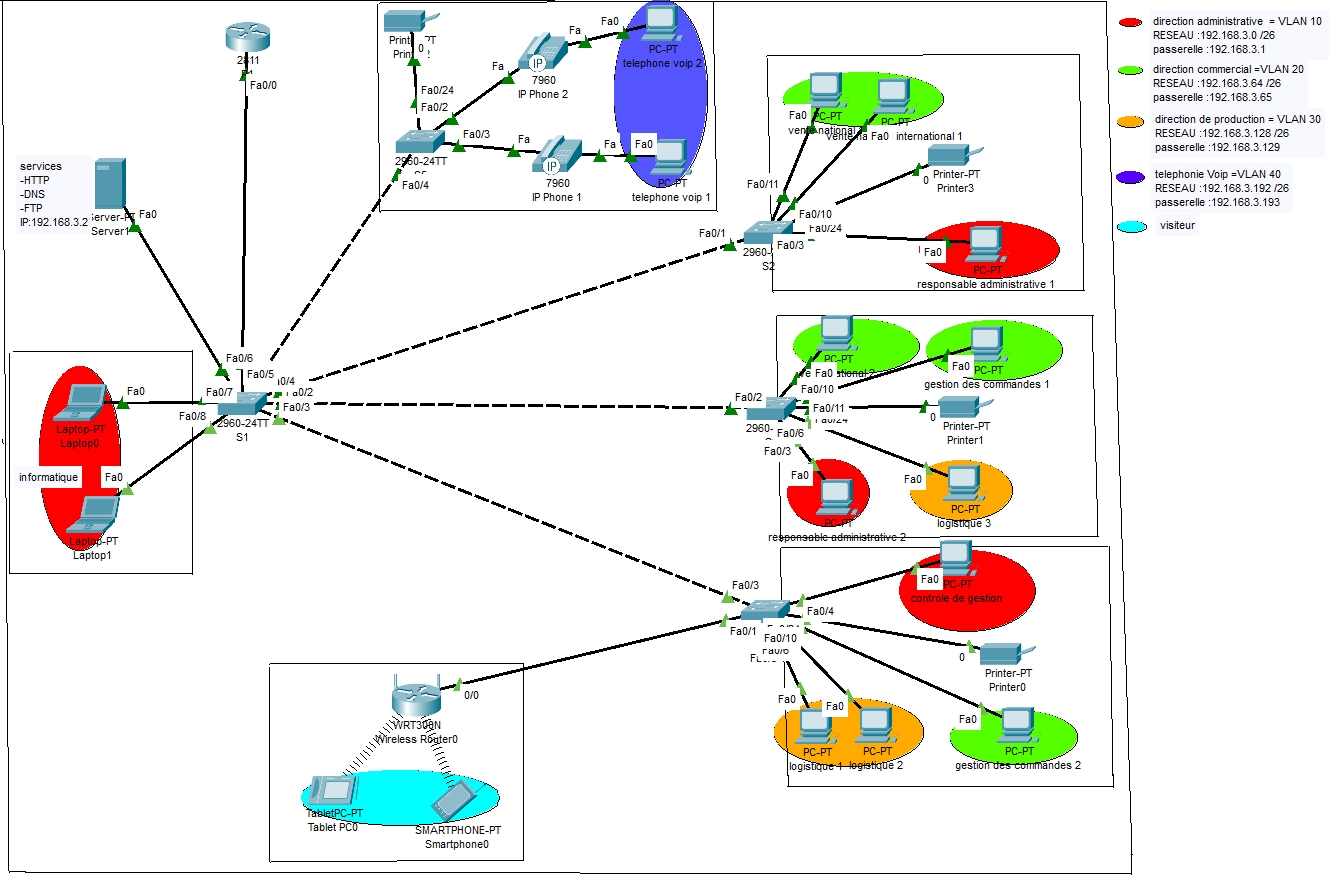
La conception de notre architecture est une des étapes essentielles permettant d'assurer la rapidité et la stabilité de notre réseau. Si notre réseau n'est pas conçu de manière adéquate, de nombreux problèmes imprévus peuvent survenir, ce qui peut entraver son fonctionnement.

* + 1. **Inventaire du matériel**

|  |  |  |
| --- | --- | --- |
| **Equipements** | **Caractéristique(s)** | **quantité(s)** |
| Switch(WS-C2960X-48LPS-L) | CPU: 600Mhz ; Mémoire: 128Mb ; RAM: 512Mb ; Port: 48 ;Type: 10/100/1000 PoE+ ;Authentification: Kerberos, RADIUS, SSH, TACAS+ . | 6 |
| Routeur (PFsense 2 LAN) | CPU: *AMD Geode LX800  500Mhz* ; Mémoire: *256Mo*  Stockage: *2Go*; Port: *2*; Type: *10/100 PoE*. | 1 |
| serveur | Serveur de fichier  Serveur d’application  Serveur web | 1 |
| carte réseau | Carte Ethernet, carte wifi | 171 |
| câble (paires torsadées) | FTP Catégorie 6 100/1000 Fast Ethernet | 600m |
| Répéteur | Port gigabit Ethernet: 2  Wi-Fi 802.11ac 5Ghz - Wi-Fi 802.11n 2.4Ghz  Compatible avec boitier internet | 1 |
| ordinateurs (dell) | Windows 10 ; ciel e-commerce ; avast business antivirus ; Processeur 1.7 GHZ ; Ecran 17'' ; RAM 4 Go ; Disque Dur 250 Go ; Multimédia ; Carte réseau intégré ; Modem intégré. | 100 |
| ordinateurs(HP) | windows 10 ; ciel e-commerce ; avast business antivirus ; Processeur 1.6 GHZ ; Ecran 17'' ; RAM  4 Go ; Disque Dur 250 Go ; Multimédia | 70 |
| Fournisseur d’Accès Internet et équipement choisi | FAI: ORANGE CI  Equipement: Fiber Box orange ci  Offre JET avec 100mb/s par liaison fibre optique | 1 |
| les téléphones VoIP | 3CX Phone System | 164 |
| Les téléphones IP | TELEPHONE IP CISCO 8841 | 6 |

NB: Dans la pratique, la Fiber Box du fournisseur d’accès à internet peut faire office de routeur.

* + 1. **Présentation du modèle type**



1. **Gestion de l’adressage**

Nous avons donc : 192.168.3.0 à 192.168.4.255 plage d’adresse donnée par le tuteur

En fonction de l’architecture que nous voulons mettre en place, nous avons besoin de 4 sous réseaux

Grâce à l’adresse 192.168.3.0 /24 nous obtenons les 4 sous réseaux suivants:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID RESEAU** | **MASQUE DE SOUS-RESEAU** | **PLAGE D’ID HOTE** | **NOMBRE D’HOTES UTILISABLES** | **@BROADCAST** |
| 192.168.3.0 | /26 | 192.168.3.1 – 192.168.3.62 | 62 | 192.168.3.63 |
| 192.168.3.64 | /26 | 192.168.3.65 – 192.168.3.126 | 62 | 192.168.3.127 |
| 192.168.3.128 | /26 | 192.168.3.129 – 192.168.3.190 | 62 | 192.168.3.191 |
| 192.168.3.192 | /26 | 192.168.3.193 – 192.168.3.254 | 62 | 192.168.3.255 |

Nous attribuons l’adresse 192.168.3.2 /26 a notre serveur qui aura pour passerelle 192.168.3.1

Nous configurerons le routeur comme DHCP afin de pouvoir fournir les adresses aux différents ordinateurs selon leurs plages d’adressage et leurs vlan

NB: Nous avons encore en réserve le réseau 192.168.4.0 /26 que nous utiliserons de manière pratique plus tard pour augmenter le réseau

1. **création des différents VLAN**
2. **Création des VLAN**

**Les tableaux ci-dessous nous donnent une répartition des adresses selon les services :**

|  |  |  |
| --- | --- | --- |
| **services** | **adresse IP de sous réseau** | **numéro VLAN** |
| Direction administrative | 192.168.3.0 /26 | vlan 10 |
| Direction commerciale | 192.168.3.64 /26 | vlan 20 |
| Direction de production | 192.168.3.128 /26 | vlan 30 |
| La téléphonie VoIP | 192.168.3.192 /26 | vlan 40 |

1. **Explication des répartitions des vlan**

Après analyse, comme indiqué ci-dessus nous avons défini quatre *(04)* VLANs répartis comme suit:

» VLAN Administration : Vlan 10

Dans ce Vlan, nous retrouverons toutes les machines de l'Administration, à savoir celle du contrôle de gestion, de l’informatique et du responsable administrative.

Ce Vlan contiendra aussi les imprimantes réseau et le serveur.

» VLAN commerciale : Vlan 20

Ce Vlan est destiné à la gestion des commandes, aux ventes nationales et internationales

» VLAN production : Vlan 30

Ce Vlan est destiné à la logistique qui se chargera de gérer les cultures vivrières

» VLAN de la téléphonie VoIP : Vlan 40

Ce Vlan sera uniquement destine à la voix sur IP pour faciliter la gestion différentes commandes par les employés de l’entreprise .Il sera répartie dans une salle unique pour une efficacité optimal.

NB : cette répartition d'une part permettra à l'Administrateur d'être plus à l'aise dans la gestion de son parc informatique et de son réseau, d'autre part elle nous permettra de bien dimensionner notre bande passante par priorité de segment

.

**CHAPITRE II : REALISATION**

A ce niveau de notre étude notre travail consistera à configurer notre modèle type en utilisant le simulateur « Cisco Packet Tracer », de faire aussi les différentes tests et la validation de notre configuration.

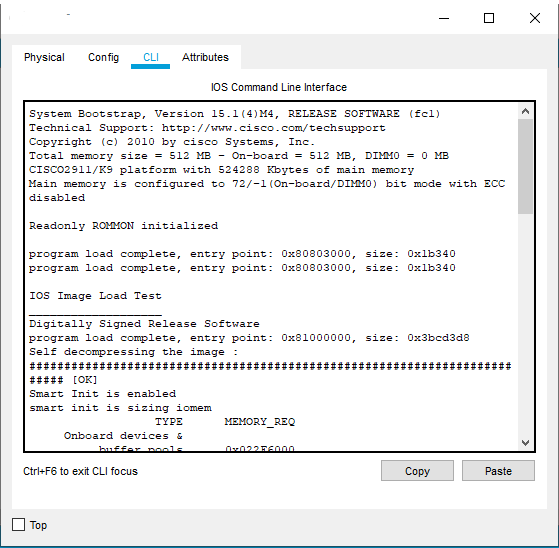
Remarque: Vue que certaine configuration ne peuvent se faire à travers le simulateur par manque de ressource nous utilisons des capture d’écrans, certains viendrons du simulateur et d’autre non pour vous montrer que les différentes configurations fonctionnent.

1. **Présentation du logiciel à utiliser et les méthodes de configuration**
   1. **Présentation de simulateur « Cisco Packet Tracer »**

Le « Cisco Packet Tracer » est un programme puissant de simulation qui permet aux étudiants d'expérimenter le comportement du réseau. En effet, Packet Tracer fournit la simulation, la visualisation, la création, l'évaluation et les capacités de collaboration et facilite l’enseignement et l’apprentissage des technologies complexes.

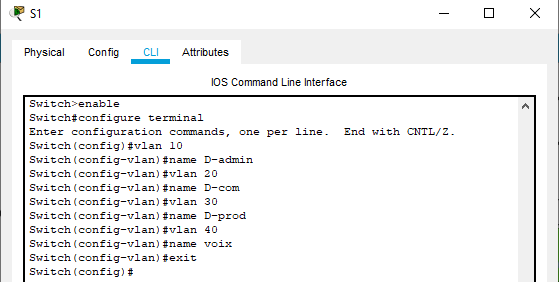
* 1. **Méthode de configuration des équipements :**

Pour configurer les équipements du modèle on utilise le CLI (Command Language Interface)



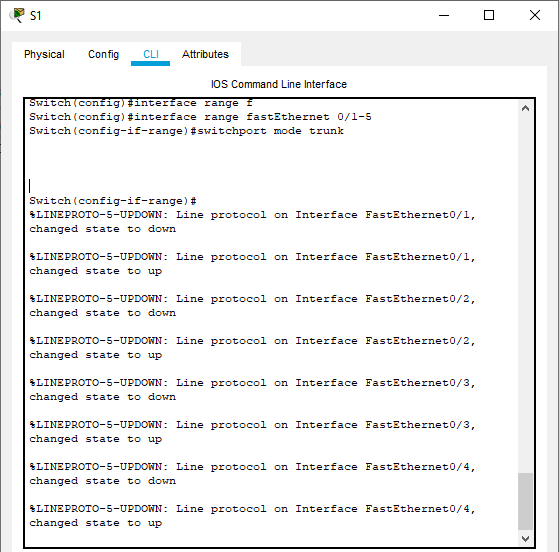
1. **Configuration des équipements** 
   1. **Configuration des commutateurs**
2. **Création des vlan**

Nous allons tout d’abord crée les 4 vlan sur les 6 Switch :



1. **Configuration des interfaces Vlans**

* Sur le Switch S1 les interfaces seront configurées comme suit



* Les autres Switch S2, S3, S4, S5 et S6 serons configurer conformément à la topologie mentionner à droite de notre architecture en se basant sur les différentes couleurs des ordinateurs

1. **configuration du vlan voix sur le Switch S5**

****

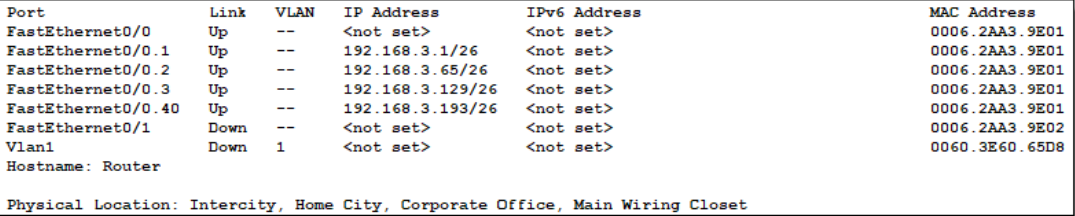
* 1. **configuration du routeur** PFsense 2 LAN

Le routeur sera configurer comme un serveur DHCP afin de fournir automatiquement les adresses IP des ordinateurs se trouvant sur des vlan différent

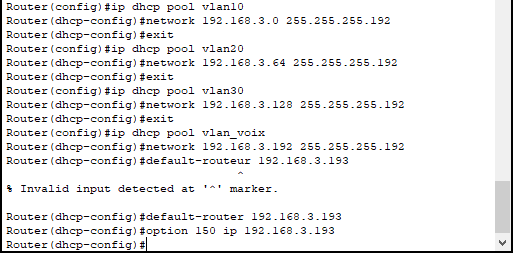
Par défaut les interfaces du routeur son éteint donc pour les allumer on fera au préalablement un NO SHUTDOWN dans le mode de configuration globale

* + - 1. **sur le simulateur**
* créations des interfaces virtuelles

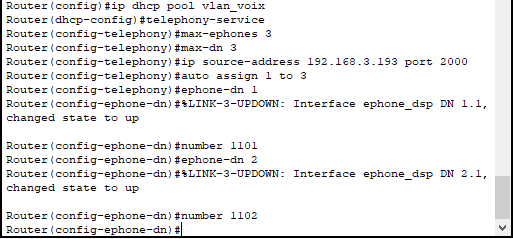
Tout d’abord nous allons créer des interfaces virtuelle dot1Q qui serons charger de gérer les différents sous-réseaux, ce qui donne le résultat suivant :



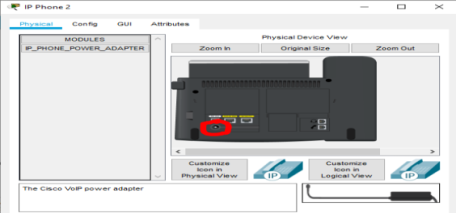
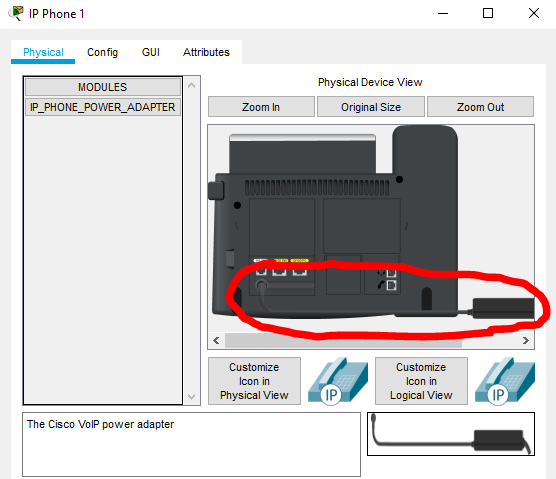
* configuration des 4 DHCP pool



* créations des téléphones et attribution des numéros



* activation des téléphones

1. 2. 

3. 4.

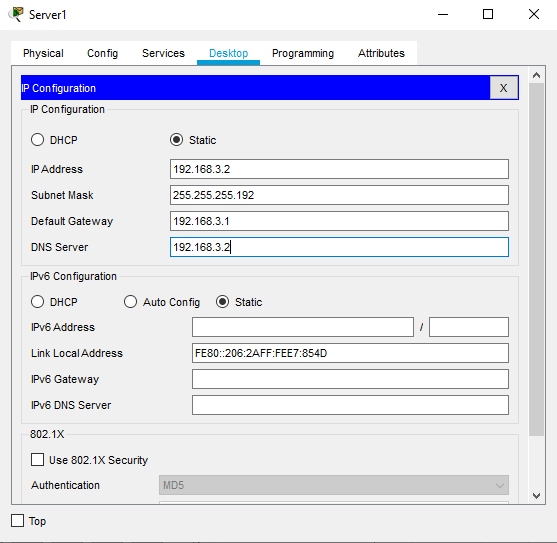
- Nous allons exclure les deux adresses suivant 192.168.3.2 et 192.168.3.3 de sorte a pouvoir les attribuer au serveur de manière statique



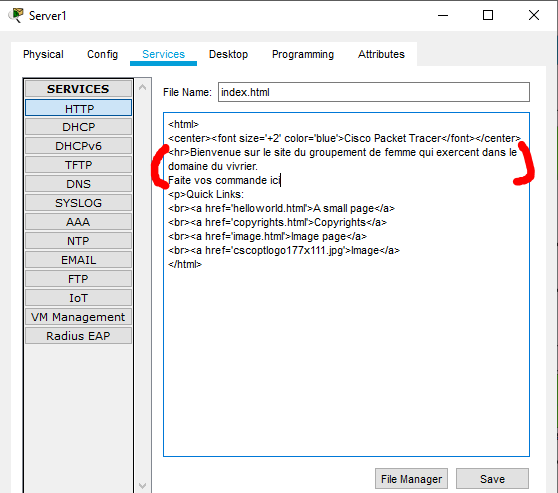
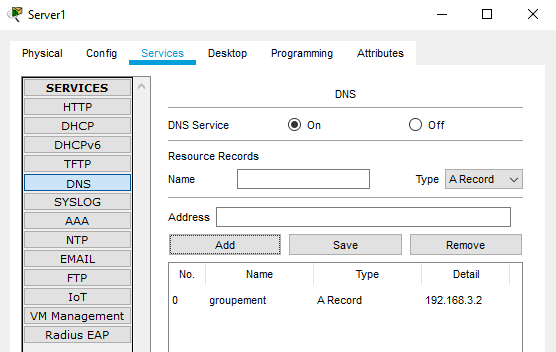
* + - 1. **configuration sur des ordinateurs réels**

Voir fichier ( pfSense \_ Installation et Configuration \_ PC2S - Bubu 1)

* 1. **Configuration du serveur et des PCs**
     + 1. **Serveur**
* Le serveur aura une adresse statique qui est la 192.168.3.2 /26

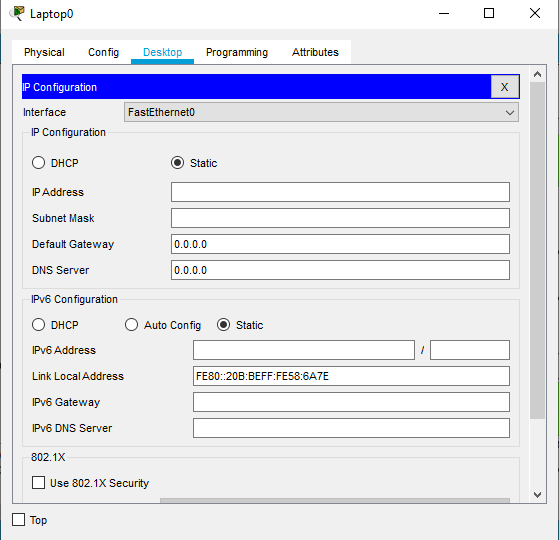
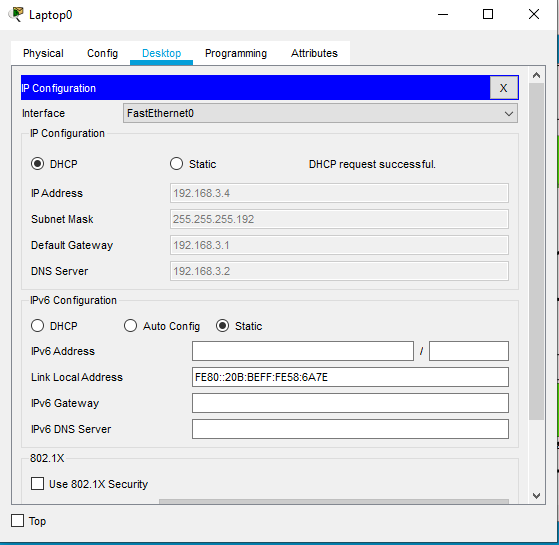


* Il possèdera 2 services HTTP et DNS pour la gestion du site en ligne

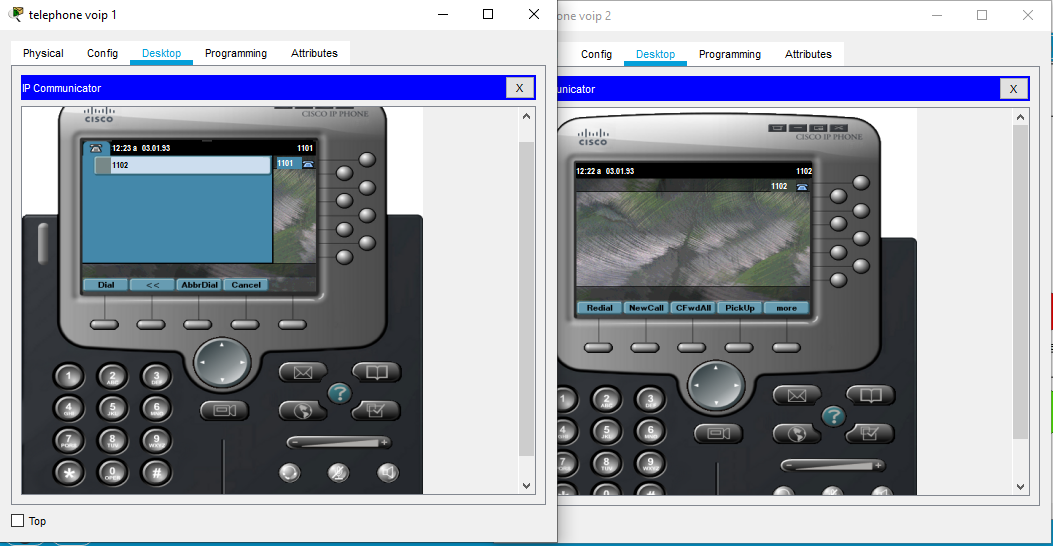
 

* + - 1. **PCs**

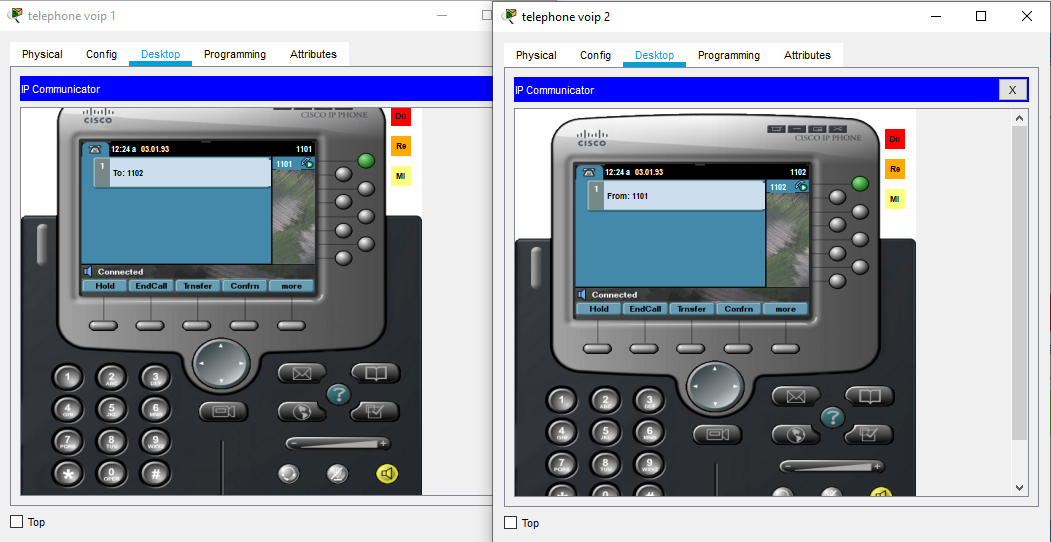
La configuration de leurs adresses IP, les masques et les passerelles serons faite de façons automatique grâce au serveur DHCP fourni par le routeur. Exemple **:** Laptop0 appartenant au service informatique de la Direction administrative

* 1. **configuration des téléphones VoIP**
     + 1. **implémentation de la téléphonie sur packet tracer**
* Le téléphone VoIP 1 possède le numéro 1101 et le téléphone VoIP possède le 1102



* Je lance un appel du téléphone voip 1 vers le 2 et on constate que les deux son connecter, la lumière verte situer à droite des deux téléphones nous le démontre



* + - 1. **De façon réel: installation de 3CX Phone System**

(Voir fichier installation 3cx phone system 16)

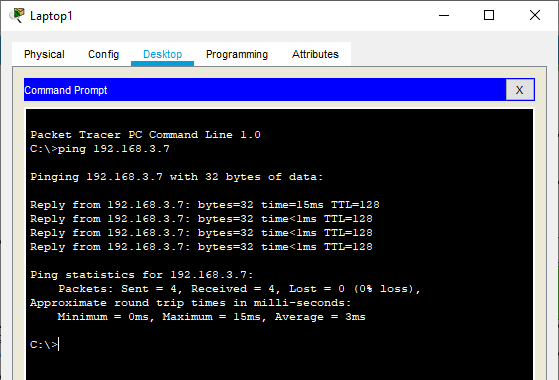
**CHAPITRE III : TEST ET VALIDATION DE CONFIGURATION**

On test dans cette partie les communications entre tous les équipements en utilisant la commande Ping. Ces tests sont faits entre équipements, inter-Vlan, entre Vlan et entre le site centrale.

Il est à noter que la commande Ping est très utile pour tester la réponse d'un ordinateur sur un réseau. Cette commande envoie des paquets avec le protocole ICMP.

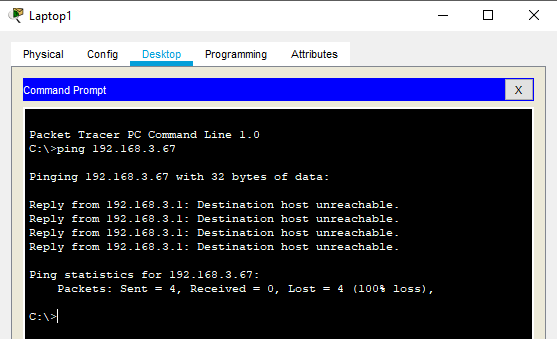
1. **test inter-vlan**

Exemple : Tests réussis entre le laptop1 de l’informatique (192.168.3.4) et le responsable administrative (192.168.3.7) qui appartienne au même Vlan10.



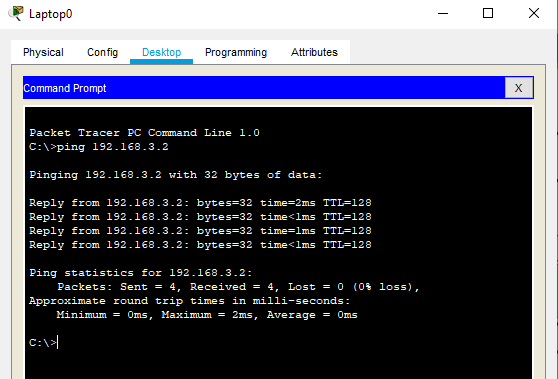
1. **test entre vlan**

Exemple : Test échoué entre laptop1 (Vlan 10) et gestion des commandes 1 (Vlan 20) qui n’appartienne pas au même Vlan

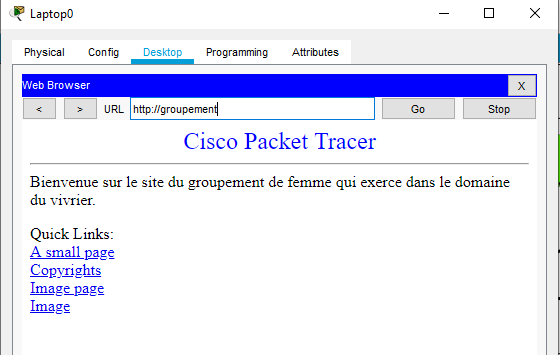


1. **Test entre un ordinateur et le serveur**

Exemple : Test réussi entre le laptop0 informatique et le serveur (192.168.3.2)



Test du site en ligne



**CHAPITRE IV : CRITIQUES ET OBSERVATIONS**

* + - 1. **CRITIQUES**

Malgré les avantages de l'informatisation (**accélération dans le traitement des informations, traitement à distance, le partages des ressources**, etc.) nous constatons en Côte d'Ivoire un grand retard au niveau des administrations étatiques.

Ce stage a représenté pour nous une belle transition entre le système étudiant et le monde de l’entreprise. En effet, durant ces trois mois, on eu l’opportunité d’appliquer des connaissances déjà acquises et d’en développer de nouvelles, et de prouver qu’on pouvait être capable de s’adapter, d’apprendre, d’exécuter, et de faire preuve de créativité dans notre travail.

Ce stage nous a permis d’acquérir et développer nos compétences comme la méthodologie, l’organisation dans notre travail, mais aussi des qualités relationnelle comme l’écoute, faire preuve d’empathie et toujours adapter nos discours par rapport aux autres membres du groupe.

* + - 1. **OBSERVATIONS**

Il faut que nos administrations soient informatisé pour accélérer les procédures de traitements d'informations et mettre en réseau les différents services ce qui ne sera pas sans avantage pour notre administration dans sa globalité.

L'utilisation de connexion Internet permettra à nos différentes administrations de se faire connaître à l'extérieur et pourquoi pas entreprendre des partenariats à certains niveaux pour rester dans l'esprit de la mondialisation.

Notre perspective consiste à intégrer un système de contrôle d’accès tels que le système 3A (Authentification, Autorisation, Audit).

Ceci permet d’offrir une solution de sécurité indépendante des plates-formes matérielles et plus robuste aux violations de droit dans la mesure où elle autorise un accès restreint à certains systèmes ou à certaines applications spécifiques.

Maintenir le système en fonctionnement ;

Rectifier les anomalies de fonctionnement et prendre en compte les demandes d'évolution ;

Établir un scénario de développement des versions ;

Planifier les corrections apportées au système pour minimiser les coûts d'intervention ;

S’assurer du bon fonctionnement des nouvelles révisions avant tout nouvelle mise en exploitation ;

Procéder à cette mise en exploitation après l'accord des parties prenantes ;

Assurer une bonne gestion de différentes configurations du logiciel par la tenue à jour de la documentation du système.

**CONCLUSION GENERALE**

Au terme de ce projet, nous avons pu exploiter nos connaissances théoriques et pratiques pour améliorer le système informatique du groupement des femmes du vivrier de Côte d’Ivoire. Ainsi, après la présentation de cette structure et de l’étude de son système informatique, nous avons présenté les composants informatiques qui peuvent intervenir dans la mise en œuvre d’une infrastructure de réseau informatique. Nous avons choisi les mieux adaptés aux besoins de l’entreprise et une étude minutieuse nous a permis de nous approprié le meilleur choix pour la mise en œuvre de notre solution.

La sécurité étant au centre du réseau informatique, nous avons adopté une politique de sécurité après avoir présenté les critères qui ont motivé ce choix.

La mise en œuvre de notre solution n’a pas été facile du point de vu conception car il fallait implémenter toute la solution dans le simulateur Cisco Packet Tracer ce qui nous imposait d’aller au-delà des connaissances acquises lors de notre formation et de valoriser le concept ingénieux que développe cette formation.

L’intérêt principal que nous avons tiré de ce projet est qu’il nous a permis d’améliorer nos connaissances, d’évaluer les différentes étapes de réalisation d’un projet et la bonne réalisation des travaux en se limitant aux ressources et à des durées de temps exactes. Nous avons pu voir la complexité de proposer un projet réalisable et avons appris à mieux nous organiser afin d’être capable de finaliser un travail.

Le travail que nous avons réalisé peut être amélioré, en utilisant d’autres simulateurs avec lesquels l’on a la possibilité d’implémenter des serveurs et des services

**ABREVIATIONS**

**AD:** Active Directory

**IP:** Internet Protocol

**DMZ:** Demilitarized Zone

**DNS:** Domain Name System

**DHCP:** Dynamic Host Configuration Protocol

**HTTP:** Hyper Text Transfer Protocol

**SQL:** Structured Query Language  
**RADIUS:** Remote Authentication Dial-In User Service

**VoIP:** Voice over Internet Protocol

**RAM:** Random Access Memory

**PC:** Personnel Computer

**BSD:** Berkeley Software Distribution

**CPU:** Central Processing Unit

**LAN:** Local Area Network

**VLAN:** Vitual Local Area Network

**PoE:** Power over Ethernet

**SSH:** Secure Shell

**IAX:** Inter-Asterisk eXchange

**SIP:** Session Initiation Protocol

**IPBX:** Internet Protocol Private Branch eXchange

**PABX:** Private Automatic Branch eXchange

**AES:** Advanced Encryption Standard

**WAP:** Wireless Application Protocol

**WIFI:** Wireless Fidelity

**UPS:** Uninterruptible Power Supply

**UTP:** Unshielded Twisted Pairs

**FTP:** Foiled Twisted Pairs

**STP:** Shielded Twisted Pairs

**SFTP:** Shielded Foiled Twisted Pairs

**SSTP:** Shielded Shielded Twisted Pairs

**BIBLIOGRAPHIE**

* *Les réseaux* *édition 2008* GUY PUJOLLE EYROLLES
* *Tout sur les réseaux sans fils* FABRICE LEMAINQUE, dunod
* *Mémoire de fin de cycle* en Réseaux et Maintenance Informatiques –ESIIUPB, DABRE Met ZOUGMORE G, mai 2010
* *Cours sur les réseaux informatique, les équipements d’interconnexions*, MOINDJIE Said Mouhamed
* Cour CISCO CCNA1, les périphériques finaux, Médias réseau. Netacad
* *Tous sur la sécurité informatique,* PILLOU Jean-François BAY Jean Philippe, dunod, 2005
* *Sécurité des réseaux et systèmes repartis.* Lavoisier, février 2002, DESWARTE Ludovic

**WEBOGRAPHIE**

* <https://fr.wikipedia.org/wiki/Gestion_libre_de_parc_informatique>
* <https://www.ordinateur.ooreka.fr>
* <https://www.openclassroom.com>
* <https://www.netcad.com>
* <https://www.vmware.com/fr/products/esxi-and-esx.html>
* [https://asteriskmx.org/asterisk-vs-elastix-vs-trixbox-vs-asterisknow-vs-freepbx-explicando-la diferencia/](https://asteriskmx.org/asterisk-vs-elastix-vs-trixbox-vs-asterisknow-vs-freepbx-explicando-la%20diferencia/)
* <https://www.callforwarding.com/blog/best-voip-softphone-iphone-users/>
* <https://www.3cx.costumer.com>
* <http://www.memoireonline.com/>
* <http://www.ifi.auf.org/rapports/tpe-promo14/tpe-ewelle-richard.pdf>
* <https://www.cisco.com/c/fr_ca/solutions/enterprise-networks/product-listing.html>
* <https://www.pc2s.fr/pfsense-installation-et-configuration/>
* <https://www.mismo.fr/materiels-informatiques/equipement-informatique-de-votre-entreprise/equipement/>
* <https://www.universalis.fr/encyclopedie/reseaux-informatiques/6-securite-dans-les-reseaux/>
* <https://www.epi.asso.fr/revue/97/b97p181.htm>