République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire de Fin d'Etudes

de MASTER ACADEMIQUE

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

Spécialité : **Réseaux, Mobilité et Systèmes Embarqués**

Présenté par

Mina CHABANE

Saadia KAROUI

Thème

Conception et Implémentation d'une Architecture Réseau par la fibre Optique

Mémoire soutenu publiquement le 29/09/ 2016 devant le jury composé de :

Président : Mr DJAMAH
Encadreur : Mme DJAMAH
Co-Encadreur: Mr HADOUS
Examinatrice : Mme SEDOUD
Examinateur : Mr SADOU

Promotion : 2015/2016

REMERCIEMENTS

Louange au dieu, seigneur de l'univers, de nos avoir donné la force, la patience et la volonté d'accomplir ce travail.

Je tiens à exprimer mes sincères remerciements à Mme DJAMEH, ma promotrice. Et aussi Mr DJAMEH pour m'avoir encadré et guidé tout au long de ce projet, pour ses critiques, la pertinence de ses remarques et ses conseils toujours opportuns.

Aussi je remercie Mr HADOUS Abdnour, notre Co-encadreur et a tout le personnel de laboratoire des équipements de télécommunication.

J'adresse mes remerciements les plus vifs aux membres du jury, pour avoir accepté de juger notre travail.

Mes sincères sentiments vont à tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce projet.

Dédicaces

Je dédie ce modeste travail :
A ma très chère mère

Affable, honorable, aimable : Tu représentes pour moi le symbole de la bonté par excellence, la source de tendresse et l'exemple du dévouement qui n'a pas cessé de m'encourager et de prier pour moi.

Aucune dédicace ne saurait être assez pour exprimer ce que tu mérites pour tous les sacrifices que tu n'as cessé de me donner depuis ma naissance, durant mon enfance et même à l'âge adulte.

A mon très cher père

Qu'Allah le garde en bonne santé, celui qui m'a toujours appris comment réfléchir avant d'agir, celui qui m'a soutenu tout au long de ma vie scolaire, celui qui n'a jamais épargné un effort pour mon bien.

A ma grand mère et grand père que dieu les protège et les garde en bonne santé.

A mes frères Reda et Hamza. A ma sœur Rekia.

A mes cousines spécialement Terkia et Aziza. A toutes mes tantes.

A ma cousine Nacira et sa famille.

A toute la famille sans exception.

A toutes mes amies qui mon soutenu jusqu'à la fin de cette expérience.

A tous ceux qui m'aiment et que j'aime.

Mina. C

Dédicaces

Je dédie ce modeste travail :

A mes chers parents.

A mes Frères et Sœurs.

A mon mari et sa famille.

A tout mes amis et Mes Collègues.

A monsieur HADOUS

A tous ceux qui m'aiment et que j'aime.

Saadia.k

Listes des Figures

Listes des Figures

Listes des Figures

Liste des tableaux

Sommaire

Sommaire

Sommaire

Chapitre III : Généralités sur la fibre optique

Chapitre IV : Généralités sur la sécurité

Chapitre V : La conception et la réalisation de la liaison fibre optique

Sommaire

Chapitre VI : L a conception et la réalisation de l'architecture réseau

Toute entreprise existante d'une certaine taille dispose en général d'un réseau informatique, même celles qui n'en sont qu'à une idée de projet viable y pense très souvent à une éventuelle mise en œuvre d'un réseau informatique au sein de leur future structure. Vu l'importance des informations qui sont souvent véhiculées dans les réseaux, ceux-ci requièrent un certain degré de sécurité. Toutefois le constat est que ceux qui en font usage de ces réseaux ignorent parfois les risques auxquelles ils sont exposés lorsqu'une mesure de sécurité n'est mise en place. Les réseaux les plus sécurisés disposent très souvent d'un outillage tant matériel que logiciel à fin de s'assurer une sécurité optimale. Pour certaines entreprises, vu les moyens dont ils disposent, ils ne peuvent se prémunir d'une telle accumulation.

Pour cela, de nombreuses techniques de sécurisation sont mises en place, citons-en :

- Les pare-feu pour le filtrage des paquets ;
- L'Annuaire « Active Directory » pour la gestion des utilisateurs ;
- La politique de groupe « GPO » ;
- La Zone Démilitarisée « DMZ » ;
- Les VPNs ;

Les systèmes numériques les plus rapides transmettaient l'information à un débit de 10 Mbits/s, le câble coaxial était parfaitement adapté à même de remplir son rôle de support de transmission. Mais avec l'apparition des nouveaux services liés au développement du multimédia, un besoin d'un débit de transmission d'informations plus élevé, et une alternative au câble coaxial sont apparus à cause des pertes trop élevées, des courtes distances de propagation, et des performances limitées. La fibre optique remplit très bien ce nouveau rôle de support de transmission. Son utilisation est désormais courante dans les réseaux de télécommunications.

Six chapitres sont consacrés à ce modeste travail :

Après l'introduction générale

Chapitre 1 : L'organisme d'accueil de l'entreprise

Chapitres 2 : Généralités sur les réseaux

Chapitre 3 : Généralités sur la fibre optique (décrit la transmission par fibre optique, ainsi que les diverses techniques de l'utilisation).

Chapitre 4 : Problématique de la sécurité (dont nous avons décrit quelques définitions et mécanismes de sécurités et quelques attaques et vers la fin nous avons présenté des mesures de protection.

Chapitre 5 : Conception et Réalisation de la sécurité réseaux (dans ce chapitre nous avons décrit l'architecture du réseau actuelle de notre organisme d'accueil et d'autre entreprises clients qu'on a pris comme exemple pour l'étude et nous avons pu ressortir les critiques à corriger, par la suite nous avons cités et définit les outils utilisés pour la réalisation de notre projet.).

Chapitre 6 : Conception et Installation du réseau fibre optique (détaille la conception du réseau et l'infrastructure utilisée et l'évaluation globale de projet).

En fin on termine notre travail avec une conclusion générale.

I. Introduction

Dans ce chapitre nous proposons une vue globale sur l'entreprise (Algérie Télécom) .Sa naissance, son objectif, sa structure, et une présentation générale du champ d'étude.

II. Présentation de l'entreprise

1- Historique

Régie par la loi 2000/03 du 5 aout 2000 .Algérie Télécom est née pour relever le défi de l'ouverture du marché des télécommunications annoncées dans les réformes engagées par le pays .Algérie Télécom jouit d'un statut d'entreprise publique économique. Ce statut établie la forme juridique d'une société par action SPA. Compte tenu du rôle que jouent les télécommunications dans le développement économique, social, cultuel et adéquation avec les objectifs assignés pour remplir les retards marqué dans ce domaine.

Algérie Télécom a inscrit des actions multiples et qu'elle doit réaliser avec succès.

Pour répondre aux besoins de sa clientèle et assurer une présentation des services et la qualité.

Le challenge d'Algérie Télécom en sa qualité d'opérateur historique est d'être leader dans don domaine et nourrir des ambitions de devenir un business partenaire incontournable à l'échelle régional.

Algérie Télécom a arrêté un programme de développement qui se décline dans :

- L'introduction de nouvelles technologies en matière de communication.
- L'introduction de nouvelles technologies à faveur des accès hauts débits.
- L'implantation d'un réseau multiservices large bande.
- La généralisation de la transmission numérique sur support optiques avec la réalisation de backbone nationales et internationale par la construction de nouveaux supports dans la technologie WDM.
- L'implantation de système de gestion et de supervision des réseaux.
- L'introduction de nouvelles techniques de gestion et acquisition d'outils d'exploitation commerciale et d'analyse quantitative et qualitative.
- La prise d'une grande part de marché du téléphone mobile.

Algérie Télécom se propose de construire des relations d'affaires à long terme avec les opérateurs économiques intéressés par le secteur des télécommunications et des technologies de l'information et de la communication.

2- Missions d'Algérie Télécom

L'activité majeure d'Algérie Télécom est de :

- Fournir des services de télécommunication permettant le transport et l'échange de la voix, de message écrit, de données numériques, d'informations audiovisuelles… etc
- Développer, exploiter er gérer les réseaux publics et privés des télécommunications.

Etablir, exploiter et gérer les interconnexions avec les opérateurs des réseaux.

3- Objectifs d'Algérie Télécom

Algérie Télécom est engagée dans le monde des technologies de l'information et de la communication avec les objectifs suivants :

- Accroitre l'offre de service téléphonique et faciliter l'accès aux services de télécommunications au plus grand nombre d'usagers, en particulier en zones rurales.
- Accroitre la qualité des services offerts et la gamme se prestation rendue et rendre plus compétitif les services de télécommunications.
- Développer un réseau national de télécommunication fiable et connecter aux autoroutes de l'information.

4- Organisation d'Algérie Télécom

Algérie Télécom est organisée en Directions Centrales, Régionales et Directions Opérationnelles de Wilaya auteur de ses métiers fixes et services, et d'autre part des fonctions supports réseaux. A cette structure s'ajoutent trois filiales spécialisées et de dimension nationales.

- La filiale de téléphonie mobile <<Algérie Télécom mobile : MOBILIS>>
- La filiale des télécommunications par satellite<< Algérie Télécom satellite : ATS>>
- La filiale des services Internet << Algérie Télécom Internet DJAWEB : ATI>>

Algérie Télécom s'implique dans le développement socio-économique du pays à travers la fourniture des services de télécommunication.

En autre, Algérie Télécom met en œuvre des moyens importants pour rattacher les localités isolées.

5- Organigramme d'Algérie Télécom

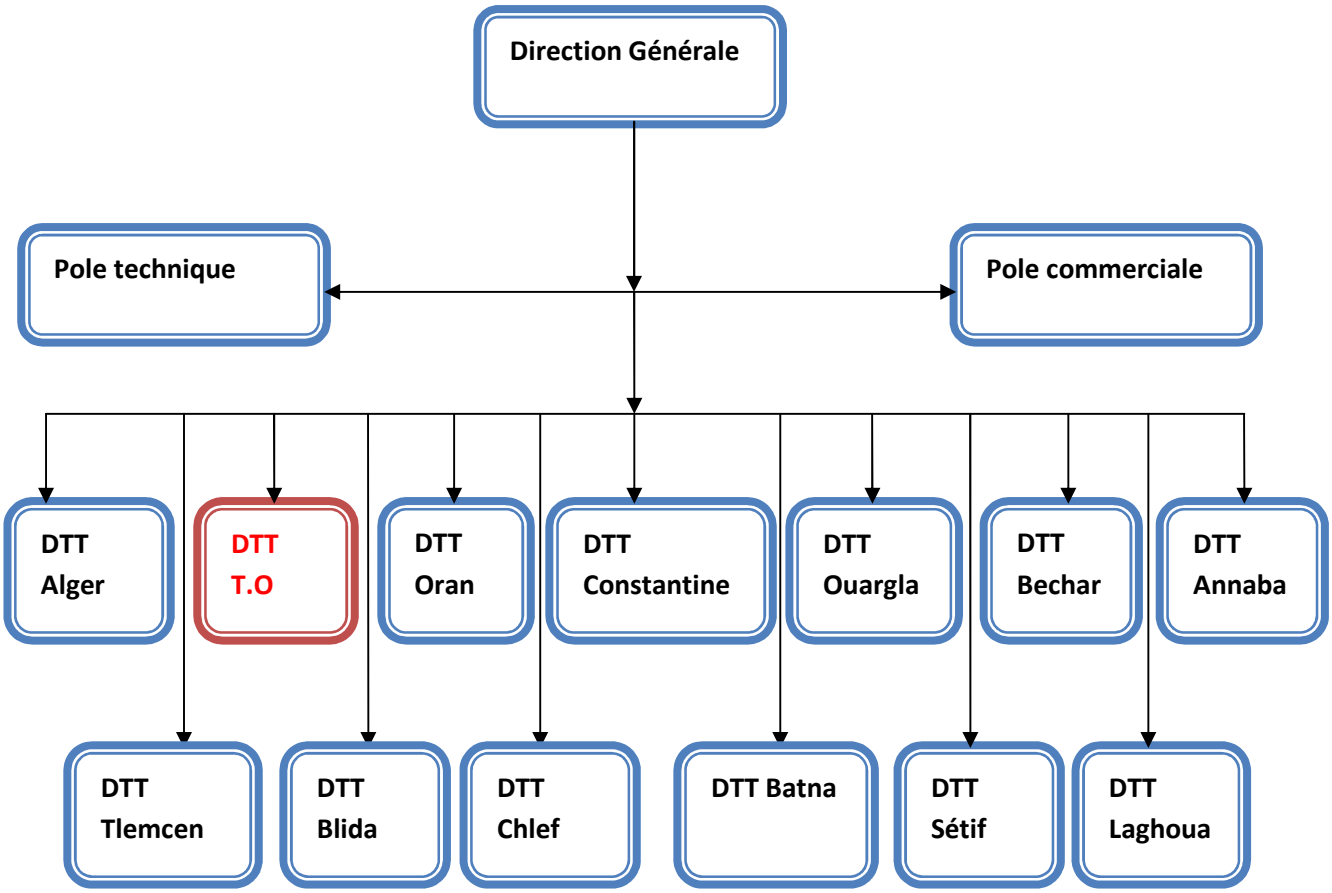


Figure 1.1 : Organisme d'Algérie Télécom

Après avoir donné une présentation globale d'Algérie Télécom, on s'intéresse maintenant à la direction Territoriale des Télécommunications (DTT) de Tizi-Ouzou.

III. Présentation de la Direction Territoriale de Télécommunications (DTT) de Tizi-Ouzou

Cette direction se divise en plusieurs sous directions, qui travaillent en collaboration pour accomplir un certain nombre d'objectifs et de missions d'Algérie Télécom.

Notre lieu d'accès se situ à la sous direction des réseaux d'entreprise ou se trouve notre champ d'étude.

1- Organisme de la direction Territorial des Télécommunications de Tizi-Ouzou

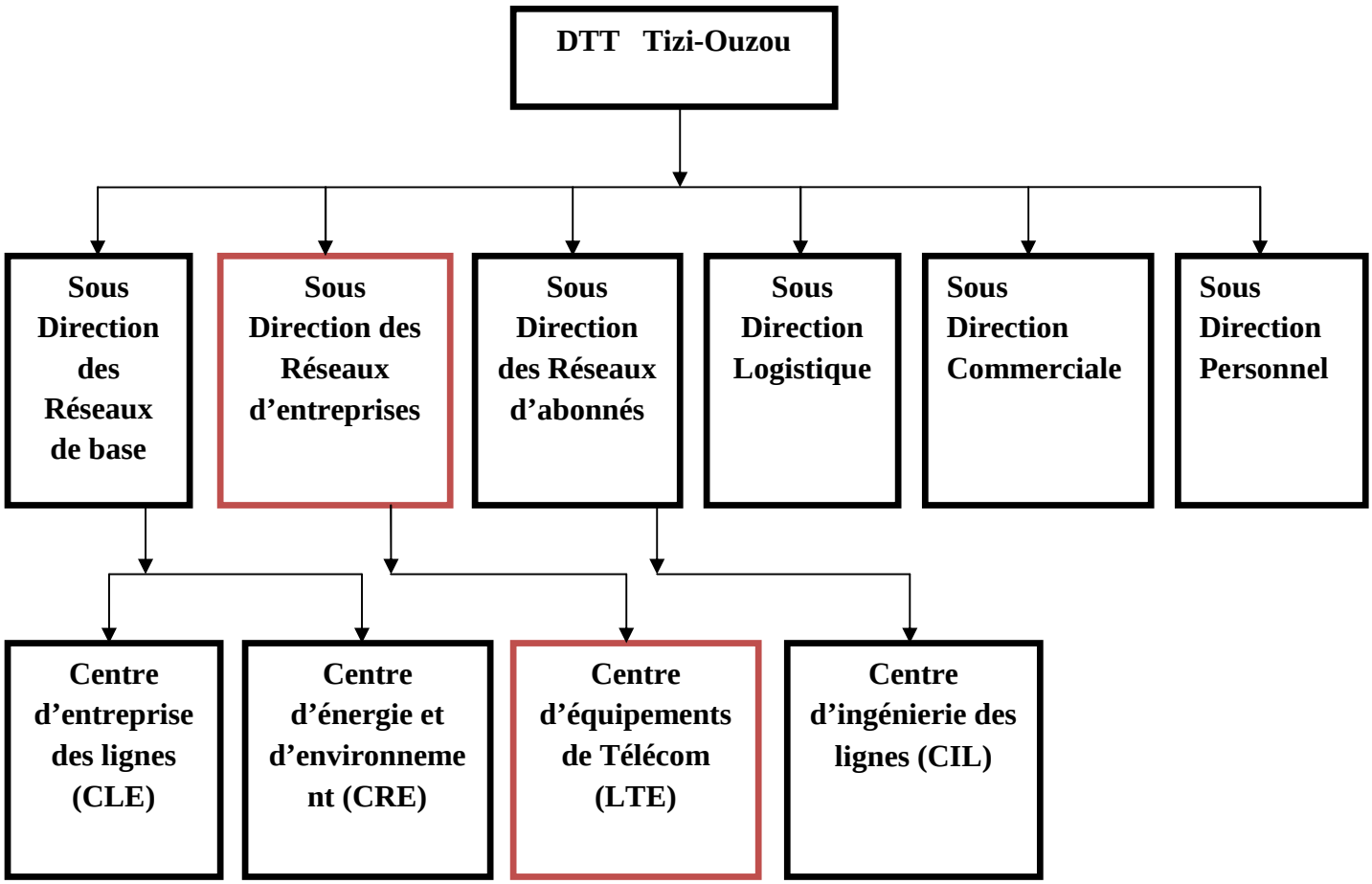


Figure 1.2 : Organigramme de la Direction Territoriale des Télécommunications

2- Description de champ d'étude

Le laboratoire des Equipements des Télécommunications (LET), suit la sous direction des réseaux d'entreprise.

Ce laboratoire régional est crée en 2009, pour répondre aux besoins des clients d'Algérie Télécom en matière de création de maintenance des réseaux d'entreprise.

Il se compose d'un chef de centre et d'une équipe d'ingénierie et de techniciens

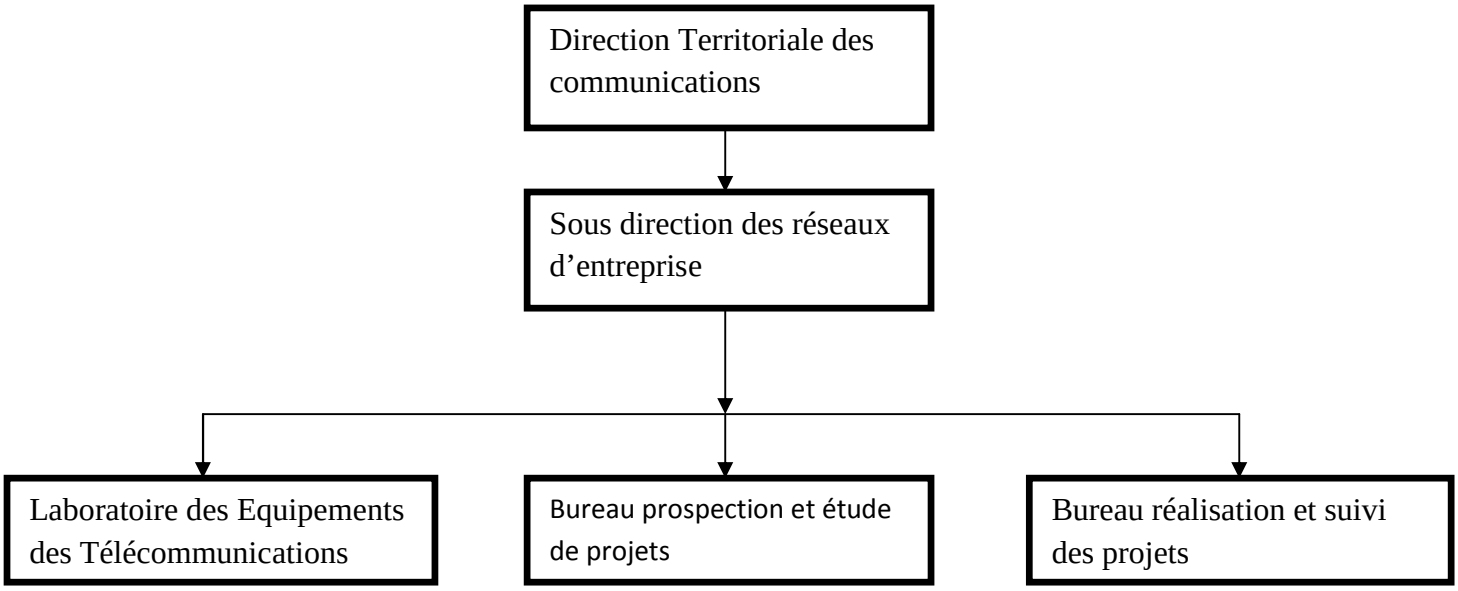


Figure 1.3 : Organigramme de champ d'étude

3- Rôle de champ d'étude

Ce laboratoire est chargé d'intervenir sur les trois wilayas : Tizi-Ouzou, Boumerdes et Bouira, pour effectuer les taches suivantes :

- Prise en charge des pannes signalées par les clients (NAFTAL, CASNOS, Banque CPA ….)
- Préparation et maintenance des équipements informatiques, bureautiques et télécommunications d'entreprises Algérie Télécom (ACTEL).

IV. Conclusion :

Dans ce chapitre nous avons tenu à donner un petit aperçu sur l'histoire de l'organisme d'accueil ainsi qu'une brève présentation de ses directions Territoriales des Télécommunications en précisant celles concernées par notre champ d'étude.

I. Introduction

Depuis les premières inventions des systèmes mécaniques jusqu'à nos jours, on a remarqué qu'à chaque époque, sa technologie dominante. Actuellement, la technologie réseaux et les domaines qu'elle inclut prennent le monopole. Aujourd'hui, les réseaux sont tellement répandus qu'ils touchent tous les aspects de notre vie quotidienne : télécommunication, commerce, banque, travail.

Les réseaux sont nés d'un besoin d'échanger des informations de manière simple et rapide entre des machines. Lorsque l'on travaillait sur une même machine, toutes les informations nécessaires au travail étaient centralisées sur cette machine. Pour des raisons de coûts ou de performances, on est venu à multiplier le nombre de machines. Les informations devaient alors être dupliquées sur les différentes machines du même site. Cette duplication était plus ou moins facile et ne permettait pas toujours d'avoir des informations cohérentes. On est donc arrivé à relier d'abord ces machines entre elles, Ce fût l'apparition des réseaux locaux. Ces réseaux étaient souvent des réseaux propriétaires. Plus tard on a éprouvé le besoin d'échanger des informations entre des sites distants. Les réseaux moyenne et longue distance commencèrent à voir le jour. Aujourd'hui, les réseaux se retrouvent à l'échelle planétaire. Le besoin d'échanger de l'information est en pleine évolution.

Dans ce chapitre, nous allons aborder la notion de réseau et son intérêt, en général, puis, en particulier, présenter l'Internet, l'Intranet et leurs services, ainsi que l'extranet.

II. Les réseaux Informatiques

1. Définition

C'est un ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques (valeurs binaires, c'est-à-dire codées sous forme de signaux pouvant prendre deux valeurs : 0 et 1). Matériellement, un réseau comprend des équipements de raccordements, pouvant être externes ou internes (carte réseau par exemple). Ces équipements sont connectés entre eux par des supports de transmission. Dans le cas ou le réseau est composé de câble et d'équipements, on parle de réseau filaire, et dans le cas où l'échange des informations se fait par l'intermédiaire des ondes, on parle de réseau sans fil. Un réseau à pour but d'offrir un certain nombre de service à ses utilisateurs, basés sur l'échange d'informations (accès à distance).

2. Intérêt de réseau :

- Le partage des fichiers et des périphériques, imprimantes et applications, donc diminution des coûts grâce aux partages des données et des ressources.
- La communication entre personnes grâce au courrier électronique, vidéoconférence.
- La communication entre processus (ordinateurs et automates industrielles).
- La garantie de l'unicité de l'information (bases de données).
- Standardisation des applications.
- Accès aux données en temps utile.
- Communication et organisation plus efficace.

3. Classification des réseaux :

a. Les différents types de réseaux

En générale, on distingue différents types de réseaux selon leur étendue.

- **Les LAN**

LAN signifie Local Area Network (en français Réseau Local). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (pour un réseau Ethernet par exemple) et 1 Gbps (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs et couvrir un bâtiment où une cité d'entreprise.

En élargissant le contexte de la définition aux services qu'apporte le réseau local, il est possible de distinguer deux modes de fonctionnement :

* dans un environnement d'"égal à égal" (en anglais peer to peer), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur à un rôle similaire
* dans un environnement "client/serveur", dans lequel un ordinateur central fournit des services réseau aux utilisateurs.

- **Les MAN**

Les MAN (Métropolitain Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local.

Un MAN est formée de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

- **Les WAN**

Un WAN (Wide Area Network ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau.

Le plus connu des WAN est Internet.

b. LES TOPOLOGIES DU RESEAUX

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à du matériel (câblage, cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique de ces éléments est appelé topologie physique. Son choix s'appuie essentiellement sur :

- ✓ Le bilan des équipements informatiques existants.
- ✓ La disposition géographique des équipements et des locaux.
- ✓ L'analyse des besoins immédiats et futurs.
- ✓ Les couts d'investissement.

On distingue la topologie physique (la configuration spatiale, visible, du réseau) de la topologie logique. La topologie logique représente la façon selon laquelle les données transitent dans les câbles. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI.

Chaque topologie représente des avantages et des inconvénients, en termes de fiabilité, de cout et de complexité. Dans cette section, nous allons présentés, quelques topologies des réseaux locaux qui sont :

- **Topologie en bus**

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau.

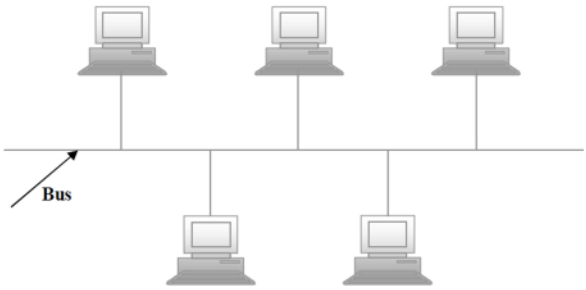


Figure 2.1 : Topologie en bus

Cette topologie a pour avantages d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si le bus est défectueuse, c'est l'ensemble du réseau qui est affecté.

- **Topologie en étoile**

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé hub ou concentrateur. Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles on peut connecter les câbles en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

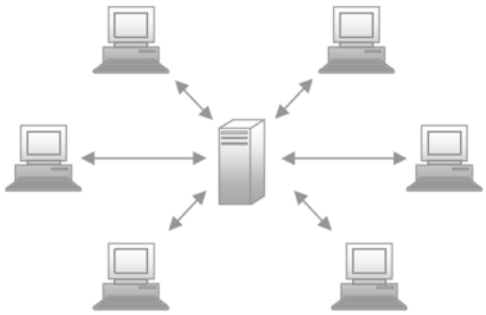


Figure 2.2 : Topologie en étoile

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car on peut aisément retirer une des connexions en la débranchant du concentrateur sans pour autant paralyser le reste du réseau. En revanche un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub).

- **Topologie en anneau**

C'est une topologie constituée d'un ensemble de dispositifs connectés par un lien de transmission unidirectionnelle et formant une boucle fermée, les ordinateurs communiquent chacun à leur tour, on a donc une boucle d'ordinateurs sur laquelle chacun d'entre eux va "avoir la parole" successivement.
Il y a principalement deux technologies utilisant ce système: le Token Ring d'IBM et le FDDI (Fiber Distributed Data Interface).

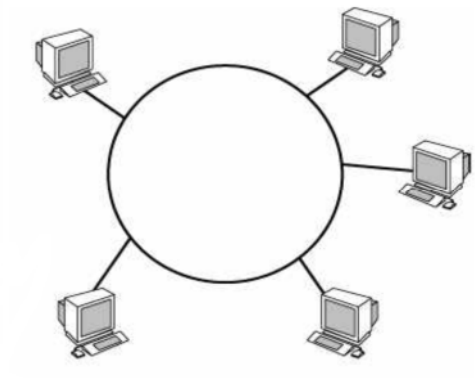


Figure 2.3 :Topologie en anneau

Avantages: un nœud peut tomber en panne sans affecter les autres nœuds du réseau.

Inconvénient: la panne d'une station rend l'ensemble du réseau inutilisable.

- **Topologie en arbre :**

Est un réseau hiérarchique reparti sur plusieurs niveaux, les nœuds d'un même niveau n'ont pas de lien entre eux mais sont reliés à un niveau supérieur. Le réseau téléphonique estun exemple caractéristique de ce type de réseau**.**

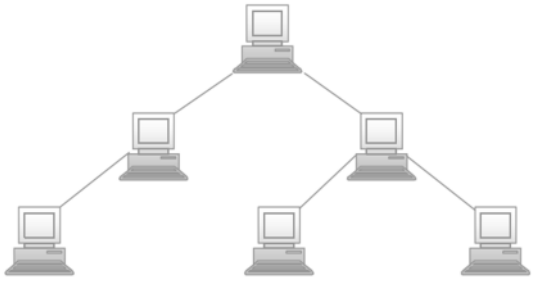


Figure 2.4 : Topologie en arbre

III. Le Modèle OSI

1. Concept et norme modèle OSI

La première évolution des réseaux informatiques a été des plus anarchiques, chaque constructeur développant sa propre technologie. Le résultat fut une quasi-impossibilité de connecter différents réseaux entre eux. Pour palier à ce problème d'interconnections, l'ISO (International Standards Organisation) décida démettre en place un modèle de référence théorique décrivant le fonctionnement des communications réseaux. Ainsi fût créé le modèle OSI, à partir des structures réseau prédominantes de l'époque : DECNet (Digital Equipment Corporations Networking développé par digital) et SNA (System Network Architecture développé par IBM).Ce modèle a permis aux différents constructeurs de concevoir des réseaux interconnectables.

2. Définition du modèle OSI

Le modèle OSI (Open Systems Interconnexion) d'interconnexion des systèmes ouverts décrit un ensemble de spécifications pour une architecture réseau permettant la connexion d'équipements hétérogènes. Le modèle OSI normalise la manière dont les matériels et les logiciels coopèrent pour assurer la communication réseau.

3. Description

Selon une publication éditée par l'ISO, un réseau est organisé en sept couches, chacune d'elle est responsable d'une action ou service permettant de préparer les informations en vue de leur transmission sur les réseaux. La figure suivante reprisant le modèle OSI proposé par l'ISO.

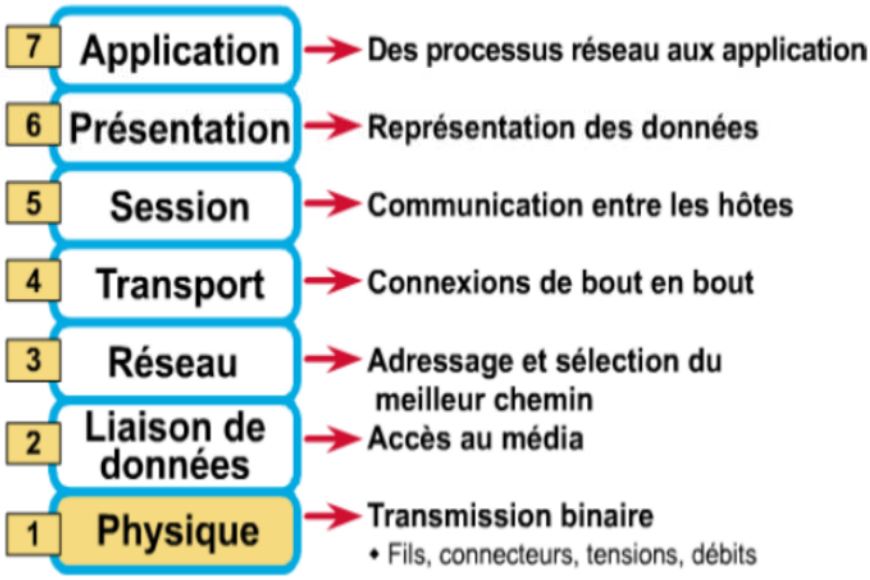


Figure 2.5 : les différentes couches du modèle OSI

4. Définition des couches du modèle OSI :

- **Couche application :**

Elle offre des services de communication à l'utilisateur du réseau, c'est elle qui rend possible des fonctions de réseau telles que : l'accès aux fichiers, aux imprimantes, l'échange de courrier électronique et partage des ressources, c est l'interface utilisateur-machine.

- **Couche présentation :**

La tache principale de cette couche consiste à mettre en forme les données dans un format standard, tel que les deux éléments qui vont dialogué se comprennent. Cette couche joue un rôle important dans un environnement hétérogène d'ordinateurs, on peut la considérer comme le traducteur du réseau.

- **Couche session :**

Elle est chargée d'établir la communication entre deux parties. Pour le faire, la couche session s'assure que l'utilisateur distant est bien présent, puis établit la connexion, si nécessaire elle prend des mesures de sécurité, telle que la validation des mots de passe.

Une fois la connexion établie, la couche session garantit que le dialogue se déroule correctement. Enfin, elle garantit que la session s'achève convenablement.

- **Couche transport :**

La fonction de base de la couche transport, est de recevoir les données de la couche session, de les découper si nécessaire en plus petites unités appelées paquets, de les passer à la couche réseau et d'assures que tous les paquets arrivent correctement.

- **Couche réseau :**

La couche réseau est chargée de l'adressage du réseau et d'indiquer aux paquets les directions à suivre pour aller de la source vers la destination.

- **Couche liaison de données :**

La couche liaison de données communique à la fois avec la couche physique située au dessous d'elle et avec la couche réseau directement au dessus d'elle. Les tâches accomplies par cette couche sont :

L'organisation des paquets de données en trames car un paquet n'est pas une entité transportable sur un support de transmission. Une trame est l'entité transportée sur le support de transmission, on dit qu'une trame est un paquet dont on peut reconnaitre le début et la fin.

Une autre fonction de cette couche est la détection d'erreurs de transmission.

- **Couche physique :**

Elle est responsable de la manipulation des détails électriques de la transmission physique d'un flot de bits sur le canal de communication.

5. Terminologie liée au modèle OSI

- **Encapsulation**

✓ Au sein d'un réseau, toutes les communications partent d'une source, et sont acheminées vers une destination. Les informations envoyées sur le réseau sont appelées données ou paquets de données. Si un ordinateur (hôte A) veut envoyer des données à un autre ordinateur (hôte B), les données doivent d'abord être préparées grâce à un processus appelé encapsulation.

✓ Ce processus conditionne les données en leur ajoutant des informations relatives au protocole avant de les transmettre sur le réseau. Ainsi, en descendant dans les couches du modèle OSI, les données reçoivent des en-têtes, des en-queues et d'autres informations. (Remarque : Le terme << en-tête >> fait référence aux informations d'adresse.).

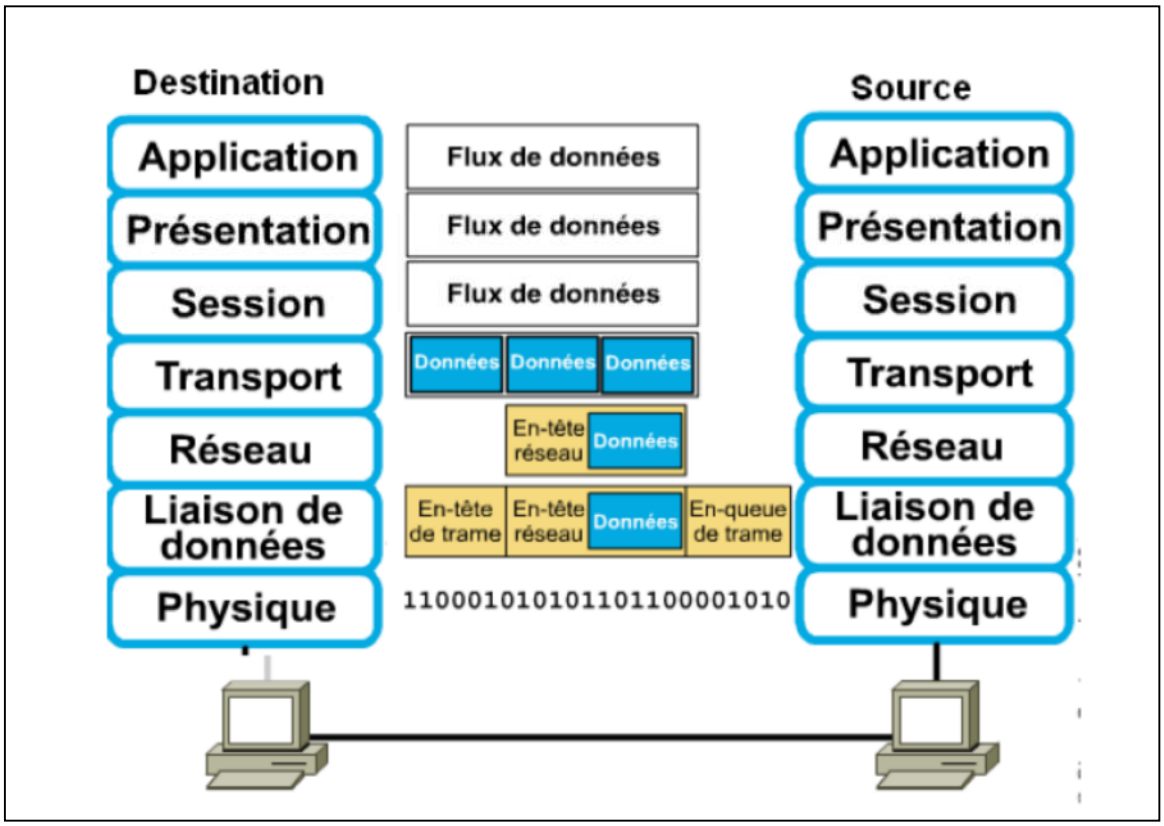


Figure 2.6 : Description générale de l'information dans le modèle OSI

- **Unité de donnée de service (SDU)**

Unité d'information d'un protocole de couche supérieure qui définit une demande de service à un protocole de couche inférieure, par exemple la couche réseau fournit un service à la couche transport, qui présente les données au sous-système de l'inter-réseau

- **Unité de donnée de protocole (PDU)**

Afin de permettre l'acheminement des paquets de données entre l'ordinateur source et l'ordinateur de destination, chaque couche du modèle OSI au niveau de l'ordinateur source doit communiquer avec sa couche homologue sur l'ordinateur de destination. Cette forme de communication est appelée communication d'égal à égal. Au cours de ce processus, le protocole de chaque couche assure l'échange d'informations, appelées unités de données de protocole (ou PDU), entre les couches homologues. Chaque couche de communication, sur l'ordinateur source, communique avec l'unité de données de protocole propre à une couche, ainsi qu'avec la couche correspondante sur l'ordinateur de destination.

- **Données**

Regroupement logique de données au niveau de la couche 7 (application), souvent composé d'un certain nombre de groupes logiques de couches inférieures, par exemple des paquets.

- **Data gramme ou message**

Regroupement logique de données envoyé comme unité de couche réseau par un média de transmission, sans établissement préalable d'un circuit virtuel. Les datagrammes IP sont les principales unités d'information sur Internet. Les termes, message, paquet et segment sont aussi utilisés pour décrire des regroupements logiques de données sur différentes couches du modèle.

- **Paquet**

Regroupement logique d'informations comportant un en-tête qui contient les données de contrôle et (habituellement) les données utilisateur. Le terme paquets est le plus souvent utilisé pour désigner les unités de données au niveau de la couche réseau.

- **Trame**

Regroupement logique de données envoyé comme unité de couche liaison de données par un média de transmission. Désigne souvent l'en-tête et la fin de trame, utilisés pour la synchronisation et le contrôle d'erreurs, qui entourent les données utilisateur contenues dans l'unité de données.

6. Transmission de données au travers le modèle OSI

La transmission de donnée à travers le modèle OSI utilise le principe de communication virtuelle en usant des interfaces inter-couches. Il y a donc encapsulation successive des données à chaque interface (H : Header, T : Trailer).

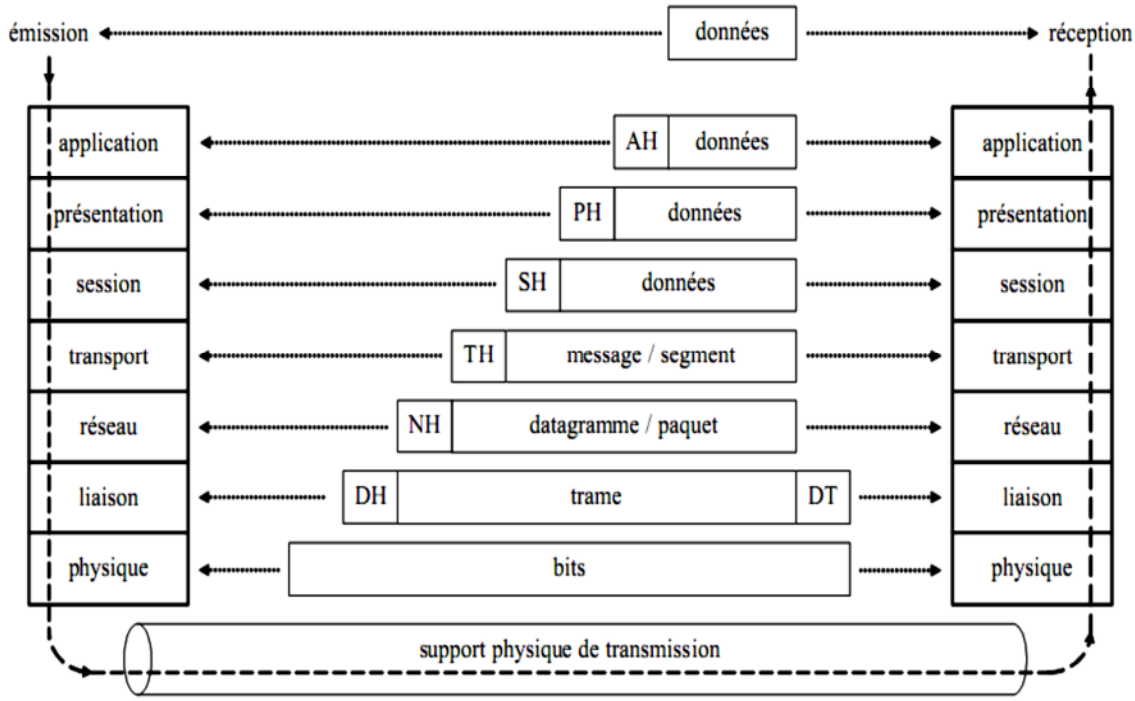


Figure 2.7: La transmission dans le modèle OSI

Il est important de noter que le modèle OSI, reste comme son nom l'indique, un Modèle, qui n'est pas scrupuleusement respecté, mais vers lequel on tente généralement de se rapprocher dans une optique de standardisation. De plus ce modèle a été historiquement établi après la mise en place de technologies ayant fait leur preuves, et il ne peut, de fais, pas toujours être rigoureusement suivi c est le cas du protocole TCP/IP.

IV. Les protocoles :

Pour échanger des données de manière structurée au sein d'un réseau, nous avons besoin des règles qui commandent le déroulement des communications.

Le protocole fondamentale du réseau est le modèle TCP /IP.

a. Le modèle TCP/IP

Le modèle TCP/IP a été développé par le DARPA (Defence Advanced Research Projet Agency) puis adopté par le DOD (Department Of Defense) aux États-Unis dans le milieu des années 70. Le modèle TCP/IP est constitué d'un ensemble de protocoles permettant à plusieurs ordinateurs de communiquer entre eux, que les ordinateurs soient locaux (réseaux locaux) ou distants (WAN). Il est intégration à Unix, par l'université de Berkeley au États-Unis. Aujourd'hui, TC/IP constitue le standard de fait dans les réseaux locaux et l'interconnexion de ceux-ci ?, il est notamment utilisé en standard pour les systèmes d'exploitation réseaux tel que Unix/LINUX, NetWare de Novell et Windows de Microsoft, ainsi qu'à l'échelle mondiale pour le réseau Internet.

➢ Que signifie TCP/IP ?

TCP/IP est une suite de protocoles. Le sigle TCP/IP signifie «Transmission Control Protocol/Internet Protocol». Il provient des noms des deux protocoles majeurs de la suite de protocoles, c'est-à-dire les protocoles TCP et IP).TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir Une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. Elle est conçue pour répondre à un certain nombre de critères parmi lesquels :

- Le fonctionnement des messages en paquet ;
- L'utilisation d'un système d'adresses ;
- L'acheminement des données sur le réseau (routage) ;
- Le contrôle des erreurs de transmission de données.

➢ Description du modèle TCP/IP :

Afin de pouvoir appliquer le modèle TCP/IP à n'importe quelles machines, c'est-à-dire indépendamment du système d'exploitation, le système de protocoles TCP/IP a été décomposé en plusieurs modules effectuant chacun une tâche précise.

De plus, ces modules effectuent ces tâches les uns après les autres dans un ordre précis, on a donc un système stratifié, c'est la raison pour laquelle on parle de modèle en couches.

Le modèle TCP/IP, reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre :

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

Tableau 2.1 : la correspondance entre le modèle OSI et le modèle TCP/IP

1. La couche application :

C'est à ce niveau que les applications accèdent au réseau, avec des protocoles tel que : FTP (File Transfer Protocol, protocole de transfert de fichier) qui fournit un moyen efficace de transfert de fichier d'un ordinateur à un ordinateur, SMTP (Simple Mail Transfer Protocol, protocole de transfert de courrier simple)utilisé pour le transfert des courriers électroniques, http (HyperText Transfer Protocol, protocole de transfert hypertexte) assure le transfert de page hyper texte entre un serveur Web et un client Web (navigateur Web).

2. La couche transport :

Elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission, définit deux protocoles différents :

TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).

b. Le protocole TCP :

Le protocole TCP a été développé pour assurer des communications fiables entre deux ordinateurs sur un même réseau, ou sur des réseaux différents. TCP établit une connexion entre l'émetteur et le récepteur avant de transférer les données (on parle dans ce cas de transfert en mode connecté), traite les données venant de la couche supérieure et les découpent en paquets TCP (appelé aussi segments TCP), qui seront communiqués à la couche inférieure, sous forme datagramme, pour être transmis à travers le réseau, retransmet les paquets lorsqu'il ne reçoit pas d'acquittement de réception de la part du destinataire (c'est la raison pour laquelle c'est un protocole fiable). A la réception, le protocole TCP s'assure du bon acheminement des paquets, en détectant d'éventuelles erreurs de transmission, et s'occupe également de contrôler le flux d'informations.

- ***Format du paquet TCP :***

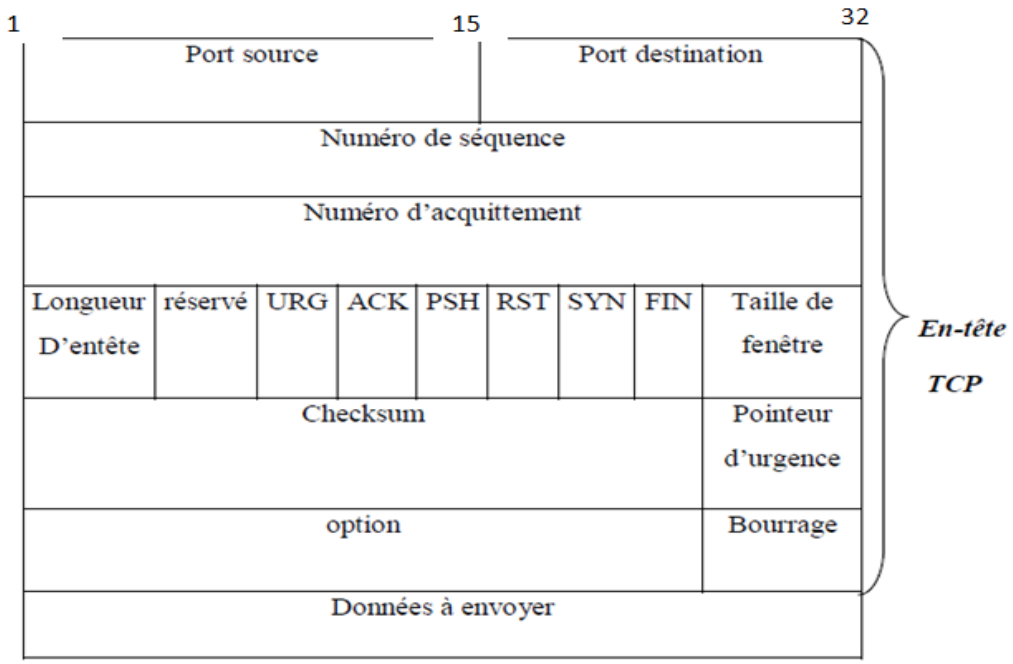


Figure 2.8 : la structure d'un datagramme TCP

- **Description des différents champs :**

- **Port source et port destination :** le port source permet d'identifier l'application qui s'exécute sur la machine locale, et le port destination permet d'identifier le service ou l'application sollicitée sur l'ordinateur distant.

- **Numéro de séquence :** les paquets TCP portent un numéro de séquence qui permet de les ordonner.
- **Numéro d'acquittement :** contient le numéro de séquence du prochain paquet que le récepteur s'attend à recevoir.
- **Longueur de fenêtre :** un champ de 4 bits, indique la longueur de l'entête du paquet TCP.
- **Les 6 champs bits de code :** permettent de spécifier le rôle et le contenu d'un paquet TCP pour l'interprétation des champs de l'entête

URG : pointeur de données de l'entête.

ACK : accusé de réception.

PSH : ce segment requiert un push.

RST : réinitialiser la connexion.

SYN : synchronisation des numéros de séquence pour initialiser une connexion.

FIN : l'émetteur a atteint la fin de son flot de données.

- **La taille de fenêtre** : un champ de 16 bits qui sert au contrôle de flux, il indique le nombre d'octet que le récepteur est prêt a accepter. Ainsi l'émetteur augmente ou diminue son flux de données en fonction de la valeur de cette fenêtre qu'il reçoit.
- **Checksum (somme de contrôle) :** est un champ qui permet de vérifier des informations reçues. A partir des données et de l'entête TCP, un algorithme est mis en œuvre pour calculer un nombre particulier, qui sera placé dans ce champ. A la réception, le destinataire effectue le même calcul, et peut ainsi vérifier qu'aucune information n'a été altérée pendant la transmission. Si une erreur de transmission a eu lieu, le récepteur n'acquitte pas le paquet, l'expéditeur ne reçoit pas d'accusé de réception ainsi il le réexpédie.
- **Le pointeur d'urgence :** il est ajouté au numéro de séquence du segment, indique le numéro du dernier octet de données urgentes. Il faut également que le bit URG soit positionné a 1 pour indiquer des données urgente que le récepteur TCP doit passer le plus rapidement possible a l'application associée a la connexion.
- **le champ bourrage :** termine l'entête TCP, il s'agit de données n'ayant aucune signification.
- **Le champ option :** permet de mettre en œuvre certaines fonctions spécifiques à un transfert de donnée.
- Le paquet se termine par **les données** à envoyer.

c. le protocole UDP :

C'est le second protocole de la couche transport, il fournit un service en mode non connecté (mode datagramme) aux applications. La **figure 2.9**, illustre un paquet UDP.

- **Format du paquet UDP :**

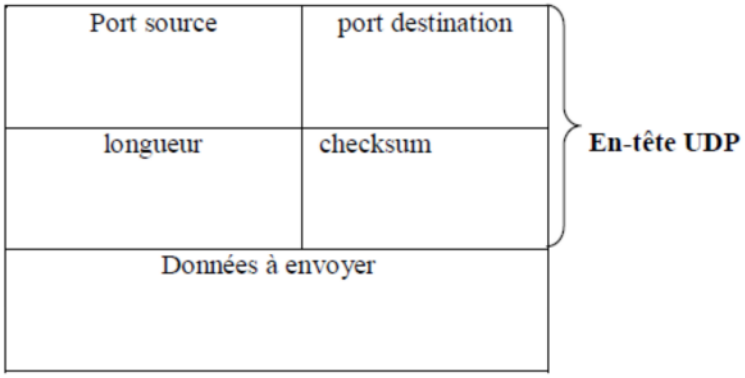


Figure 2.9 : la structure d'un datagramme UDP

De même que TCP, UDP utilise la notion de port, qui permet de distinguer les différentes applications qui s'exécutent sur un ordinateur. Le champ longueur, donne la longueur de paquet UDP. Les erreurs sont détectées, mais pas corrigés (présence du champ checksum, mais aucun champ pour un éventuel accusé de réception). Le protocole est donc non fiable. Les paquets ne sont pas numérotés donc le séquence ment n'est pas garanti.

3. La couche inter-réseau :

Elle est la couche la plus importante du modèle TCP/IP. Elle est chargée des fonctions suivantes :

- attribuer une adresse unique à chaque machine du réseau (adresse IP).
- Indiquer aux paquets les directions à suivre pour aller d'un point à un autre du réseau (routage).
- La gestion de la fragmentation des paquets, et leurs réassemblages à la réception.

Elle contient 3 protocoles :

- Le protocole IP
- Le protocole ICMP
- Le protocole ARP

3.a. Le protocole IP :

Le protocole IP comme UDP est un protocole sans connexion qui ne contrôle pas les erreurs de transmission, il s'attache avant tout à acheminer des paquets TCP à travers un ensemble de réseau interconnecté. Il assure les principales fonctions de la couche inter-réseau :

L'adressage

La fragmentation des données

Le routage

- ***Format du paquet IP :***

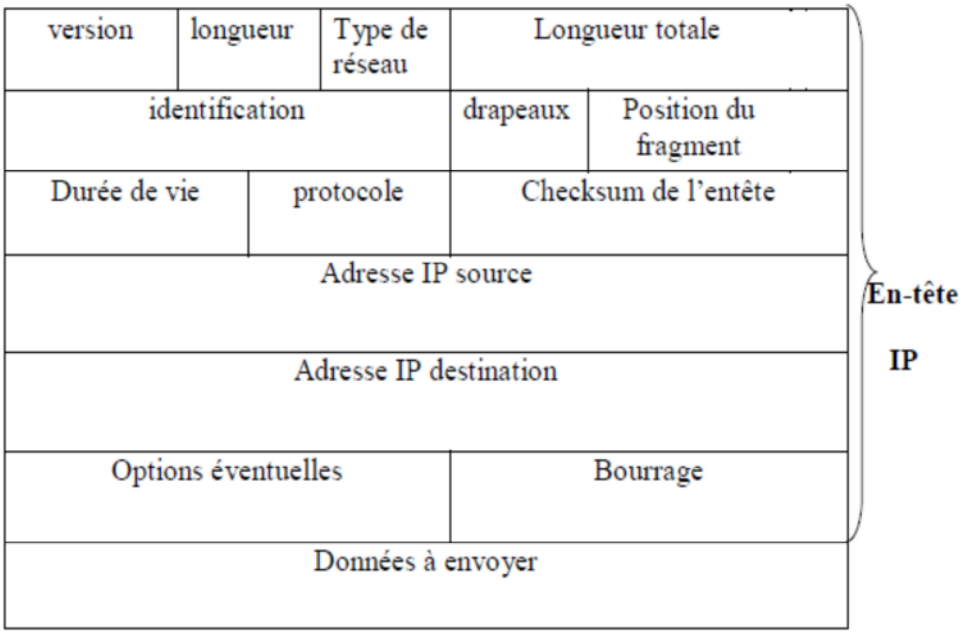


Figure 2.10 : structure d'un datagramme IP

- **Description des déférents champs :**
  - **Le champ version :** codé sur 4 bits, il permet d'identifier la version de protocole IP utilisé (il existe 2 versions du protocole IP : la version 4normalisé à la fin des années 70 appelé IPV4 et la version 6 normalisé à la fin des années 90, elle est appelé IPV6. Jusqu'ici nous avons parlé de IPV4).
  - **Le champ longueur :** il est codé sur 4 bits, il indique la longueur de l'entête IP, et de ce fait il marque le début des données dans le datagramme.

- **Le champ TOS (Type Of Service, type de service) :** codé sur 8 bits, indique la façon dont le datagramme doit être traité.
- **Le champ longueur total :** indique la taille totale du datagramme (entête et les données à envoyer) en octets.
- **Le champ identification :** est donné par l'émetteur, et permet au récepteur d'identifier les fragments d'un même datagramme (tous les fragments d'un même datagramme porte le même numéro).
- **Le champ drapeaux :** codé sur 3 bits, renseigne les systèmes intermédiaires sur la possibilité ou non de fragmenter le datagramme.
- **Le champ position du fragment :** il est codé sur 13 bits, indique la position du fragment dans le datagramme d'origine.
- **Le champ duré de vie :** codé sur 8 bits, indique le nombre maximal de routeurs à travers lesquels le datagramme peut passer.
- **Le champ protocole :** codé sur 8 bits, identifie le protocole utilisé parla couche supérieure.
- **Le champ checksum de l'entête :** permet de s'assurer que les données de l'entête seulement n'ont pas été altérées durant la transmission.
- **Les adresses IP source et destination :** qui sont les informations les plus importantes de cet entête, puisque ce sont qui vont permettre d'acheminer les données sur le réseau, vers la bonne destination.
- **Le champ option et bourrage :** le champ option permet de mettre en œuvre certains transferts particuliers, ce champ est toujours complété par des bits de bourrage.

3. b. Le protocole ICMP :

Comme son nom l'indique, le protocole ICMP (Internet Control Message Protocol) utilisé par IP et par des protocoles de niveau supérieur, envoie etreçoit des informations d'état concernent les transmissions en cours. Il sert à lagestion du protocole IP, il permet par exemple, de collecter les erreurs quisurviennent lors de l'émission de message.

3.c. Le protocole ARP (Address Resolution Protocol) :

Chaque ordinateur connecté au réseau a deux adresses : une adresse IP et une adresse MAC (adresse physique, adresse de la carte réseau). A l'intérieur d'un même réseau, deux ordinateurs ne peuvent communiquer que s'ils connaissent leurs adresses physiques

respectivement. Il est donc nécessaire d'établir un mécanisme de mise en correspondance de ces adresses MAC et IP. La résolution de ce problème est confiée au protocole ARP qui permet de trouver l'adresse MAC à partir d'une adresse IP.

4. La couche Accès réseau

La couche accès réseau est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau.

Ainsi, la couche accès réseau contient toutes les spécifications concernant la transmission de données sur un réseau physique, qu'il s'agisse de réseau local

(Ethernet, Token ring, Anneau à jeton), de connexion à une ligne téléphonique ou n'importe quel type de liaison à un réseau. Elle prend en charge les notions suivantes:

- Acheminement des données sur la liaison ;
- Coordination de la transmission de données (synchronisation) ;
- Format des données ;
- Conversion des signaux (analogique/numérique) ;
- Contrôle des erreurs à l'arrivée.

V. Architecture des réseaux

- Un serveur sur un réseau local est un ordinateur qui met des ressources partagées à la disposition des utilisateurs du réseau.
- Un client est un ordinateur qui utilise une ou plusieurs ressources d'un ou plusieurs serveurs.
- Une station de travail est un ordinateur utilisé par un utilisateur.

1. Les ressources partagées peuvent être des :

- ✓ dispositifs de stockage de masse (disques durs, CD-ROM, …).
- ✓ dispositifs d'impression (imprimantes ……).
- ✓ des moyens de communications (modems, fax, liaison avec des ordinateurs distants,...)
- ✓ des applications (Sauvegarde, SGBD, Messagerie, ...).

2. Les principaux serveurs :

- ✓ Le serveur web
- ✓ Le serveur DNS
- ✓ Le serveur d'impression
- ✓ Le serveur de fichiers
- ✓ Le serveur mail
- ✓ Le serveur d'applications
- ✓ Le serveur de base de données. Etc…..

3. Le modèle client /serveur

a. Introduction

Le modèle client/serveur repose sur une communication d'égal à égal entre les applications. La communication est réalisée par le dialogue deux à deux entre des processus.

Dans ces processus, l'un est le client, l'autre est le serveur. Ces derniers ne sont pas identiques mais forment un système coopératif.

Cette coopération se traduit par un échange de données : le client initie l'échange via une requête. Le serveur est en attente d'une éventuelle requête client.

- **Client : (client)** Processus demandant l'exécution d'une opération à un autre processus par envoi d'un message (requête) contenant le descriptif de l'opération à exécuter et attendant la réponse à cette opération par un message en retour .Il est toujours l'initiateur de dialogue.
- **Serveur : (server)** Processus accomplissant une opération sur demande d'un client, et transmettant la réponse à ce client. Il est toujours en attente d'une requête.
- **Réponse : (reply)** Message transmis par un serveur à un client suite à l'exécution d'une opération contenant les paramètres de retour de l'opération.
- **Requête : (request)** Message transmis par un client à un serveur décrivantl'opération à exécuter pour le compte client.

b. Principe de fonctionnement

- Un système client/serveur fonctionne selon le schéma suivant :

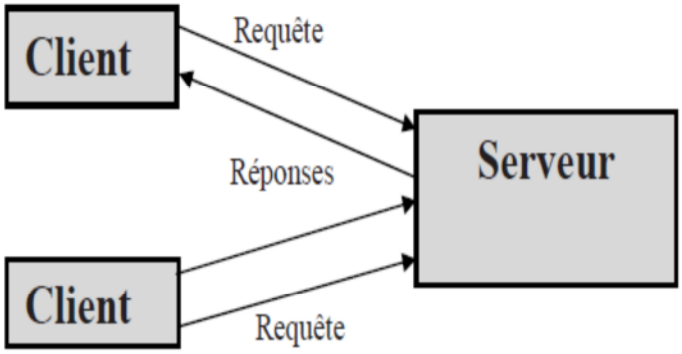


Figure 2.11: Fonctionnement architecture client serveur

- **Les clients** émettent des requêtes de demande de service vers le serveur.
- **Le serveur** reçoit la demande et répond à la machine cliente.

Le serveur et les clients sont identifiés par une adresse sur le réseau, tandis que le service demandé est identifié par un numéro de port sur la machine concernée.

c. Avantages de l'architecture client/serveur

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

- ✓ des ressources centralisées : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction.
- ✓ une meilleure sécurité: car le nombre de points d'entrée permettant l'accès aux données est moins important.
- ✓ une administration au niveau serveur : les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés.
- ✓ un réseau évolutif: grâce à cette architecture il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure de ce dernier.

d. Inconvénients du modèle client/serveur

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles:

- ✓ **un maillon faible** : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est structuré autour de lui. Une panne du serveur entraînerait la paralysie de tout le réseau.

e. Classification des architectures client/serveur

❖ **Architecture à deux niveaux**

L'architecture à deux niveaux (aussi appelée architecture 2tiers) caractérise le système Client/serveur dans lequel le client demande une ressource au serveur qui la lui fournit directement (le serveur ne fait appel à aucune application pour fournir ce service).

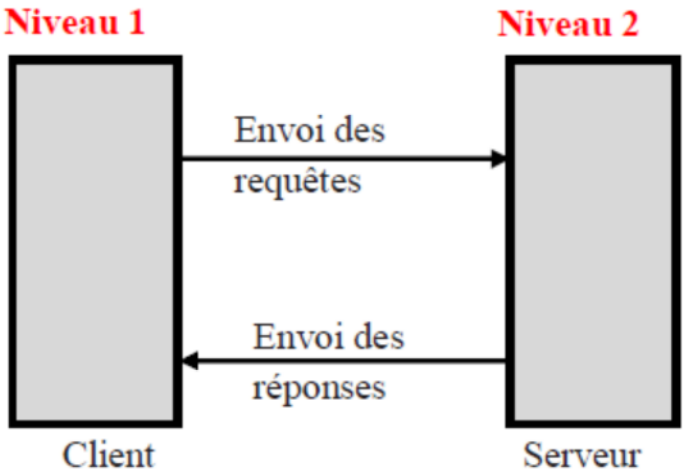


Figure 2.12 : Architecture à deux niveaux

❖ **Architecture à trois niveaux**

Dans l'architecture à trois niveaux (aussi appelée architecture 3tiers), il existe un niveau intermédiaire entre le serveur et le client :

- ✓ niveau 1 : Le client demandeur de ressources
- ✓ niveau 2 : le serveur chargé de fournir la ressource mais qui fait appel a un autre serveur pour certaines demandes de ressources
- ✓ niveau 3 : le serveur secondaire (généralement un serveur de base de données), fournit les ressources au premier serveur.

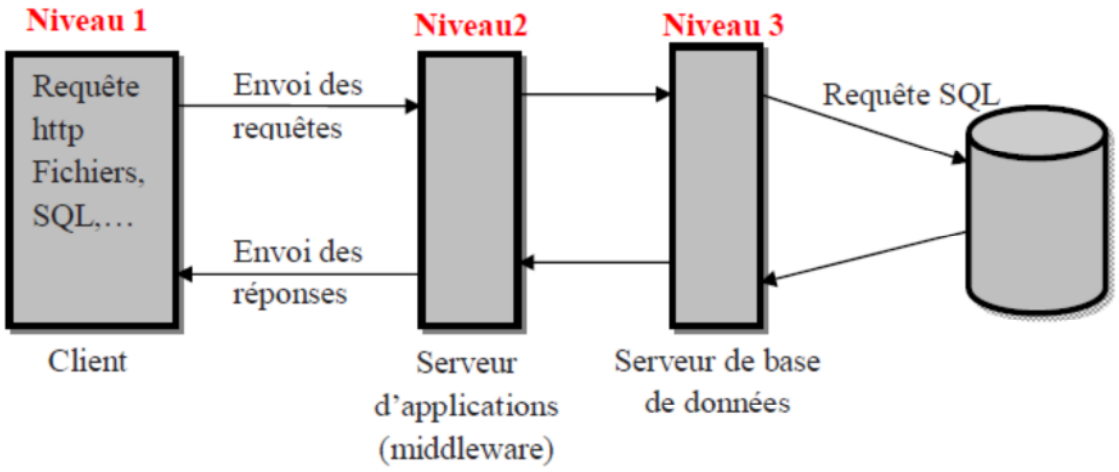


Figure 2.13 : Architecture 3tiers (_à trois niveaux)

❖ **Architecture multi niveau**

Dans l'architecture à 3 niveaux, chaque serveur (niveaux 2 et 3) effectue une tâche (un service) spécialisée. Un serveur peut donc utiliser les services d'un ou plusieurs autres serveurs afin de fournir son propre service. Par conséquent, l'architecture à trois niveaux est potentiellement une architecture à N niveaux...

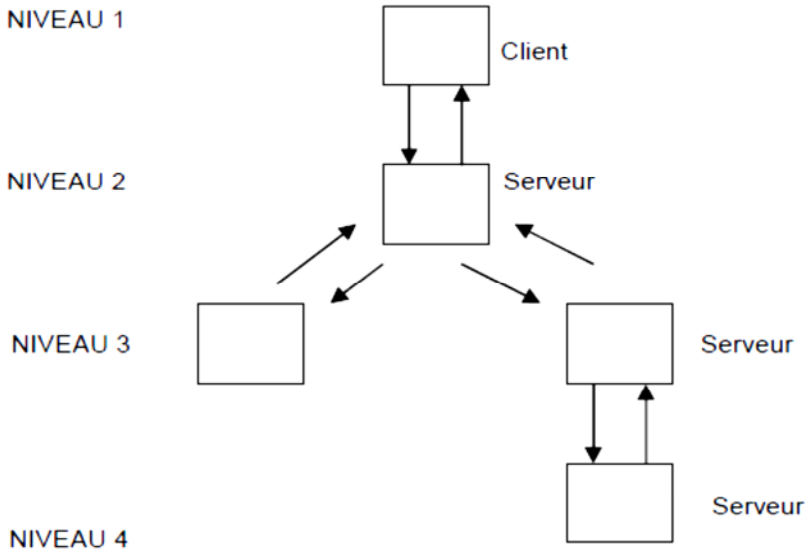


Figure 2.14: architecture C/S multi-niveaux

f. Le Middleware

❖ Définition

Le middleware peut se définir comme un mécanisme logiciel assurant le dialogue entre différentes applications ou portions d'une même application réparties sur plusieurs postes, clients ou serveurs.

Il existe différents types de middlewares :

- ✓ Les moniteurs transactionnels (CICS, Tuxedo…),
- ✓ Les messageries inter-applicatives asynchrones (MQSeries…),
- ✓ Les ORB (VisiBroker, Orbix…),
- ✓ Les appels de procédure à distance (RPC),
- ✓ Les middlewares d'accès aux données (ODBC, EDA/SQL.).

❖ Rôle de middleware

- prend en compte les requêtes de l'application cliente,
- les transmet au serveur de manière transparente,
- prend en compte les données résultat du serveur vers le client,
- Résout le problème d'intégrité des logiciels.

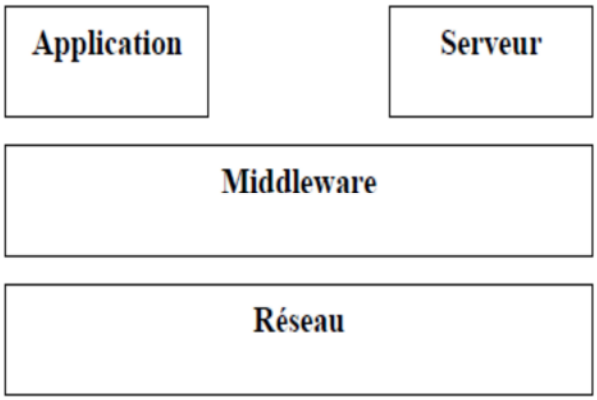


Figure 2.15 : Le Middleware comme Complément de services du réseau permettant la réalisation du dialogue client/serveur

4. Architecture Peer to Peer (P2P) (égal à égal):

Dans une architecture d'égal à égal (appelée aussi « poste à poste », en anglais peer to peer, notée P2P), contrairement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié. Ainsi chaque ordinateur dans un tel réseau joue à la fois le rôle de serveur et de client. Cela signifie notamment que chacun des ordinateurs du réseau est libre de partager ses ressources. Un ordinateur relié à une imprimante pourra donc éventuellement la partager afin que tous les autres ordinateurs puissent y accéder via le réseau.

a. Qu'est ce que le Peer2Peer ?

Cela signifie que chaque ordinateur se connecte à tous les autres ordinateurs et non plus à un unique ordinateur serveur. Le P2P est basé sur un protocole qui permet de partager des fichiers entre de nombreux ordinateurs d'utilisateurs et qui ne nécessite pas de serveurs pour le stockage des fichiers.

Le graphique ci-dessous va nous permettre de préciser un peu mieux le fonctionnement d'un réseau P2P :

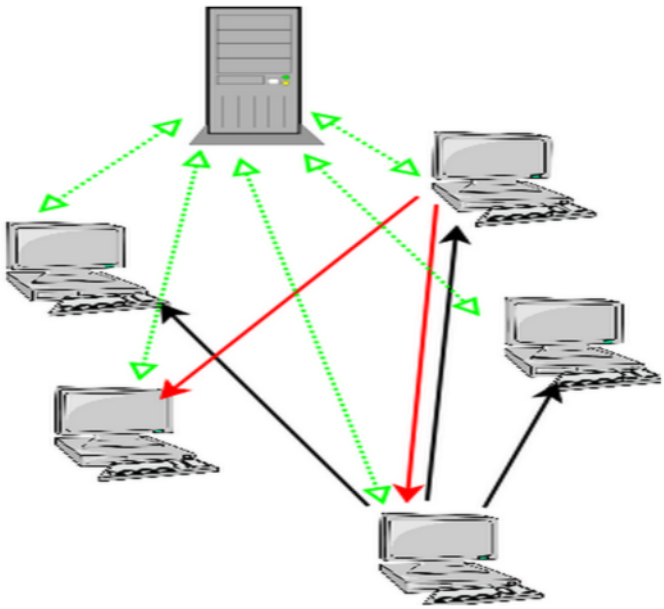


Figure 2.16 : l'architecture générale P2P

Les flèches noires et rouges indiquent les échanges entre les ordinateurs de chaque utilisateur. Chacun contient des fichiers qu'il partage avec d'autres. La subtilité réside dans le fait que chaque ordinateur est à la fois un client et un serveur. En effet chaque ordinateur va demander aux autres des morceaux de fichiers (donc il est un client), mais il va aussi donner des bouts

de fichiers (donc il est serveur). Par abus de langage on dira que le logiciel de P2P est un "client" de P2P, on ne parle pas de serveur pour le logiciel de l'utilisateur.

b. Fonctionnement type des clients P2P

• Le client P2P se connecte à un serveur. Celui-ci lui donne une liste des ordinateurs possédant le fichier recherché. Ensuite le client se connecte aux différents ordinateurs et va rechercher des morceaux du fichier voulu. Il va rassembler ses petits bouts de fichier pour reconstituer le fichier complet. De plus, pendant tout le temps de téléchargement des fichiers, l'ordinateur client va aussi partager les morceaux qu'il a eu (et devient donc aussi un serveur).

c. Avantages de l'architecture peer to peer:

• L'architecture d'égal à égal possède les avantages suivants :

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

• Les réseaux P2P ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés. On peut donc utiliser Windows NT Workstation, Windows pour Workgroups ou Windows XP car tous ces systèmes d'exploitation intègrent toutes les fonctionnalités du réseau P2P.

La mise en œuvre d'une telle architecture réseau repose sur des solutions standards :

• Placer les ordinateurs sur le bureau des utilisateurs

• Chaque utilisateur est son propre administrateur et planifie lui-même sa sécurité

• Pour les connexions, on utilise un système de câblage simple et apparent

Il s'agit généralement d'une solution satisfaisante pour des environnements ayant les caractéristiques suivantes :

• Moins de 10 utilisateurs

• Tous les utilisateurs sont situés dans une même zone géographique

• La sécurité n'est pas un problème crucial

• Ni l'entreprise ni le réseau ne sont susceptibles d'évoluer de manière significative dans un proche avenir

d. Administration d'un réseau P2P:

• Le réseau P2P répond aux besoins d'une petite entreprise mais peut s'avérer inadéquat dans certains environnements. Le choix d'un type de réseau dépend de son "Administration" :

• Gestion des utilisateurs et de la sécurité

• Mise à disposition des ressources

• Maintenance des applications et des données

• Installation et mise à niveau des logiciels utilisateurs

• Dans un réseau poste à poste typique, il n'y a pas d'administrateur. Chaque utilisateur administre son propre poste. D'autre part tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent (données dans des répertoires partagés, imprimantes, cartes fax etc.)

VI. Internet :

1. Définition :

Internet est l'abréviation du terme anglais « interconnected networks » que l'on peut traduire par «réseaux interconnectés», c'est donc un réseau, en réalité une fédération de réseaux à l'échelle mondiale. Ces différents réseaux regroupés ont en commun certains protocoles et offrent certains services similaires. Ce réseau planétaire repose sur un protocole fédérateur qui en est le ciment : la pile TCP/IP, à savoir principalement les protocoles IP et TCP ainsi que différents autres protocoles qui leur sont associés.

Internet est maintenant le plus grand réseau du monde, regroupant universités, organismes de recherche, administrations, entreprises ou simples particuliers appartenant à de très nombreux pays de part le monde.

2. Les services d'Internet :

Pour accéder aux multiples services qu'offre Internet, il faut avoir accès au réseau (ISP) et disposer d'une implémentation TCP/IP et d'une application TCP/IP.

a. Messagerie électronique (e-mail) :

La messagerie est l'un des services les plus connus et usités d'Internet. Le mail ou E-Mail (pour Electronic-Mail) permet à tout utilisateur d'Internet d'envoyer et de recevoir des messages dans le monde entier. Il ne faut cependant pas penser qu'un message n'est qu'uniquement composé de texte. Si cela était vrai au début d'Internet, on peut aujourd'hui associer à un message toute sorte de documents ou fichiers comme des sons, images, animations etc.

b. Les nouvelles (news) :

Les groupes d'intérêt (newsgroups) sont des forums spécialisés dans lesquels les utilisateurs peuvent échanger des informations. Il existe de nombreux groupes sur des sujets pas forcement technique puisqu'ils vont de l'informatique à la politique. Chaque groupe a son style, ses usages et son étiquette qu'il convient de respecter scrupuleusement.

c. Telnet :

Telnet est le nom d'un protocole et d'un logiciel permettant de se connecter à une machine distante, afin de pouvoir y travailler. Il est utilisé pour permettre l'accès à certains services d'informations, tels des bibliothèques, annuaires ou encore des jeux en mode texte (appelés MUDs) ou des services de dialogue (un peu comme l'IRC).

d. La téléphonie :

Est un service encore peu connu et utilisé. Il permet de concevoir en direct une communication pourvu que les utilisateurs aient à leur disposition carte de son, microphone et haut-parleur.

e. WAIS (Wide Area Info Serveurs):

Est un système client-serveur qui permet d'effectuer des recherches d'information dans des bases de données thématiques.

f. World Wide Web (WWW):

Le Word Wide Web, est un système hypermédia distribué fonctionnant en mode client-serveur sur Internet, il permet tout ce qui précède et ajoute des liens vers d'autres ressources et des facilités multimédias (son, graphique, vidéo).

VII. Intranet :

1. Définition :

Un intranet est un ensemble des services Internet (par exemple un serveur Web) interne à un réseau local, c'est à dire accessible uniquement à partir des postes d'un réseau local et invisible de l'extérieur. Il consiste à utiliser les standards clients serveurs de l'Internet(en utilisant les protocoles TCP/IP). Un intranet repose généralement sur une architecteur à trois niveaux, composée :

- de clients (navigateur internet généralement) ;
- d'un ou plusieurs serveurs d'application (middleware): un serveur web permettant d'interpréter des scriptes (PHP) ou autres, et les traduire en requêtes SQL afin d'interroger une base de données ;
- d'un serveur de base des données.

De cette façon, les machines clientes gèrent l'interface graphique, tandis que les différents serveurs manipulent les données. Le réseau permet de véhiculer les requêtes et les réponses entre clients et serveurs.

2. Les services d'un intranet :

Service	Technologie utilisée
Services de transport	Réseau local, interconnexion réseau…
Services d'administration	Administration, supervision, télémaintenance…
Services de sécurité	Authentification, filtrage…
Services de partage de l'information	Serveur de fichiers, serveur de données…
Services de communication	Communication et travail coopératif
Services d'annuaires	Annuaires des utilisateurs, annuaires des serveurs…
Services de développement	Atelier de génie logiciel
Services d'accès aux informations et applications	Client-serveur universel

Tableau 2.2 : Les services d'un intranet et les technologies utilisées

3.Avantages d'un Intranet :

Un intranet permet de constituer un système d'information à faible coût (concrètement le coût d'un intranet peut très bien se réduire au coût du matériel, de son entretien et de sa mise à jour, avec des postes clients fonctionnant avec des navigateurs gratuits). D'autre part, étant donné la nature "universelle" des moyens mis en jeu, n'importe quel type de machine peut être connecté au réseau local, donc à l'intranet.

VIII. Extranet :

Un extranet est une extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau.

L'accès à l'extranet doit être sécurisé (authentification par nom d'utilisateur et mot de passe) dans la mesure où cela offre un accès au système d'information à des personnes situées en dehors de l'entreprise. De cette façon, un extranet, n'est ni un intranet, ni un site Internet, il s'agit d'un système supplémentaire offrant par exemple aux clients d'une entreprise, à ses partenaires ou à des filiales un accès privilégié à certaines ressources informatiques de l'entreprise par l'intermédiaire d'une interface Web.

La différence entre Internet et Intranet :

La différence fondamentale entre un intranet et l'Internet réside dans le fait que les utilisateurs qui ont accès à un intranet sont connus et identifiables. Il est certain que cette approche procure bon nombre d'avantages à l'entreprise. Néanmoins, l'entreprise devra fournir des efforts considérables pour sécuriser les interconnexions et protéger les données non destinées au grand public.

IX. Conclusion

Au cours de ce chapitre, nous avons présenté certains concepts des nouvelles technologies de l'information et de la communication, à savoir : les réseaux informatiques, l'internet et l'architecture client/serveur. Cela est motivé par le fait que notre travail s'intègre dans le domaine des réseaux et plus particulièrement les réseaux informatiques qui s'articulent sur une architecture du type client/serveur. Les différents concepts traités dans ce chapitre nous aiderons à comprendre au mieux notre mode d'opération et les notions fondamentales pour mener à bien notre application. Dans le chapitre suivant, nous allons présenter l'organisme d'accueil ainsi que les objectifs de notre application.

I. Introduction

Ce présent chapitre se focalise sur la partie technique de la fibre optique. Il permet de comprendre les éléments de base des réseaux informatiques. Plus précisément, il concerne le choix de la fibre optique pour des transmissions à grande distance, et de prendre en connaissance la structure générale des systèmes de transmission par fibres optiques.

II. Historique

À l'époque des Grecs anciens**,** le phénomène du transport de la lumière dans des cylindres de verre était déjà connu. Il était, semble-t-il, mis à profit à merveille par des artisans du verre pour créer de magnifiques pièces décoratives. De plus, les techniques de fabrication utilisées par les artisans vénitiens de la renaissance pour fabriquer les « millefiori » ressembleraient beaucoup aux techniques de fabrication de la fibre optique actuelle. L'utilisation du verre en conjonction avec la lumière ne date donc pas d'hier.

En 1854, le physicien irlandais John Tyndall, donna la première démonstration scientifique du principe de la réflexion totale interne devant la Société Royale Britannique. Sa démonstration consistait à guider la lumière dans un jet d'eau déversé d'un trou à la base d'un réservoir. En injectant de la lumière dans ce jet, il put démontrer le principe qui est à la base de la fibre optique. L'idée de courber la trajectoire de la lumière, de quelque façon que ce soit, était plutôt difficile à faire accepter à l'époque puisqu'il était établi que la lumière voyage en ligne droite. Cependant, elle suivait bien la courbure du jet d'eau, démontrant ainsi qu'elle pouvait être déviée de sa trajectoire rectiligne.

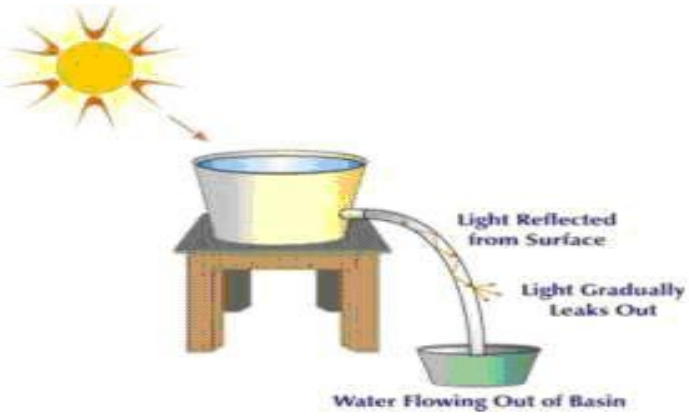


Figure 3.1 : Expérience de John Tyndall.

En 1927, le principe de la fibre optique est connu mais pas exploité. Ce n'est qu'en 1950 que la première application de la fibre optique eu lieu, lorsque le fibroscope flexible fut inventé par Van Heelet Hopkins. Cet appareil permettait la transmission d'une image le long de fibres en verre. Il fut particulièrement utilisé en endoscopie, pour observer l'intérieur du corps humain, et pour inspecter des soudures dans des réacteurs d'avions. Mais à cette période, à cause de la mauvaise qualité des fibres utilisée, la transmission ne pouvait se faire sur une grande distance.

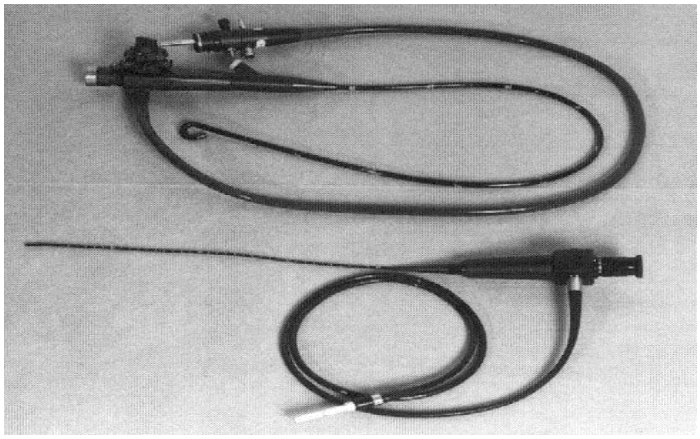


Figure 3.2 : Fibroscope.

L'invention du laser en 1960 a permis de transmettre un signal avec assez de puissance sur une grande distance.

En 1964, Charles Kao décrivit et expérimenta un système de communication à longue distance et à faible perte en mettant à profit l'utilisation conjointe du laser et de la fibre optique. C'est l'expérience qui est considéré comme la première transmission de données par fibre optique.

En 1966 que sera transportés sur de grandes distances des signaux optiques sur une fibre, mais il faudra des années pour maîtriser les procédés de fabrication et contrôler la composition des matériaux qui influe de manière décisive sur les pertes. C'est ainsi que l'activité de recherche sur les fibres optiques à base de verre de silice a débuté, car ce matériau pouvait constituer un milieu à pertes suffisamment faibles pour la transmission de fréquences optiques de la région du proche infrarouge et être utilisée dans un système de télécommunications optiques à longue distance. On parviendra alors à obtenir des atténuations assez faibles pour que devienne possible la transmission des signaux sur des distances suffisamment grandes pour présenter un intérêt pratique. Partie en 1960 de 1000 dB/km,

l'atténuation est descendue à 20 dB/kmen 1975**,** puis à 0.2 dB/km en 1984 (pour des longueurs d'onde proches de 1550 nm), ce qui représente 1% du signal après 100 km. Le record actuel est de0.149 dB/km à 1550nm, obtenu sur une fibre de silice pure. Il faut noter, par ailleurs, que cette valeur d'atténuation est très proche de la limite théorique intrinsèque aux matériaux à base d'oxyde de silice.

III. Présentation générale des fibres optiques

1. Définition

La fibre optique est définie comme étant un support de transmission, des signaux numériques sous forme d'impulsions lumineuses modulées. La fibre optique est un fil de verre transparent très fin qui conduit un signal lumineux codé permettant de véhiculer une large quantité d'informations. C'est un fil de verre, entouré d'une gaine réfléchissante qui a une propriété principale de servir de tuyau dans lequel on peut faire circuler de la lumière.

2. Caractéristiques de la fibre optique

a. Structure

La partie optique de la fibre est constituée d'un cœur, d'indice de réfraction $n_c(r)$, centré sur l'axe de la fibre et entourée d'une gaine annulaire, d'indice de réfraction $n_g(r)$ inférieur à n_c (r).

Schématiquement, en partant de l'extérieur on rencontre successivement (figure 3) :

- une couche de protection mécanique en matière plastique. En effet, la fibre de silice est protégée par un revêtement de quelques dizaines de micromètres, qui l'isole des agents corrosifs du milieu extérieur et lui confère sa très grande flexibilité. Les matériaux le plus souvent utilisés pour ce revêtement protecteur sont des polymères (polyuréthane...)
- une gaine optique, zone où $n_g(r)$ reste constant.
- un cœur au voisinage de l'axe où $n_c(r)$ présente un maximum (le signal lumineux est propagé dans et à proximité du cœur)

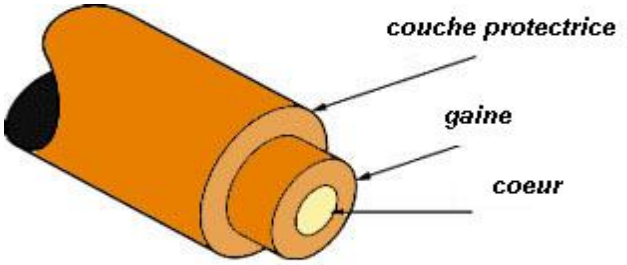


Figure 3.3 : Constitution d'une fibre optique

Le diamètre externe d'une fibre de silice peut varier entre quelques dizaines et plusieurs centaines de micromètres (typiquement de 125 µm). Le diamètre du cœur, constant sur la longueur de la fibre, varie de quelques micromètres pour les fibres monomodes jusqu'à plusieurs centaines de micromètres pour les fibres multi modes.

b. Les différents types de fibre Optique

Les fibres optiques peuvent être classées en deux catégories selon leurs caractéristiques, la longueur d'onde utilisée et les modes de propagation de la lumière: les fibres multi modes, et les fibres monomodes.

- **Les fibres optiques multi modes (Multi-liaison)**

  Les fibres multimodes ont été les premières sur le marché. Elles ont pour caractéristiques de transporter plusieurs modes (trajets lumineux) simultanément c a dire Multi liaison. Du fait de la dispersion modale, on constate un étalement temporel du signal. En conséquence, elles restent utilisées uniquement pour des bas débits et de courtes distances. La dispersion modale peut cependant être minimisée (à une longueur d'onde donnée) en réalisant un gradient d'indice dans le cœur de la fibre. Elles sont caractérisées par un diamètre de cœur de plusieurs dizaines à plusieurs centaines de micromètres. Parmi les fibres multimodes, on distingue les fibres à faible indice ou saut d'indice (débit limité à 50 Mbps) et les fibres à gradient d'indice (débit limité à 1 Gbps). Les longueurs d'onde les plus utilisées sont 850nm et 1300 nm.

La fibre multimode à saut d'indice possède une région du cœur uniforme relativement large comparé à la gaine et qui représente près de 96% du diamètre total de la fibre (Figure 4).

Le cœur est composé de verre (SiO2) dopé. Elle est le support privilégié pour des applications des réseaux informatiques courte distance, sa bande passante est alors limitée. Le faisceau

laser se propage en ligne droite et se réfléchit sur les parois de la gaine qui a un indice de réfraction inférieur au cœur.

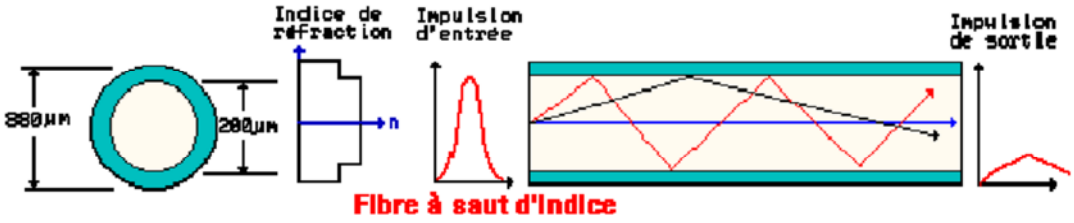


Figure 3.4: Fibre multi mode à saut d'indice

La fibre à gradient d'indice dont le cœur est constituée de couches de verre successives ayant un indice de réfraction proche. La variation de cet indice de réfraction cœur/gaine présente une courbe parabolique avec un maximum au niveau de l'axe (Figure 5).
Les rayons lumineux suivent un parcours sinusoïdal. La bande passante est comprise entre 600 et 3000 MHz/km. Les diamètres les plus fréquents sont 62.5 µm et 50 µm. Ce type de fibre est le plus utilisé pour les moyennes distances. Un des avantages est que la dispersion modale est diminuée avec cette fibre. Il y a donc une meilleure réception du signal.

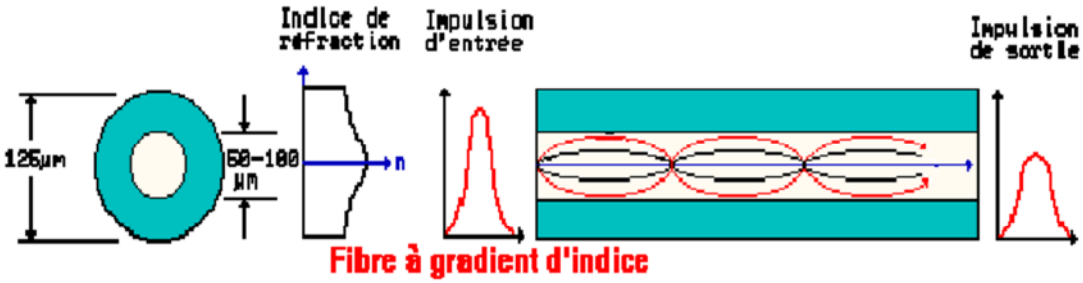


Figure 3.5 : Fibre multi mode à gradient d'indice

- **Les fibres optiques monomodes**

Dans une fibre monomode, le cœur est très fin, ce qui permet une propagation du faisceau laser presque en ligne droite (Figure 6). De cette façon, elle offre peu de dispersion du signal

et celle-ci peut être considérée comme nulle. La bande passante est presque infinie, supérieure à 10 GHz/km avec une longueur d'onde de coupure 1.2 µm. Le diamètre du cœur (9 µm) et l'ouverture numérique sont si faibles que les rayons lumineux se propagent parallèlement avec des temps de parcours égaux. Ce type de fibre est surtout utilisé en liaison longue distance. Le petit diamètre du cœur des fibres nécessite une grande puissance d'émission qui est délivrée par des diodes laser.

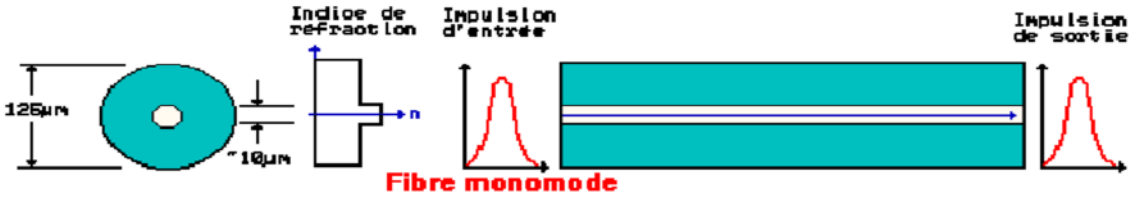


Figure 3.6 : Fibre monomode

3. Avantages des fibres optiques

La fibre optique est une des plus grandes avancées technologiques en matière de câblage puisqu'elle perd tous les désavantages des câbles électriques (puissance, impédances,...). Elle présente en termes de transmission une faible atténuation, une très grande bande passante et l'insensibilité aux perturbations électromagnétiques.

- **Faible taux d'atténuation**

Comparée aux autres supports de transmission existants, la fibre optique présente une atténuation faible et quasiment constante sur une énorme plage de fréquences, permettant ainsi d'envisager la transmission de débits numériques très importants. Pour des débits de 1 Gbps, l'impulsion lumineuse connaît un taux d'erreur considéré comme nul ($<10^{-9}$p erreur/bit) jusqu'à 200 km. Ces atouts ont permis les réalisations des liaisons intercontinentales.

- **Enorme Bande passante**

La fibre optique est un media permettant de transférer des données numériques à très haut débit : vidéo, son, image.

Le principal pivot des communications optiques à haut débit est la bande passante qu'elles peuvent utiliser. Théoriquement, le nombre d'informations transmisses par seconde ne peut excéder la fréquence de l'onde porteuse (soit au plus un bit par période de l'onde).

C'est pour cette raison que les signaux optiques sont très utiles, dont les fréquences vont de

10^{14}à 10^{15} Hz autorisant un débit d'information très élevé.

- **Insensibilité aux perturbations électromagnétiques**

La technologie optique est très utile dans des environnements difficiles et agressifs, riches en perturbations électromagnétiques comme les milieux industriels denses qui sont susceptibles de générer des erreurs de transmission sur des liaisons cuivre. La fibre optique est insensible aux perturbations et elle n'en produit pas (deux fils électriques placés côte à côte se perturbent mutuellement, ce qui n'est pas le cas avec des fibres optiques), ce qui assure une diaphonie nulle et une grande sécurité contre les intrusions.

De plus, elle ne peut provoquer d'étincelles (comme pourraient le faire des câbles électriques) et sa technologie ne faisant pas intervenir le métal, elle résiste à la corrosion.

4. Système de communication par fibre optique

Comme le montre la figure 7 l'information (données, voix, vidéo,..) venant de la source est transcrite sous forme codée en signal électrique pour que l'émetteur l'envoie, la fibre agit comme une guide d'onde optique afin que les photons puissent traverser le chemin optique vers le récepteur. Arrivée au détecteur, le signal subit une conversion optique-en électrique, décodé, et envoyé vers sa destination.

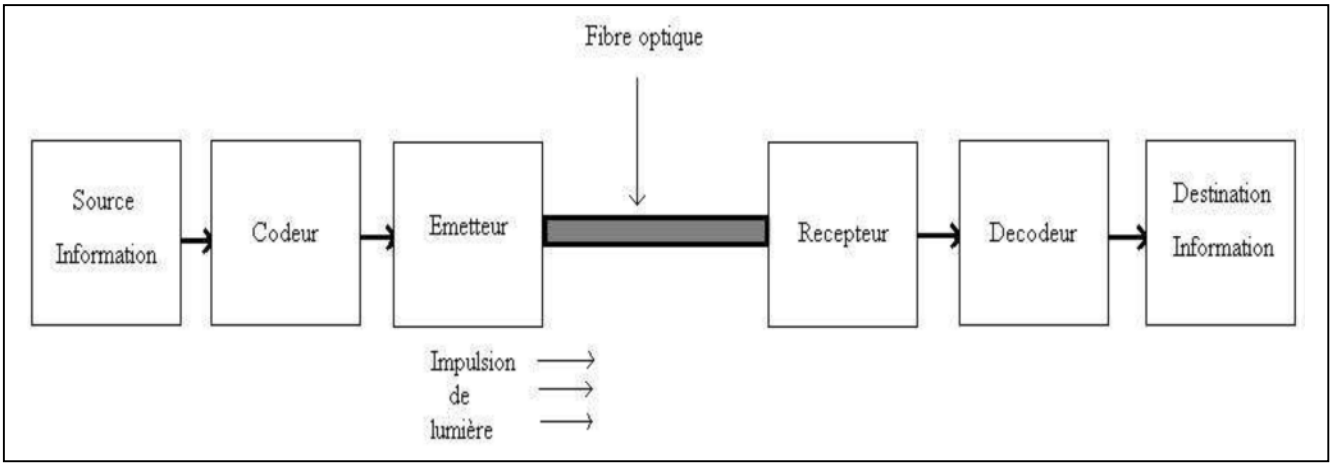


Figure 3.7 : Système de communication par fibre optique

a. Les émetteurs

Le composant émetteur a deux rôles. D'abord il doit être source de la lumière émise sur la fibre. Et deuxièmement, il doit moduler cette lumière de telle façon qu'elle représente les données binaires émises par la source d'information. La source optique doit pouvoir générer assez de puissance optique telle que l'atténuation attendue sur le chemin soit respectée. La source optique doit aussi être facile à moduler par un signal électrique et capable d'une haute

rapidité de modulation. Deux types de jonction photoémettrice peuvent être utilisés comme source optique d'un émetteur :

- Les LED (Light-Emitting diode)

Les LED sont simples, et ont une assez bonne linéarité et coûtent moins cher, mais génèrent une faible puissance.

- Les LD (Laser Diodes)

Le laser génère une lumière cohérente, puissante ; mais il coûte cher.

b. Les récepteurs

Les récepteurs optiques doivent détecter la lumière issue de la fibre optique et la convertit en un signal électrique. Le récepteur doit démoduler cette lumière pour déterminer les signaux binaires correspondants. Le récepteur exécute donc la fonction conversion
optique-électrique. La photodiode joue le rôle de ce récepteur.

c. Modulateurs Optiques

Un modulateur dans le système fibre optique est un agent de changement qui a pour but de convertir les impulsions « Marche/Arrêt » électriques en impulsions de lumière.
Les modulateurs optiques utilisent la plus simple de modulation appelée modulation directe, cette méthode utilise un laser qui émet si le bit à coder est un « 1 »ou n'émet pas si le bit coder est zéro « 0 ».

d. Les Câbles

Un câble à fibres optiques est composé d'un nombre de fibres pouvant aller de deux à plusieurs dizaines de fibres, et ce, en fonction des besoins. Le plus souvent dans les réseaux locaux d'entreprise, ce nombre est de 6 à 24.
Deux structures élémentaires permettent la réalisation de câbles optiques: les câbles à revêtement lâche et les câbles à revêtement serré.

- Les câbles à revêtement lâche (Loos tube câble), Ce câble est constitué de plusieurs tubes contenant chacun plusieurs fibres optiques. Ces dernières sont libres au sein du tube. Ce câble est utilisé pour les liaisons inter-bâtiments.
- Les câbles à revêtement serré (tight tube câble) dans lesquels une gaine plastique est directement appliquée sur la fibre ; ce qui la renforce mécaniquement et lui apporte la souplesse nécessaire à la réalisation de cordons.

e. Multiplexage

La demande croissante de capacité dans les systèmes de transmission par fibre optique impose l'utilisation de techniques permettant d'augmenter le débit d'information. L'une de ces techniques repose sur le multiplexage. Parmi les types de multiplexage les plus couramment utilisés dans les systèmes de transmission terrestres et sous-marins, on distingue le multiplexage en longueur d'onde (WDM: *Wavelength Division Multiplexing*), le multiplexage temporel (TDM : *Time division multiplexing*), le multiplexage en polarisation (PDM: *Polarization Division Multiplexing*) et le multiplexage spatial (SDM: *Space Division Multiplexing*). Le SDM peut consister à multiplexer plusieurs fibres dans un même câble ou à utiliser des fibres multimodes ou multi-cœurs pour la propagation des signaux optiques. Je ne détaillerai pas ce type de multiplexage mais des efforts de recherche sont activement menés aujourd'hui dans cette direction comme nous l'avons vu dans la partie introduction de ce manuscrit. Dans cette partie je vais décrire ces différentes formes de multiplexage.

- **Multiplexage temporel**

Le multiplexage TDM consiste à générer un signal modulé à partir de Sb signaux modulés obtenus à partir de séquences temporelles de symboles. Le temps symbole associé aux différents signaux modulés à multiplexer, T_s est égal à S_bT_{sm} où T_{sm} est le temps symbole associé au signal modulé obtenu après multiplexage. La Figure 8 décrit le principe du multiplexage temporel dans le cas simplifié où l'information est contenue dans deux séquences de données binaires.

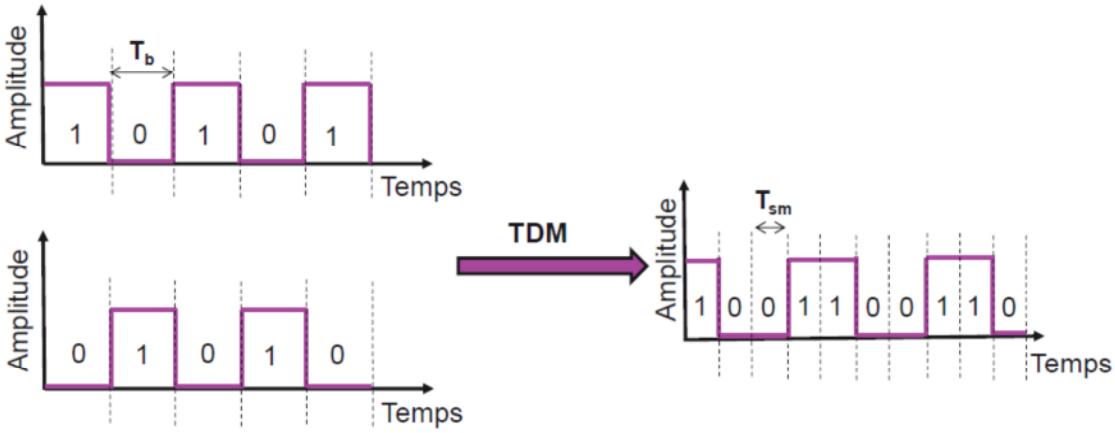


Figure 3.8: Principe du multiplexage temporel dans le cas simplifié de deux séquences binaires

Le débit d'information est alors multiplié par S_b. La hiérarchie numérique utilisée dans les réseaux de télécommunication est basée sur le multiplexage temporel. C'est le cas de la hiérarchie numérique synchrone (SDH: Synchronous Digital Hierarchy) et dont le module de base appelé module de transport synchrone (STM)-1 (STM: Synchronous Transport Module). Les systèmes multiplexés en temps sont très sensibles à l'interférence entre symboles du fait que les différentes impulsions lumineuses se succèdent rapidement.

- **Principe du multiplexage en longueur d'onde**

Le multiplexage WDM est une technique permettant de transmettre dans une même fibre plusieurs signaux optiques modulés de longueurs d'onde porteuse différentes. La complexité des émetteurs et récepteurs augmente avec le nombre de canaux WDM car cette technique nécessite autant d'émetteurs/récepteurs que de signaux multiplexés. Par la suite, le canal de transmission correspondra à un signal modulé à transmettre. Les différents canaux WDM sont dé multiplexés en fin de propagation à l'aide de filtres optiques ou de démultiplexeurs. La Figure 9décrit le principe du multiplexage en longueur d'onde dans le cas de trois canaux WDM.

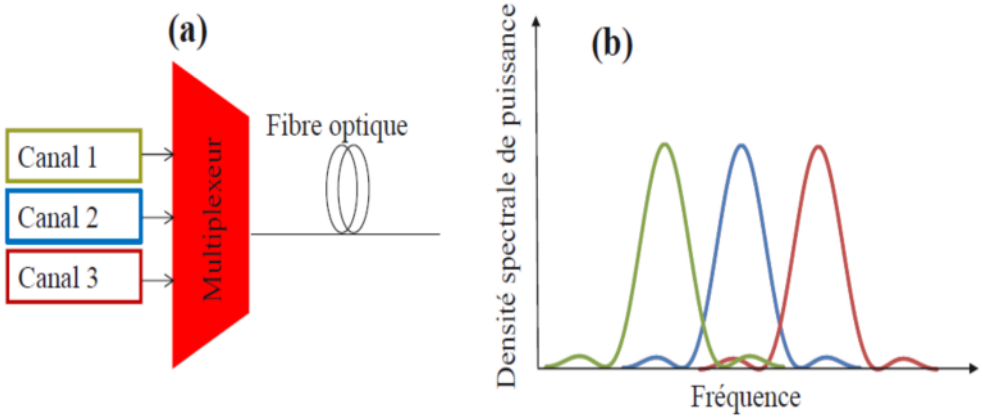


Figure 3.9 : Principe du multiplexage en longueur d'onde (a). Illustration des signaux linéaire dans le cas de trois canaux de transmission (b).

- **Principe du multiplexage en polarisation**

Le multiplexage en polarisation consiste à transmettre des informations différentes suivant deux états de polarisation orthogonaux du signal optique. L'intérêt est de pouvoir transmettre deux fois plus de débit sur une même bande optique. La densité spectrale d'information est alors doublée. Nous illustrons sur la Figure 10 le multiplexage en polarisation dans une configuration où les canaux sont multiplexés en longueur d'onde. Le multiplexage en polarisation est réalisé à l'émission. En effet un séparateur de composante en polarisation (PBS : Polarization Beam Splitter) utilisé à la suite du la se continu permet de séparer le champ optique en deux composantes de polarisations orthogonales. Pour chaque canal WDM, les deux composantes du signal en polarisation sont ensuite modulées puis recombinées à l'aide d'un second PBS encore appelé PBC (Polarization Beam Combiner). Par la suite nous noterons // et ⊥ ces deux états de polarisation orthogonaux.

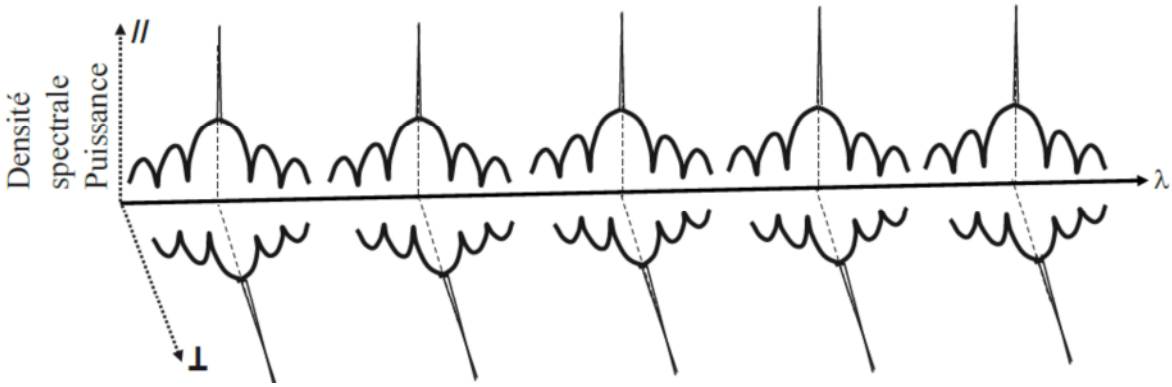


Figure 3.10: Principe du multiplexage en polarisation dans le cas d'un multiplexage en longueur d'onde.

5. Problèmes de transmission par fibre optique

Bien que très performante, la fibre optique subit plusieurs problèmes lors de la propagation du signal : les dispersions et les atténuations.

- **Les dispersions**

Lorsqu'une impulsion se propage en régime linéaire dans une fibre optique, elle subit un phénomène de dispersion qui se traduit par un étalement temporel. Plusieurs types de dispersion existent, contribuant tous à l'étalement de l'impulsion au cours de sa propagation dans le guide.

La dispersion intermodale est la cause principale de l'élargissement des impulsions dans les fibres optiques multi modes. Cet élargissement est provoqué par les différences de temps de

parcours des rayons (ou des modes). La dispersion intermodale est l'élargissement temporel maximum d'une impulsion par unité de longueur de fibre. L'obtention d'une dispersion inter modale réduite se fait en utilisant une fibre à gradient d'indice. Dans le cas d'une fibre optique monomode, cette dispersion est nulle et ne sera donc pas prise en compte.

Quand à la dispersion chromatique, qui est la cause principale de l'élargissement des impulsions dans les fibres optiques monomodes dont le profil est à symétrie de révolution.

Deux effets physiques contribuent à la variation de l'indice de groupe avec la longueur d'onde, d'une part la dépendance de l'indice de la silice avec la longueur d'onde (dispersion du matériau) et d'autre part, le fait que, à profil d'indice fixé, l'indice effectif du mode fondamental dépend des dimensions du guide par rapport à la longueur d'onde (dispersion du guide**)**.

- **Les atténuations**

L'atténuation par connexion, le couplage source-fibre ou fibre-détecteur est l'un des éléments essentiels de la liaison par fibre optique, celui-ci est effectué par des connecteurs d'extrémités. Cette liaison nécessite aussi le raccordement des fibres entre elles d'une manière démontable (connecteurs fibre à fibre) ou permanent. Toute interconnexion doit causer le minimum de pertes.

IV. Les réseaux optiques :

Les réseaux optiques permettent de transporter des signaux sous forme optique et non électrique dans les réseaux classiques. Les avantages de l'optique sont nombreux et seront développés plus loin dans ce chapitre. Les réseaux optiques peuvent être classés en deux catégories : le réseau tout optique, et le réseau non tout optique.

1. Réseau tout optique(ou réseau transparent)

Ce type de réseau n'intègre que des équipements optiques, c'est-à-dire que dans la chaîne de transmission, la conversion optique-électrique n'a pas lieu. La lumière est routée sous sa forme originale et ne subira pas de conversion optique-électrique jusqu' à la destination. Un réseau tout optique ne possède pas de mémoire pour stocker des paquets. Ce type de réseau coûte très cher.

2. Réseau non tout optique

Les réseaux optiques actuels (ne fonctionnant pas en mode tout optique) convertissent et traitent les paquets optiques en électronique, ensuite les gardent pendant le temps nécessaire pour obtenir la ligne demandée. Ce type de réseau est moins cher car les équipements utilisés, électroniques, existent depuis plusieurs années. La figure 11 représente les systèmes optiques.

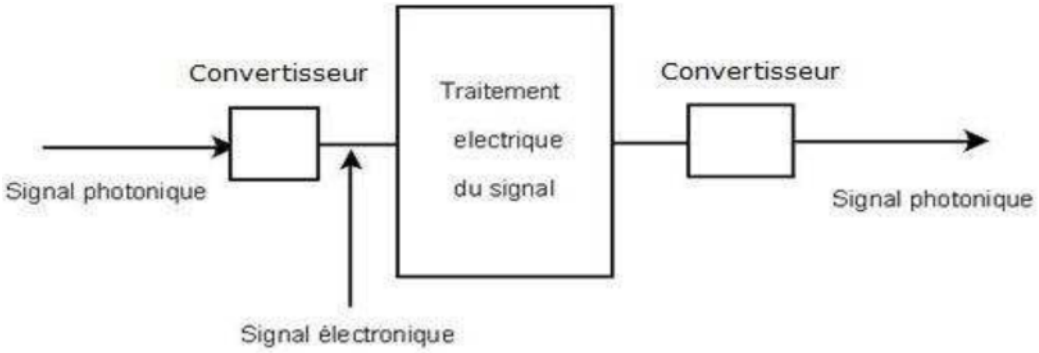


Figure 3.11 : Systèmes optiques

V. TRANSMISSION PAR FIBRE OPTIQUE

1. Propagation dans la fibre optique

- **Propagation d'onde lumineuse**

Lorsqu'un faisceau lumineux heurte obliquement la surface qui sépare deux milieux plus ou moins transparents, il se divise en deux : une partie est réfléchie tandis que l'autre est réfractée. L'indice de réfraction, grandeur caractéristique des propriétés optiques d'un milieu, est le rapport entre la vitesse de la lumière c dans le vide (Cv=299 792 Km/s)et celle de l'onde dans le milieu considéré. Plus l'indice est grand, plus la lumière s'y déplace lentement.
La propagation du signal optique est basée sur la loi de Descartes. Lorsqu'un rayon lumineux entre dans une fibre optique à l'une de ses extrémités avec un angle adéquat, il subit de multiples réflexions totales internes (Figure12). Ce rayon se propage alors jusqu'à l'autre extrémité de la fibre optique, en empruntant un parcours en zigzag.

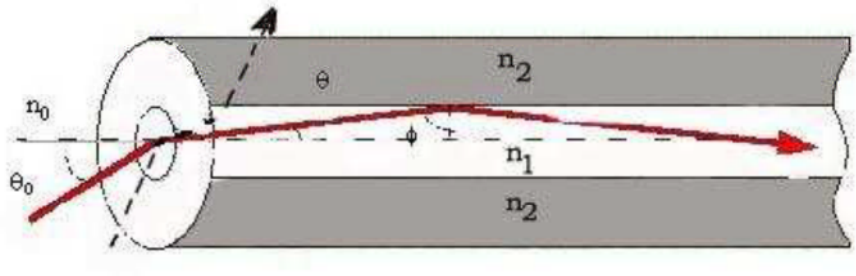


Figure 3.12 : Propagation du signal dans une fibre optique

- **Lois de Descartes**

- Les trois rayons (incident, réfléchi et réfracté) sont dans le même plan (plan d'incidence).
- L'angle d'incidence i1 et l'angle de réfraction i2 sont liés par la relation :

$n_1 \sin i_1 = n_2 \sin i_2$

Avec n1 et n2 sont les indices des deux milieux.

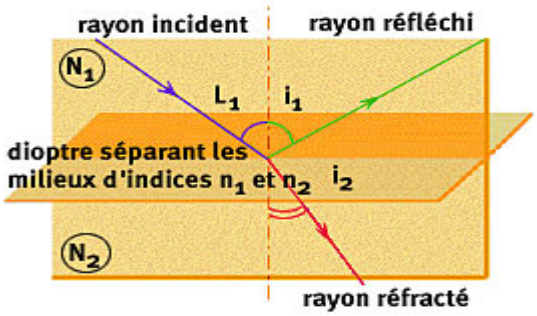


Figure 3.13 : Lois de Descartes

- **Angle limite**

Si $n_1 > n_2$, il est théoriquement possible d'avoir $i_1 = \frac{\pi}{2}$ .Dans ce cas il n'y a pas réfraction mais réflexion totale. On notera i_{iL} l'angle d'incidence correspondant à $i_2 = \frac{\pi}{2}$

La loi de Descartes devient alors:

$$n_1 = \sin(i_{2L}) = n_2 \sin(\frac{\pi}{2}) = n_2$$

D'où $$i_{iL} = \arcsin(\frac{n_2}{n_1})$$

- **Principe de l'ouverture numérique (ON)**

Pour qu'un rayon lumineux arrive à la sortie de la fibre, il doit subir plusieurs réflexions tout au long de la fibre. Or à chaque réflexion une partie de la lumière est réfractée et donc absorbée par la gaine. Le rayon finit alors par être complètement atténué (Figure 14). Cependant il est possible de choisir l'angle d'incidence pour qu'il n y a pas de réfraction soit $i_i < i_{iL}$ .La lumière injectée en entrée arrivera donc en sortie sans aucune atténuation. On définit alors l'ouverture numérique d'une fibre optique en fonction de l'angle d'incidence limite i_{iL} qui permet d'assurer une transmission sans pertes théoriques.

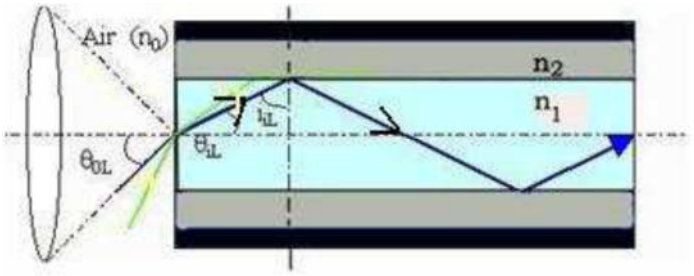


Figure 3.14 : Ouverture numérique d'une fibre optique

Les rayons lumineux à l'intérieur de la fibre attaquent l'interface cœur/gaine à des angles différents. Ceux qui ont un angle supérieur à l'angle limite i_{iL} sont transmis dans le cœur par réflexion totale ; les autres se réfractent dans la gaine et sont rapidement atténués.

Soit n_1 l'indice de réfraction du cœur, n_2 celui de la gaine et n_0 celui de l'air (n_0 =1).

On cherche l'angle incident Θ_{0L} à l'entrée de la fibre, correspondant à l'angle limite i_{iL}.

D'après la loi de Descartes on a :

$$n_0 \sin(\theta_0) = n_1 \sin(\theta_1)$$

Avec $\theta_1 = \frac{\pi}{2} - i_1$ et $n_0 = 1$

Soit:

$$\sin(\theta_{0L}) = n_1 \sin\left(\frac{\pi}{2} - i_{iL}\right) = n_1 \cos(i_{iL}) = n_1\sqrt{1-\sin^2(i_{iL})}$$

Or $$i_{iL} = \arcsin\left(\frac{n_2}{n_1}\right) \Rightarrow \sin(\theta_{0L}) = n_1\sqrt{1-\left(\frac{n_2}{n}\right)^2}$$

On définit alors l'ouverture numérique (ON) d'une fibre par:

$$ON = \sin(\theta_{0L}) = \sqrt{n_1^2 - n_2^2}$$

VI. Conclusion

Dans ce chapitre, nous avons présenté des généralités sur la fibre optique qui est un support de taille pour la transmission fiable de l'information- sachant que les performances réalisées par cette technologie répondent valablement aux besoins des opérateurs des télécommunications ainsi qu'aux utilisateurs privés.

I. Introduction

La sécurité réseau est un enjeu majeur des technologies numériques modernes. Avec le développement de l'Internet et de la notion du partage en général, les besoins en sécurité sont de plus en plus importants. Le développement d'applications Internet telles que le commerce électronique, les applications médicales ou la vidéoconférence, implique de nouveaux besoins comme, l'identification des entités communicantes, l'intégrité des messages échangés, la confidentialité de la transaction, l'authentification des entités, l'anonymat du propriétaire du certificat, l'habilitation des droits, la procuration, etc.. dans ce chapitre on vas parler sur les déférents attaques les mécanisme se la sécurité…

II. Définitions

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

- Sécurité (Safety) protection de systèmes informatiques contre les accidents dus à l'environnement, les défauts du système.
- Security (Security) protection des systèmes informatiques contre des actions malveillantes intentionnelles.

Une vulnérabilité (ou faille) est une faiblesse dans un système informatique.

En général, Le risque en termes de sécurité est caractérisé par l'équation suivante :

- **La menace** représente le type d'action susceptible de nuire dans l'absolu.
- **La vulnérabilité** (appelée parfois faille) représente le niveau d'exposition face à la menace dans un contexte particulier.
- **La contre-mesure** est l'ensemble des actions mises en œuvre en prévention de la menace.

Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système.

III. Services de Sécurité

Un service qui augmente la sécurité des traitements et des échanges de données d'un système. Un service de sécurité utilise un ou plusieurs mécanismes de sécurité (outil conçu pour détecter, prévenir et lutter contre une attaque de sécurité).parmi ces service on trouve :

- **Confidentialité** : c'est est la protection contre les attaques passives des données transmises. Plusieurs niveaux de protection de la confidentialité sont envisageables. Le service le plus général protège toutes les données transmises entre deux utilisateurs pendant une période donnée. Des formes restreintes de ce service peuvent également être définies, incluant la protection d'un message élémentaire ou même de champs spécifiques à l'intérieur d'un message. Un autre aspect de la confidentialité est la protection du flot de trafic contre l'analyse. Cela requiert qu'un attaquant ne puisse observer les sources et destinations, les fréquences, longueurs ou autres caractéristiques du trafic existant sur un équipement de communication.
- **Authentification** : Le service d'authentification permet évidemment d'assurer l'authenticité d'une communication. Dans le cas d'un message élémentaire, tel un signal d'avertissement, d'alarme, ou un ordre detir, la fonction du service d'authentification est d'assurer le destinataire que le message a bien pour origine la source dont il prétend être issu. Dans le cas d'une interaction suivie, telle une connexion d'un terminal à un serveur, deux aspects sont concernés.

En premier lieu, lors de l'initialisation de la connexion, il assure que les deux entités sont authentiques (c'est-à-dire, que chaque entité est celle qu'elle dit être). Ensuite, le service dont assurer que la connexion n'est pas perturbée par une tierce partie qui pourrait se faire passer pour une des deux entités légitimes à des fins de transmissions ou de réceptions non autorisées.

- **Intégrité**: À l'instar de la confidentialité, l'intégrité s'applique à un flux de messages, un seul message, ou à certains champs à l'intérieur d'un message. Là encore, la meilleure approche est une protection totale du flux. Un service d'intégrité orienté connexion, traitant un flot de messages, assure que les messages sont reçus aussitôt d'envoyés, sans duplication, insertion, modification, réorganisation ou répétition.

La destruction de données est également traitée par ce service. Ainsi, un service d'intégrité orienté connexion concerne à la fois la modification de flux de messages et le refus de service. D'un autre côté, un service d'intégrité non orienté connexion, traitant des messages

individuels sans regard sur un contexte plus large, fournit généralement une protection contre la seule modification de message.

- **Non-répudiation**: La non-répudiation empêche tant l'expéditeur que le receveur de nier avoir transmis ou reçu un message. Ainsi, lorsqu'un message est envoyé, le receveur peut prouver que le message a bien été envoyé par l'expéditeur prétendu. De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le message a bien été reçu par le receveur prétendu.
- **Contrôle d'accès**: Dans le contexte de la sécurité des réseaux, le contrôle d'accès est la faculté de limiter et de contrôler l'accès à des systèmes et des applications via des maillons de communications. Pour accomplir ce contrôle, chaque entité essayant d'obtenir un accès doit d'abord être authentifiée, ou s'authentifier, de telle sorte que les droits d'accès puissent être adaptés à son cas.

Une seule entrave à l'un de ces principes remet toute la sécurité en cause.

IV. Les types de piratage informatique

IV.1.Les hackers : ce sont « des passionnés des réseaux ». Ils veulent comprendre le fonctionnement des systèmes informatiques et tester à la fois les capacités des outils et leurs connaissances. En général, les hackers s'introduisent dans les systèmes par passion pour l'informatique et pas dans l'objectif de détruire ou de voler des données.

IV.2. Les Crackers : Sont des criminels informatiques dont leur but principal est de détruire ou voler des données, de mettre hors service des systèmes informatiques ou de 'kidnapper' un système informatique en vue de demander une rançon.

IV.3. Le « carding » : Ces pirates s'attaquent principalement aux systèmes de cartes à puces (en particulier les cartes bancaires) pour en comprendre le fonctionnement et en exploiter les failles.

IV.4. Le phreaking : c'est le détournement de services de télécommunication par divers procédés, dans le but d'éviter les grosses factures de téléphone ou les oreilles indiscrètes. Un autre type de piratage téléphonique est l'utilisation détournée des téléphones cellulaires. Avec ce type de téléphones, aucune connexion physique n'est nécessaire, et il est facile d'écouter les conversations au moyen de scanners GSM et autres. Les téléphones cellulaires sont aussi facilement reprogrammables : les malfaiteurs peuvent ensuite les utiliser sans payer leurs communications, qui seront facturées aux véritables propriétaires.

IV.5. Les Attaques

5.1. Définition

Une attaque est une agression contre une machine locale ou distante pas une personne n'ayant pas le droit sur elle. Tout ordinateur connecté à un réseau informatique peut potentiellement être vulnérable à une attaque.

Sur internet, des attaques ont lieu en permanence à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont en réalité généralement lancées automatiquement à partir d'une machine infectée (virus , chevale de trois, ….), à des fins non connues de la victime et généralement préjudiciable

5.2. Les différentes étapes d'une attaque :

Les attaques de la plus simple à la plus complexe fonctionnent suivant le même schéma:

- **Identification de la cible:** Cette étape est indispensable à toute attaque organisée, elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles.par exemple l'interrogation des serveurs DNS…
- **Le scanning:** L'objectif est de compléter les informations réunies sur une cible visée. Il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles, et des informations de topologie détaillée (OS, versions des services, règles des pare-feu…).
- **L'exploitation:** Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible.
- **La progression:** Il est temps pour l'attaquant de réaliser son objectif. Le but ultime étant d'obtenir les droits de l'utilisateur «root» sur un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations, nettoyage des traces...).

Il existe plusieurs techniques de piratage informatique:

A. Cheval de Troie

Un cheval de Troie (Trojan Horse en anglais) est un logiciel d'apparence légitime, conçu pour exécuter des actions à l'insu de l'utilisateur. En général, il utilise les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée (fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel qui permet à un pirate informatique de prendre, à distance, le contrôle de l'ordinateur). Les chevaux de Troie informatiques sont programmés pour être installés de

manière invisible, notamment pour corrompre l'ordinateur hôte. La principale différence entre les virus, les vers et les chevaux de Troie est que ces derniers ne se répliquent pas. Ils sont divisés en plusieurs sous-classes comprenant entre autres les portes dérobées, les logiciels espions, les injecteurs, etc. On peut en trouver sur des sites malveillants ou autres. Cela dépend de ce que l'utilisateur télécharge.

B. Skimming

Le terme skimming vient de l'anglais « to skim », écrémer. Le skimming consiste à manipuler les automates et terminaux de paiement (bancomats, distributeurs de billets et terminaux de paiement dans les commerces, les stations-service, la restauration, etc.). Pour ce faire, les escrocs se servent d'un équipement spécial introduit dans les automates ou à proximité, qui copie les données contenues sur la piste magnétique de la carte bancaire, de débit ou de crédit et enregistre le code NIP. Les malfaiteurs agissent généralement en bandes organisées.

C. Zombie

En sécurité informatique, une machine zombie est un ordinateur contrôlé à l'insu de son utilisateur par un hacker. Ce dernier l'utilise alors le plus souvent à des fins malveillantes, par exemple afin d'attaquer d'autres machines en dissimulant sa véritable identité.
Un zombie est souvent infesté à l'origine par un ver ou cheval de Troie.
Un réseau de machines zombies peut être constitué et contrôlé par une ou plusieurs personnes, afin d'obtenir une capacité considérable et d'avoir un impact plus important.
Des « armées de zombies », c'est-à-dire de grandes quantités d'ordinateurs compromis, sont utilisées dans les attaques de type « déni de service » ou des tâches diverses comme les envois en masse de courriers non sollicités (spam).
Un réseau de machines zombies peut aussi être utilisé afin de fournir aux hackers une puissance de calcul phénoménale, leur permettant de déchiffrer un code en un temps considérablement plus court que sur une machine seule.

D. Déni de Service

Une attaque par déni de service (en anglais Denial of Service, DoS) est une attaque qui a pour but de mettre hors jeu le système qui est visée.
Ainsi, la victime se voit dans l'incapacité d'accéder à son réseau. Ce type d'attaque peut aussi bien être utilisé contre un serveur d'entreprise qu'un particulier relié à internet. Tous les systèmes d'exploitation sont également touchés : Windows, Linux, Unix, ...

E. Sniffing

Le reniflage (en anglais Sniffing) est une technique qui consiste à analyser le trafic réseau. Lorsque deux ordinateurs communiquent entre eux, il y a un échange d'informations (trafic). Mais, il est toujours possible qu'une personne malveillante récupère ce trafic. Elle peut alors l'analyser et y trouver des informations sensibles.

Exemple : Soit une entreprise possédant 100 ordinateurs reliés entre eux grâce à un hub. Maintenant, si un pirate écoute le trafic réseau entre 8h et 10h (heure de connexion du personnel), il pourra lire tous les noms d'utilisateurs ainsi que leur mot de passe.

Comment s'en protéger ?

Utiliser de préférence un Switch (commutateur) plutôt qu'un hub.

Utiliser des protocoles chiffrés pour les informations sensibles comme les mots de passe.

Utiliser un détecteur de sniffer.

F. Scanning

Le scanning consiste à balayer tous les ports sur une machine en utilisant un outil appelé scanné. Le scanner envoie des paquets sur plusieurs ports de la machine. En fonction de leurs réactions, le scanner va en déduire si les ports sont ouverts. C'est un outil très utile pour les hackers. Cela leur permet de connaitre les points faibles d'une machine et ainsi de savoir par où ils peuvent attaquer. D'autant plus que les scanners ont évolué.

Aujourd'hui, ils peuvent déterminer le système d'exploitation et les applications associées aux ports.

Comment s'en protéger ?

Scanner sa machine pour connaitre les ports ouverts

Surveiller les ports ouverts avec un firewall et fermer ceux qui ne sont pas utiles

Utiliser un IDS (détecteur d'intrusion) ou mieux un IPS (prévention d'intrusion)

G. Social Engineering

Le social engineering est l'art de manipuler les personnes. Il s'agit ainsi d'une technique permettant d'obtenir des informations d'une personne, qu'elle ne devrait pas donner en temps normal, en lui donnant des bonnes raisons de le faire. Cette technique peut se faire par téléphone, par courrier électronique, par lettre écrite, ... Cette attaque est souvent sous estimée puisqu'elle n'est pas d'ordre informatique. Pourtant, une attaque par social engineering bien menée peut se révéler très efficace. Elle n'est donc pas à prendre à la légère.

Comment s'en protéger ?

Avoir du bon sens pour flairer l'arnaque

Se méfier des personnes que l'on ne connaît pas

H. Cracking

Le crackage des mots de passe consiste à deviner le mot de passe de la victime. Malheureusement, beaucoup d'utilisateurs mal avertis de cette technique mettent des mots de passe évidents comme leur propre prénom ou ceux de leurs enfants. Ainsi, si un pirate, qui a espionné sa victime auparavant, teste quelques mots de passe comme le prénom des enfants de la victime, il aura accès à l'ordinateur. D'où l'utilité de mettre des bons mots de passe. Mais même les mots de passe les plus robustes peuvent être trouvés à l'aide de logiciels spécifiques appelés craqueur (John theripper, L0phtCrack pour Windows).

Comment ça marche ?

Les craqueurs de mots de passe s'appliquent souvent à un fichier contenant le nom des utilisateurs ainsi que leur mot de passe encrypté.

Ces fichiers sont nécessaires pour permettre l'authentification sur un système. L'encryptage des mots de passe s'effectue à l'aide d'une fonction de hachage. Les fonctions de hachage sont des fonctions univoques, c'est à- dire qu'il est impossible de les inverser pour décrypter un mot de passe encrypté. Une autre particularité importante des fonctions de hachage est que deux mots de passe différents auront forcément un hachage différent.

Ainsi, il est impossible de décrypter un mot de passe encrypté. En revanche, il est possible d'encrypter un a mot au moyen de cette fonction et de comparer le résultat avec le mot de passe encrypté. S'il y a correspondance, on a deviné le mot de passe. Mais, il est fastidieux d'encrypter des milliers de mots pour trouver les mots de passe. C'est là qu'intervient l'utilité d'un craqueur.

I. Attaque hybride :

Le logiciel teste tous les mots de passe stockés dans un fichier texte et y ajoute des combinaisons. Par exemple, thomas01. Cette méthode est redoutable également puisque beaucoup de personnes mettent des chiffres après leur mot de passe pensant bien faire.

J. Attaque brute-force :

Le logiciel teste toutes les combinaisons possibles. Ainsi ce genre d'attaque aboutit à chaque fois. Heureusement, tester toutes les combinaisons prends beaucoup de temps. D'où l'utilité de

changer de mots de passe régulièrement. Le fichier contenant les mots de passes encryptés est donc à protéger.

Chaque système d'exploitation à sa méthode. Expliquons les méthodes employées par Windows NT, et Unix.

- Windows NT : Ce fichier s'appelle la base SAM. Ce fichier est verrouillé par le noyau dès son démarrage. Ainsi, un utilisateur ne peut pas copier le fichier, ni le lire. Mais, il existe des méthodes permettant de se le procurer.
- Unix : Ce fichier est en fait séparer en deux fichiers shadow et passwd. Le fichier passwd contient les noms d'utilisateurs accessibles par tout le monde, et le fichier shadow contenant les mots de passe, accessible uniquement par root.

Comment s'en protéger ?

Choisir un mot de passe robuste et ne pas l'écrire sur un support (papiers, ...) puisque rien n'empêche un pirate de fouiller les poubelles par exemple.

Un mot de passe robuste doit satisfaire à plusieurs critères :

- plus de 8 caractères
- utiliser la casse (majuscule/minuscule)
- utiliser des chiffres

Une bonne méthode consiste à apprendre par cœur une phrase et à prendre les premières lettres du mot. Changer régulièrement de mot de passe pour éviter que ce dernier ne soit trouvé par un tel outil.

K. Spoofing

L'usurpation (en anglais spoofing) consiste à se faire passer pour quelqu'un d'autre. Il y a beaucoup d'utilité pour un pirate d'usurper une identité. Voici quelques exemples d'usurpations, mais ce ne sont pas les seules :

- Usurpation de l'adresse IP : Une adresse IP correspond en gros à l'adresse postale d'un ordinateur. Ainsi, en changeant d'adresse IP, on peut se faire passer pour un autre ordinateur et obtenir des informations sensibles qui ne nous sont pas destinées.
- Usurpation de l'adresse e-mail : Lors de la réception d'un courrier électronique, nous pouvons lire l'adresse de l'expéditeur. Mais, il est possible de changer l'adresse. Ainsi, un pirate peut vous envoyer un mail en usurpant l'adresse de votre supérieur.
- Usurpation WEB : Ceci est le principe du phishing Généralement, quand on parle d'usurpation ou de spoofing, on parle de l'usurpation de l'adresse IP.

Comment s'en protéger ?

On ne peut pas empêcher quelqu'un d'usurper une identité. En revanche, il faut à tout prix être sûr de l'identité de la machine avec laquelle on dialogue.

Utiliser des protocoles sécurisés comme ssh qui empêche le spoofing.

L. Man in the Middle

Man in the Middle signifie l'homme au milieu. Cette attaque a pour but de s'insérer entre deux ordinateurs qui communiquent. Soient deux ordinateurs A et B voulant dialoguer. Maintenant, si un pirate décide de se faire passer pour l'ordinateur A auprès de B et de B auprès de A, ainsi, toute communication vers A ou B passera par le pirate, l'homme au milieu.

Quels sont les risques ?

Le pirate peut donc intercepter tout le trafic, à savoir les informations sensibles comme les mots de passe. Mais, pire encore, le pirate peut modifier le trafic avant de le renvoyer vers l'autre ordinateur.

Ainsi, si vous voulez commander un livre sur internet à 10 euros, et que le pirate change votre commande, vous pouvez très vite vous retrouver à dépenser des milliers d'euros.

Comment s'en protéger ?

Sur Internet, n'achetez que sur des sites sécurisés.

Les sites sécurisés commencent par "https" au lieu de "http". Il y a également un cadenas en bas de votre navigateur. Sur un réseau, utilisez des protocoles sécurisés.

M. Hijacking

Un pirate peut craquer (cible) le mot de passe de la session. Mais si vous choisissez un mot de passe robuste, cela lui prendra beaucoup de temps.

Alors pourquoi ne pas attendre que la victime se connecte sur la session et prendre sa place ? Ainsi, le pirate contourne le processus d'authentification. Et justement, il le fait, c'est le principe du détournement de session (en anglais hijacking). Ensuite, s'il veut pouvoir dialoguer avec le serveur, il doit mettre hors-jeu la victime. Pour cela, il peut lui lancer une attaque par déni de service (cible). Mais, il peut aussi se mettre en écoute et enregistrer tout le trafic en espérant recueillir des informations sensibles comme des mots de passe.

Quels sont les risques ?

Si le pirate possède des informations sensibles comme un nom d'utilisateur et son mot de passe, il pourra alors revenir sur le système lorsqu'il le souhaitera a l'aide d'une backdoor. Pire encore, si la machine possède des liens d'approbation, l'attaquant en bénéficiera. Et il sera dur

d'identifier que le système est compromis puisqu'il utilise le compte d'une personne autorisée. D'où l'importance de détecter cette attaque.

Comment s'en protéger ?

S'assurer que la communication est sécurisée.

N. Buffer OverFlow

Un débordement de tampon (en anglais Buffer OverFlow ou BoF) est une attaque très utilisée des pirates. Cela consiste à utiliser un programme résidant sur votre machine en lui envoyant plus de données qu'il n'est censé en recevoir afin que ce dernier exécute un code arbitraire. Il n'est pas rare qu'un programme accepte des données en paramètre. Ainsi, si le programme ne vérifie pas la longueur de la chaîne passée en paramètre, une personne malintentionnée peut compromettre la machine en entrant une donnée beaucoup trop grande.

Comment ça marche ?

Les données entrées par l'utilisateur sont stockées temporairement dans une zone de la mémoire appelée tampon (en anglais buffer). Prenons l'exemple d'un logiciel qui demande votre prénom. En admettant que le programme prévoit dix caractères pour ce dernier et que l'utilisateur en mette vingt. Il y aura débordement de tampons puisque les dix derniers caractères ne seront pas stockés dans la bonne variable mais dans le tampon pouvant provoquer un crash de la machine. Mais, un pirate exploite cette faille malignement et parvient à se procurer d'un accès à la machine avec des droits identiques à celle du logiciel.

Comment s'en protéger ?

Malheureusement, vous ne pouvez pas y faire grand chose. En effet, le principe de cette attaque est différent des autres, dans le sens où ce n'est pas la protection de l'ordinateur qui vous protégera d'un débordement de tampon puisqu'elle utilise le manque de rigueur de la part des programmeurs de logiciels en raison du manque de temps.

O. Virus :

Un virus est un segment de programme qui, lorsqu'il s'exécute, se reproduit en s'adjoignant à un autre programme (du système ou d'une application), et qui devient ainsi un cheval de Troie. Puis le virus peut ensuite se propager à d'autres ordinateurs (via un réseau) à l'aide du programme légitime sur lequel il s'est greffé. Il peut également avoir comme effets de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. PsybOt, découvert en 2009, est considéré comme étant le seul virus informatique ayant la capacité d'infecter les routeurs et modems haut-débit.

P. Ver:

Un ver est un programme autonome qui se reproduit et se propage à l'insu des utilisateurs. Contrairement aux virus, un ver n'a pas besoin d'un logiciel hôte pour se dupliquer. Le ver a habituellement un objectif malicieux, par exemple : espionner l'ordinateur dans lequel il réside; offrir une porte dérobée à des pirates informatiques; détruire des données sur l'ordinateur infecté; envoyer de multiples requêtes vers un serveur internet dans le but de le saturer.

Le ver Blaster avait pour but de lancer une attaque par déni de service sur le serveur de mises à jour de Microsoft.

Q. porte dérobée (backdoor) :

Ouvreur d'un accès frauduleux sur un système informatique, à distance.

R. Logiciel espion (spyware) :

Collecteur d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation, et en envoyant celles-ci à un organisme tiers.

I. Politique de sécurité :

Pour qu'un système puisse fournir des services de sécurité, plusieurs mécanismes peuvent être mis en place, tel que le chiffrement, les signatures numériques, les certificats… nous allons présenter dans ce qui suit quelques mécanismes qui assurent les services de sécurité les plus importants.

IV.6.Cryptage et décryptage

Les données lisibles et compréhensibles sans intervention spécifique sont considérées comme du texte en clair. La méthode permettant de dissimuler du texte en clair en masquant son contenu est appelée le cryptage. Le cryptage consiste à transformer un texte normal en charabia inintelligible appelé texte chiffré. Cette opération permet de s'assurer que seules les personnes auxquelles les informations sont destinées pourront y accéder. Le processus inverse de transformation du texte chiffré vers le texte d'origine est appelé le décryptage.

La Figure 1 illustre ce processus.

Figure 4.1 : Cryptage et décryptage

6.1. Définition de la cryptographie

La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage de données. Elle vous permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse les lire.

Alors que la cryptographie consiste à sécuriser les données, la cryptanalyse est l'étude des informations cryptées, afin d'en découvrir le secret. La cryptanalyse classique implique une combinaison intéressante de raisonnement analytique, d'application d'outils mathématiques, de recherche de modèle, de patience, de détermination et de chance. Ces cryptanalystes sont également appelés des pirates.

6.2. Mécanismes de la cryptographie

Un algorithme de cryptographie ou un chiffrement est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est associé à une clé (un mot, un nombre ou une phrase), afin de crypter le texte en clair. Avec des clés différentes, le résultat du cryptage variera également.

La sécurité des données cryptées repose entièrement sur deux éléments : l'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clé.

Un système de cryptographie est constitué d'un algorithme de cryptographie, ainsi que de toutes les clés et tous les protocoles nécessaires à son fonctionnement.

PGP est un système de cryptographie.

6.3. Les méthodes de cryptographie actuelle :

Pour assurer la confidentialité d'un document électronique, on a qu'à chiffrer le texte du document. Cette opération consiste à appliquer une fonction mathématique (en fait c'est un ensemble de fonctions) avec des caractéristiques très particulières sur le texte. Cette fonction utilise une variable, la clé de chiffrement, qui est une suite de bits quelconque. Une fois le

texte chiffré, il est illisible. Pour obtenir la version lisible, il faut le déchiffrer, c'est-à-dire appliquer une autre fonction mathématique, compatible avec la première, avec une autre variable, la clé de déchiffrement. Ces 2 fonctions mathématiques sont appelées algorithmes de chiffrement. La valeur de la clé de déchiffrement dépend évidemment de la valeur de la clé de chiffrement et uniquement le possesseur de la clé de déchiffrement peut déchiffrer le texte. Lorsque l'on désire transmettre un document confidentiel à un correspondant à travers le réseau, on chiffre le document sur son poste de travail avec une clé de chiffrement et on envoie la version chiffrée. Le destinataire déchiffre le document sur son poste de travail avec la clé de déchiffrement, qu'il est le seul à connaître. Si une troisième personne intercepte le texte durant le transfert, il ne pourra pas le déchiffrer car il ne connaîtra pas la valeur de la clé de déchiffrement.

Il faut noter que les algorithmes de chiffrement, c'est à dire les formules mathématiques, sont publics et ont fait l'objet de standardisation. C'est le secret de certaines clés qui permet à ces algorithmes d'assurer le service de confidentialité et non la confidentialité de l'algorithme lui même.

Il y a deux grandes familles d'algorithmes de chiffrement : les algorithmes symétriques et asymétriques.

A. Algorithmes symétriques :

Dans les algorithmes symétriques, aussi appelés algorithmes à clé secrète, la clé de chiffrement est la même que la clé de déchiffrement. De ce fait, pour que le texte chiffré ne soit lisible que par le destinataire, la valeur de cette clé doit être un secret partagé entre l'émetteur et le destinataire uniquement. Ceci explique le qualificatif de « clé secrète ». DES est l'algorithme symétrique historiquement le plus connu. Il utilise des clés (de chiffrement et de déchiffrement) qui font 56 bits (c'est la taille réellement utilisée). Une version améliorée, qui le remplace maintenant, Triple DES utilise des clés de 112 bits.

Les premiers algorithmes symétriques datent de la fin des années 70 et utilisent des fonctions mathématiques « simples ». L'avantage est que les opérations de chiffrement et de déchiffrement sont rapides à exécuter sur des ordinateurs classiques.

Par contre, le problème est la gestion des clés. En effet, chaque clé que l'on utilise avec un correspondant doit être secrète et unique. On a donc autant de clés que de correspondants et il faut trouver un moyen d'échanger chaque clé secrète avec chaque correspondant de manière sûre. Si ceci est possible entre un groupe restreint de personnes, c'est impossible à plus grande échelle, par exemple pour échanger des messages chiffrés avec tous nos correspondants sur l'Internet.

B. Cryptographie Asymétrique

La cryptographie à clef publique utilise deux clefs. La première demeure privée, tandis que la seconde est publique. Si l'on utilise la clef publique pour chiffrer un message, la clef privée permet de le déchiffrer. Autrement dit, il suffit de chiffrer un message à expédier à l'aide de la clef publique du destinataire, et ce dernier peut ensuite utiliser la clef privée pour le déchiffrer

6.4. La signature numérique

La cryptographie à clef publique8 rend possible l'utilisation des signatures numériques. Celles-ci permettent de corroborer l'origine d'un message. Pour «signer» un message, on utilise une fonction mathématique qui produit un résumé du message (Hash). Le résumé obtenu est chiffré à l'aide de la clef privée de l'expéditeur. Le résultat, qui constitue la signature numérique, est annexé au message. Le destinataire du message peut ensuite s'assurer de l'origine du message et de l'intégrité de l'information qu'il contient en déchiffrant la signature numérique au moyen de la clef publique de l'expéditeur, puis en comparant le résultat avec le résumé obtenu en appliquant la même fonction mathématique au message reçu. Cela semble un peu compliqué, mais en pratique, il suffit de cliquer sur une icône à l'écran pour lancer tout le processus.

IV.7.Para feu

7.1. Définition d'un pare feu

Pour parer aux attaques réseau, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture est basé sur un firewall. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela représente une sécurité supplémentaire rendant le réseau ouvert sur Internet beaucoup plus sûr.

De plus, il peut permettre de restreindre l'accès interne vers l'extérieur. En effet, des employés peuvent s'adonner à des activités que l'entreprise ne cautionne pas, le meilleur exemple étant le jeu en ligne. En plaçant un firewall limitant ou interdisant l'accès à ces services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.

Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données. Il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseaux suivantes:

- Une interface pour le réseau à protéger (réseau interne).

- Une interface pour le réseau externe.

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système Firewall sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le trafic ;
- Le système soit sécurisé ;
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

7.2. Fonctionnement d'un système Firewall

Un système Firewall contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow)
- De bloquer la connexion (deny)
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées :

« TOUT CE QUI N'EST PAS EXPLICITEMENT AUTORISE EST INTERDIT »

- Soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

IV.8.VPN « Virtual Private Network »

VPN ont aujourd'hui pris une place importante dans les réseaux informatique et l'informatique distribuée. Nous verrons ici quelles sont les principales caractéristiques des VPN.

8.1. Principe général

Un réseau VPN repose sur un protocole appelé « protocole de tunneling ». Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en

empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.
Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans Ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de dés encapsulation.

8.2. Fonctionnalités des VPN

8.2.1. Les VPN d'accès

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé.
L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. Il existe deux cas :
L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.

8.2.2. L'Intranet VPN

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage « infaillible ». Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable.

8.2.3. L'Extranet VPN

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

8.3 Caractéristiques fondamentales d'un VPN

Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes :

- Authentification d'utilisateur. Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel.
- Gestion d'adresses. Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pourvoir se connecter facilement au réseau et recevoir une adresse.
- Cryptage des données. Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
- Gestion de clefs. Les clefs de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.

IV.9.DMZ « Zone Démilitarisée »

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « zone démilitarisé » (notée DMZ pour De Militarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile. La figure ci-dessous montre la position d'une DMZ au sein d'un réseau. Les serveurs situés dans la DMZ sont appelés « bastions » en raison de leur position d'avant poste dans le réseau de l'entreprise.
La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ autorisé ;
- Trafic du réseau externe vers le réseau interne interdit ;

- Trafic du réseau interne vers la DMZ autorisé ;
- Trafic du réseau interne vers le réseau externe autorisé ;
- Trafic de la DMZ vers le réseau interne interdit ;
- Trafic de la DMZ vers le réseau externe interdit.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.
Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

IV.10.NAT « Network Address Translation »

10.1. Principe du NAT

Le mécanisme de traduction (translation) d'adresses « NAT » a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4 (le protocole IPv6 répondra à terme à ce problème).
En effet, en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines nécessitant d'être connectées à internet de l'être.
Le principe du NAT consiste donc à utiliser une adresse IP routable (ou un nombre limité d'adresses IP) pour connecter l'ensemble des machines du réseau en réalisant, au niveau de la passerelle de connexion à internet, une translation (littéralement une « traduction ») entre l'adresse interne (non routable) de la machine souhaitant se connecter et l'adresse IP de la passerelle.
D'autre part, le mécanisme de réduction d'adresses permet de sécuriser le réseau interne étant donné qu'il camoufle complètement l'adressage interne. En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de la même adresse IP.

10.2. “Translation” statique

Le principe du NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur (ou plus exactement la passerelle) permet donc d'associer à une adresse IP privée (par exemple 192.168.0.1) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.

La “translation” d'adresse statique permet ainsi de connecter des machines du réseau interne à internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où n adresses IP routables sont nécessaires pour connecter n machines du réseau interne.

10.3. Avantages et inconvénients du NAT statique

En associant une adresse IP publique à une adresse IP privée, nous avons pu rendre une machine accessible sur Internet. Par contre, on remarque qu'avec ce principe, on est obligé d'avoir une adresse publique par machine voulant accéder à Internet. Cela ne va pas régler notre problème de pénurie d'adresses IP... D'autre part, tant qu'à donner une adresse publique par machine, pourquoi ne pas leur donner cette adresse directement plutôt que de passer par un intermédiaire ? A cette question, on peut apporter plusieurs éléments de réponse. D'une part, il est souvent préférable de garder un adressage uniforme en interne et de ne pas mêler les adresses publiques aux adresses privées. Ainsi, si on doit faire des modifications, changements, interventions sur le réseau local, on peut facilement changer la correspondance entre les adresses privées et les adresses publiques pour rediriger les requêtes vers un serveur en état de marche. D'autre part, on gâche un certain nombre d'adresses lorsqu'on découpe un réseau en sous-réseaux (adresse de réseau, adresse de broadcast...), comme lorsqu'on veut créer une DMZ pour rendre ses serveurs publiques disponibles. Avec le NAT statique, on évite de perdre ces adresses.

Malgré ces quelques avantages, le problème de pénurie d'adresses n'a toujours pas été réglé. Pour cela, on va se pencher sur la NAT dynamique.

V. Conclusion

Quels que soient les moyens mis en œuvre, du fait de l'ouverture vers l'extérieur, les réseaux seront de plus en plus vulnérables. Dans ses conditions, il appartient à chaque entreprise démesurer le risque et le coût d'une indisponibilité de leur système, de la divulgation d'information...et déterminer une politique dite de sécurité, d'en mesurer les coûts et d'assurer en permanence une veille technologique pour que les moyens employés restent efficaces devant l'évolution des menaces.

I. Introduction

La conception est une étape décisive à la création d'un réseau, elle permet dès le début de garantir la rapidité et la stabilité du réseau. Si un réseau n'est pas conçu d'une manière adéquate, de nombreux problèmes imprévisibles risquent de se produire et de nuire à sa croissance. La conception est donc un travail de profondeur, demandant une véritable compétence venant du concepteur, en effet il ne suffit pas d'interconnecter les ordinateurs. Ainsi, le Chapitre traite tous les détails nécessaires à la réalisation effective du réseau.

II. INFRASTRUCTURE DU RESEAU

Le débit transporté dans les réseaux des télécommunications ne cesse d'augmenter ; le transport des voix, des données, et des images en sont les causes principales. De plus, avec l'expansion de l'utilisation de l'Internet à l'échelle mondiale, de nombreux nouveaux services à haut débit ont été développés à la fois pour les particuliers, les entreprises et les universités (débit entre 1 et 100 Mbit/s).

Pour répondre au mieux aux besoins des utilisateurs du réseau, il est nécessaire de connaître les infrastructures déjà en place. Notons au préalable, qu'en matière de conception, il est nécessaire de répondre non seulement aux besoins identifiés aujourd'hui, mais également d'anticiper l'évolution des usages de demain.

a) Situation actuelle

- Présentation du site

Actuellement, la Direction Territoriale des Télécommunications, à Tizi-Ouzou est constituée de 10 départements :

Département Personnel

Département Commerciale

Département Logistique

Département des Réseaux d'abonnés

Département des Réseaux d'entreprises

Département des Réseaux de base (c'est a ce niveau on va faire notre serveur central)

Département Centre d'énergie et d'environnement

Département Centre d'entreprise des lignes

Département Centre d'équipements de Télécom

Département Centre d'ingénierie des lignes

Certains de ces départements disposent déjà de matériels informatiques, mais insuffisants et assez vétustes, ainsi que des réseaux internes qui ne sont pas interconnectés. La plupart des départements ayant des ordinateurs ne sont pas connectés à l'Internet et se trouvent donc isolés des autres départements. Cette situation constitue un handicap.

b) Les distances physiques entre les départements

Pour assurer la mise en place des réseaux à fibre optique au sein du la Direction, il faut connaître d'abord les distances physiques qui séparent le centre informatique avec les différents départements. Le tableau 3 ci-dessous présente ces distances.

Département	Distances (m)
Réseaux de base – Centre des entreprises des lignes	50
Réseaux de base –Réseaux abonnée	80
Réseaux de base –Réseaux des entreprises	190
Réseaux des entreprises –équipement de télécom	30
Centre des entreprises des lignes -Centre d'énergies et d'environnement	20
Réseaux de base – Logistique	80
Réseaux de base – Personnel	60
Centre d'énergies des lignes –Réseaux abonnée	10
Réseaux de base – Commerciale	500

Tableau 5.1 : Les distances physiques entre les départements

III. Regroupements des besoins de conception

L'Internet est le vecteur d'information dominant dans les réseaux de télécommunications actuels. Il a permis de développer de nombreux services, surtout ceux qui sont liés aux multimédias. Afin de satisfaire les exigences des usagers et d'assurer ainsi une meilleure qualité aux services proposés par les fournisseurs d'accès, les applications proposées sont de plus en plus gourmandes en bande-passante.

Côté utilisateurs, une enquête des besoins a été réalisée auprès des différentes cibles : départements, services administratifs…Les besoins se basent sur les échanges actuels, Emails, fichiers textes, tableurs, quelques images, et aussi sur les connexions permanentes à l'Internet. En tant que justification du haut débit, les utilisateurs pensent à des transmissions qui supportent les grandes applications comme la vidéo (vidéoconférence).

Comme la Direction Territoriale des Télécommunications s'étale sur une zone relativement vaste, avec ses bâtiments et blocs dispersés et éloignés les uns des autres. On doit employer un réseau de communication de type LAN ou réseau local qui répondra aux besoins pour les années à venir.
On constate alors que la fibre optique est l'une des solutions pour résoudre les problèmes actuels : elle offre

- Le moyen de transfert le plus rapide par rapport aux autres câbles,
- Les supports de communications à longue portée,
- Le support de communications à haut débit.
- Et un meilleur rapport qualité/prix.

Par rapport au câblage à paires torsadées dont la portée maximale est de 100 mètres.

IV. ARCHITECTURE DU RESEAU

Le modèle OSI peut être divisé en deux groupes, la partie haute et la partie basse.
Nous allons travailler en particulier dans la couche physique.

a. Architecture physique

Le câblage physique est l'un des éléments les plus importants à prendre en considération lors de la conception d'un réseau. Les médias de câblage que nous allons utiliser pour la couche 1 comprennent le câble à paires torsadées, blindées de catégorie 5 (STP) et le câble à fibre optique. Une topologie physique en étoile étendue est adaptée à notre situation.
La figure représente l'interconnexion physique des réseaux locaux de chaque département entre eux, cette connexion est assurée par le support en fibre optique et/ou en paire torsadée. L'architecture présente un avantage indéniable sur l'évolutivité du réseau. Car le réseau est réalisé dans un commutateur unique central se trouvant sur le centre informatique du site, facilitant ainsi le renouvellement des principaux équipements. On peut imaginer aussi un réseau en topologie en bus ou en anneau qui parcoure chaque département et auquel on connecte les *Switchs*, mais cette solution n'est pas convenable car le débit est limité par la technologie utilisée.
Certains départements sont directement connectés au commutateur central se trouvant dans le Centre Informatique (Fig.5.1, Fig.5.2). Cette solution permet de réduire le coût global de l'installation car elle minimise la longueur des fibres optiques utilisées.

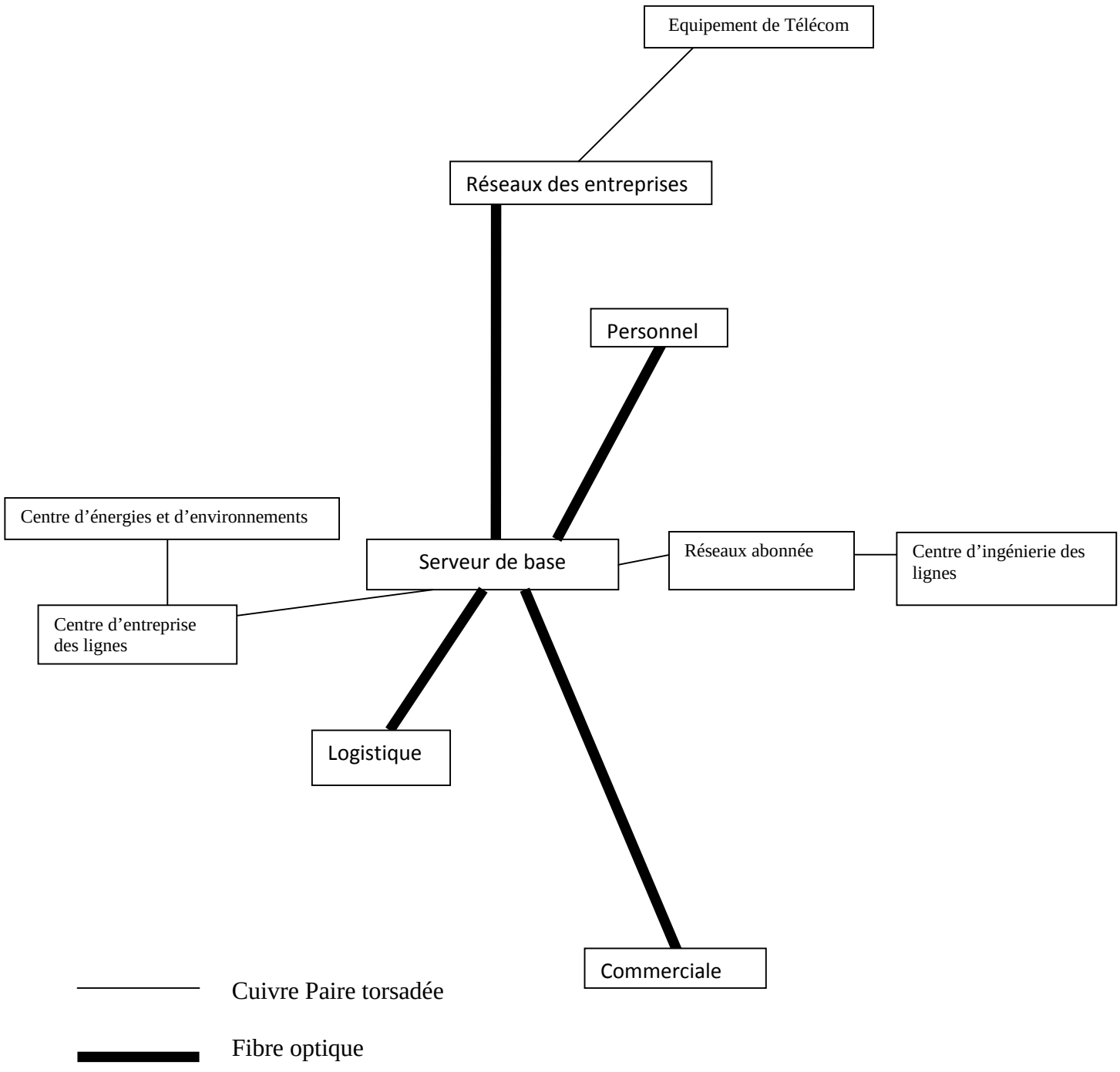


Figure 5.1 : Schéma physique de l'infrastructure de liaison

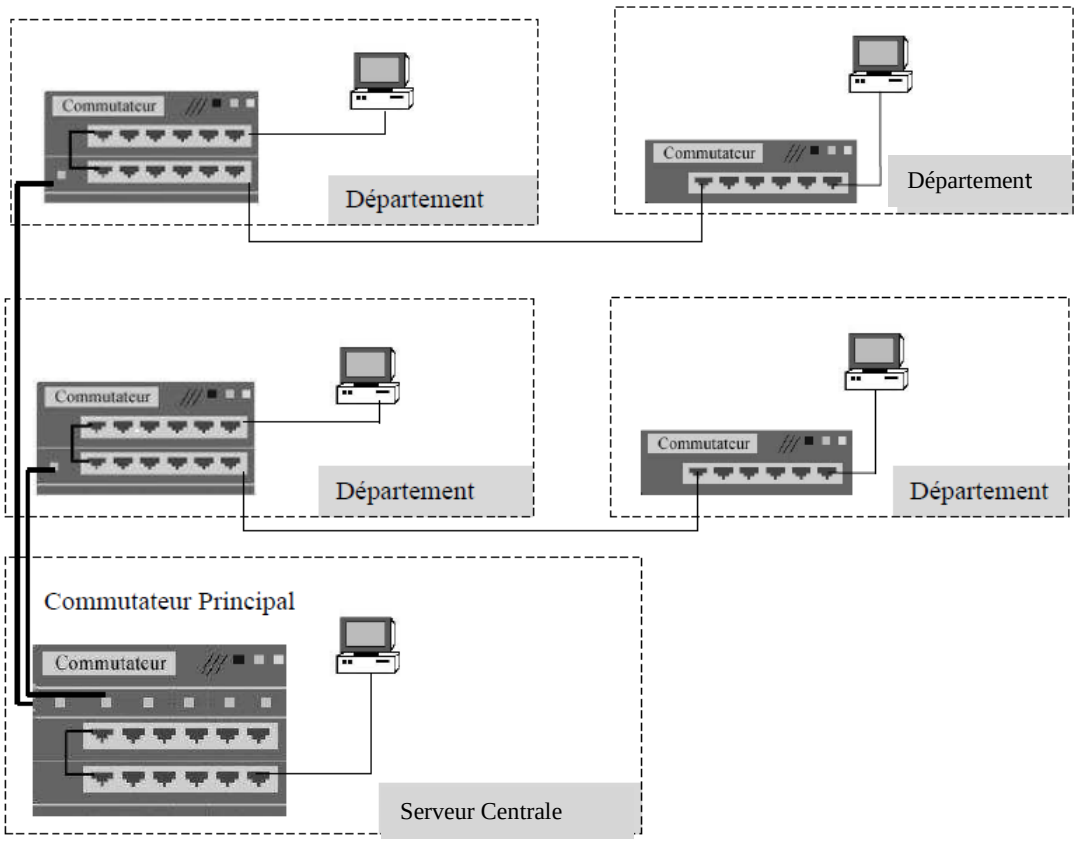


Figure 5.2 : Raccordement physique des équipements

b. Les équipements actifs

Les éléments actifs constituant le réseau sont décrits brièvement ci-après.

- **Routeur**

Le routeur est un équipement concernant la couche 3 du modèle OSI ; ainsi il peut connecter différentes technologies de couche 2, telles qu'Ethernet, Token-Ring et FDDI.

Un routeur est un commutateur de niveau 3, il commute les protocoles de la couche réseau, tels que l'IP, appelé encore routage. Ce mécanisme consiste à analyser l'adresse de destination du paquet IP et à la transmettre sur le bon port. En tant que machine clé d'un réseau, un routeur est un dispositif (interface) recevant et émettant les trames au format adéquat ; il constitue aussi une partie logiciel qui fonctionne comme un système d'exploitation permettant une administration matérielle.

- **Commutateur ou Switch**

La commutation est une technologie qui permet d'atténuer la congestion au sein des LAN Ethernet, en réduisant le trafic et en augmentant la bande passante. Les commutateurs LAN sont souvent utilisés pour remplacer des concentrateurs partagés (Figure). Ils sont conçus pour fonctionner avec les infrastructures de câblage déjà en place. Ainsi, ils peuvent être installés sans perturber le trafic réseau existant.

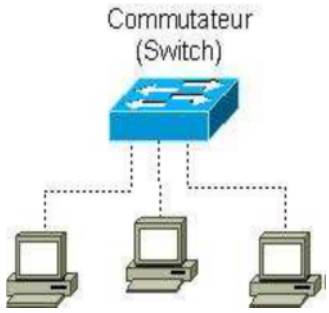


Figure 5.3 : Commutateur ou Switch

- **Convertisseur de Média (Media Converter)**

La technologie de la conversion permet de connecter des types de médias disparates (câblage) dans des réseaux équipés d'un câblage non homogène. La plupart du temps, on utilise les Convertisseurs de Média dans des installations de câblage réseau où coexistent un câblage cuivre STP (paire torsadée blindée) et un câblage à fibre optique. Ce convertisseur réduit considérablement le coût du réseau. En effet, les équipements réseau à interface optique coûtent plus chers que leur équivalent en cuivre, ceci est largement lié au coût supérieur de leurs composants et à leur moindre volume.
On mettra donc un Convertisseur de Media sur chaque terminaison de fibre optique dans le réseau. Cet équipement sera transparent car elle n'affecte en rien à la circulation des données sur le réseau.
La figure 5.4 illustre le fonctionnement d'un Convertisseur de Média.

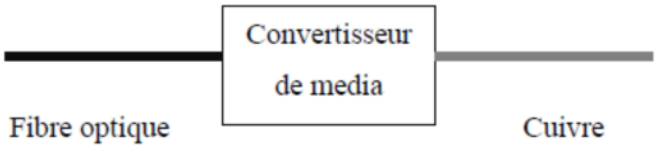


Figure 5.4 : Fonctionnement d'un Convertisseur de Media

- **Cartes réseaux**

Une carte est considérée comme un composant de couche 2 du modèle OSI, parce que chaque carte réseau dans le monde porte identifiant unique appelé adresse MAC (Media Access Control). Cette adresse est utilisée pour contrôler la communication des données de l'hôte dans le réseau. Tous les ordinateurs sur le réseau en possèdent au moins une.

V. INFRASTRUCTURE DE L'INSTALLATION

L'essentiel des coûts de mise en œuvre d'un réseau optique réside dans les travaux de génie civil. Ces infrastructures réalisées dès les premières phases devront satisfaire aux exigences de croissance du réseau. La mise en place du réseau à fibre optique sur la Direction nécessite plusieurs étapes pour que le réseau soit déployé correctement et fonctionne sans erreur, dès la mise en service.

a. Cheminement et circulation des câbles

Le câblage volant (à l'intérieur ou à l'extérieur des bâtiments) ne peut pas être considéré à grande échelle. En effet au-delà de dix postes, il devient rapidement source de problèmes. Le câblage extérieur est enfui sous terre, et le câblage intérieur va passer au dessus des plafonds et circule dans une goulotte le long des murs. Cette méthode de câblage a l'avantage de la sécurité. Mais les liaisons en cuivre inter-bâtiments sont aériennes. Il est essentiel de mettre en place un système de câblage permanent et évolutif.

- Distribution intérieure et extérieure des câbles

Les câbles à fibre optique, insensibles aux perturbations électromagnétiques, pourront être installés, si besoin est, dans les gaines techniques existantes pour les câbles d'énergie. Ou encore avec les câbles en cuivre dan un nouveau tube qui longe les murs ou au-dessus des plafonds. Les câbles pour les distributions extérieures sont dotés de renfort mécanique, adaptés à l'environnement qui l'entoure. Les Infrastructures doivent être conçues pour respecter les conditions imposées par les contraintes. La figure présente le schéma bloc de l'infrastructure de déploiement.

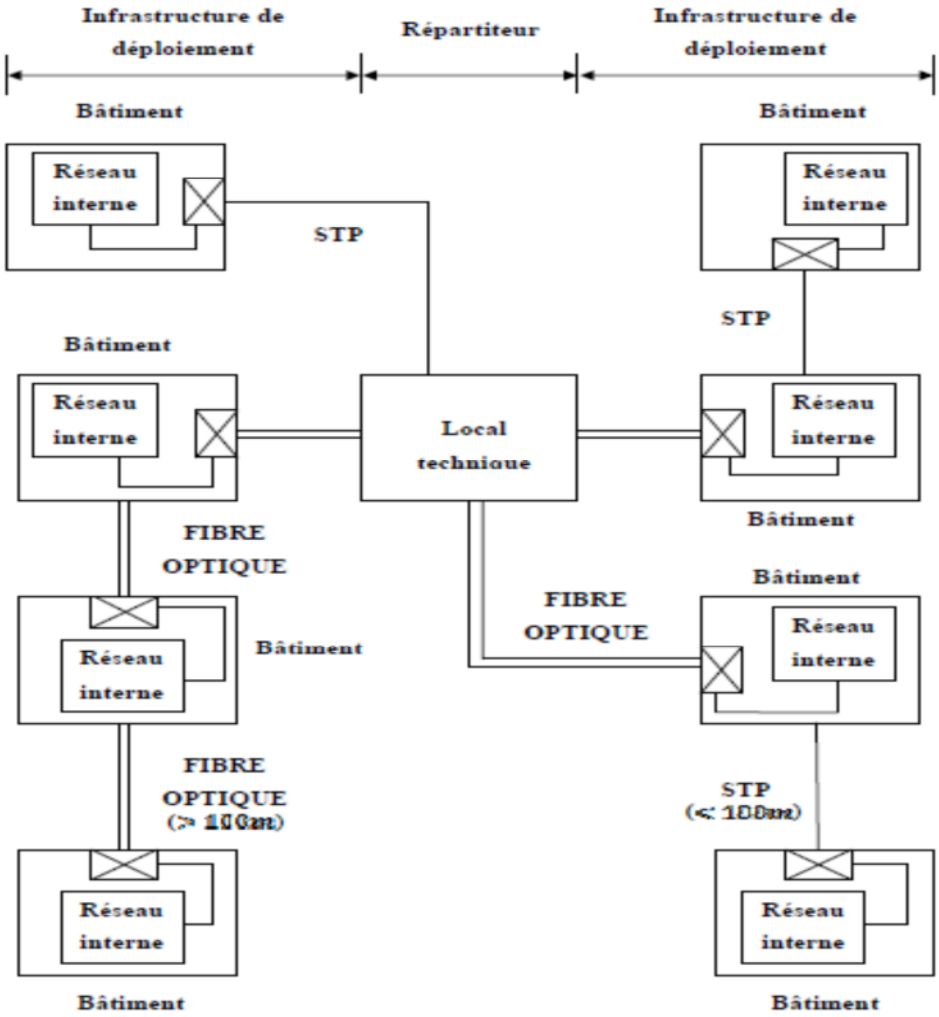


Figure 5.5: schéma bloc du déploiement des câbles

- **Chemins des câbles**

La planification pour des longueurs de câbles appropriées est extrêmement importante pour une installation de fibre optique pour deux raisons. La plus importante est que les épissures causent des pertes dans la qualité et la puissance du signal, dans le cas où les câbles seraient trop courts et qu'il faudrait les relier. Les câbles coûtent chers, donc surtout ne pas les jeter. La deuxième raison est que les épissures prennent beaucoup de temps et sont très couteux.

- **Les distances et les câbles à utiliser**

Nous allons regrouper en deux au maximum bâtiments pour minimiser le coût de l'installation. Le choix du câble dépend de la distance que ce câble va parcourir. La distance de transmission maximale pour le câblage en cuivre est de 100 m. Par contre, la distance de transmission pour la fibre optique multimode à gradient d'indice 62.5/125 est de 2km.

Le tableau récapitule les distances et les types de câbles à utiliser. Lors de la réalisation des travaux, les mesures exactes seront faites par des personnes expérimentées, et seront exactes et précises. Car il est pratiquement impossible pour les concepteurs de prévoir tous les états et les conditions des terrains, et ce n'est pas aux concepteurs de le faire.

La mesure sur le terrain doit être faite pour que les longs morceaux de câbles ne soient pas recoupés et les morceaux courts ne soient pas gaspillés.

Département	Distances (m)	Liaison
Réseaux de base – Centre des entreprises des lignes	60	Fibre optique
Réseaux de base –Réseaux abonnée	90	Fibre optique
Réseaux de base –Réseaux des entreprises	200	Fibre optique
Réseaux des entreprises –équipement de télécom	40	STP
Centre des entreprises des lignes -Centre d'énergies et d'environnement	30	STP
Réseaux de base – Logistique	90	Fibre optique
Réseaux de base – Personnel	70	Fibre optique

Centre d'énergies des lignes –Réseaux abonnée	20	STP
Réseaux de base – Commerciale	510	Fibre optique

Tableau 5.2: distances et câbles utilisées

- **Canalisation sous-terraine**

Dimension du canal

La canalisation doit être assez profonde pour la sécurité des câbles, mais pas trop profonde pour la facilité de l'installation. Un compromis est le standard de 70 cm de profondeur et de 40 cm de largeur, comme le montre la figure.

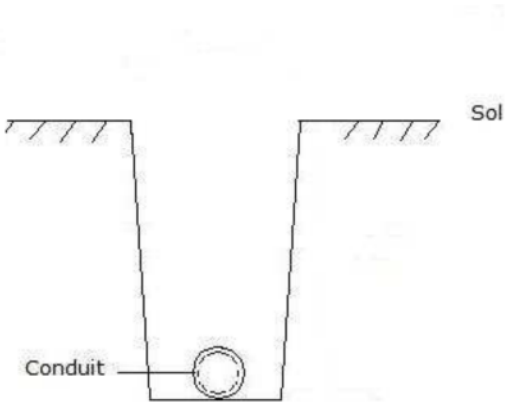


Figure 5.6 : Canalisation

Conduits et fourreaux

Les conduits protègent les câbles contre les rongeurs et contre l'humidité. Les conduits sont en effets en polychlorure de vinyle (P.V.C) qui ont une forte résistance, une longue durée de vie et insensible à la rouille. Ils facilitent aussi l'installation d'autres câblages futurs et les actions de tirage s'en trouvent moins difficiles à entamer.

La bonne conception impose que les câbles ne doivent pas occuper la totalité du conduit mais laisser 60 à 70 pour cent de l'espace disponible du tuyau. Le diamètre d'un câble bi-fibre étant en moyenne de 5 mm, un diamètre de conduit 80mm est convenable.

- **Mise en place des chambres de tirages**

Une chambre de tirage sert à tirer les câbles, elle donne accès aux conduits souterrains. Ces chambres de tirage sont espacées typiquement de 50 m et d'un maximum de
100 m et chaque fois qu'une topologie particulière s'impose : changement de niveau, de direction, etc...

La pénétration d'humidité étant le principal facteur de dégradation des câbles optiques, une attention particulière sera portée pour s'en prémunir : installation, dans le domaine du possible, dans les parties hautes des fourreaux, permettant de diminuer les risques de séjours prolongés dans les chambres de tirages inondées, il est nécessaire de boucher les extrémités des conduits pour qu'ils soient étanches. Le haut de la chambre peut être verrouillé pour sécuriser l'endroit.

La figure suivante montre une chambre de tirage (unités en cm).

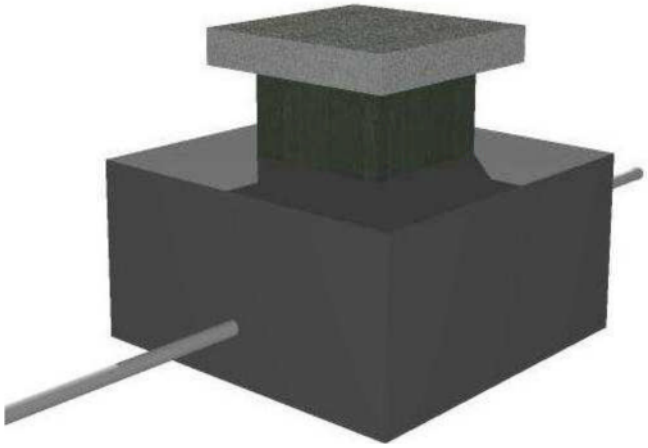


Figure 5.7 : chambre de tirage en trois dimensions

b. Choix des câbles et des raccordements

Choix des câbles utilisés

Les câbles pour utilisation à l'extérieur sont dotés de protections spéciales. L'utilisation de ces types de câbles s'impose donc pour notre situation. Plus précisément des câbles bi-fibres multimode en gradient d'indice 62.5/125 µm, car ils sont faits pour la situation. La figure montre un câble bi-fibre avec protection.

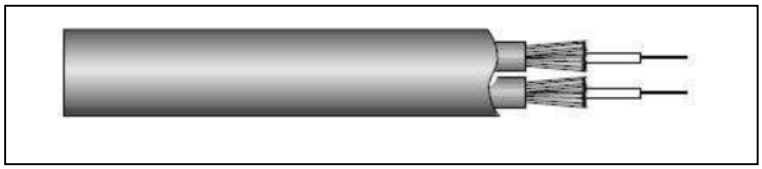


Figure 5.8 : câble avec protection

- **Choix des raccordements**

Il y a deux manières de mettre bout à bout deux fibres optiques (pour le couplage source-fibre ou fibre-détecteur), par épissure (fusion de deux fibres) c'est un raccord définitif ou par connecteur pour les raccords démontables. Dans les deux cas (surtout le deuxième), cela entraîne des pertes à cause de l'écartement, de l'excentrement et du désalignement.

Nous Adoptons le raccordement avec les connecteurs de type ST qui sont le plus couramment déployés dans les réseaux optiques surtout pour les fibres multimodes (62.5/125 µm) et dans le cas des câbles paires torsadées, il est préférable en effet d'utiliser les connecteurs RJ45.

c. Condition de pose des câbles

- **Contraintes lors de l'installation**

Les contraintes spécifiques relatives à la technologie optique sont d'ordre mécanique et climatique (rayons de courbure, résistance à la traction).

- **Force maximale de traction**

La résistance en traction d'un câble a été dimensionnée par rapport à l'environnement dans lequel le câble sera posé (intérieur, extérieur, ...) et à ses caractéristiques intrinsèques (diamètre, poids, type de gaine). Le non respect de ces valeurs peut entraîner des dégradations sir réversibles de la fibre.

Rayon de courbure

Le rayon de courbure minimal recommandé lors de l'installation est spécifié par chaque constructeur. Au-delà de cette limite, il y a une forte atténuation du signal ou même la perte totale de ce dernier, la rupture de la fibre ou la rupture du câble. Ce rayon est habituellement, mais pas toujours, spécifié comme 20 fois le diamètre du câble à courber. Une valeur moyenne du rayon minimal de courbure est de 200mm.

d. **Budget de puissance (analyse de perte de puissance)**

Un réseau fibre optique doit avoir une marge de perte de puissance adéquate pour fonctionner correctement. La puissance arrivée au récepteur doit être supérieure à sa sensibilité, et une marge doit être tenue au dessus de cette sensibilité. Les pertes se situent au niveau de la fibre optique, connecteurs et convertisseurs de media.

e. Local technique et équipements

- **Le Local technique**

Le local technique est le point essentiel du réseau local, sans lequel il ne peut fonctionner correctement. Il présente le point fort de l'installation dans la mesure où il abrite plusieurs appareils sensibles (Switch, routeur,..) et sur lequel pèse des menaces importantes (écoute, piratage,…).

Bien que ces équipements soient souvent regroupés dans une même salle, il est nécessaire de séparer les différents types de matériels.

- **Répartiteur de type " baie "**

Ce répartiteur est une armoire munis d'un capot avec serrure qui est bien placée dans le local technique, sa largeur et profondeur peuvent varier entre 800x800 cm, 600x800 cm, avec porte fermant à clé pour la sécurité mais l'arrière de la baie doit être dégagée pour en faciliter l'accès (Figure).

La baie accueille un panneau de brassage dans sa partie haute (notamment les tiroirs àfibres optiques) et les équipements actifs dans ses parties basses.

La taille de 800x800 a notre préférence, car elle offre suffisamment d'espaces latéraux pour y faire passer des cordons de brassage et suffisamment de profondeur pour y loger tous types d'équipements actifs.

- **Les tiroirs fibres optiques**

La gestion des câbles optiques est effectuée grâce à des tiroirs fibres optiques qui se trouvent dans la baie. Leur conception doit permettre de les utiliser dans tous les cas de mise en œuvre:

- terminaison de câble par connecteurs,
- utilisation mixte (épissure et connecteurs).

Ils doivent offrir les caractéristiques suivantes:

- encombrement faible,
- face avant pour recevoir au minimum 12 ou 24 connecteurs,
- logement pour la fixation, la gestion et l'organisation des câbles en arrivé.

VI. Conclusion

La conception d'un réseau est un travail de profondeur dont il faut en comprendre le fondement, ainsi nous avons abordé l'étude par les bases de la mise en réseau, puis en étudiant l'infrastructure du réseau. Nous avons ensuite établi l'architecture du réseau et les plans d'installation.

I. Conception

Au cours de trois mois de stage pratique mené à la direction Territoriale des Télécommunications de Tizi-Ouzou, une étude approfondie du Réseau de la direction a été faite avec l'aide de notre Co-encadreur ***Mr HADOUS Abdnour.***

L'étude de l'existant, point clé de notre démarche, est une étape essentielle qui vise à représenter l'architecture de notre travail. Nous porterons une attention particulière sur le service où sera implémentée notre solution.

Dans ce chapitre, nous allons effectuer une étude de l'existant de la direction et ressortir la problématique qui nous a conduits à mener ce travail et à proposer notre solution.

I.1. Architecture du réseau existant

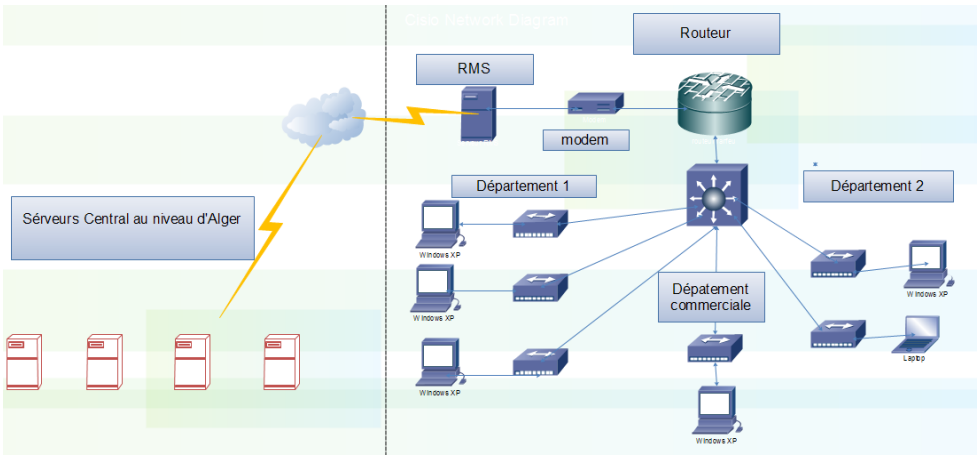


Figure 6.1 : Architecture actuelle de la Direction.

I.2. Critiques :

Après étude des différents services de l'organisme d'accueil, on a extrait les remarques suivantes :

- Le système est surchargé ce qui le rend très lent.
- Absence d'un Serveur Web et même aucun serveur n'est installé à leur niveau.
- Circulation des informations sur les supports de stockage (flash disque….).
- Vu l'absence d'un pare-feu l'Architecture physique n'est pas conforme à une architecture de sécurisation.
- Absence de contrôle sur l'état de travail des utilisateurs.
- Le système devient de plus en plus lent, cette lenteur est une conséquence de la topologie choisie pour les caractéristiques des serveurs utilisés.

- Perte de temps en cherchant la source de la panne qui souvent se situe au niveau d'Alger.

I.3. Suggestion et solution:

Après avoir détecté toutes ces critiques, nous avons pensé à une autre architecture réseau plus sécurisée. Notre solution consistera à :

- Installer un réseau local administré sous Windows serveur 2012 et d'autre système d'exploitation client (Windows 7,8, 10).
- Mettre en place un Annuaire «Active Directory» (AD) pour une gestion centralisée des ressources et planification des accès à ces ressources à travers les paramètres de sécurité dans Windows server 2012 appelé «GPO» (Group Policy Object).
- Mettre en place un pare-feu pour la sécurité du réseau Local.
- Configurer un «VPN» pour l'accès distant sécurisé.
- Installer deux serveurs web avec équilibrage de charge réseau et un serveur de messagerie dans une «DMZ» (zone démilitarisée).
- Segmenter le réseau local en «VLAN» par département.

I.4. La nouvelle architecture proposée :

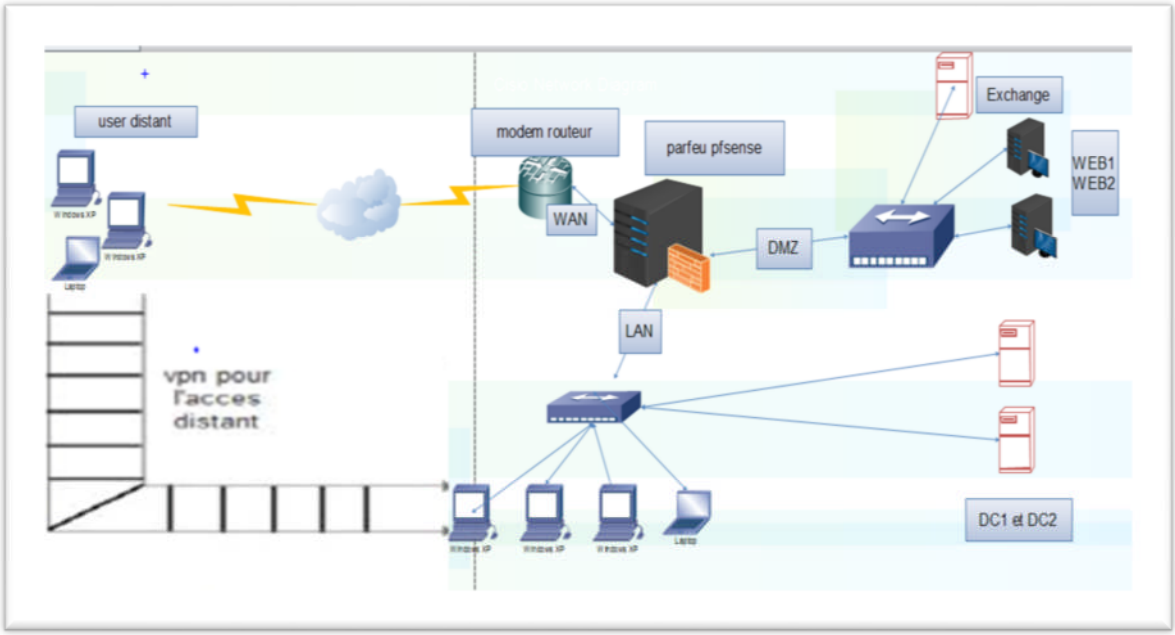


Figure 6.2 : L'architecture proposée.

Dans cette nouvelle architecture, le réseau de la direction sera constitué de trois parties: le réseau local« LAN», la zone démilitarisée «DMZ» et le réseau externe «WAN».

Pour ce faire, un pare-feu Linux «PfSense» a été mis en place avec trois cartes réseau : l'une vers l'interface «WAN», la deuxième vers l'interface «LAN», et la dernière vers la «DMZ». Ce firewall sur lequel des paramètres de sécurité tels que les règles d'accès, et le «VPN» ont été implémentés jouera aussi le rôle d'une passerelle entre le réseau local de la direction et le réseau extérieur(INTERNET).

- **Réseau local**

Dans le «LAN», nous avons implémenté un serveur «Active Directory», on a implémenté deux annuaires « Active Directory » en mode multi-maître. Les utilisateurs du «LAN» sont créés et gérés par ces annuaires, en offrant à chacun d'eux des droits d'accès ou non aux applications

- **Zone démilitarisée :**

Deux serveurs Web avec équilibrage de charge entre les deux et un serveur de Messagerie (Exchange) ont été installés.

- **Réseau externe :**

Un routeur (Vyatta) sous ''LINUX'' doté de deux cartes réseau, l'une connectée vers l'interface «WAN» du firewall et l'autre vers un réseau public a été configuré pour la simulation d'Internet.

Pour que les utilisateurs puissent continuer leurs travails de n'importe quel endroit un «VPN» pour l'accès distants au réseau local de la direction a été mis à leur disposition, ce qui va engendrer un gain de temps et un travail dans des conditions convenant à l'utilisateur.

I.5. Présentation des outils utilisés :

a. La VMware Workstation 12.0:

Pour l'émulation du réseau *VMware Workstation 12.0* a été utilisé. Ce dernier est un logiciel qui permet de créer des machines virtuelles fonctionnant sur le système d'exploitation d'une machine physique (architecture hébergée), Chaque machine virtuelle dispose de son processeur virtuel, de sa mémoire, de son disque virtuel et de ses propres périphériques d'entrées/sorties. Le *Vmware* prend en charge plusieurs systèmes d'exploitation (*Windows, Linux*), il permet l'exécution simultanée de plusieurs *OS* à condition que les ressources physique de l'ordinateur soient suffisantes. Les différentes machines virtuelles peuvent être connectées en réseaux et peuvent communiquer entre elles et avec des machines physiques, comme s'il s'agissait de machines réelles.

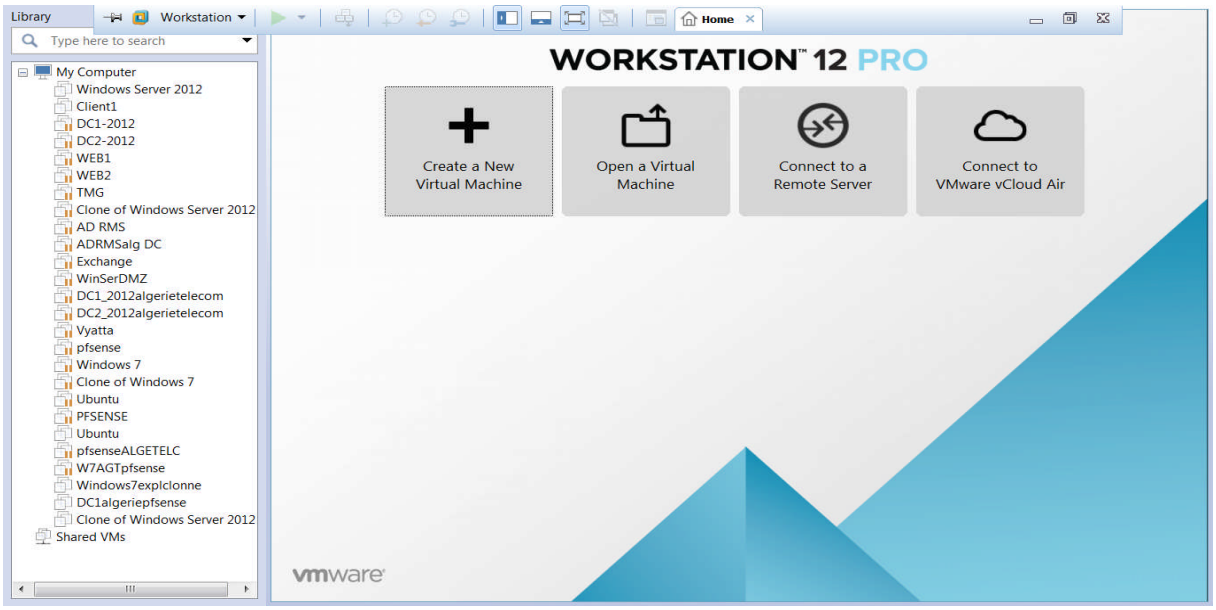


Figure 6.3: VMware Workstation 12.0

b. Évolution de Windows Server :

Windows *Server 2012 R2* offre des performances de qualité et prend en charge des scénarios d'usage à grande échelle, c'est une plateforme d'entreprise fournissant plus de fonctionnalités par rapport aux autres versions de Windows Server, il fournit cinq fois plus de support pour le processeur logique, une mémoire physique 4 fois plus grande, et 16 fois plus de support pour la mémoire par machine virtuelle.

Figure 6.4: Windows Server 2012 R2.

c. Pare-feu PFSENSE:

PfSense est un système d'exploitation à part entière, open source, utilisé pour mettre en œuvre un parefeu, un routeur ou une solution permettant la fourniture d'autres services réseaux. *PfSense* est une distribution *FreeBSD 1*personnalisée.

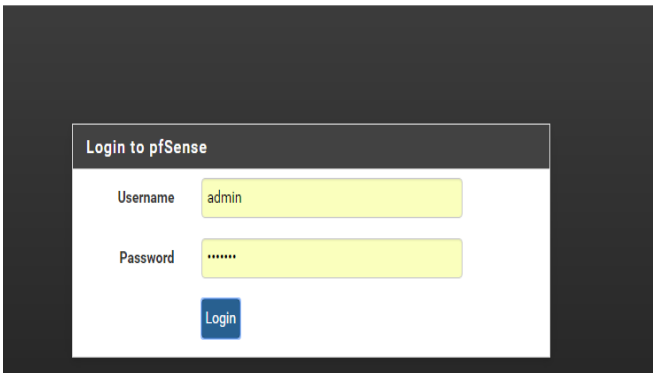


Figure 6.5 : interface web pfSense.

d. Routeur VYATTA:

Vyatta est une distribution très utile dans les environnements virtualisés. *Vyatta* est un *OS* assurant des fonctions de routage, il peut donc servir se connecter à Internet, il peut être utilisé comme firewall dans un réseau et il peut aussi permettre de séparer un ordinateur d'un réseau local et ainsi disposer d'un réseau local connecté mais indépendant d'un autre. On pourrait ainsi comparer *Vyatta* aux *OS* des grands constructeurs de matériels réseaux comme *IOS* de *Cisco Systems* ou *JUNOS* de *Juniper Networks*.

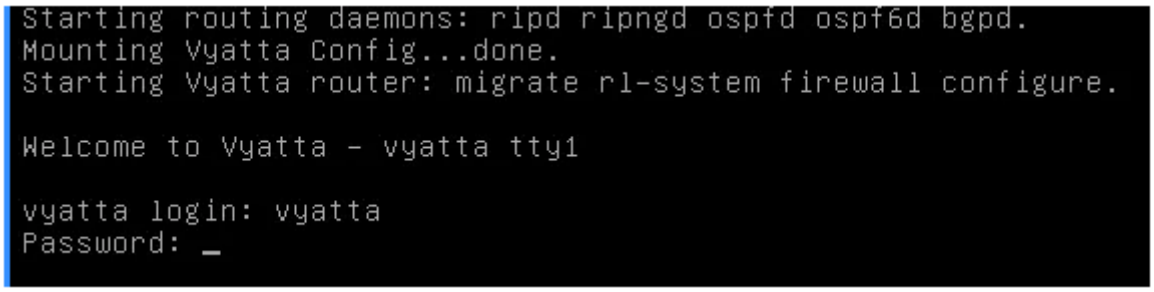


Figure 6.6 : Interface routeur Vyatta.

e. Le simulateur Packet Tracer : est un simulateur de matériel réseau *Cisco* (routeurs, commutateurs). Cet outil est créé par *Cisco Systems* qui le fournit gratuitement aux centres de formation, étudiants et diplômés participant, on ayant participé, aux programmes de formation *Cisco* (*Cisco Networking Academy*).

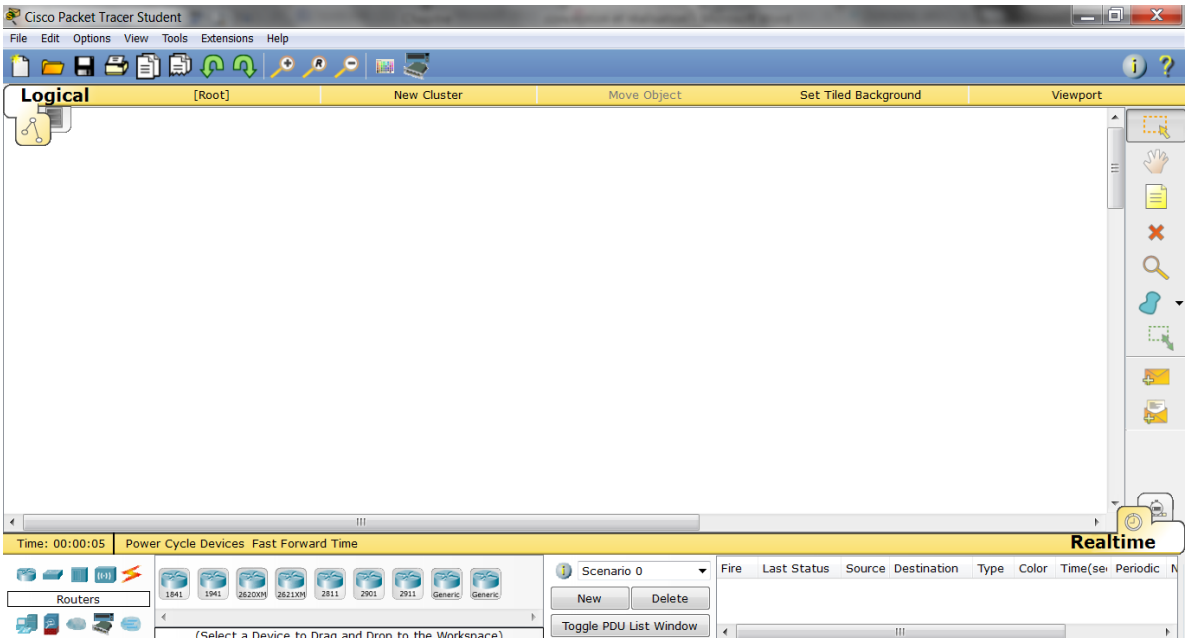


Figure 6.7: Packet Tracer.

f. Les caractéristiques du PC utilisé :

- Processeur I3 x64 bits
- RAM 4G
- Disque dur 500G
- Système Windows 7 professionnel x64 bits
- Prise en charge de la virtualisation.

II. Réalisation :

II.1. Les machines à utiliser :

Pour la réalisation de l'application, les machines suivantes ont été préparées:

- Deux contrôleurs de domaine fonctionnant en multi-maître (DC1,DC2).
- Deux serveurs webs (WEB1 et WEB2).
- Un serveur de messagerie (Exchange).
- Une machine pour le pare-feu (Pfsense).
- Une machine pour le routeur (Vyatta).
- Une machine (windows 7) pour représenter un utilisateur distant.
- Une machine (windows 7) pour désigner un utilisateur local.
- Une machine (Windows XP) pour désigner un client de domaine.

II.2. I 'installation des contrôleurs de domaine:

Active directory est la mise en œuvre par Microsoft des services d'annuaire *LDAP* pour les systèmes d'exploitation Windows. 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.

Après avoir installé *Windows server 2012 R2* data center sur deux machines, un contrôleur de domaine « DC1 » a été installé sur la première machine. Une fois la configuration de déploiement choisie, une nouvelle forêt est ajoutée avec le nom du domaine « Algerietelecom.com ». Le déploiement du contrôleur de domaine, pour avoir un deuxième contrôleur de domaine « DC2 », a été effectué sur la deuxième machine. Ce dernier sert à la réplication du DC1 pour le remplacer en cas de panne ou interruption.

L'installation des deux contrôleurs est la même à la différence du choix de l'étape montrée ci-dessous.

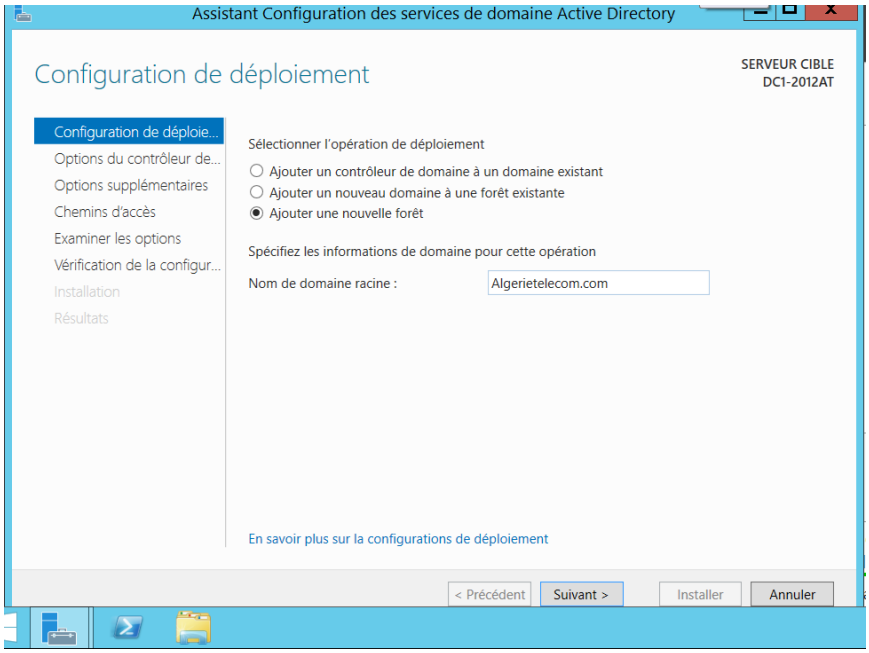


Figure 6.8 : Crée le premier contrôleur de domaine

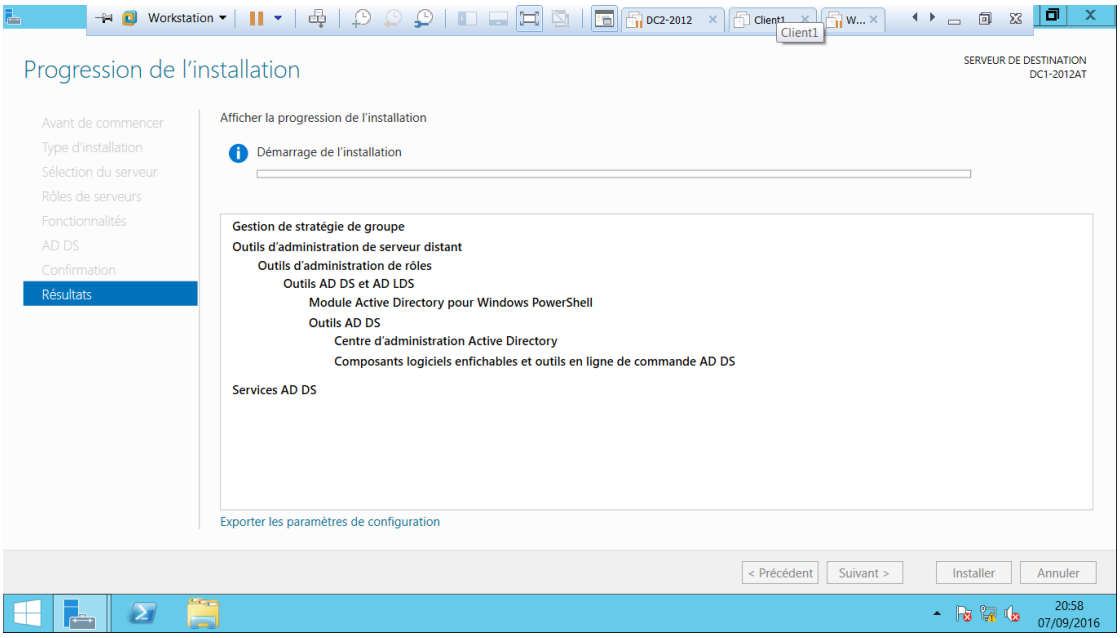


Figure 6.9 : Installation de DC1.

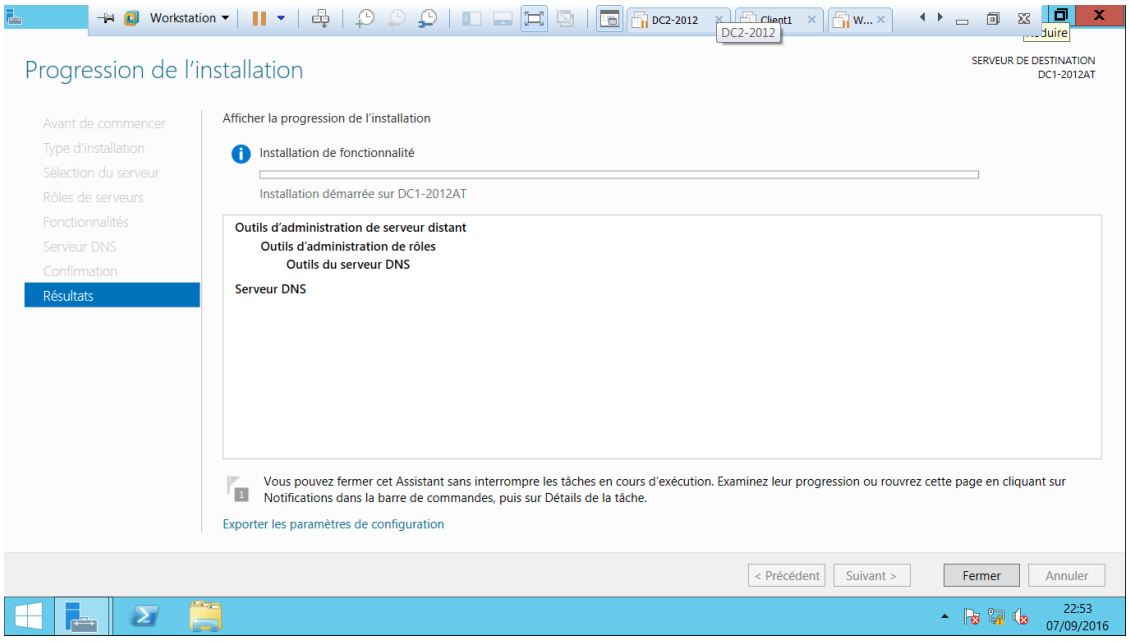


Figure 6.10 : Installation de serveur DNS

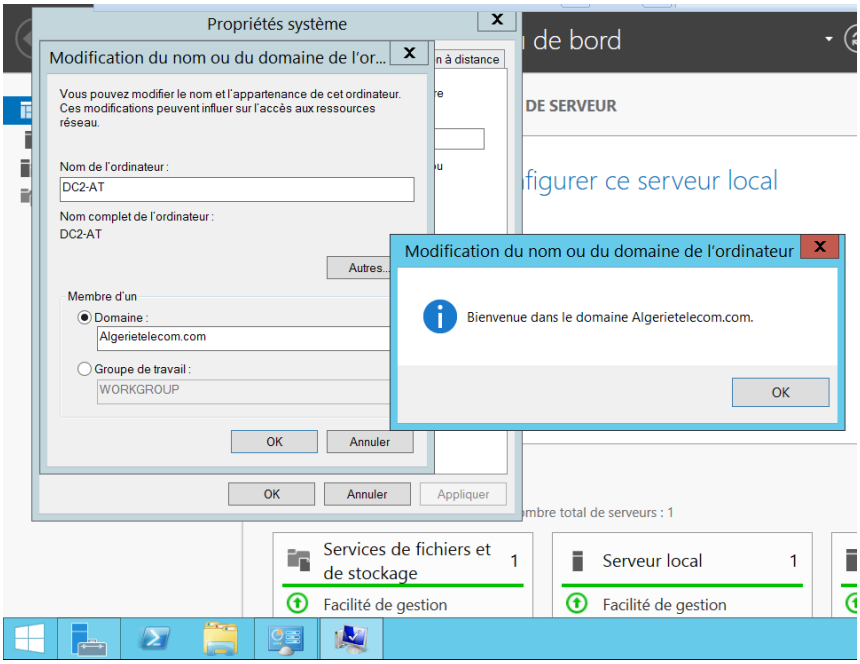
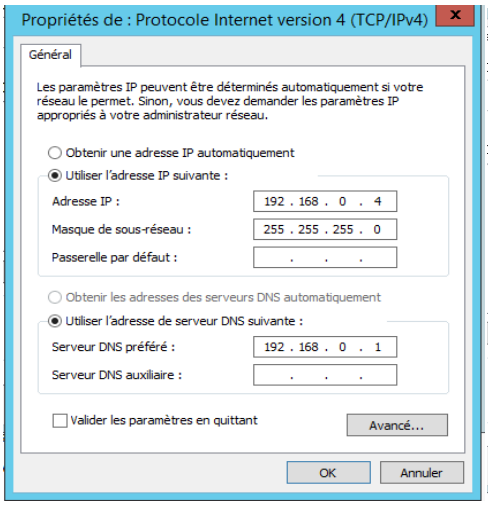


Figure 6.11 : Ajouter DC2 au domaine DC1.



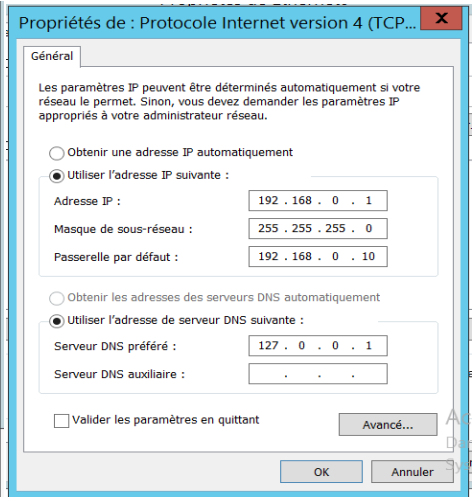


Figure 6.12 : Carte réseau DC1 **Figure 6.13 :** Carte réseau DC2

- **Ajouter une machine au domaine :**

Toute machine créée, qu'elle soit un serveur ou un utilisateur, elle doit être intégrée au domaine et doit être dans le même réseau LAN que le domaine.

Pour ajouter un membre, il faut accéder aux propriétés systèmes et modifier le domaine de l'ordinateur comme le montre la figure suivante :

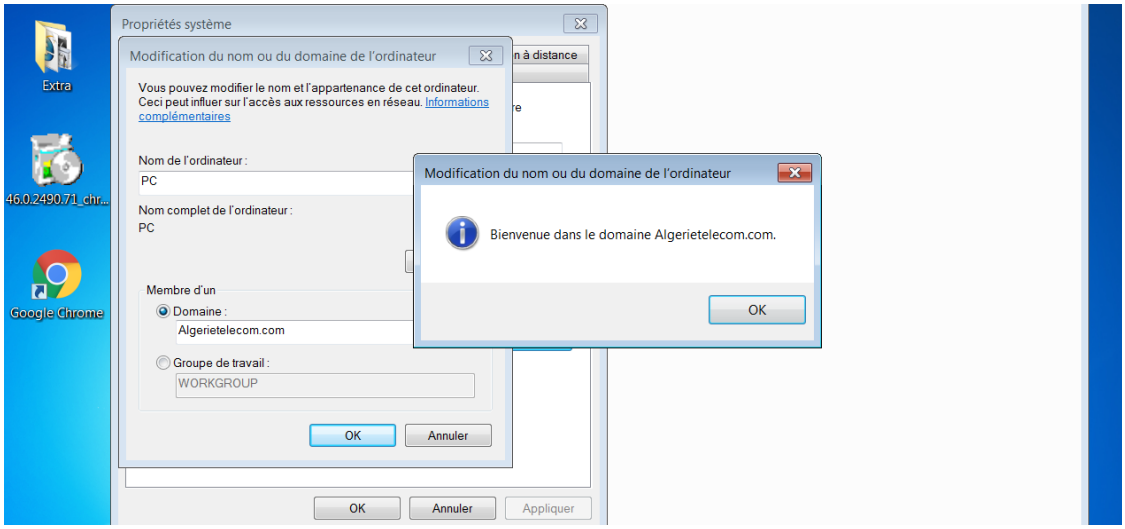


Figure 6.14 : ajout d'un utilisateur au domaine et résultat de l'action d'ajout.

II.3. Mise en place du pare-feu PFSENSE :

❖ Configuration des cartes réseaux :

L'installation préalable du PFSENSE exige l'ajout et la configuration de 3 cartes réseaux :

La première externe (interface «WAN» « le0 ») avec l'adresse 172.16.2.1/24.

La deuxième interne (interface LAN « le1 ») avec l'adresse 192.168.50.1/24.

La troisième pour la «DMZ» « le2 » avec l'adresse 172.16.1.1/24.

Au niveau des paramètres de l'hôte pfsense nous avons associé :

• 'Le0' au réseau pfsenseLAN

• 'Le1' au réseau pfsenseDMZ

• 'Le2' au réseau pfsenseWAN

❖ Lancement de l'installation

Figure 6.15: interface pfSense.

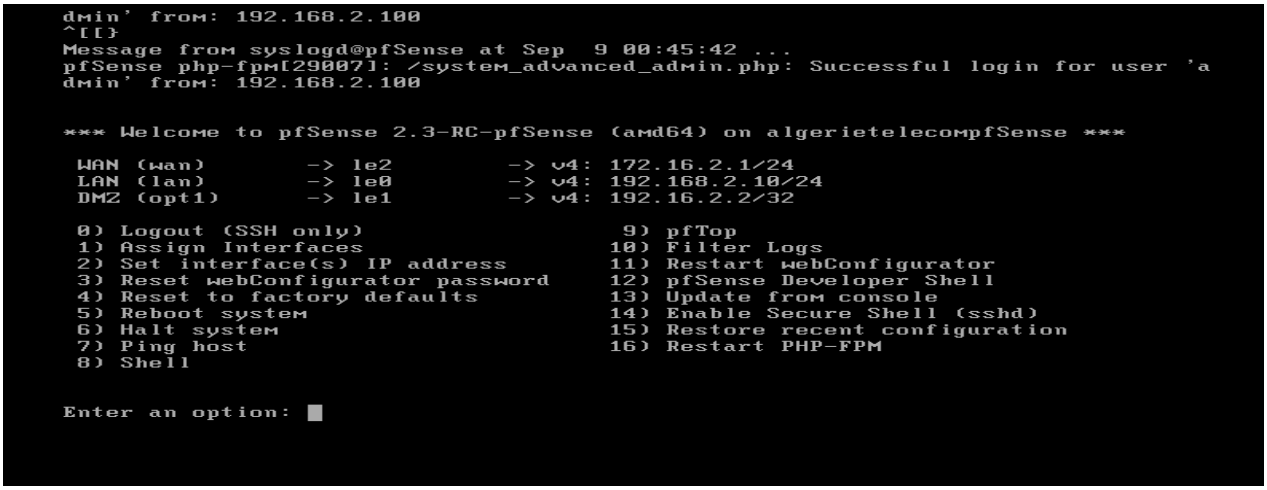


Figure 6.16 : Configuration des cartes réseaux de pfsense

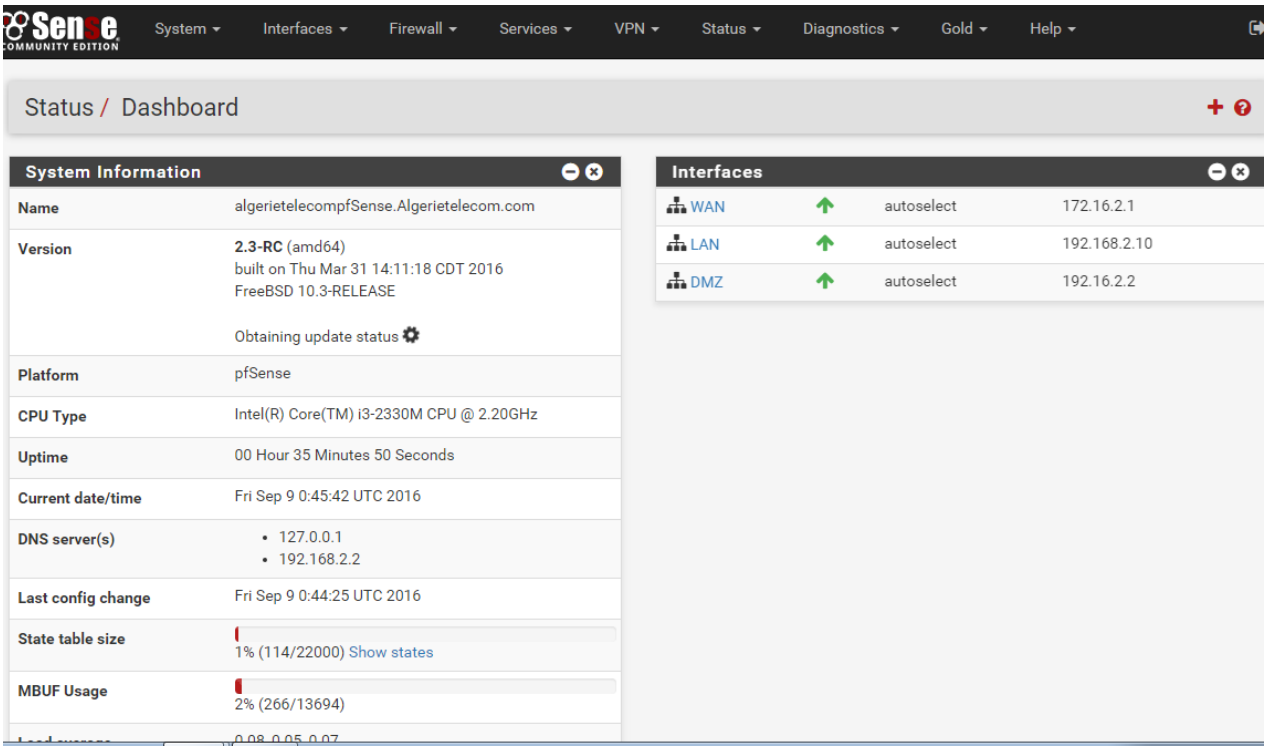


Figure 6.17 : configuration des trois cartes réseaux

❖ **Règles de pare feu pfsense**

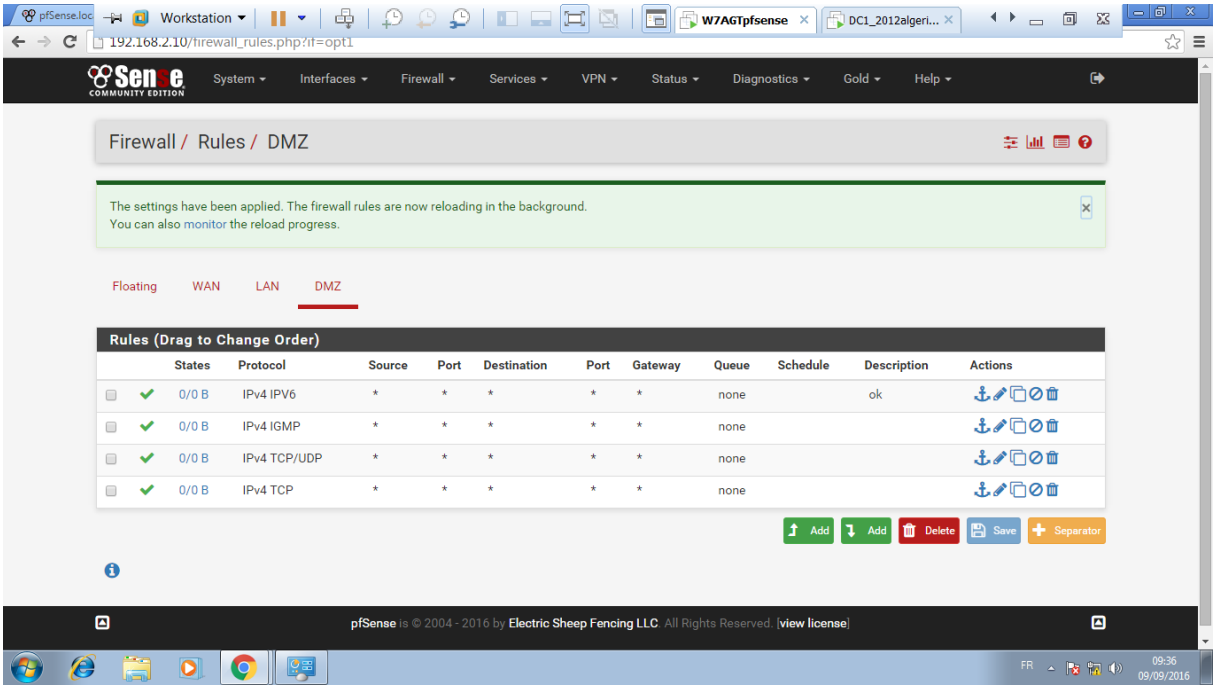


Figure 6.18 : Liste des rôles de la carte réseau DMZ

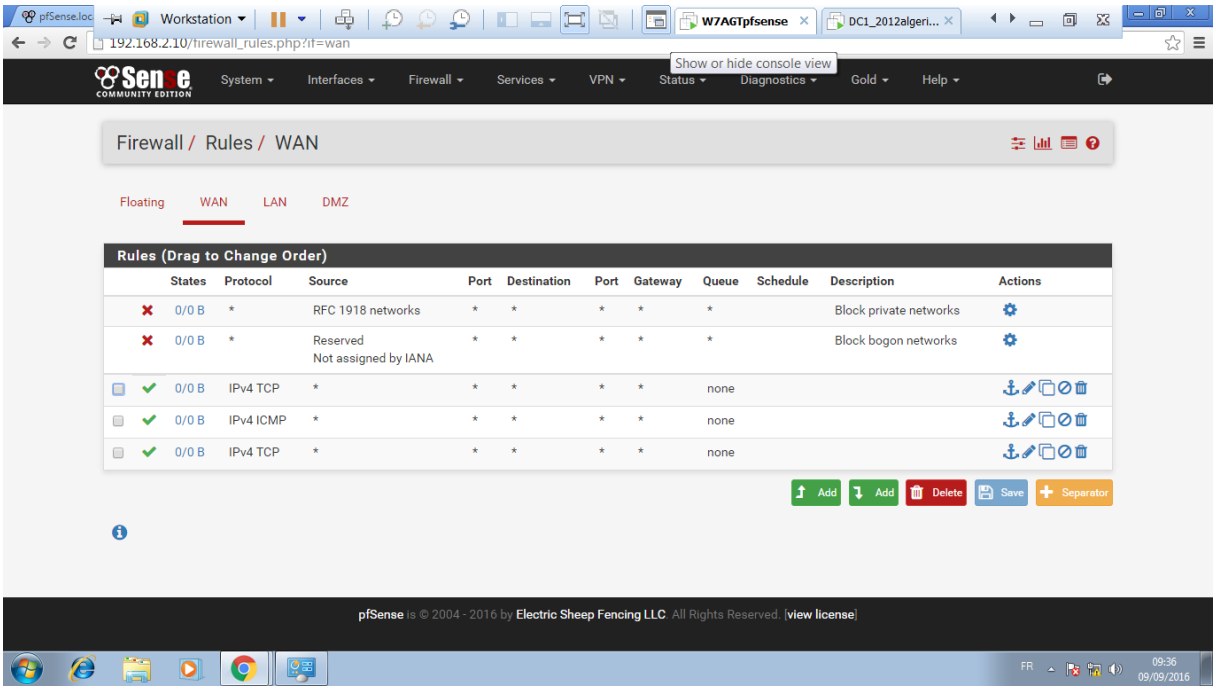


Figure 6.19 : Liste des règles de la carte réseau WAN

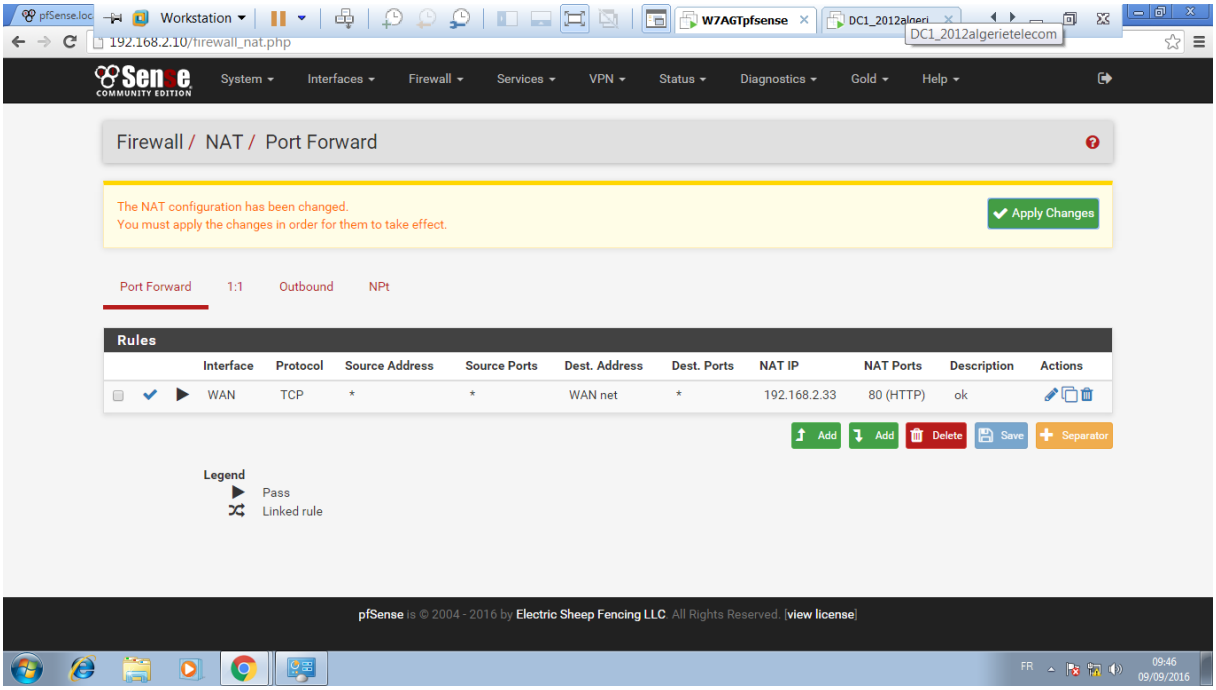


Figure 6.20 : Règles NAT

❖ Création d'un planning

Les plannings permettent de préciser des périodes d'activation des règles. Ils sont principalement utilisés avec les règles de firewall. Si une règle de firewall spécifie un calendrier, la règle est activée uniquement pendant cette période.

- Se rendre dans le menu Firewall | Schedules ;
- Saisir le nom du calendrier ;
- Saisir une description pour le calendrier ;
- Spécifier les jours et la tranche horaire correspondant au calendrier ;
- Valider les changements par le bouton Save ;
- Éditer une règle et dans ses paramètres avancés, spécifier le calendrier nouvellement créé ;

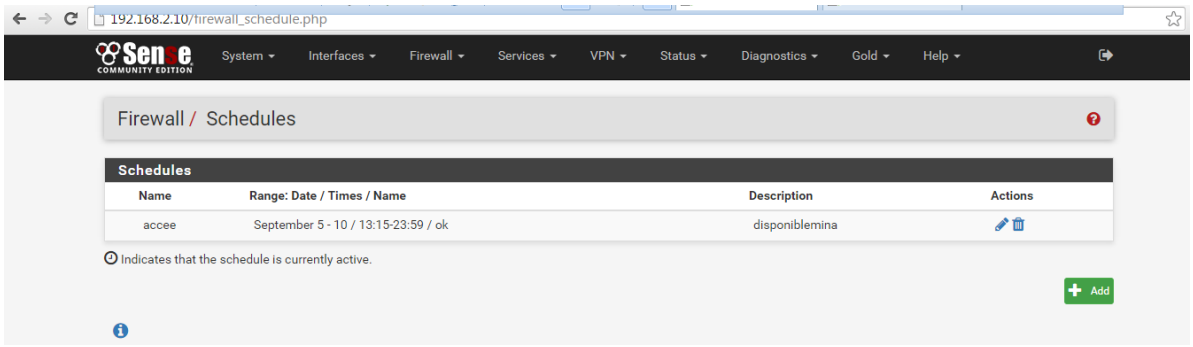


Figure 6.21 : Firewall Schedules

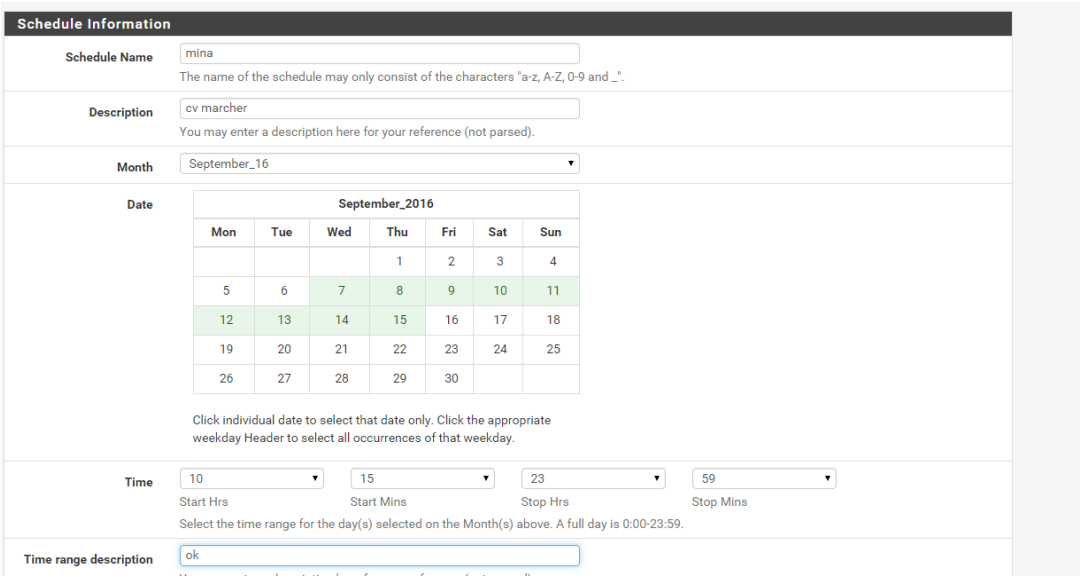


Figure 6.22 : ajout d'un calendrier

Une des failles du système consiste à accéder à certains sites interdits en utilisant https au lieu de http. Par exemple, aller sur https://192.168.2.10

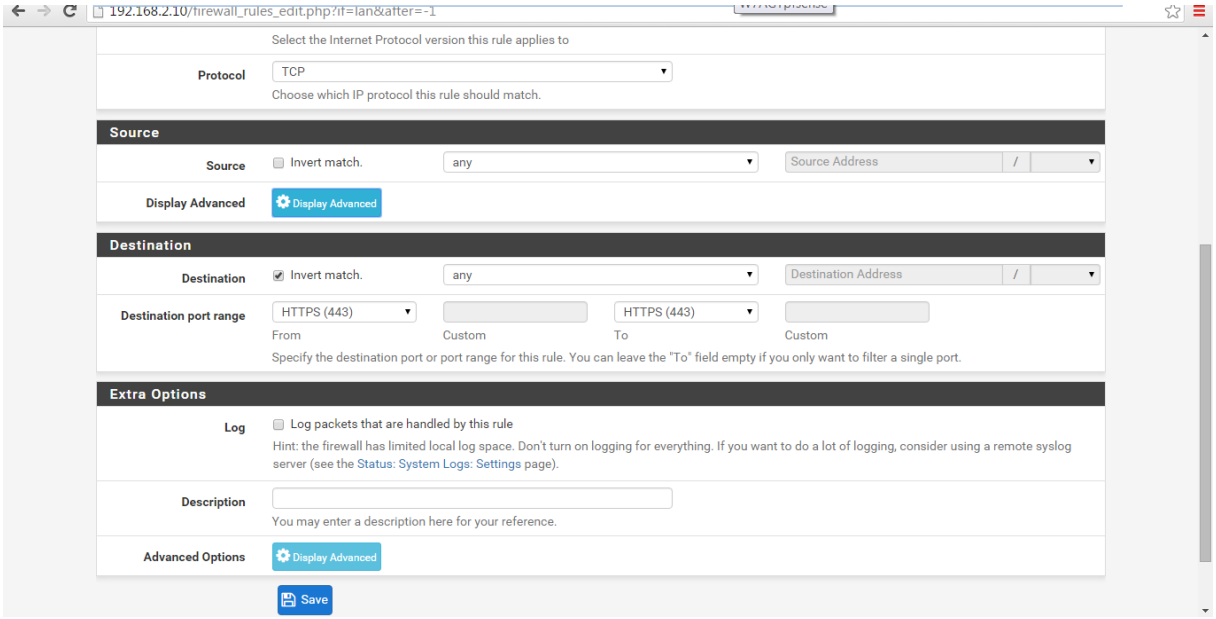


Figure 6.23 : bloquer le trafic https

Maintenant site https://192.168.2.10, sera bloqué.

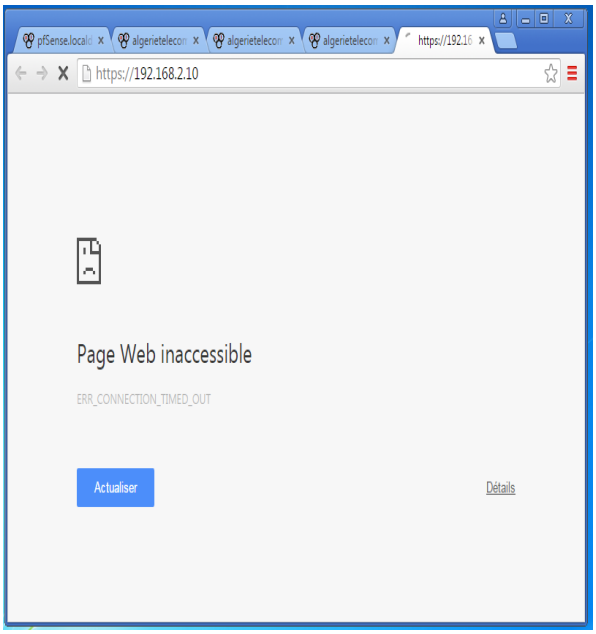


Figure 6.24 : https bloqué

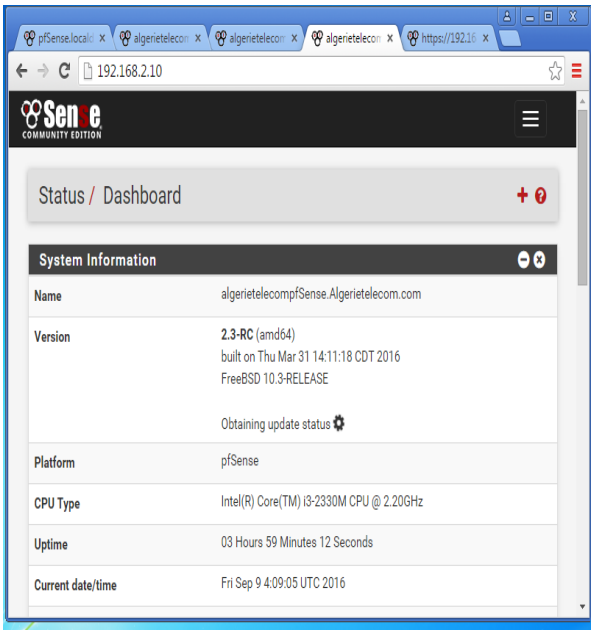


Figure 6.25 : http marche

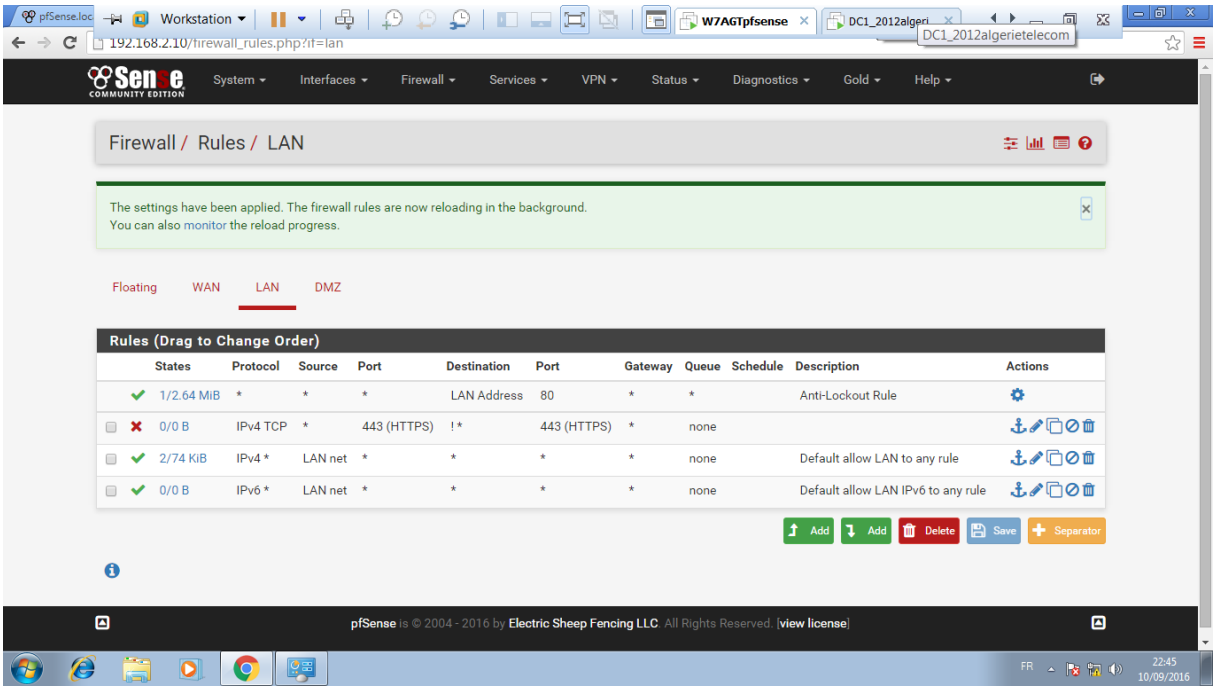


Figure 6.26 : les règles de LAN

II.4. Mise en place du routeur «VYATTA» :

La configuration matérielle de notre *VM* va devoir respecter quelques points. *Vyatta* est un routeur, il va lui falloir plusieurs interfaces réseaux. Pour notre cas, 2 cartes réseaux suffisent. La RAM et le processeur importent peu, quant à l'espace disque, 3Go devrait suffire.

- **Configuration des cartes réseaux :**

La première externe (interface «WAN»« le0 ») avec l'adresse 172.16.2.2/24.

La deuxième interne (interface LAN« le1 ») avec l'adresse 10.10.10.1/24.

Pour interconnecter ce dernier au firewall pfSense,'le0' a été connecté vers pfsenseWAN

L'interface LAN 'le1' a été mise sur distant.

II.7.2) Lancement de l'installation :

Après avoir bien placé l'ISO du « vyatta », et allumé la machine virtuelle, l'écran ci-contre s'affiche, pour booter sur « vyatta » il faut cliquer sur la touche **entrée**.

Figure 6.27 : installation VYATTA.

Notre installation s'est bien passée, donc nous finissons devant une demande de login *vyatta* et un mot de passe, qui sont par défaut : «vyatta». Comme le montre la figure suivante :

```
Copying system files to /dev/sda1:
 99% [=================================================>]
OK
I found the following configuration files
/opt/vyatta/etc/config/config.boot
Which one should I copy to sda? [/opt/vyatta/etc/config/config.boot]:

Enter password for administrator account
Enter password for user 'vyatta':
Retype password for user 'vyatta':
I need to install the GRUB boot loader.
I found the following drives on your system:
 sda    5368MB


Which drive should GRUB modify the boot partition on? [sda]:

Setting up grub: OK
Done!
vyatta@vyatta:~$ reboot_
```

Figure 6.28 : Installation réussis VYATTA.

II.5. Application de la solution VPN sous pfsense

Pour réaliser cette solution, il faut suivre par les étapes suivantes

- Installation du package « OpenVPN Client Export Utility »
- Création d'un certificat d'autorité
- Création du compte utilisateur
- Création du serveur « OpesVPN »
- Puis télécharger le fichier de configuration
- Installer « Open VPN » sur la machine cliente (distante)
- On peut vers la fin tester la connexion VPN par l'utilisateur qu'on créé

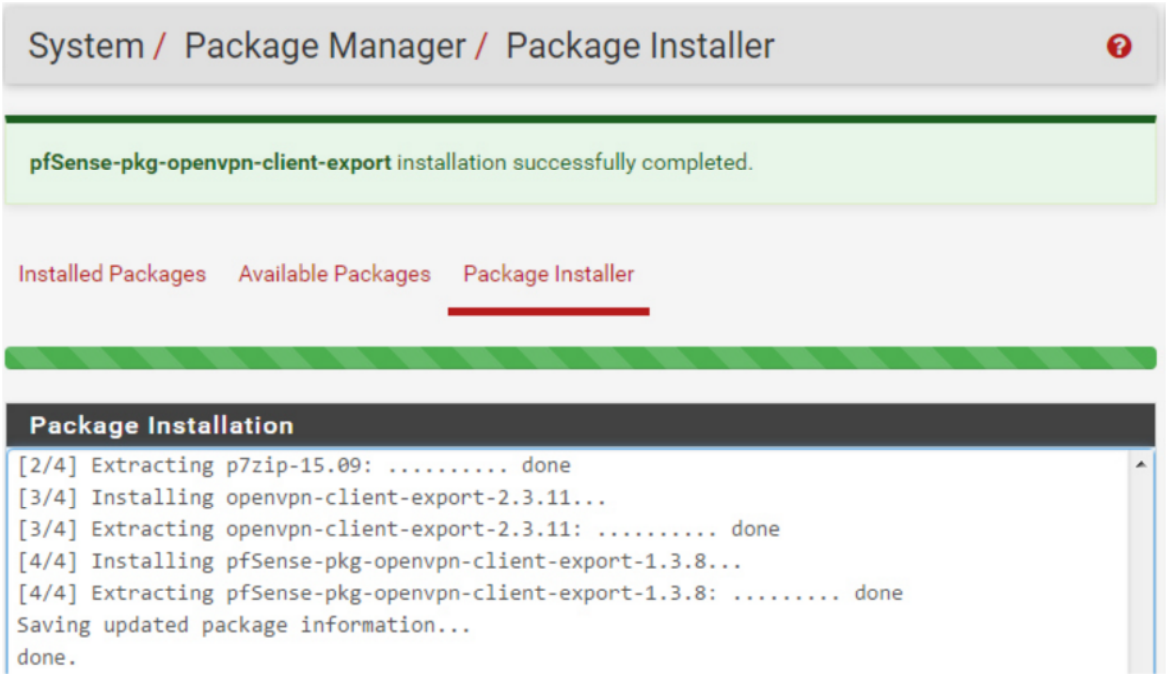


Figure 6.29: installation du package « OpenVPN Client Export Utility »

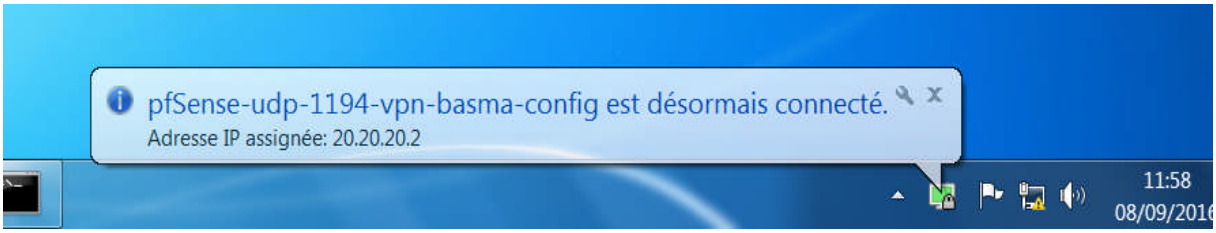


Figure 6.30 : connexion «VPN» établie.

Figure 6.31 : liste des utilisateurs connectés via le «VPN».

II.6. Création de la gestion des stratégies de groupe «GPO»:

Pour la bonne gestion des unités, groupe, et des utilisateurs, la politique «GPO» aux différentes unités du domaine est appliquée.

- Unité Organisationnelle « OU » : Dans cette phase les différentes unités d'organisation prévues dans notre champ d'étude seront créées.
- L'option «Utilisateurs et ordinateurs Active Directory» permet de sélectionner le domaine de travail et de spécifier les unités d'organisations désirées.
- Sous l'option Algerietelecom.com → nouveau → Unité d'organisation, les unités sont créées.

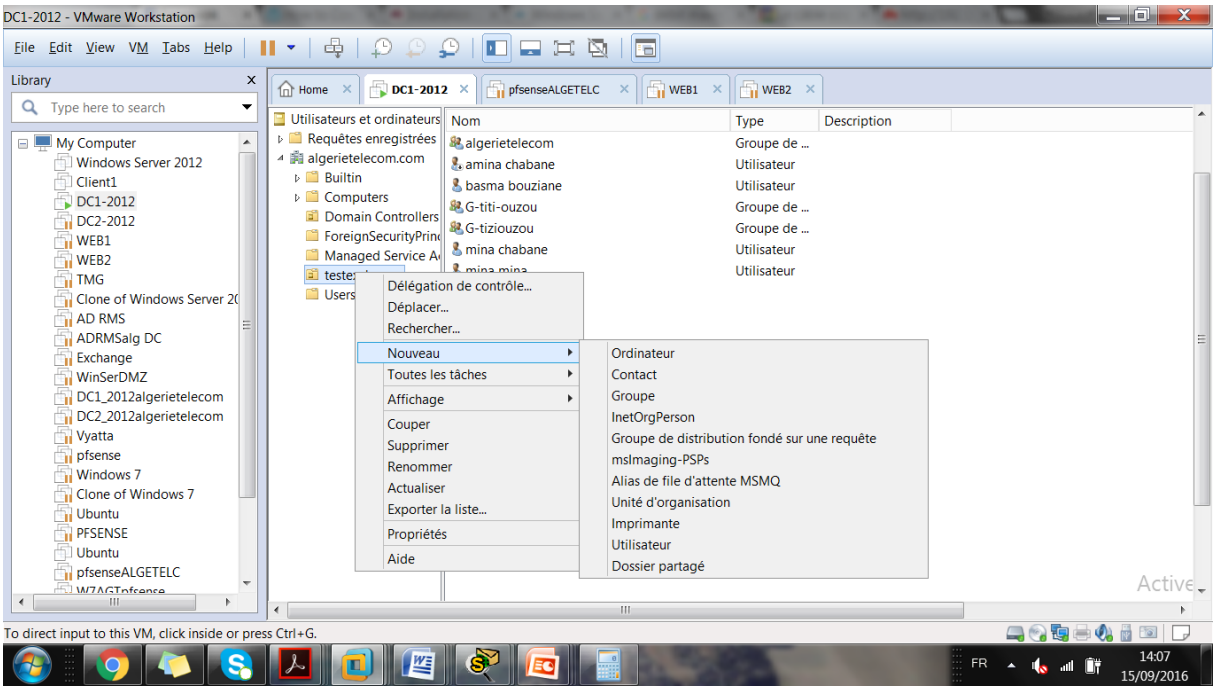


Figure 6.32: Création d'une unité d'organisation.

- **Groupe Polycy Manager GPM**

Le GPM permet la mise en place des GPO sur certaine groupes pour gérer leurs acès aux ressources.

Pour créer GPO dans le gestionnaire de serveur se fait par le biais de l'option :

Outil → Gestion de la stratégie de groupe → Domaine → Algerietelecom.com sélectionner l'unité organisationnelle sur laquelle la GPO sera créée.

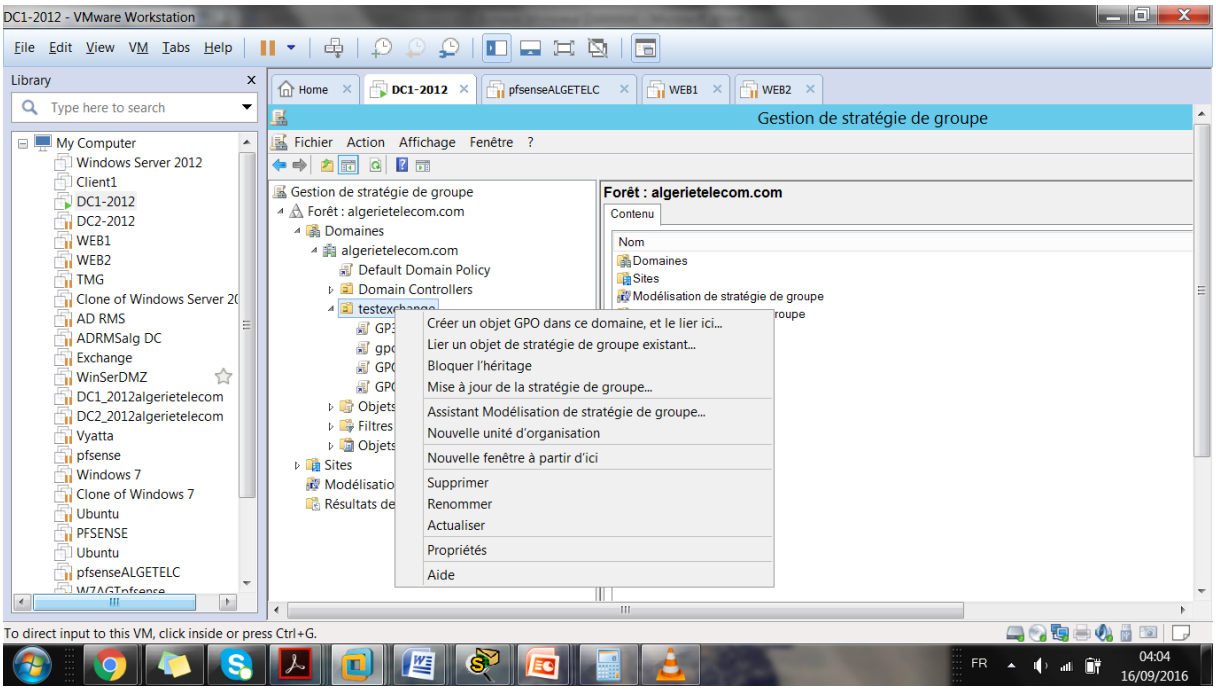


Figure 6.33 : Création d'une «GPO».

Un nom pour la GPO puis l'option « modifier »

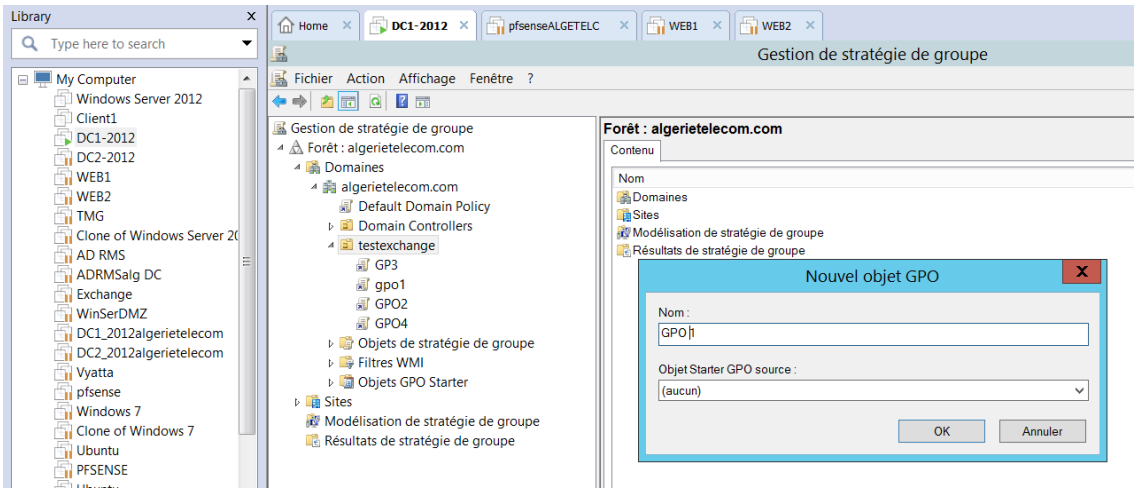


Figure 6.34 : Nom de la GPO

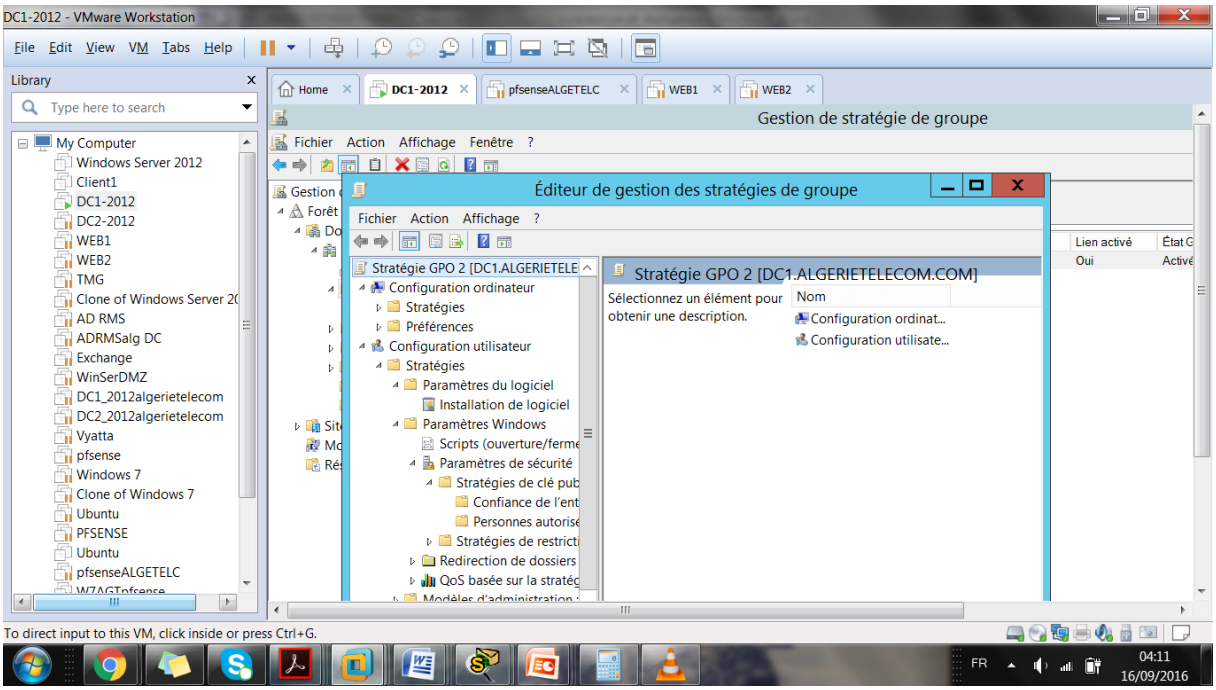


Figure 6.35 : Option « modifier »

Nous avons la possibilité d'autoriser ou interdire l'accès à des fonctionnalités pour l'utilisateur ou l'ordinateur.

On a prit un exemple où on a désactivé l'accès au panneau de configuration et à l'invite de commande pour un ensemble d'administrateur se trouvant dans la même unité.

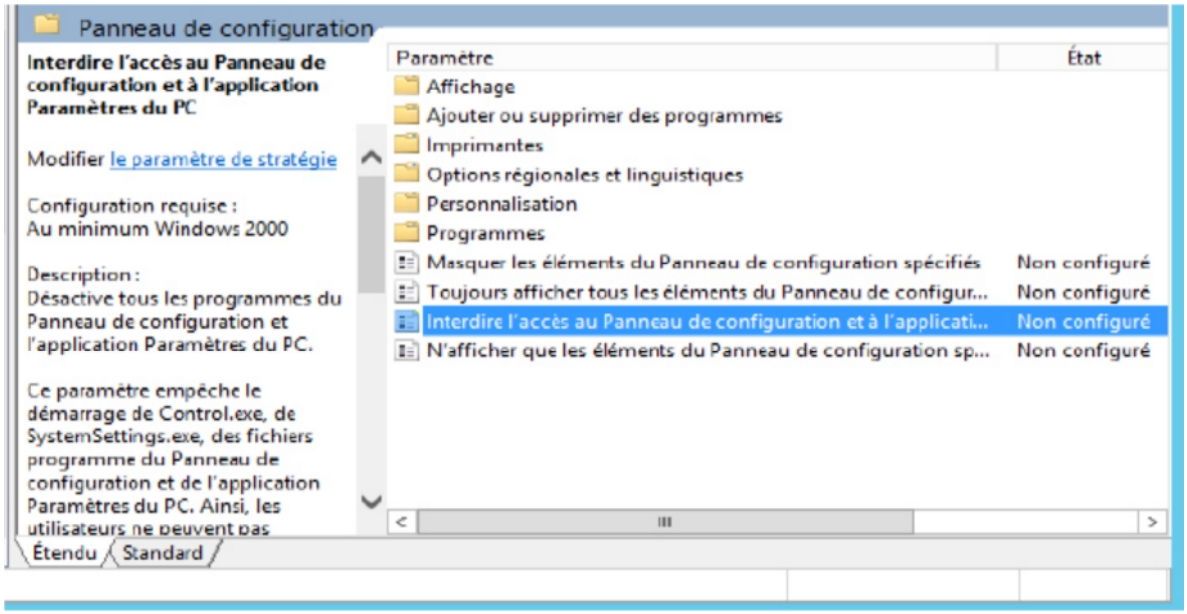


Figure 6.36 : Modifier la gestion du panneau de configuration

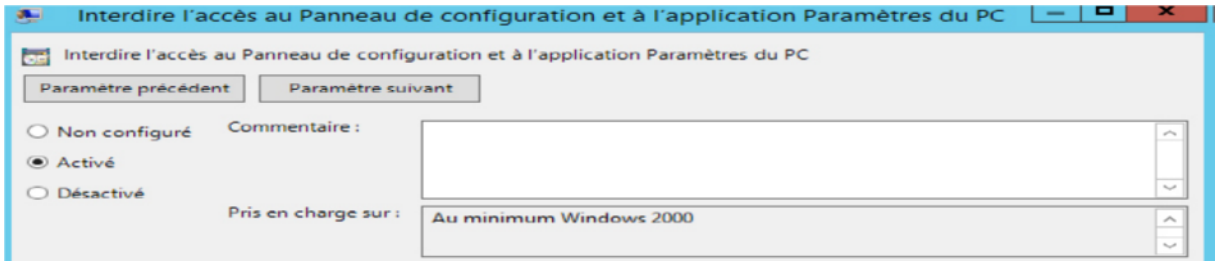


Figure 6.37 : Interdire l'accès en cliquant sur désactiver

Pour vérifier si le processus est pris en compte, nous cliquons sur démarrer et nous constatons que le menu panneau de configuration n'apparait pas. Et lorsqu'on accède aux propriétés nous recevons un message d'erreur, comme celui de prochaine figure

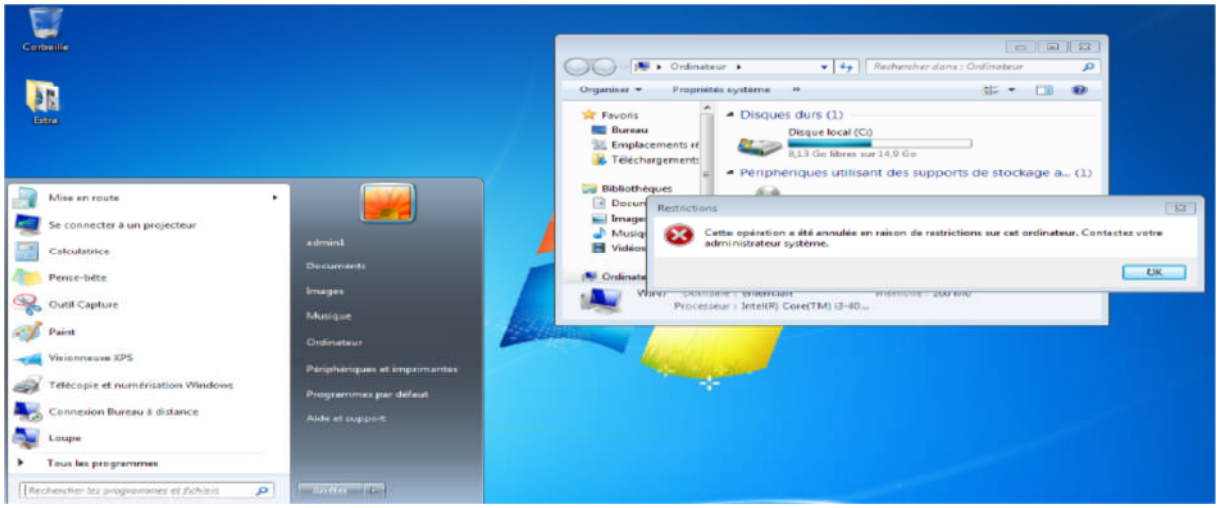


Figure 6.38 : Panneau de configuration désactivé.

Et voici le résultat d'accès« CMD »

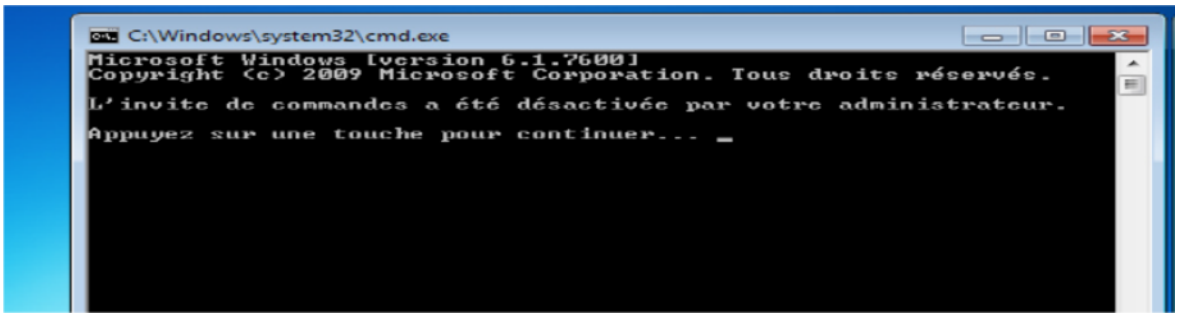


Figure 6.39: CMD désactivé.

II.7. Installation de serveur de messagerie « EXCHANGE »

- Les étapes d'installation de « Exchange Server »

✓ Joindre la machine au domaine « Algerietelecom.com »

✓ Activer les services nécessaires pour l'installation de « Exchange Server » comme (ASP.NET, ISS, SMTP)

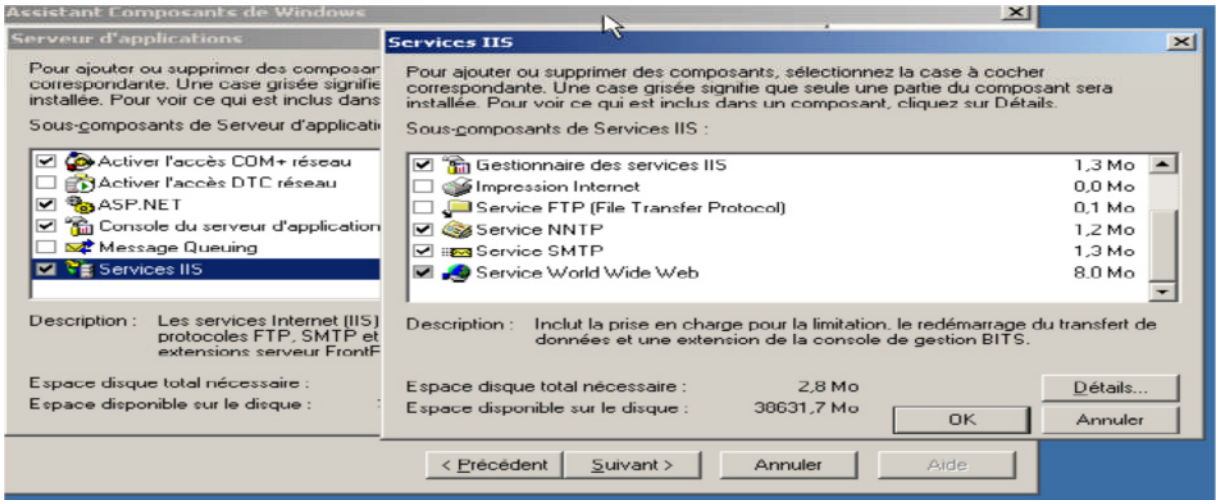


Figure 6.40: Activation des services nécessaires.

✓ Préparer la Foret

✓ Préparer le domaine

✓ Lancer le programme d'installation

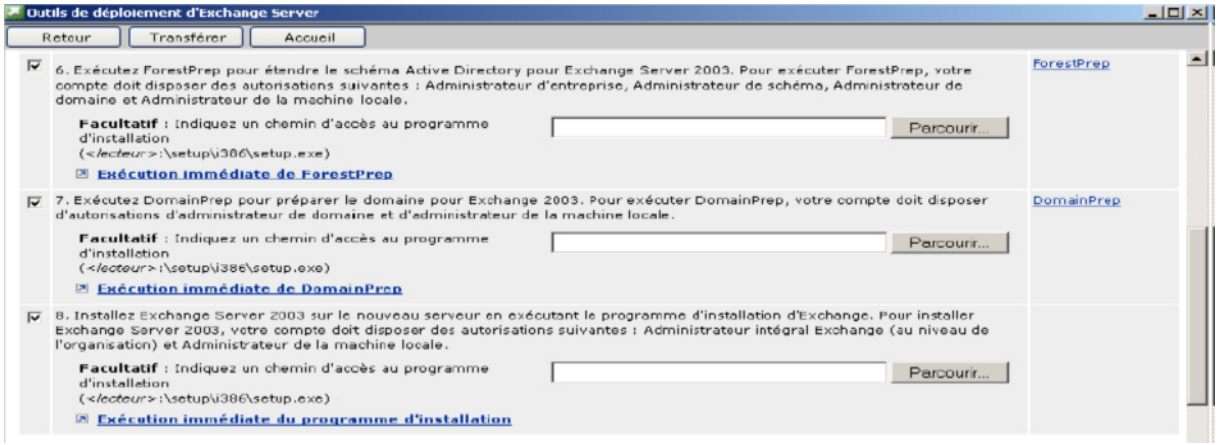


Figure 6.41 : Lancement de l'installation de « EXCHANGE SERVER »

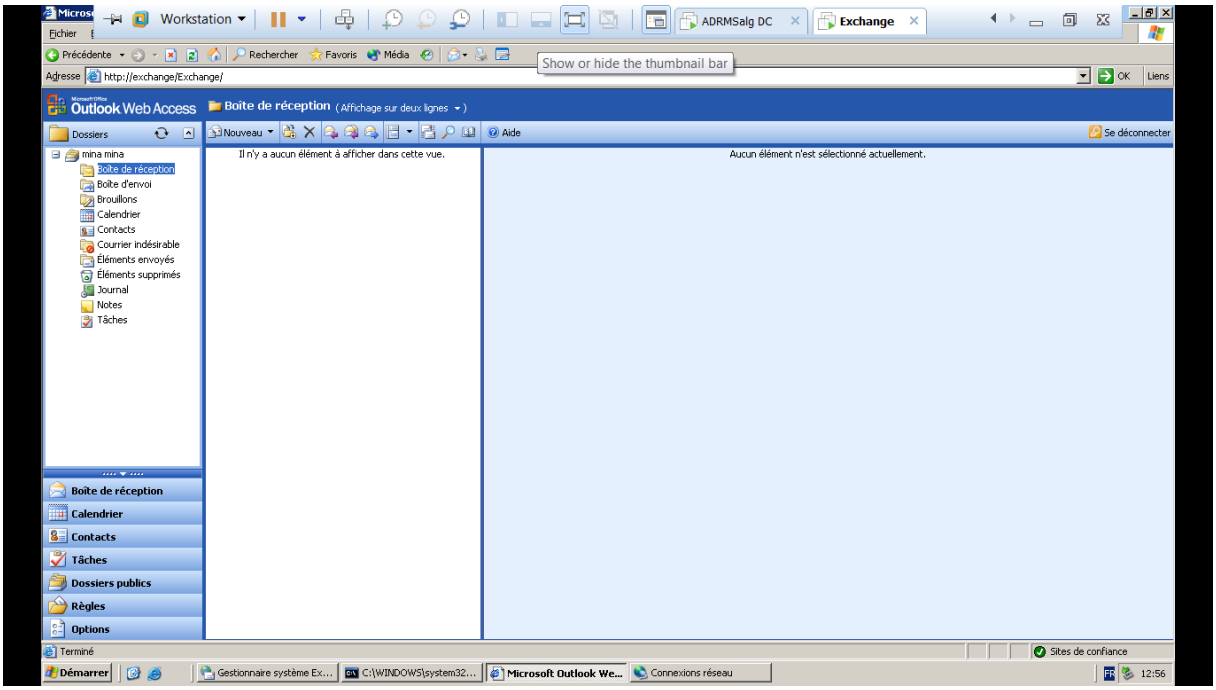


Figure 6.42 : Installation réussie.

❖ **Configuration d'Exchange Server**

➢ Création d'une stratégie de banque de boite aux lettres pour configurer les limites de stockage des boites aux lettres :

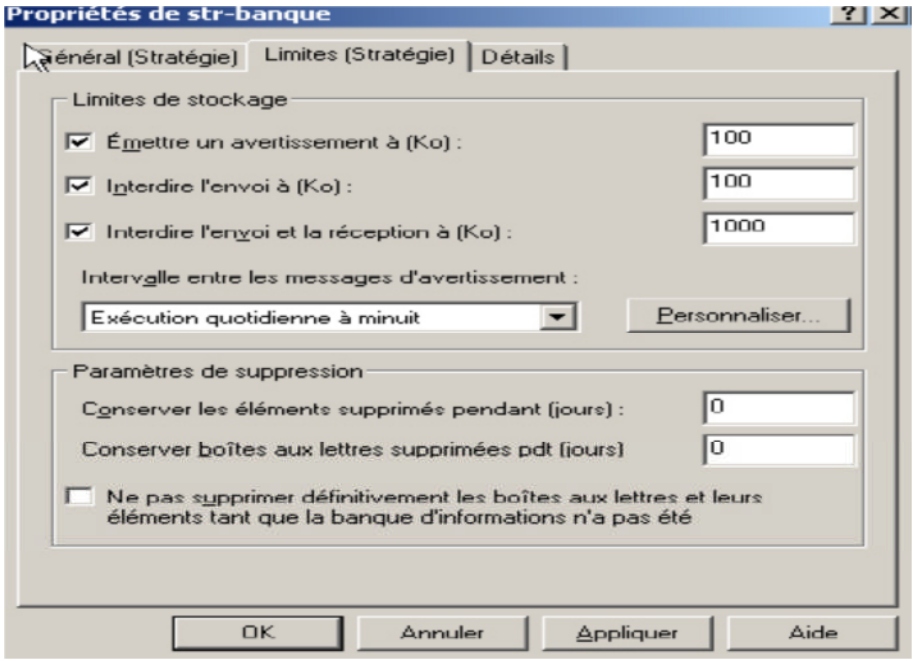


Figure 6.43 : Stratégie de banque créée.

En envoyant un message de l'administrateur à l'administrateur, en utilisant une pièce jointe qui dépasse les limites décrites dans notre stratégie, on remarque ce message d'erreur :

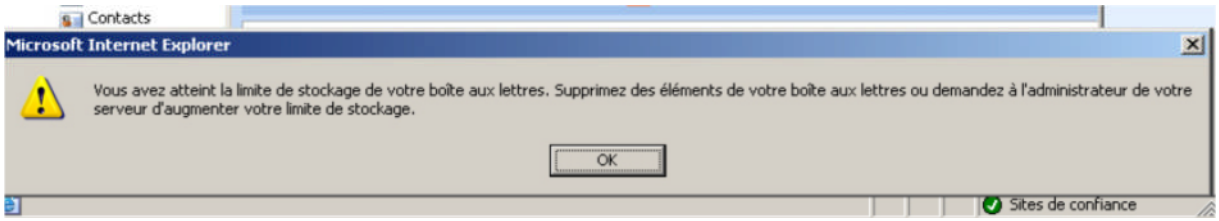


Figure 6.44 : Alerte de dépassement de la limite de stockage.

❖ **Création d'une stratégie de destination :**

Utilisée pour définir les domaines pour lesquels les serveurs Exchange devraient accepter le courrier électronique et générer les adresses de messagerie des destinataires à l'aide de ces domaines.

Exemple : configurer le format des adresses SMTP pour les employés de Tizi-Ouzou.

- Filtre : champ ville=Tizi-Ouzou.
- Adresse de messagerie SMTP : «%g.%s@Algerietelecom.com»(%g : Prénom, %s : Nom)

Donc les utilisateurs vont avoir automatiquement une adresse de messagerie qui porte le format : prénom.nom@Algerietelecom.com

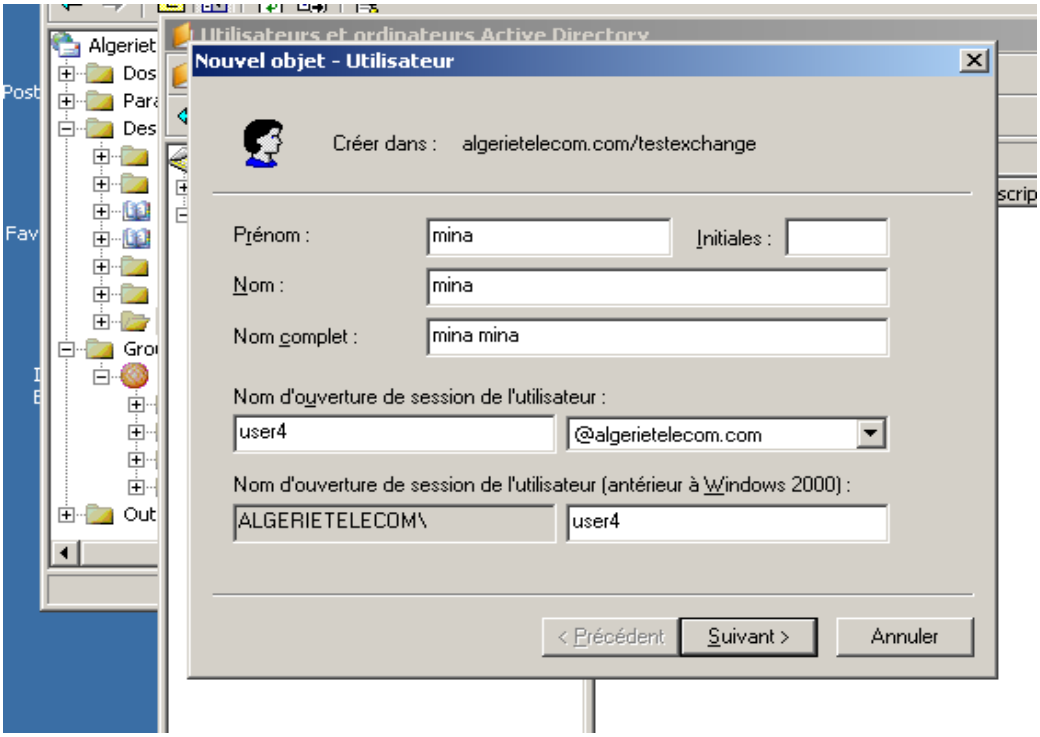


Figure 6.45 : Création d'un utilisateur.

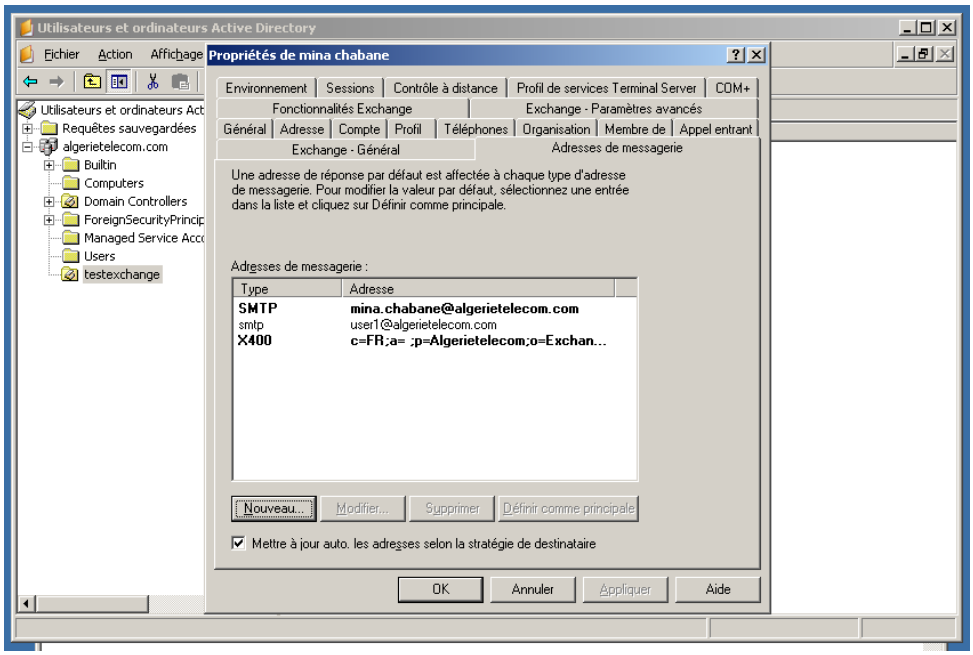


Figure 6.46 : adresse: mina.chabane@algerietelecom.com

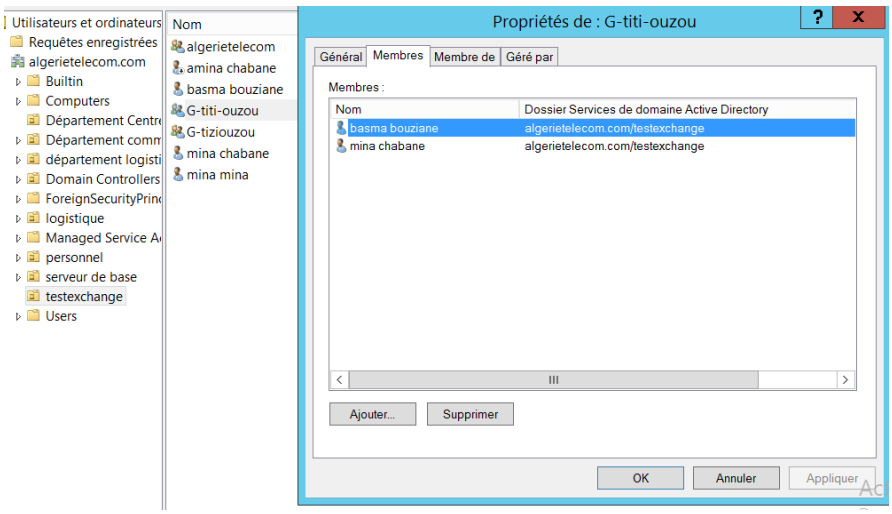


Figure 6.47 : les membres de groupe G-tiziouzou

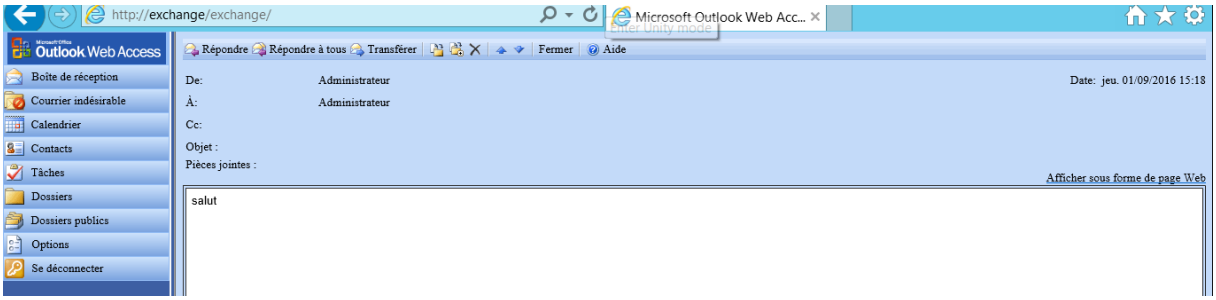


Figure 6.48 : Exchange réussit

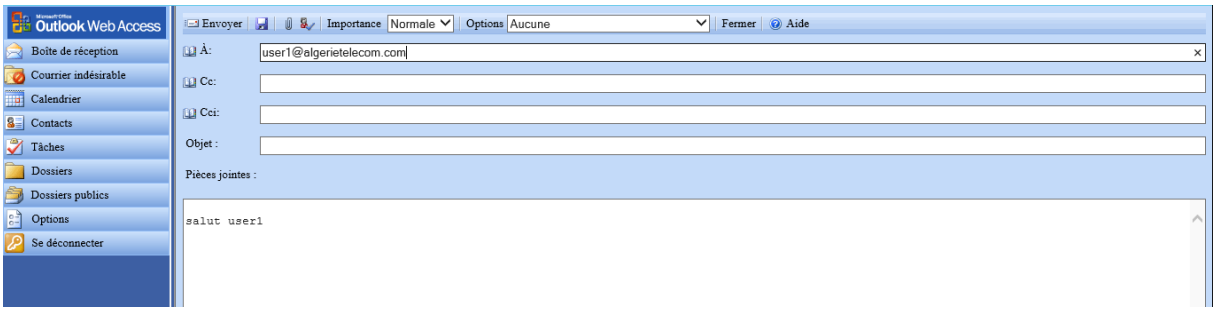
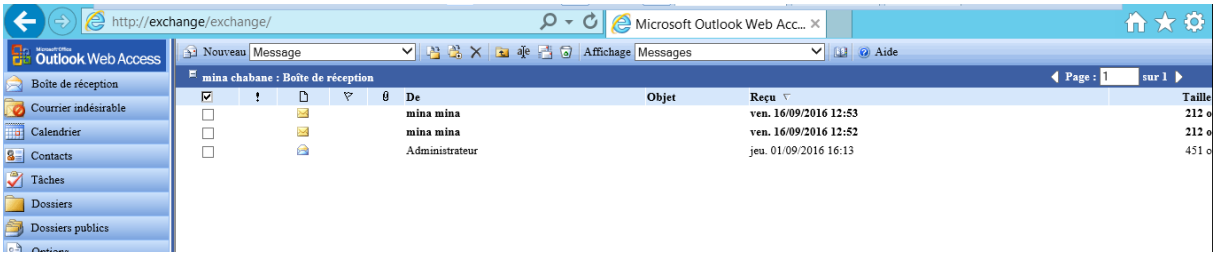


Figure 6.49 : envoie de message vers user1@algerietelecom.com



Figue 6.50 : la boite de réception du compte minachabane@algerietelecom.com

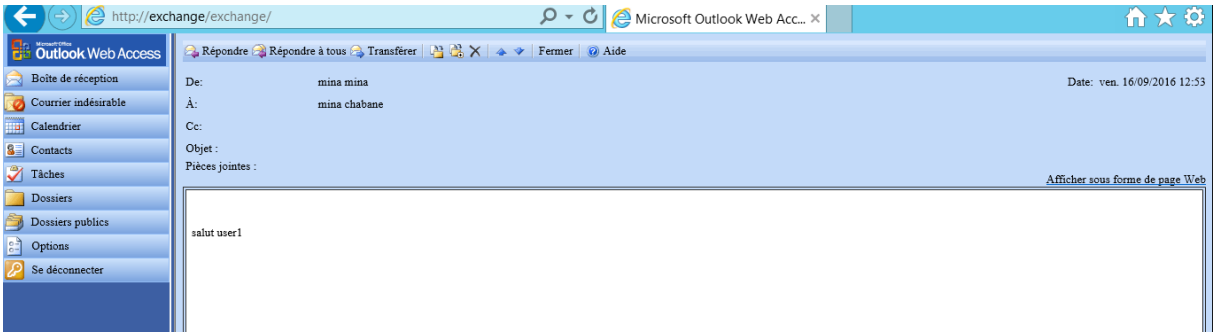


Figure 6.51 : message bien reçu

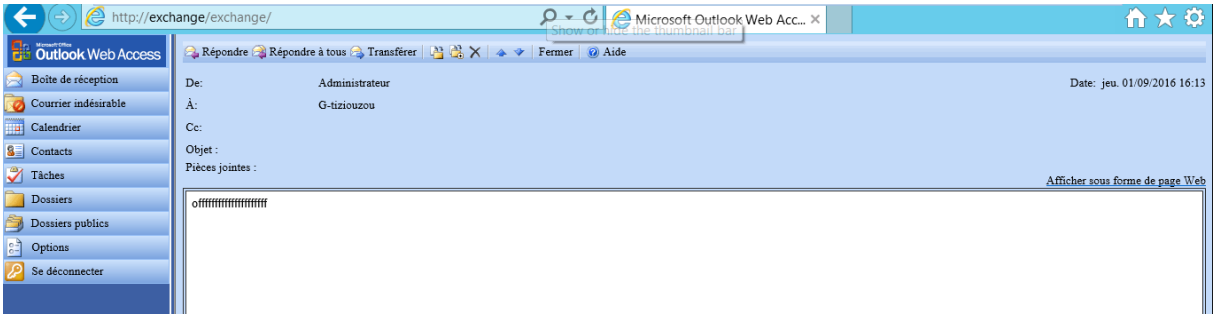


Figure 6.52 : un message envoyé par l'administrateur au groupe G-tiziouzou bien reçu

II.8. Implémentation d'un cluster d'équilibrage de charge réseau:

Ce type de cluster devient utile et intéressant lorsqu'un seul serveur ne suffit plus pour tenir toute la charge, mais aussi lorsqu'il a un temps de réponse insuffisant par rapport aux besoins des utilisateurs.

Le cluster NLB c'est-à-dire de répartition de charge réseau. Ce type de cluster devient utile et intéressant lorsqu'un seul serveur ne suffit plus pour tenir toute la charge, mais aussi lorsqu'il a un temps de réponse insuffisant par rapport aux besoins.

- **L'architecture**

Le cluster sera composé de deux serveurs sous *Windows Server 2012 R2*, accompagné d'un serveur *Active Directory contrôleur de domaine* du domaine Algerietelecom.com. Les serveurs devant être liés au cluster se nomment web-serv1 et web-serv2, le serveur Active Directory quant à lui se nomme DC1.

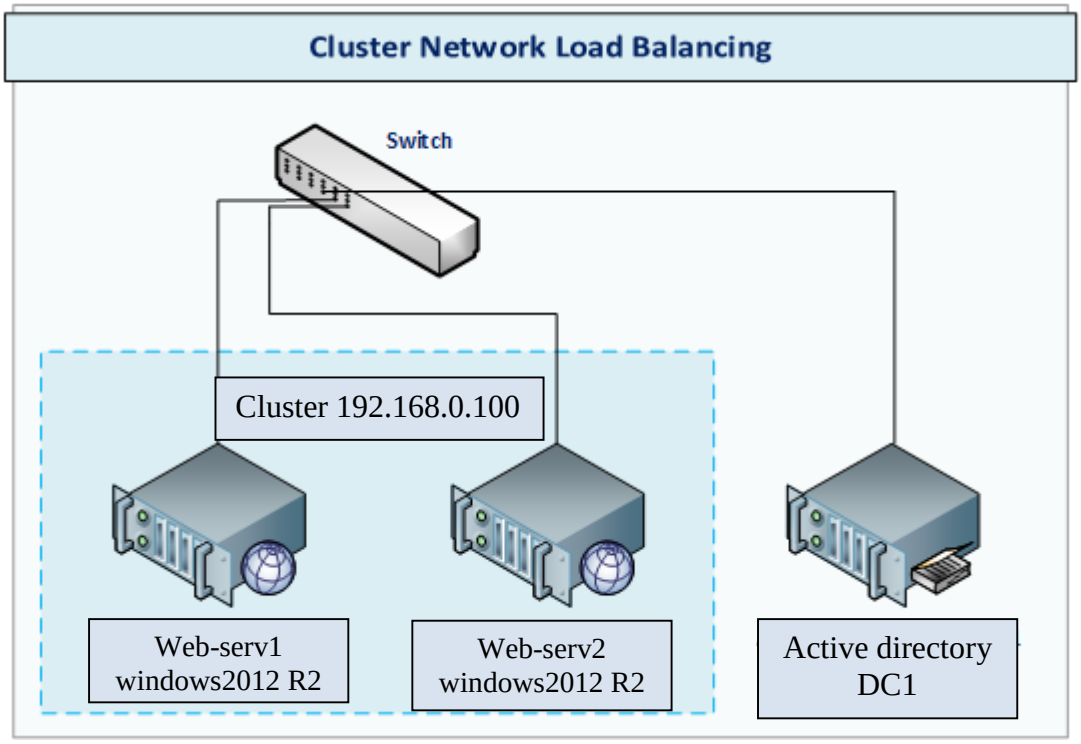


Figure 6.53 : cluster d'équilibrage de charge réseau.

- **Installation du serveur Web IIS:**

Le rôle du serveur Web de *Windows Server 2012* est de partager des informations avec des utilisateurs sur internet, intranet ou extranet. Le serveur Web *IIS* permet d'avoir une plateforme web unifiée. Une fois installé, une page par défaut s'ouvre sur le port 80.

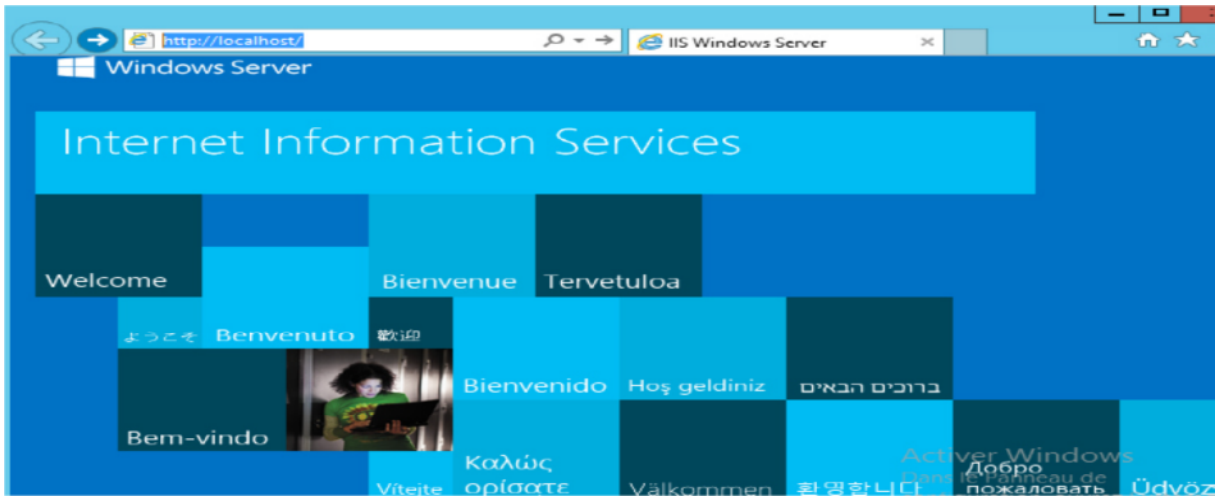
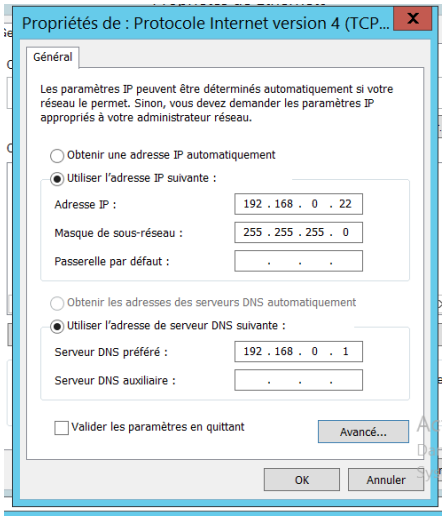


Figure 6.54 : Fenêtre IIS- 85 par défaut



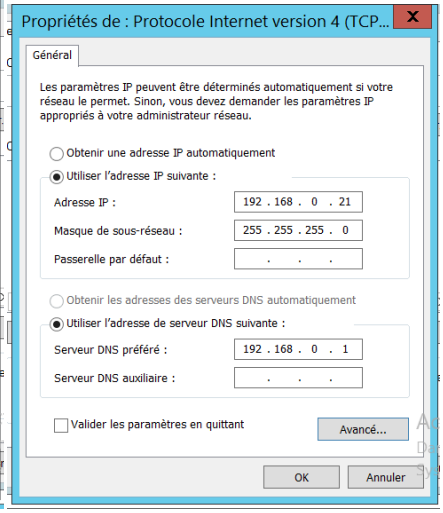


Figure 6.55 : adresse IP de web-serv1 **Figure 6.56 :** adresse IP de web-serv2

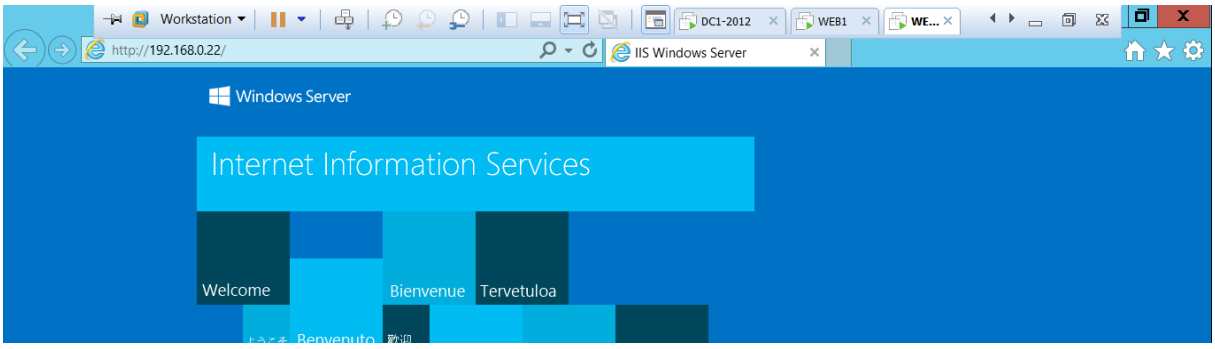


Figure 6.57 : avant de crée le cluster sur web-serv2

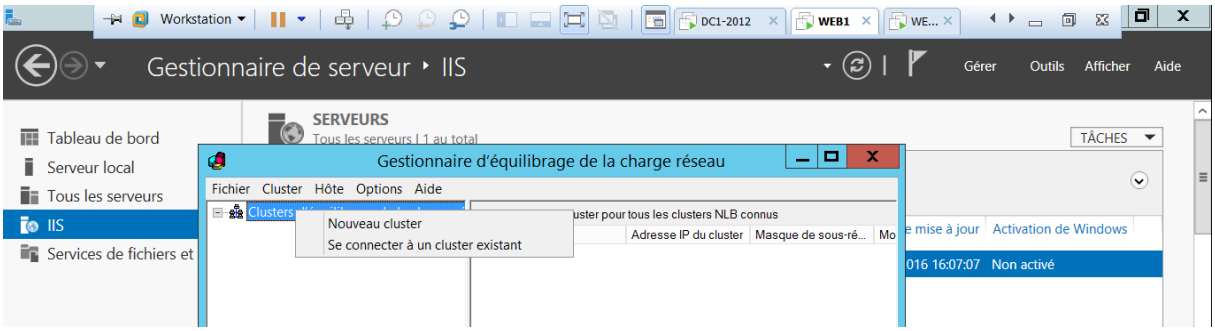


Figure 6.58 : création du Cluster NLB

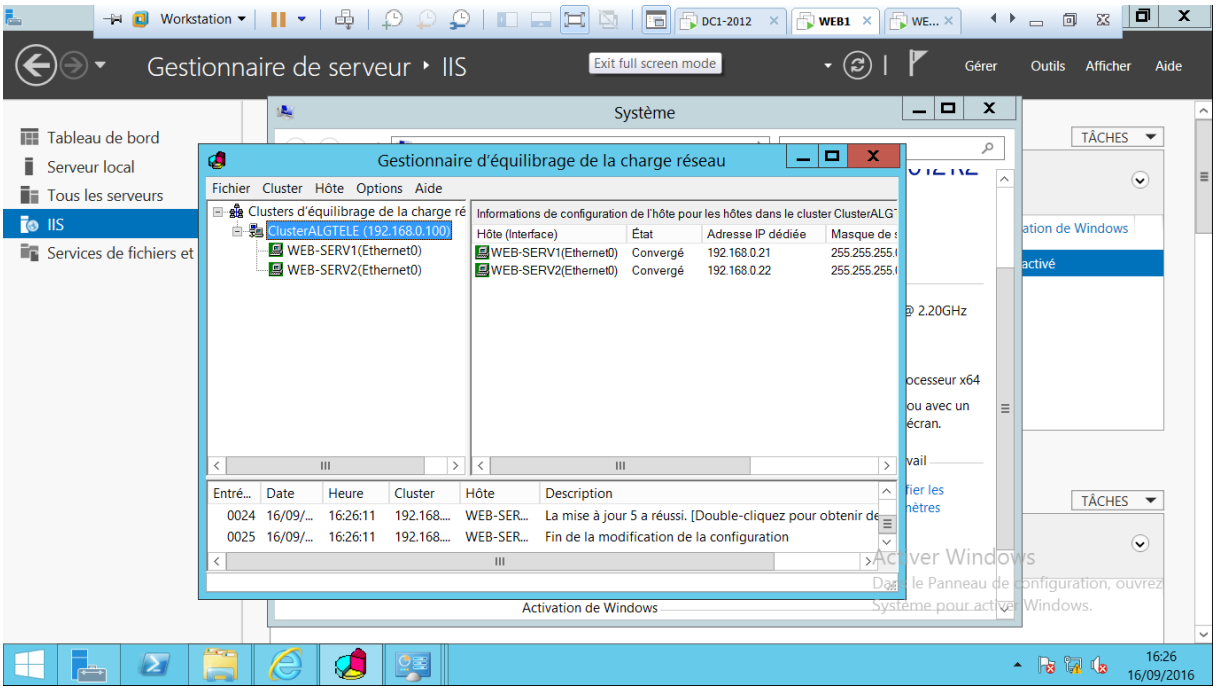


Figure 6.59 : Le cluster ALGTELE bien crée

La création du cluster NLB est désormais terminée.

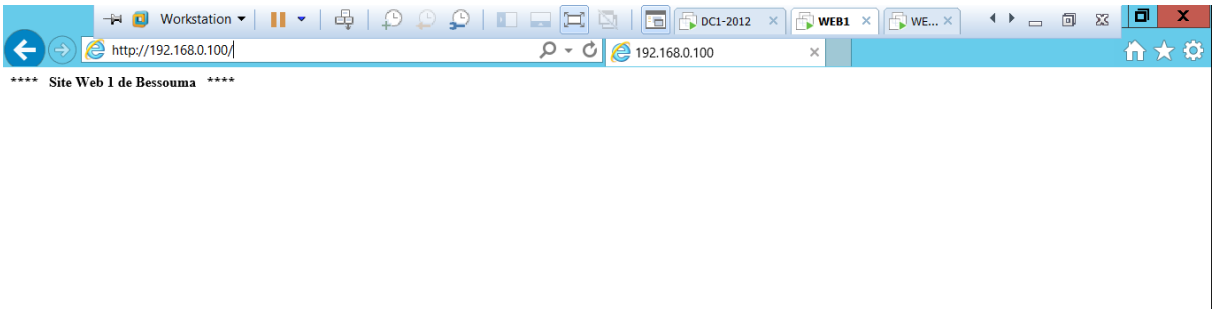


Figure 6.60 : le cluster marche bien

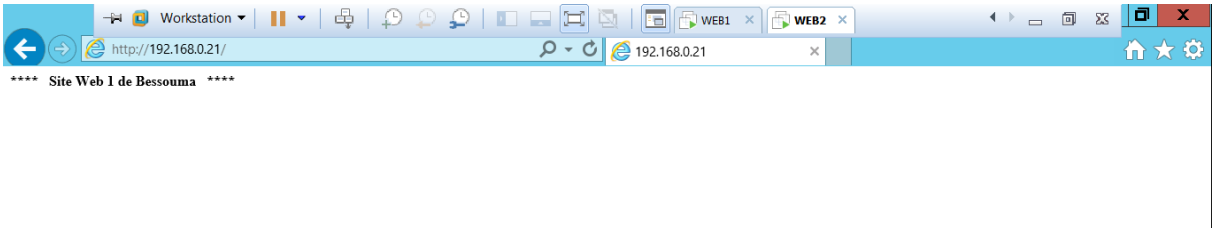


Figure 6.61 : Apres création de cluster

II.9. Configuration des VLANs

Les *VLANs* offrent un moyen de regrouper des périphériques dans un LAN. Ils permettent à un administrateur de segmenter les réseaux en fonction de facteurs tels que la fonction, l'équipe de projet ou l'application.

Chaque VLAN est considéré comme un réseau logique distinct et les paquets destinés aux stations n'appartenant pas au VLAN doivent être transférés par un périphérique de couche 3 ce qui est appelé inter-routage

Nous avons choisi de segmenter le réseau par département, et implémenter le routage inter-VLAN pour permettre la communication entre les différentes unités.

- **Plan d'adressage :**

Pour une meilleure et optimale affectation d'adresse réseau, nous avons opté pour la méthode *VLSM* pour l'adresse réseau principale : 192.168.0.0./22, qui consiste à :

- Découper un réseau (ou sous-réseau) en d'autres sous-réseaux, ceux-ci peuvent être découpés en sous-réseaux plus petits.
- La longueur de chaque sous-réseau est variable et peut être ajustée à la capacité d'adressage voulue.
- Les adresses IP d'hôtes sont attribuées à partir des adresses des sous-réseaux de sous réseaux utilisés.
- Les autres plages sont libres pour une éventuelle extension.

Le tableau suivant récapitule le plan d'adressage adopté :

Nom de VLAN	ID VLAN	Nombre d'hôte	Adresse sous réseau	Passerelle	Masque sou réseaux
Logistique	10	8	192.168.2.128	192.168.2.129	/27
Personnel	20	51	192.168.0.128	192.168.0.129	/25
Reseauentreprise	30	10	192.168.2.32	192.168.2.33	/27
Equipementtele	40	20	192.168.1.128	192.168.1.129	/26
Energieenv	50	9	192.168.2.96	192.168.2.97	/27
Entrepriseligne	60	10	192.168.2.0	192.168.2.1	/27
Reseaudon	70	50	192.168.1.0	192.168.1.1	/25
energieligne	80	10	192.168.2.64	192.168.2.65	/27
reseaubase	90	10	192.168.1.192	192.168.1.193	/26
Serveur	100	4	192.168.4.0	192.168.4.1	/27

Tableau 6.1 : représentant le plan d'adressage.

Le schéma suivant illustre le principe VLAN

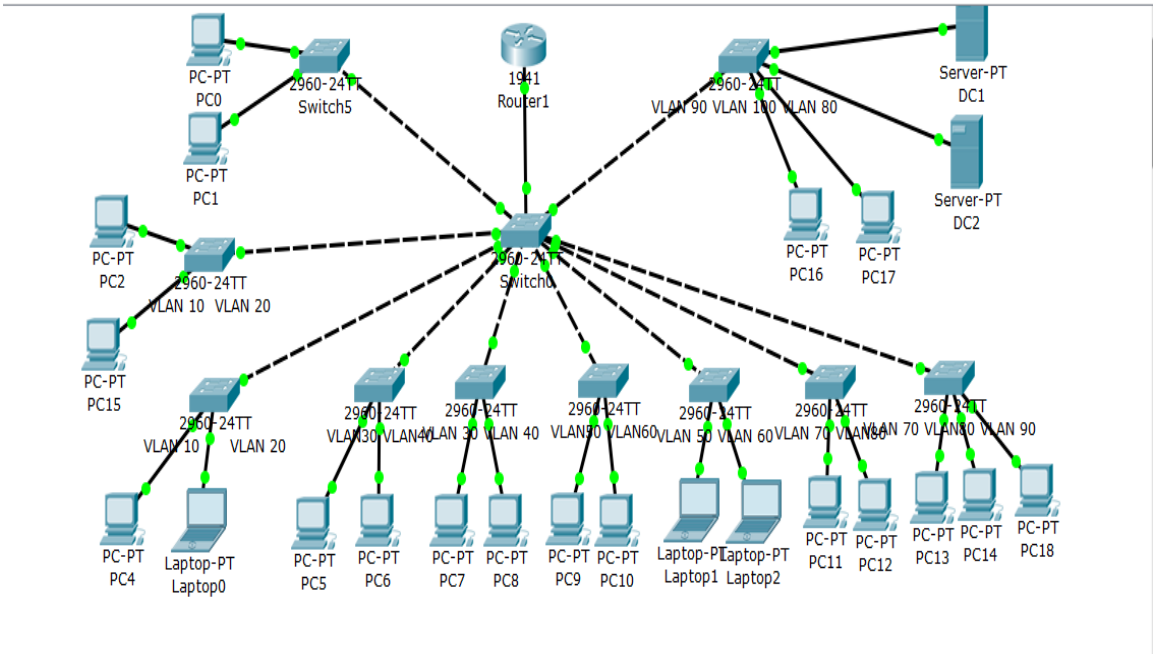


Figure 6.62 : schéma de simulation des «VLANs».

III. Conclusion

Le réseau est sécurisé et les usagers externes ne peuvent accéder qu’à la DMZ, par contre ils ne pourront pas accéder au réseau LAN, ni même percevoir son existence, ainsi la segmentation logique de l’architecture physique en VLAN et la mise en place d’un annuaire Active Directory pour la gestion centralisée des ressources, le réseau interne est aussi sécurisé.

Ce travail a été principalement axé sur l'implémentation d'une architecture réseau au sein de la direction Territoriale des Télécommunications de Tizi-Ouzou. L'objectif de ce travail consiste en le déploiement d'une nouvelle infrastructure réseau plus sécurisée en explorant des techniques de transmission plus évoluées garantissant la disponibilité et l'intégrité des données, et ce en la mise en œuvre de différentes politiques de sécurité du réseau local telles que les techniques de filtrage des paquets à travers un pare-feu, la segmentation en VLANs, les GPOs dans Windows server, l'externalisation du serveur web et messagerie dans une zone démilitarisée permettant l'isolation du LAN et le WAN, la configuration d'un tunnel sécurisé pour l'accès distant au LAN etc.….

Sécuriser un tel système consiste à assurer la confidentialité, l'intégrité et la disponibilité de ses données et ressources. De nombreux travaux ont été réalisés et plusieurs dispositifs de sécurité ont été proposés pour garantir ces propriétés. Parmi ces dispositifs les pare-feu occupent une place de premier ordre et sont des éléments cruciaux pour le renforcement d'une politique de sécurité. Ils sont largement déployés pour la sécurisation des réseaux informatiques. Le pare-feu est l'outil le plus utilisé pour sécuriser un réseau grâce à ses capacités de renforcer une politique de sécurité et d'enregistrer tous les aspects du trafic réseau.

La réalisation de ce projet était une occasion pour nous d'emprunter de nouveaux chemins dans le monde complexe de l'Informatique :

- Ce stage nous a permis de mettre en pratique et de consolider les connaissances acquises durant notre cursus universitaire et de nos recherches personnelles.
- L'implémentation de cette application nous a été un moyen de cerner aussi des connaissances pratiques qui nous étaient inconnues auparavant, à savoir l'utilisation simultanée de multiple plate-forme (Microsoft/Linux).
- L'utilisation de 'Windows Server 2012 R2' nous a offert la chance de renforcer et d'approfondir nos près requis.
- Grâce à ce travail, nous avons pu nous familiariser avec le monde du travail en entreprise car connaitre les pressions et les occupations des employés nous donnent l'opportunité de nous préparer psychologiquement pour faire face à cette réalité.

Nous estimons que la solution proposée à notre organisme d'accueil «Direction Territoriale des Télécommunications» permettra de colmater les brèches constatées au niveau du département informatique.

Toutefois, bien que notre application présente plusieurs fonctionnalités, elle reste toujours sujette à des améliorations et compléments

Nous espérons que ce modeste travail sera d'un grand intérêt pour les futurs utilisateurs et qu'ils y trouveront satisfaction.

LAN: Local Area Network

IP: Internet Protocol

HTTP : HyperText Transfert Protocol

GBIC : Gigabit Interface Converter

DTC : Data Terminal Circuit

DDP : Panneau de Distribution Direct

MDP : Panneau de Distribution Modem

AUI : Association des Utilisateurs Internet

BNC : Bayonet Neil-Concelman Connector

DCT : Discrete Cosine Transform

DVD : Digital Versatil Disque ou Digital Vidéos Disque

DDS : Digital Data Sotrage

SEI : Service Exploitation Informatique

SDSI : Service Développement des Systèmes Informatiques

MAN: Métropolitain Area Network

PAN: Personnel Area Network

WAN: Wide Area Network

OSI : Internationnal Standardization Organisation

DNS: Domain Name Service

ASCII : American Standard Code For Information Interchange

FTP : File Transfert Protocol

TFTP : Trivial File Transfert Protocol

SNMP : Simple Network Management Protocol

NFS: Network File Systèm

SQL: Strutured Query Langage

RPC: Remote Produre Call

TCP: Transport Control Protocol

UDP : Unit Data Protocol

RDP: Remote Desktop Protocol

RDS: Remote Desktop Services

RSA: Rone Rivest, Adi Shamir ET Leonard Adelman

SaaS: Software as a Service

SAN: Storage Area Network.

S-HTTP: Secure Hyper Text Transport Protocol

SLA: Service Level Agreement

SQL: Structured Query Language

SSH: Secure Shell

SSL: Secure Sockets Layer

SYN: Synchroniser

TCP: Transport Control Protocol

TLS: Transport Layer Security

TSE: Terminal Server

VLAN: Virtual Local Area Network

VM: Virtual machine

VPN: Virtual Private Network

DOD: Department Of Defense

WWW: Word Wide Web

SDH: Synchronous Digital Hierarchy

STM: Synchronous Transport Module

PBS : Polarization Beam Splitter

PBC: Polarization Beam Combiner

DoS : Denial of Service

BoF : Buffer OverFlow

BIBLIOGRAPHIE

Mémoires :

Mémoire master: « Sécurisation des Communications Client-serveur sur Multiples Plates-Formes (Microsoft/Linux) »
Réalisé par : Mr Zaidi Samir et Mr Soumah Salifou ;
Dirigé par : Mr B.Djamah. Promotion : 2015

Mémoire Ingénieur « La sécurité dans les réseaux »
Réalisé par Mr Yazid Fekhar
Proposé et dirigé par : Mr B.Djamah. Promotion : 2006/2007

Mémoire Ingénieur « Conception et Installation d'un réseau fibre optique Au campus Universitaire Vontorvorona »
Réalisé par MILAZAVATA Mahairae Tsimiondra
Année Universitaire : 2006/2007

Mémoire ingénieur « Conception et réalisation d'un software Client VPN IPSEC. Cas : ENIEM »
Réalisé par M^{elle} TOUAT KAHINA et M^{elle} HANIFI AMEL.
Promotion : 2008 /2009.

Document de l'entreprise « FIBRE OPTIQUE »

Anne d'édition 2009

WEBLIOGRAPHIE

http://www.it-connect.fr/installation-de-pfsense%EF%BB%BF/

http://irp.nain-t.net/doku.php/010fibroptique:020_fibre_optique

http://www.it-connect.fr/cours-tutoriels/administration-systemes/windows-server/

http://vroomblog.com/installation-dun-routeur-virtuel-vyatta-et-configuration-de-base/

https://rbgeek.wordpress.com/2013/05/21/how-to-configure-vyatta-as-dhcp-server-for-lan/

https://www.privateinternetaccess.com/forum/discussion/18111/openvpn-step-by-step-setup-for-pfsense-firewall-router-with-video

www.wikipédia.com