

<b>I. Introduction</b>	<b>3</b>
<b>II. Elaboration du cahier des charges :</b>	<b>3</b>
<b>A. Présentation du projet :</b>	<b>3</b>
<b>B. Etude de l'existant :</b>	<b>3</b>
1. PRESENTATION DE L'EXISTANT	4
a) Les équipements d'interconnexion :	4
b) Architecture du réseau :	6
2. ANALYSE DES BESOINS :	8
a) Les besoins fonctionnels :	8
b) Les besoins non fonctionnels :	9
3. PROBLEMATIQUE ET SOLUTION :	9
<b>C. Etude de la solution sans fil :</b>	<b>9</b>
1. Mise en place d'une architecture du réseau sans fil :	10
2. Mise en place d'une solution de gestion et de partage de fichier :	12
a) Sélection d'une meilleure plateforme :	12
b) Mise en place de la plateforme de gestion et de partage PYDIO :	12
c) Connexion et Configuration de Pydio	12
d) Présentation des interfaces de Pydio :	15
3. Choix de la norme :	17
a) L'évolution du WIFI :	17
4. Sécurité :	20
a) Méthodes d'authentification du protocole « Pfsense » :	21
b) Méthodes de chiffrement du réseau sans fil :	22
<b>III. Mise en place du réseau :</b>	<b>24</b>
<b>A. Etude du matériel :</b>	<b>24</b>
1. Les équipements d'interconnexion :	24
a) Ressources matérielles :	24
b) Ressources Logicielles :	29
<b>B. Evaluation Du Coûts :</b>	<b>30</b>
<b>C. Etude et configuration du serveur :</b>	<b>30</b>
1. Configurer le serveur DNS	31
2. Configurer le fichier de zone	33
3. Configurer le serveur esclave DNS	35
4. Configuration de base du système	36
a) Introduction	36
b) Démarrage de la machine	36
c) Installation des paquets nécessaires	37
d) Configuration et activation des paquets :	37
e) Configuration et préparation du serveur web :	38
f) Configuration de la base de données (MySQL)	38
g) Téléchargement de Pydio (gestion et partage de fichier)	39
<b>IV. Etude et configuration des postes client :</b>	<b>41</b>
<b>A. Configurer le client DNS Windows</b>	<b>41</b>
<b>B. Configurer les clients DNS Linux</b>	<b>42</b>
<b>C. Mise en place d'une plateforme de tests :</b>	<b>43</b>

D. Elaboration d'un devis :	44
V. Conclusion	45
VI. Annexe 1 :	47
1. Configuration des points d'accès :	47
2. Configuration Routeur :	47

## I. Introduction

---

Ces dernières années, les technologies sans fil ont connues un essor considérable que ce soit au niveau commercial ou dans le domaine des recherches, ceci revient aux multiples avantages qu'elles offrent (mobilité, faible coûts, etc.). Mais, comparer aux interfaces filaires, peu nombreuses sont les interfaces sans fil qui offrent un débit rapide (ondes hertziennes, l'infrarouge).

Les réseaux sans fil ont été créés pour permettre aux utilisateurs d'effectuer des communications de tel sorte à garder la connectivité des équipements, tout en ayant gain de mobilité et sans avoir recours aux `fils' utilisés dans les réseaux traditionnels et qui encombrant ces derniers. Connaissant actuellement un succès très important dont leur nombre croît très rapidement au sein des entreprises et du grand public. Ils offrent en effet une flexibilité largement supérieure aux réseaux filaires.

## II. Elaboration du cahier des charges :

---

### A. Présentation du projet :

La croissance continue dans le développement des technologies sans fil et des ordinateurs ainsi la nécessité de satisfaire les utilisateurs en leur offrant une liberté de se déplacer tout en gardant la connectivité, promet un avenir florissant pour les systèmes WLAN en particulier les systèmes le Wi-Fi.

Ce projet présente une étude d'une infrastructure de réseau sans fil pour le département à l'aide d'une technologie sans fil, utilisant les ondes radio qui éliminent les câbles. Pour ce faire une description de cette norme étant nécessaire en citant quelques caractéristiques et notions de base.

La sécurité est aussi un objet qu'il ne faut pas négliger, puisqu'elle joue un rôle important dans un réseau sans fil ou le support de transmission est difficile voir impossible de contrôler. Pour cela on essayera de donner des différentes Solutions afin d'y remédier face aux cybers attaques contre le réseau wifi et la protection de nos données serveurs.

### B. Etude de l'existant :

Nous ne saurions débuter ce travail sans avoir une idée claire et précise sur l'existant quel qu'il soit.

Après quoi, nous avons réellement débuté le travail en menant différentes recherches. Cette méthodologie de travail nous a permis d'avoir une connaissance large de l'existant.

## 1. PRESENTATION DE L'EXISTANT

Une bonne compréhension de l'environnement informatique aide à déterminer la portée du projet d'implémentation de la solution. Il est essentiel de disposer d'informations précises sur l'infrastructure réseau physique actuelle et les problèmes qui ont une incidence sur le fonctionnement du réseau. En effet, ces informations affectent une grande partie des décisions que nous allons prendre dans le choix de la solution sans fil et de son déploiement.

A l'instar d'un acheminement de données fiable au travers un réseau entre les différentes unités que disposent le département, comme les salles de lectures, laboratoires TP ...etc, La mise en place d'un réseau filaire RJ45 basé sur la technologie Ethernet, a été adopté sous une structure dite « étoile » afin d'assurer et de procurer :

- Un transfert de fichiers entre les appareils.
- Partage de ressources (partage de la connexion à internet, partage d'imprimante, disques partagés, etc.).
- Mobilité (dans le cas d'un réseau sans fil).

### ***a) Les équipements d'interconnexion :***

Dans une architecture, le matériel d'interconnexion représente le cœur du réseau, ce dernier se constitue des équipements d'interconnexion suivants :

#### ❖ Un serveur :

Ce serveur participant au bon fonctionnement du système réseau et de la mise en relation entre appareils à la gestion des données possède :

- 8 slots pour disque dur, possédant actuellement deux disques durs de la technologie du système RAID avec une capacité d'un téraoctet.

A l'aide de ce regroupement redondant de disques indépendants et ainsi lors de la défaillance de l'un des disques, le contrôleur RAID désactive le disque défaillant et une fois ce disque défectueux remplacé le contrôleur RAID reconstitue le miroir et par conséquent on obtiendra une récupération de données vu qu'ils sont interchangeable à tout moment.

- 4 cartes réseaux (une seule est connectée) + 5 ème BIA.
- Ports USB.
- Un port VGA (connecteur de type D-sub) .

- 32 slots mémoire (RAM), Soit avec une capacité de 64 go ou 32go + une RAM 32go (extensible).

#### ❖ Carte graphique :

Activée en permanence (24h/24) et Connectée au serveur à l'aide d'un connecteur PCI, avec une capacité de 6 Go de RAM, elle est utilisée à des fins de calculs intensifs notamment les plébiscités de l'intelligence artificiel.

#### ❖ Switch Manageable « administrable » :

Se trouve au niveau de la salle serveur et possède :

- 24ports : un port est relié à la carte réseau et 23 sorties disponibles.
- 4 ports à coté possédant un débit énorme.

Offre des possibilités de configuration qui permettent de modifier et de gérer son fonctionnement : VLAN, CLI, routage IP, etc. et c'est particulièrement utile pour identifier les problèmes et jouer le rôle d'un Pare-Feu, et ainsi la gestion et la configuration des adresses MAC.

#### ❖ Switch Cisco :

Un équipement disposant de fonctions avancées, qu'il vaut mieux configurer. Pour ce faire, il faut ajouter une adresse IP et une passerelle par défaut.

#### ❖ Switch ordinaire :

Un équipement qui fonctionne comme un pont multiport et qui permet de relier plusieurs segments d'un réseau informatique entre eux, analyse et vérifie l'adresse MAC de sortie et l'envoi vers cette adresse.

#### ❖ Hub :

Un boîtier chargé d'acheminer les données d'un ordinateur à un autre. Intervient à la couche une (physique), n'est qu'un simple concentrateur, et est bien moins intelligent que les switches. Il est incapable de filtrer les informations, et transmet ainsi les données qu'il reçoit à tous les ordinateurs du réseau.

#### **Le hub possède deux types de ports ou connecteurs physiques :**

- Les ports pour la connexion des machines.
- Le port pour extension du réseau auquel se connecte un autre concentrateur (il n'y en a généralement qu'un seul par concentrateur).

### ❖ Points d'accès :

C'est une borne wifi, qui, branchée à un réseau filaire va permettre de se connecter en Wifi. Cette borne va donc être reliée jusqu'à votre box, ou un switch Ethernet, par l'intermédiaire d'un câble Ethernet. Toutefois en évitant les interférences en utilisant les canaux.

Une box internet c'est donc une boîte dans laquelle il y a : un modem, un routeur, une borne d'accès Wi-Fi, un switch, un pare-feu, un serveur qui permet d'orchestrer tout ça.

### **b) Architecture du réseau :**

Comme mentionner en haut de ce projet (article), l'architecture réseau local en RJ45 actuelle du département adopté est dite : **étoile.**

Pour faire communiquer les différents matériels du réseau, deux solutions ont été mises en place :

- **Un câblage filaire :**

Avec une topologie physique en étoile dans laquelle les ordinateurs de bureau sont chacun connecté aux switch « D-Link » par l'intermédiaire d'un câble RJ45 répartis comme suit :

Le **Switch manageable** dit administrable est relié aux deux commutateurs situés dans l'armoire du couloir. Ces derniers permettent de partager une connexion filaire et ont pour rôle de relier plusieurs postes de travail à l'aide d'un câblage physique encapsulé dépendamment de la présence ou non de Switch, ou de routeurs dans les différentes salles du département : (voir la figure 1 ci-dessous)

- **Les salles qui dispose un Switch :**

Les câbles Ethernet des prises RJ45 (celles pour brancher les câbles Ethernet) directement dans les murs sont reliés au port VLAN du Switch de telle sorte que ce câble unisse Switch et Ordinateurs.

- **Les salles qui dispose routeur :**

À l'aide d'un autre câble Ethernet, le port RJ45 du switch est raccordé à l'un des ports Ethernet du routeur qui va ensuite propager une connexion sans fil.

- **Les salles qui ne dispose ni switch ni routeur :**

Les ordinateurs sont directement relié grâce aux câbles Ethernet au switch ordinaire de la petite baie de brassage spécifique au switch.

(Le nombre de câbles utilisés = le nombre de prises RJ45 dans la salle).

- **Un réseau sans fil (Wifi) :**

Une architecture composée de 5 points d'accès, dont chacun est dispatché dans ces pièces :

- LABO 1.
- LABO 7.
- LABO 10 .
- Salle de lecture principale .
- Salle de lecture actuellement dédiée aux Etudiants Master 2.

Ces points d'accès servent à relier des machines distantes de quelques dizaines de mètres comme illustrations les ordinateurs spécifiquement équipés d'une carte Wifi (IEEE 802.11), ou les téléphones portables ...etc .

Le WIFI joue le rôle de la borne d'accès qui est elle-même reliée au switch et qui capte toutes les communications qui circulent dans les airs, offrant un service de 9 à 12 accès aux utilisateurs.

Tous les ordinateurs fixes fonctionnent et se communiquent en réseau avec la topologie étoile au travers du Switch qui est relié à son tour au serveur par l'intermédiaire du switch managéable (pour l'accès au serveur WEB).

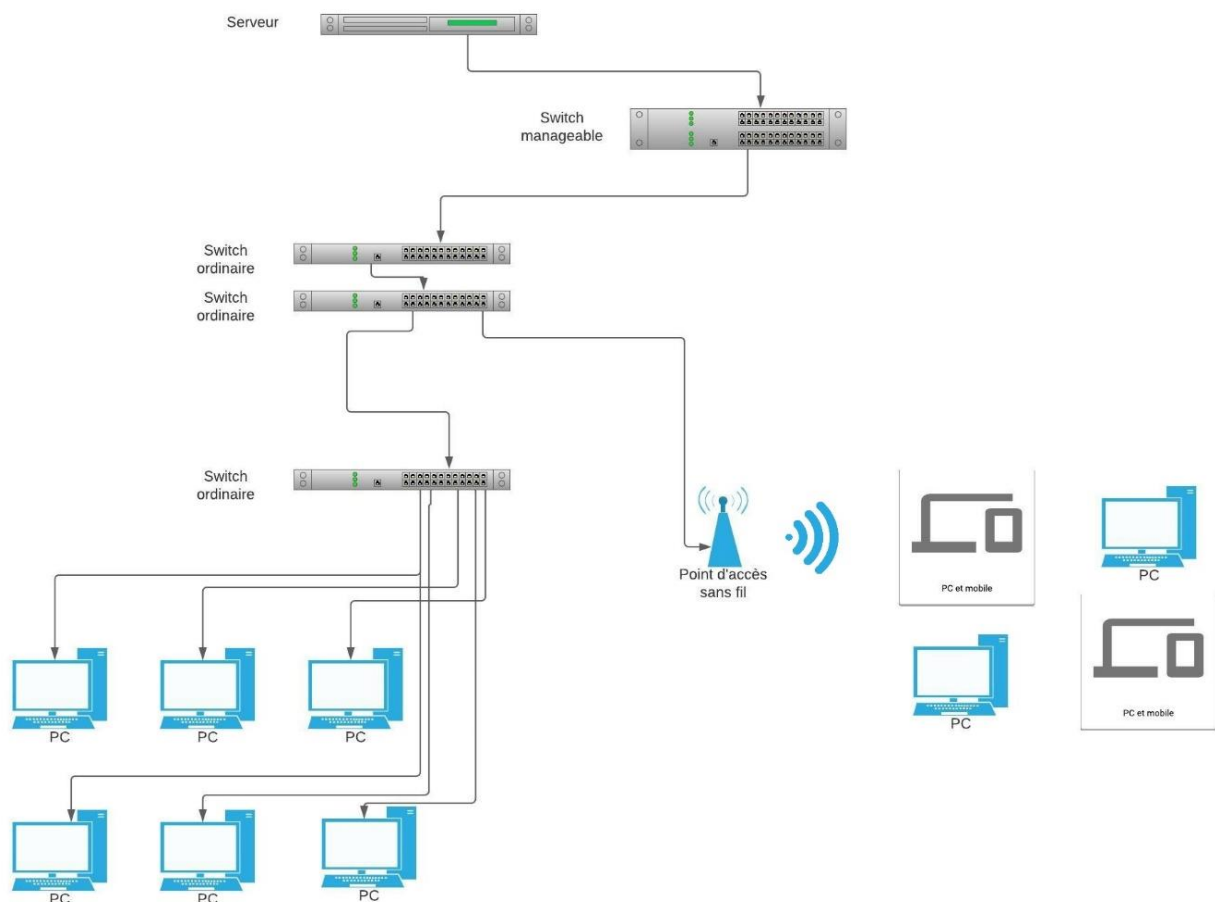


Figure II-1: Architecture du réseau filaire actuel

**Cette architecture comprend entre autres comme point forts :**

- Disposition d'un Switch administrable.
- Disposition d'un serveur performant.
- La salle serveur est très bien protégée avec onduleurs.
- Une connexion internet haut débits à 4Mbps.

**L'étude du réseau du département, nous a permis de déterminer un nombre important de contraintes pouvant réduire ses performances, voir sa dégradation, on a :**

- Un plan d'adressage réseau moins optimal et évolutif.
- Les équipements du réseau Utilisent une authentification Par défaut (Login par défaut).
- Pas de sécurité logicielle pour les réseaux existants (filtrage, authentification).
- Présence de dorsale (réseau cœur) à base de paires torsadées catégorie 2.
- Le positionnement (excentré) du point d'accès du Wifi ne permet pas de couvrir toute la zone du département, par conséquent certains étudiants ne peuvent pas accéder à internet via Wifi.
- Câblage informatique ancien qui occupe de la place dans les armoires.
- Au niveau du réseau wifi, l'allocation des adresses se fait de façon dynamique sans une demande d'authentification, ce qui fait quand un point d'accès sans-fil est connecté à un réseau matériel dont la sécurité se base sur le contrôle d'accès physique et fait confiance à tous les utilisateurs du réseau local, n'importe qui dont le point d'accès sans-fil est à la portée peut se rattacher au réseau et faire des dégâts.
- L'absence d'une segmentation du réseau en vlan ou en sous-réseau favorise l'action des utilisateurs pirates.
- les vitesses de transferts de données en Wifi sont toujours assez frustrantes dans de nombreuses situations (Téléchargement d'un gros fichier, streaming...).

## **2. ANALYSE DES BESOINS :**

Suite à la critique de l'existant, quelques besoins ont été relevés afin de pallier aux contraintes précédemment mentionnées.

### **a) Les besoins fonctionnels :**



Ce sont les besoins exprimés par le service technique « l'administrateur réseau du département » pour mener à bien ce projet.

Dans ce cadre, nous allons :

- Proposer une architecture physique d'interconnexion sans fil avec débits adaptés.
- L'accès Internet haut débits à 4Mbps pour plus de 200 utilisateurs.
- Centraliser la gestion des adresses et d'éviter des conflits d'adresses IP.
- La sécurité des accès au réseau (mot de passe : longueur, caractères spéciaux, filtrage, cryptage).
- Toute procédure de paramétrage d'un point d'accès sans-fil devrait mettre l'accent sur la sécurité besoin d'élargir la portée du rayonnement du Wifi afin de couvrir toute la zone souhaitée.
- Besoin d'authentifier toute personne souhaitant se connecter au réseau Wifi pour accéder à internet.

### ***b) Les besoins non fonctionnels :***

Les besoins non fonctionnels représentent les exigences implicites auxquelles le système doit répondre.

Ainsi à part les besoins fondamentaux, notre système doit répondre aux critères suivants :

- La performance du réseau (temps de réponse) .
- Besoin d'incompatibilité matériel (carte réseau dite adaptateur).
- La simplicité d'utilisation des services implémentés.
- La centralisation de l'administration, enseignants et de la gestion des utilisateurs.
- La fiabilité (moyenne de temps de bon fonctionnement).
- Besoin de performance des commutateurs.
- Besoin de sécurité des commutateurs.

## **3. PROBLEMATIQUE ET SOLUTION :**

L'objectif principal de ce projet est de mettre en place une infrastructure réseau sans fil optimisée pour le département d'Informatique.

### **C. Etude de la solution sans fil :**

## 1. Mise en place d'une architecture du réseau sans fil :

Lors de notre présente autopsie, nous avons étudié et identifié les principales composantes du réseau actuel de notre département, forcés de constater qu'il y a un problème sur l'utilisation et l'implémentation actuelle du réseau sans fil, qui est très limité.

C'est pourquoi nous avons décidé de mettre en place une architecture qui va combiner sécurité et facilité d'usage. Le but original de notre réflexion est de diversifier l'utilisation actuelle du réseau sans fil, tout en tenant compte des aspects de compatibilité avec l'ensemble des matériels (actuels et futurs) d'une part, et d'autre part avec l'ensemble des protocoles réseaux en interconnexion.

Notre architecture est présentée comme une couche de services réseau, elle est composée de plusieurs équipements réseau et d'interconnexion :

Pour assurer les aspects de sécurité, de performance et de disponibilité, nous avons opté pour le serveur de virtualisation (cela va nous éluder la mise en place de beaucoup de serveurs physiques). Par conséquent, on obtiendra donc au final donc une couche matérielle (le serveur) et une autre couche virtuelle en installant un système d'exploitation de virtualisation (**VMware ESXI**) sur notre serveur.

La nouvelle architecture du département sera composée de :

- **10 points d'accès** très puissants de marque **Tenda** qui seront distribués dans les différents laboratoires de TP et de recherches (**Labo1, Labo4, Labo5, Labo8, Labo9, Labo LARI, Salle de lecture**). Ainsi, ce dispositif permet aux périphériques sans fil situant dans le périmètre du département de se connecter au un réseau câblé sous forme de **hotspots WiFi**.
- **13 switchs TP-link :**
  - **10 switch :** chaque labo sera équipé d'un switch.
  - **1 switch :** un autre switch qui jouera le rôle du chef d'orchestre, par définition, il va orchestrer tous les switchs dispatchés dans chaque labo en les reliant.
  - **1 switch :** le bureau des enseignants sera équipé d'un switch.

Ces switchs vont servir de support de communications et vont permettre le partage et l'interaction de données entre les différents types de composants du réseau.

- **Une carte réseau dite adaptateur réseau sans fil :**

Elle sera insérée à l'intérieur de chaque ordinateur sur le port PCI-Express (ou PCI s'il est assez ancien) de la carte mère pour permettre de faire en sorte que l'ordinateur ait une connexion sans fil avec le routeur sans fil ou tout autre périphérique réseau. Et offrir la possibilité d'interaction entre plusieurs périphériques sans fil à l'ordinateur sans utiliser d'USB ou d'Ethernets pour recevoir ou transmettre les données.

- **Les câbles RJ45 Cat 5 et Cat 6 :**

Le câble D-Link catégorie 5 sert de moyen de liaison pour la transmission de données à des débits allant de 10 à 1 000 Mbit/s à l'intérieur du département.

Le câble D-Link catégorie 6 sert de moyen de liaison pour la transmission de données à l'extérieur du département.

- **Amplificateur wifi netgear ex7300 :**

Il a pour fonction principale d'augmenter la puissance du signal du réseau émis par notre routeur principal **TP-LINK Archer AX6000** sans qu'aucun câble ne soit tiré et que nous allons le placer dans la salle LARI afin d'exploiter une meilleure connexion au niveau des amphithéâtres.

- **Routeur wifi : TP-LINK Archer AX6000**

Cet appareil permettant de créer un réseau Wi-Fi dans notre département en étant relié au switch administrable se trouvent dans la salle du serveur. Ainsi, il fait en sorte de propager le réseau sans fil et les informations provenant d'Internet aux différents points d'accès du modèle Tenda i24 et par la suite ces derniers feront distribuer le réseau à nos appareils personnels.

**Présentation de la relation entre ces différents composants à l'aide d'un schéma :**

Pour pouvoir former un réseau informatique, les différents équipements devront communiquer entre eux à travers des câbles Ethernet comme l'illustration ci-dessous l'indique :

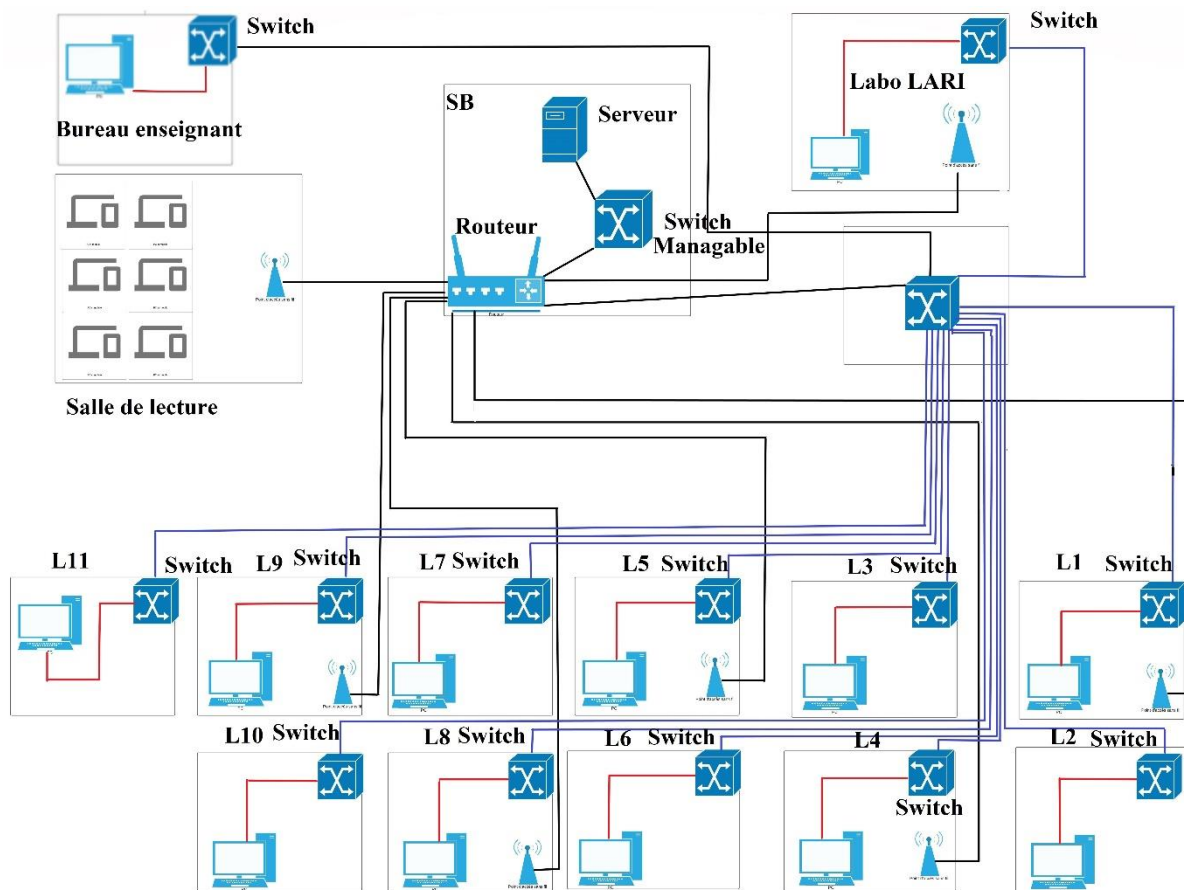


Figure II-2: Architecture réseau sans fil proposée

## **2. Mise en place d'une solution de gestion et de partage de fichier :**

### **a) Sélection d'une meilleure plateforme :**

Une fois la solution de gestion et partage de fichier sélectionnée. Nous sommes passer à l'étape de sélections des meilleures plateformes disponibles sur le marché et notre choix c'est fait en fonction de ces point précis, **la stabilité, logiciel libre, la disponibilité du support, la fréquence de mise à jour, l'opinion des utilisateurs.**

Après une multitude d'analyse, test, recherche. Nous avons tiré une plateforme qui respecte la majorité des 5 critères sur lesquelles nous nous sommes basés :

- **Pydio**

Notre choix s'est porté sur Pydio, car en plus du respect total de nos critères, cette plateforme propose de nombreuse fonctionnalité tout prête qui attire notre attention, comme (compteur de fichier partager, contrôle du destinataire, compteur de vue sur un partage et log des destinataires).

### **b) Mise en place de la plateforme de gestion et de partage PYDIO :**

Pour la mise en place nous avons commencé par installer un serveur linux sur une machine, puis nous avons procéder à la configuration de base des dépôts et la mise à jour de tout le système et logiciel, une fois avoir fini tout cela, nous sommes passés à l'installation des prérequis qui sont indispensables pour le bon fonctionnement de Pydio.

### **c) Connexion et Configuration de Pydio**

Pour nous connecter au serveur Pydio il nous a suffi d'entré l'adresse de ce dernier dans une barre de recherche d'un navigateur exécuté sur une machine cliente du réseau de l'institut comme suite, en premier lieu en nous affiche une fenêtre de diagnostic de l'état de tous ces prérequis comme on le voit sur cette image .

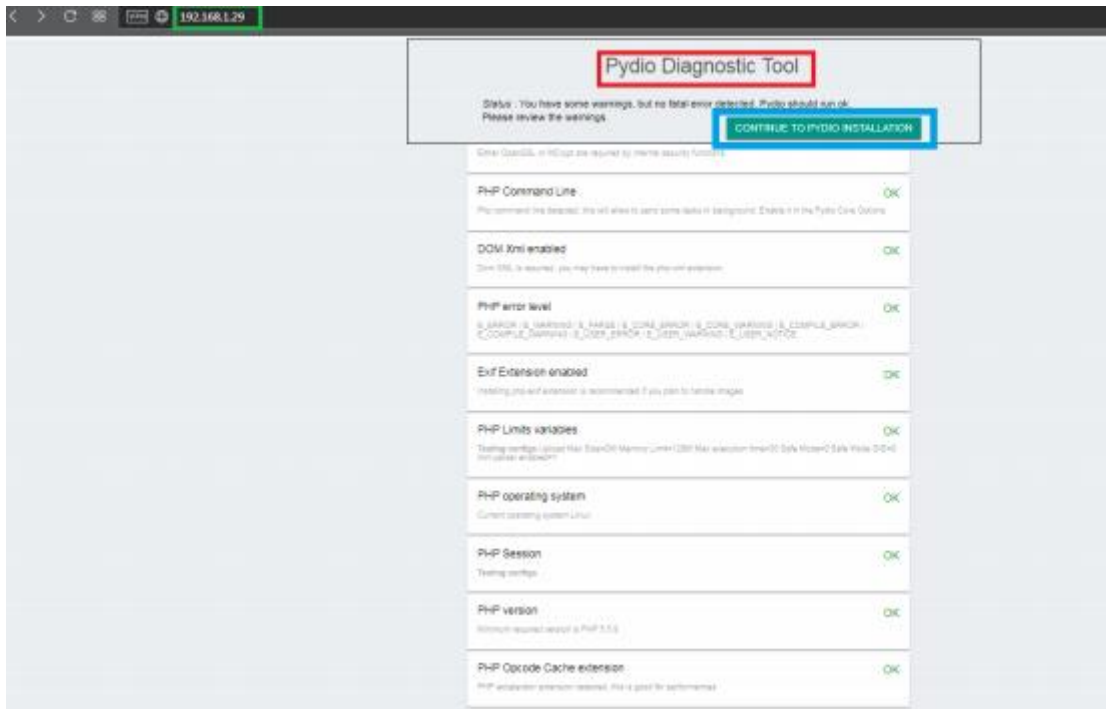


Figure II-3: Première connexion au serveur pydio

Puis une fois les vérifications finies, nous transitons sur la configuration de base de Pydio via son setup wizard (configuration assisté), et en premier nous devons configurer la langue .



Figure II-4: configuration du langage du serveur

Puis nous passons à la configuration du nom et du message de bienvenue et nous renvoi à l'étape suivante qui consiste à attribuer un nom et un mot de passe de connexion pour le compte administrateur.

The first screenshot shows the 'Paramètres de l'application' (Application Settings) step. It includes fields for 'Titre de l'application' (Application Title) set to '2INTPartners/Pydio', a 'Message de bienvenue' (Welcome Message) set to 'Bienvenue sur le gestionnaire de fichier 2INT', and a 'Message supplémentaire' (Additional Message) field. A 'SUIVANT' (Next) button is at the bottom.

The second screenshot shows the 'Authentification' (Authentication) step. It includes fields for 'Identifiant de l'administrateur' (Administrator Username) set to 'admin', 'Identifiant alphanumérique' (Alphanumeric Username), 'Nom affiché pour l'administrateur' (Administrator Display Name) set to 'admin', and 'Nom de l'utilisateur' (User Name). There are password fields for 'Mot de passe de l'admin' (Administrator Password) and 'Confirmer' (Confirm). A 'SUIVANT' (Next) button and a 'RETOUR' (Back) button are at the bottom.

Figure II-5: configuration du domaine et de l'utilisateur

Et finalement nous passons à la troisième et quatrième étape qui consiste à configurer la base de données qui sera utilisé par Pydio et les options avancées qui ces dernières consistent à finaliser la configuration et ajouter l'adresse mail de l'administrateur du réseau.

The third screenshot shows the 'Base de données' (Database) step. It includes fields for 'Base de Données' (Database) set to 'MySQL', 'Host' set to '127.0.0.1', 'Base de Données' (Database) set to 'pydio', 'Utilisateur' (User) set to 'pydio', and 'Mot de passe' (Password) set to 'pydio'. A 'TESTER LA CONNEXION' (Test Connection) button and a 'RETOUR' (Back) button are at the bottom.

The fourth screenshot shows the 'Options Avancées' (Advanced Options) step. It includes fields for 'Encodage détecté' (Detected Encoding) set to 'UTF-8', 'Detecté Server URL' set to 'http://192.168.1.29/', 'Activer le cache (recommandé)' (Activate cache (recommended)) with a toggle switch, 'Activer les courriels' (Activate emails) with a toggle switch, 'Programme d'envoi de courriels PHP' (PHP email program) set to 'Mail', and 'Courriel de l'administrateur' (Administrator email) set to 'admin@2int.local'. A 'TESTER LA CONNEXION' (Test Connection) button and a 'RETOUR' (Back) button are at the bottom.

Figure II-6: figure de configuration de base de données et serveur local

Et voici que la page s'actualise et nous offre le panneau d'authentification et cela va permettre d'accéder au compte administrateur et à l'interface de gestion de Pydio.



Figure II-7: Authentification

#### **d) Présentation des interfaces de Pydio :**

Pydio possède deux interfaces distinctes : une pour l'utilisateur et une autre pour l'administration du serveur Pydio. Celle de l'utilisateur est relativement simple, ce qui la rend facile d'utilisation, et celle de la configuration des paramètres est assez chargée mais pas compliquée car tout est détaillé sous forme de commentaires, ce qui aide et facilite la configuration.

1) Une interface utilisateur et relativement simple, elle dispose de :

- a. **En premier, représenté par la couleur verte :** nous avons les Workspaces, ces derniers regroupent les fichiers pour vous permettre d'organiser vos données. Ils peuvent être seulement accessibles par vous-même ou partagés par plusieurs utilisateurs. Et tous les dossiers qui seront partagés par les autres utilisateurs vous apparaîtront ici.
- b. **En second représenté par la couleur bleu :** nous avons le moteur de recherche pour trouver des fichiers dans tous les workspaces qui vous appartiennent.
- c. **En troisième représenté par la couleur marron :** nous avons l'onglet des widgets qui permet d'ajouter, de télécharger ou supprimer les widgets.
- d. **En quatrième et dernier onglet :** nous avons la page où sera affiché le résultat d'une recherche ou les fichiers contenus dans un dossier ou toute autre chose, mais si aucune tâche n'est effectuée, cet onglet affiche automatiquement l'historique de l'utilisation de votre compte.



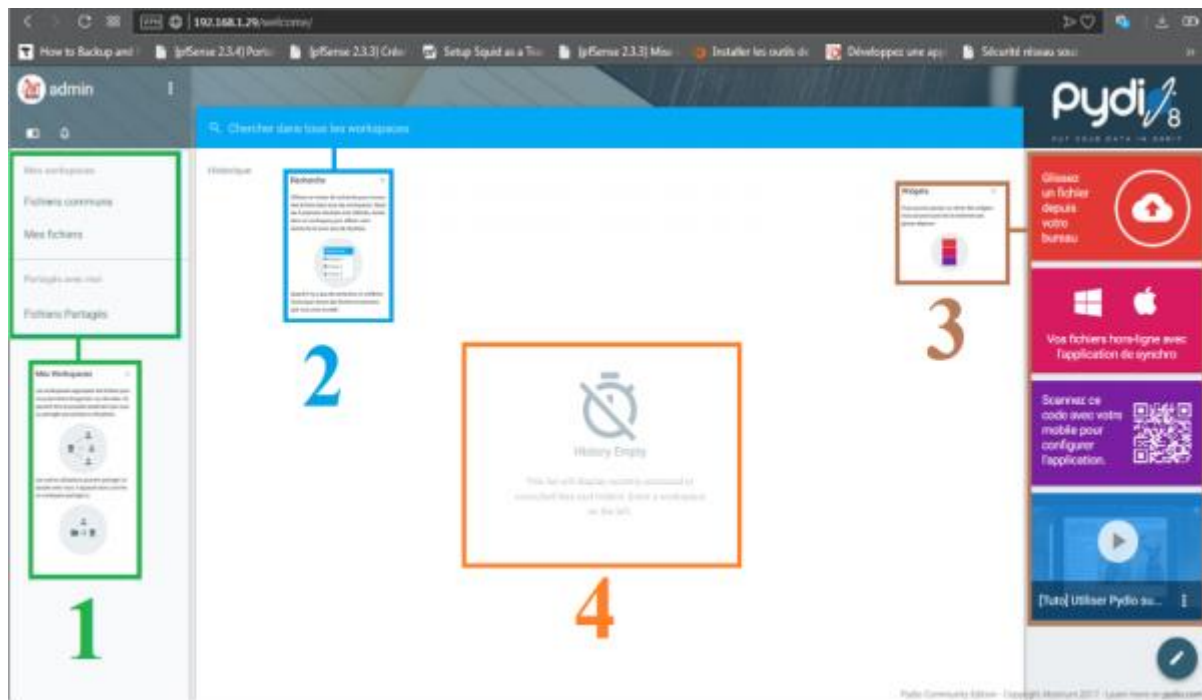


Figure II-8: interface web Pydio

Interface administrateur n'est pas plus compliqué que celle de l'utilisateur, en y accédant au compte administrateur en cliquant sur un menu, se trouvant à droite de la photo de profil et en entrant dans l'onglet paramètre, on remarque :

- **En premier encadré en vert**, nous avons un menu déroulant qui offre plusieurs outils de gestion des utilisateurs, comptes, droit d'accéder...
- **En second encadré en marron**, une console qui offre plusieurs outils de surveillance et d'administration de la plateforme.
- **En troisième position dans un rectangle orange**, nous disposons de l'aide et des tutoriels pour la formation à la gestion de Pydio.
- **Le quatrième onglet ici dans un cadre jaune**, est un accès rapide pour contribuer au projet, car Pydio est un projet libre et open source ce qui permet à n'importe quel programmeur ou codeur d'y contribuer ou de signaler des bugs et failles.
- **Le cinquième et dernier onglet qui est représenté par la couleur verte**, est réservé à la publicité des produits Pydio.



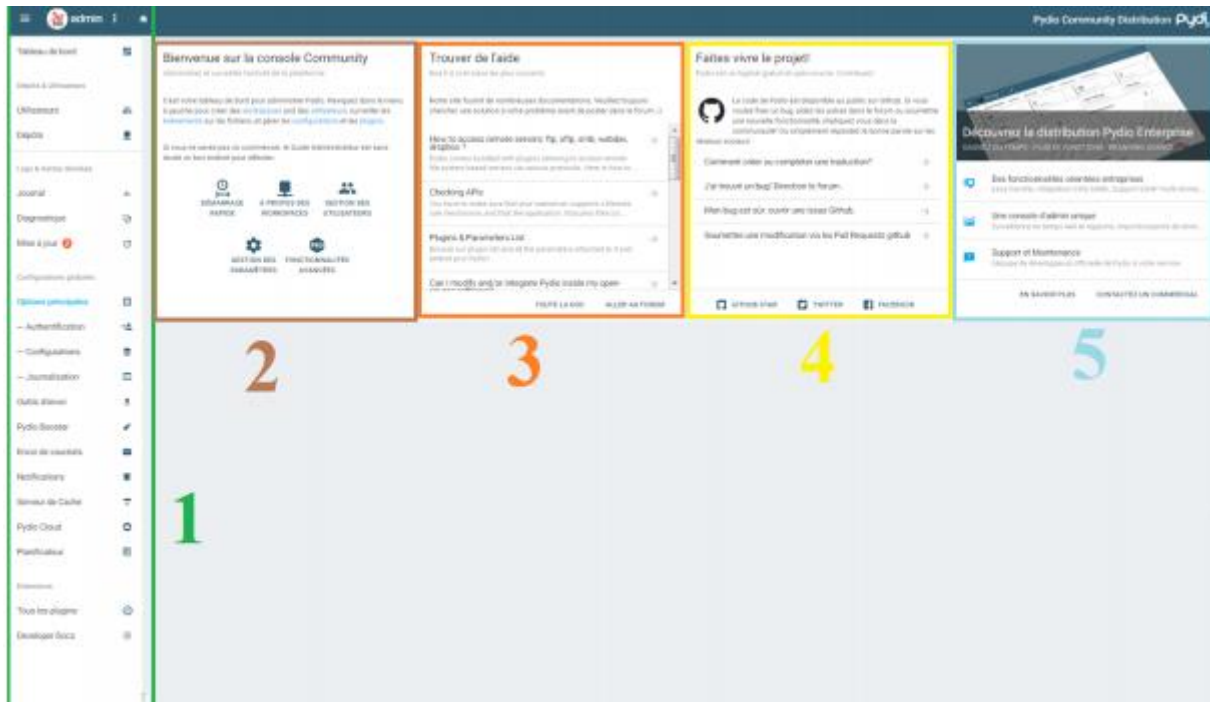


Figure II-9: Interface Administration

### 3. Choix de la norme :

#### ***a) L'évolution du WIFI :***

C'est dans les années 90 que la première version du Wifi fait son apparition et c'est à Apple qu'on doit cette invention qui s'appelle à l'époque le AirPort . Quelques années plus tard le terme de Wifi se généralise pour toutes les normes sans fil **802.11**.

Il en existe plusieurs aujourd'hui et toutes les normes relatives au wifi sont reconnaissables par leurs identifiant 802.11 suivi d'une lettre pour indiquer de la génération utilisée. Aujourd'hui on a accès à cinq normes différentes et deux nouvelles normes ont vu le jour il y a peu et devraient être utilisées dans les années qui viennent sur les appareils connectés :

802.11	Débit max (Théorie)	Portée	Fréquence (Ghz)
802.11 - 1997	2 Mbit/s	20 m	2.4
802.11a (1999)	54 Mbit/s	35 m	5
802.11b (1999)	11 Mbit/s	35 m	2.4
802.11g (2003)	54 Mbit/s	38 m	2.4
802.11n (2009)	72 – 288 Mbit/s	70 m	2.4
802.11n (2009)	150 – 600 Mbit/s	35 m	5
802.11ac (2013)	433 – 1300 Mbit/s	35 m	5
802.11ac(2013)	433-2600 Mbit/s	35 m	5
802.11ad (2012)	Jusqu'à 6750 Mbit/s	10 m	60
802.11ah (2016)	8 Mbit/s	100 m	0.9

### Le wifi 802.11ac : La toute-puissance du Wifi

La norme wifi 802.11ac est arrivée par étapes, en 2013 c'est la première vague d'appareils équipés de cette norme qui voient le jour, quelques années plus tard la seconde vague équipe les smartphones et dépasse la première génération. Cette nouvelle norme Wifi n'utilise que la fréquence 5Ghz sur des largeurs de bande de 20, 40, 80 ou 160 Mhz

Le débit disponible avec ces appareils est de 433 Mbit/s sur la bande 80 Mhz avec une antenne. On peut passer à un débit maximal de 1300 Mbit/s .

Pour se rendre bien compte de la puissance de cette nouvelle norme on peut comparer le débit à la norme 802.11 g de 2003, on remarque alors qu'un téléphone mobile connecté avec 1 flux spatial atteint 433 Mbit/s soit presque 10x plus que les 54 Mbit/s de l'ancienne norme.

L'autre gros changement est dans la diffusion des ondes : le « **Beamforming** ». Pour faire simple les communications sans fil fonctionnent pour l'instant de la manière suivante : l'émetteur transmet à pleine puissance un signal en cercle autour de lui, captant les récepteurs dans toute la zone et laissant d'autres zones « mortes » qui font elles-mêmes des interférences inutiles. Le principe du « **Beamforming** » est de toujours diffuser en cercle mais dès détection du récepteur de **concentrer un signal directionnel** vers lui.

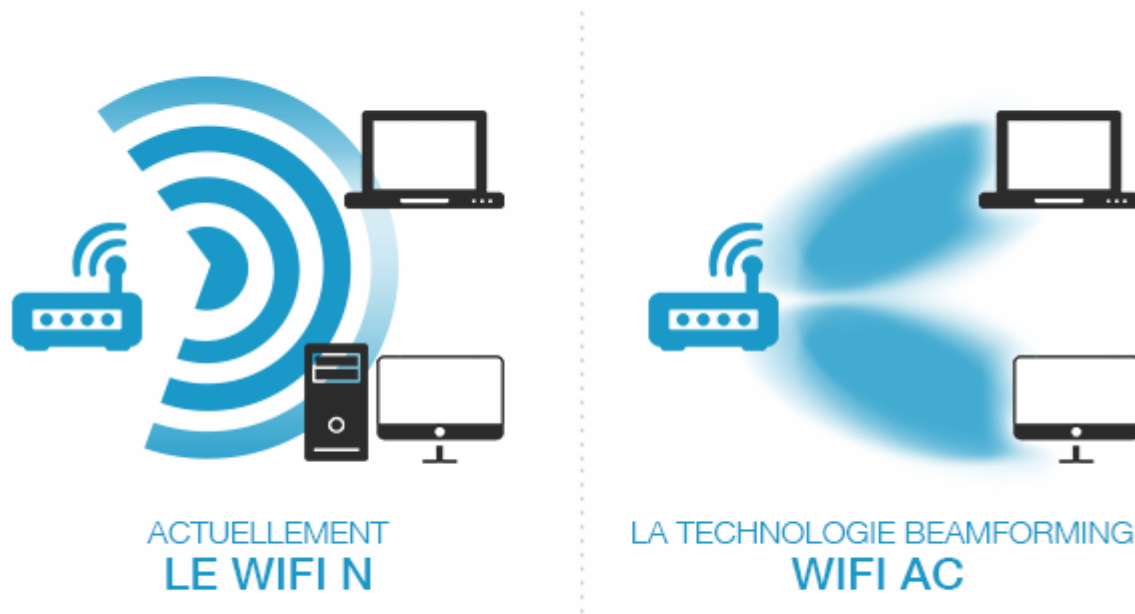


Figure II-10: illustration la diffusion des ondes : le " Beamforming"

Pour éviter les problèmes et permettre à tout le monde de se connecter facilement pour cela la norme la plus adéquate à envisager pour notre projet est la norme 802.11ac

L'avantage de ce réseau wifi est la compatibilité avec les routeurs, les cartes réseaux et points d'accès des constructeurs majeurs (D-link, Netgear, Linksys).

Finalement il n'y a que des avantages, grâce à ces changements dans le fonctionnement et la méthode de diffusion du signal, **Le WiFi 802.11ac sera moins perturbé, plus rapide, plus intense et par conséquent réduira la consommation des appareils équipés.**

	802.11n	802.11n IEEE Specification	802.11ac Wave 1 Today	802.11ac Wave2 WFA Certification Process Continues	802.11ac IEEE Specification
Band	2.4 GHz & 5 GHz	2.4 GHz & 5 GHz	5 GHz	<b>5 GHz</b>	5 GHz
MIMO	Single User (SU)	Single User (SU)	Single User (SU)	<b>Multi User (MU)</b>	Multi User (MU)
PHY Rate	450 Mbps	600 Mbps	1.3 Gbps	<b>2.34 Gbps - 3.47 Gbps</b>	6.9 Gbps
Channel Width	20 or 40 MHz	20 or 40 MHz	20, 40, 80 MHz	20, 40, 80, <b>80-80, 160 MHz</b>	20, 40, 80, 80-80, 160 MHz
Modulation	64 QAM	64 QAM	256 QAM	256 QAM	256 QAM
Spatial Streams	3	4	3	<b>3-4</b>	8
MAC Throughout*	293 Mbps	390 Mbps	845 Mbps	<b>1.52 Gbps- 2.26 Gbps</b>	4.49 Gbps

Figure II-11: Tableau de comparaison des caractéristiques des normes Wifi

#### 4. Sécurité :

L'avènement du sans-fil à travers le Wifi n'est pas sans poser des problèmes en comparaison aux réseaux filaires. Facilement accessible, un réseau Wifi peut poser des problèmes de sécurité.

Lorsqu'un appareil est connecté à un réseau sans fil, ou wifi, un hacker a seulement besoin d'un **récepteur** qui se trouve dans le cercle des signaux radios émis. Il est donc important d'assurer une sécurité wifi maximale afin de pouvoir utiliser les réseaux de communication sans fil sans aucune restriction.

#### Politique de sécurité adoptée à la nouvelle architecture du réseau sans fil proposée :

On propose une solution de sécurité informatique intégrée au cœur des fonctions de sécurité et complète dite : « **Pfsense** ».

**pfSense** est une distribution de **firewall** pour **router** open source basée sur **FreeBSD**. Il est installé sur un ordinateur physique ou une machine virtuelle pour créer un **pare-feu / routeur** dédié pour un réseau informatique. Il peut être configuré et mis à niveau via une interface Web et ne nécessite aucune connaissance du **système FreeBSD**.

Très fréquemment rencontré dans les PME et les petites structures, pfSense offre une solution complète de routage, filtrage, VPN et partage de connexion. Il est basé sur pf, et intègre un grand nombre de composants tiers : **serveur DHCP/DNS, serveur de temps, proxy web, monitoring...** La configuration se fait entièrement via une interface web.

*Lorsqu' on parle de PfSense, on peut le représenter comme une plateforme riche de sécurité. il est caractérisé par une large bibliothèque de package avec une intégration facile..... Tout simplement, c'est un redoutable outil.*

#### **Pfsense : jusqu'où va ce firewall ?**

De plus en plus développés, les programmes Pfsense réunissent de nombreuses fonctions en une seule et même solution :

- **Le logiciel antivirus.**
- **Le programme anti-espions.**
- **Les filtres contre les spams.**
- **Le pare-feu pour le réseau.**
- **L'analyse de toutes les requêtes web en temps réel.**
- **La prévention et l'identification des intrusions.**
- **Le filtrage des contenus.**
- **La protection contre les fuites d'informations.**
- **La génération de rapports.**
- **Accès à distance et support réseau privé virtuel (VPN) site à site.**
- **Fonction de passerelle de sécurité Web (anti logiciels malveillants, filtrage d'URL et de contenu).**
- **Prévention d'intrusion sur réseau, avec focus sur le blocage des attaques contre les PC Windows et serveurs non protégés.**

Ces Appliance Pfsense simplifient considérablement la sécurisation d'un environnement informatique. Le fait de cumuler plusieurs protections permet de faire face aux menaces les plus sophistiquées, sachant que les pirates du web ne cessent de perfectionner leurs méthodes d'action !

Pfsense permet aux administrateurs réseaux et à leurs équipes de travailler plus efficacement et d'améliorer leur productivité. Finies la gestion et la mise à jour de solutions de protection à points multiples, provenant de fournisseurs différents avec IUG, interfaces et consoles d'administration différentes.

Pfsense offre tout ce dont un professionnel de la sécurité a besoin : pare-feu, antivirus, filtrage e-mail et contenu Web, gestion d'applications et fonctionnalités réseau (routage, équilibrage de charge) - dans une seule Appliance. Elle se caractérise par une configuration aisée, une capacité de résolution des problèmes améliorée, une vision unifiée de la stratégie de sécurité de l'entreprise, une réduction des coûts et des interruptions.

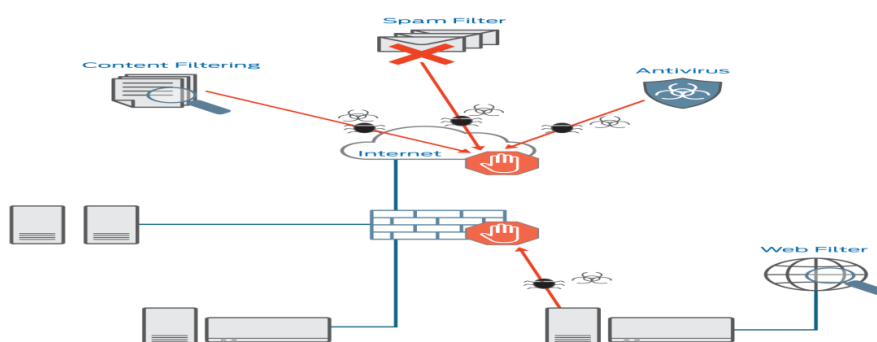


Figure II-12: Architecture du fonctionnement de pfsense et appliances

### **a) Méthodes d'authentification du protocole « Pfsense » :**

**None :** aucune authentification n'est proposée

**Active Directory SSO :** ce mode authentifie les utilisateurs avec leurs comptes AD en cours d'utilisation, sans aucune intégration de la part de l'utilisateur final.

*.Active Directory Single Sign – On (SSO) doit être configuré dans le menu Service d'authentification .*

**Agent (administration) :** L'utilisateur doit s'authentifier via l'agent d'authentification (téléchargeable depuis le portail) .

**Apple OpenDirectory SSO :** Même principe avec ADD SSo, en utilisant Apple OpenDirectory comme service d'authentification, en plus de générer Kerberos keyfile sur le serveur et de l'uploader sur UTM

**Authentification basique :** Un champ d'authentification (boîte de dialogue) simple sera présenté à l'utilisateur pour introduire le USER/PWD pour utiliser le proxy .

**Navigateur :** une fenêtre pop-up sera présentée à l'utilisateur, avec une interface graphique (personnalisable), pour introduire les coordonnées User/PWD .

## Au résumé

Cet outil open source est capable de se connecter à un annuaire LDAP, en l'occurrence ici l'Active Directory de Microsoft, afin de centraliser l'authentification auprès de différents services comme l'accès à l'interface d'administration, l'accès VPN ou encore la connexion au portail captif. Bien que dans certains cas, le point de liaison entre pfSense et l'Active Directory sera Radius.

**Avec pfSense, il est possible de déclarer la connexion à un AD pour authentifier les utilisateurs (certains utilisateurs, pas tous), pour déléguer l'administration du pare-feu.** Par exemple, on va définir un groupe qui aura le droit de configurer la partie portail captif du pare-feu, on va attribuer des droits à un groupe, et ce groupe correspond à un groupe de l'AD. On peut avoir un second groupe qui pourra seulement accéder aux logs du pare-feu, par exemple.

On pourrait tout à fait créer des groupes locaux sur pfSense, avec des utilisateurs locaux, mais c'est quand même plus sympa d'interroger directement l'AD pour ne pas avoir à subir les changements de login et/ou de mot de passe. En plus, ce n'est pas monstrueux comme config.

## ***b) Méthodes de chiffrement du réseau sans fil :***

### *Un tunnel VPN, c'est quoi au juste ?*

Déjà, VPN signifie **Virtual Private Network**, traduit littéralement en **Réseau virtuel privé**. Un tunnel VPN est donc un tunnel chiffré qui va relier un ou plusieurs sites distants sans que d'autres machines puissent intercepter ou modifier les données y transitant.

**La mise en place d'un tunnel VPN Pfsense dit : « OpenVPN » comme protocole de chiffrement (cryptage) de notre réseau sans fil .**

- **OpenVPN :**

C'est à la fois un protocole utilisant SSL pour sécuriser les données et en même temps un logiciel open source. Il nécessite un logiciel et l'installation de la configuration peut s'avérer plus complexe que les autres, mais il est le plus rapide/sécurisé d'entre eux.

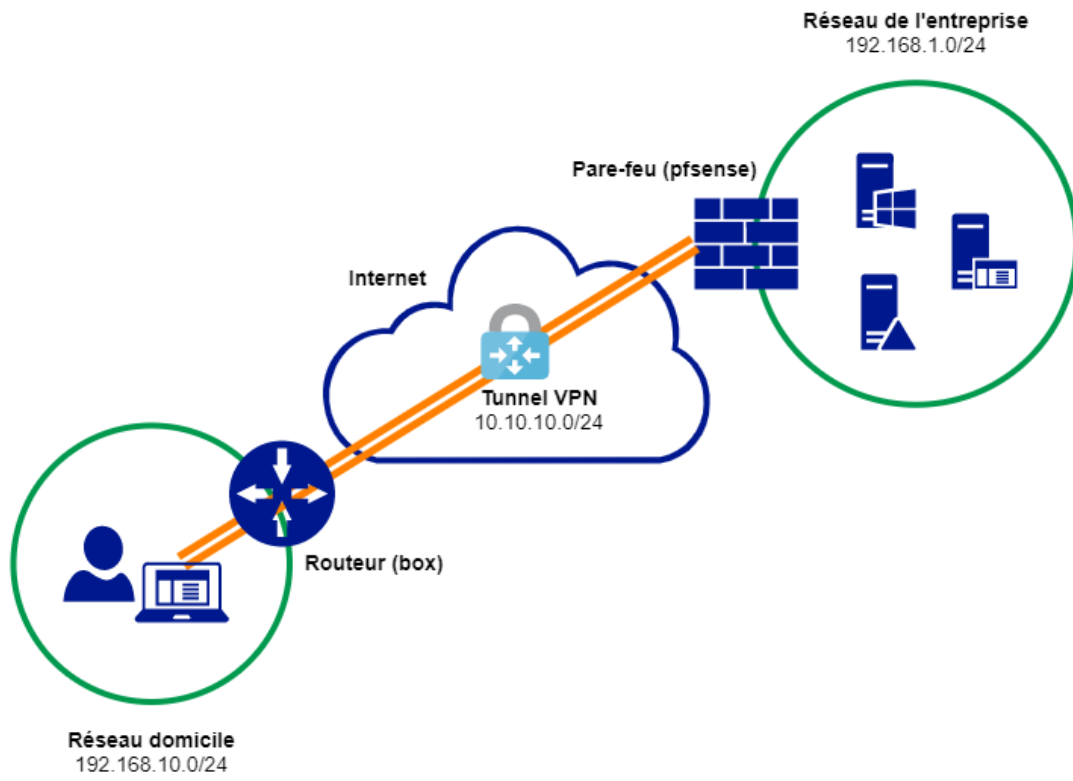


Figure II-13: Méthode de chiffrement du réseau

### III. Mise en place du réseau :

#### A. Etude du matériel :

##### 1. Les équipements d'interconnexion :

Dans une architecture, le matériel d'interconnexion représente le cœur du réseau. S'il est mal configuré (équipement mangeable), il peut avoir des effets néfastes sur le trafic réseau, allant à la détérioration de celui-ci. Le réseau sans fil proposé comporte des commutateurs qui de par leur fonction permettent de réduire les domaines de collision, et un routeur auquel toutes les technologies ont accès, ce qui laisse le droit à tout un chacun de le manipuler à sa guise.

**La nouvelle infrastructure réseau que nous avons proposée se constitue des équipements d'interconnexion suivants :**

#### ***a) Ressources matérielles :***

##### ➤ Serveur :

- Le serveur actuel utilisé :
- CPU : ProLiant dl380 gen9
- HDD : 1 TO

##### ➤ Switch manageable :

##### ➤ Point d'accès :

- **Modèle :** Tenda i24 .
- **Caractéristiques techniques :**
  - **Numéro de Type :** i24
  - **Marque nom :** Tenda.
  - **Type d'interface :** 1\*10/100/1000 base-TX port .
  - **Débit données :** - 2.4 GHz :1 - 300 Mb/s, 5 GHz : 6 – 867 Mb/s .
  - **Dimensions :** 178 mm \*178 mm \*38 mm.
  - **Standard:** IEEE802.1ac/a/b/g/n.



- **Mode de fonctionnement AP, Client + AP.**
- **Gamme de fréquence : 2.4 GHz, 5 GHz.**
- **Max client connecté : 2.4 GHz : 128 + 5 GHz : 128.**
- **Alimentation : 1- IEEE 802.3af/at & ;12V.**

➤ **Routeur :**

- **Modèle : TP-LINK Archer AX6000.**
- **Caractéristiques techniques :**
  - **Routeur Wi-Fi 6 AX6000.**
  - **Processeur Quad-Core 1.8 GHz et 1 Go de RAM**
  - **Wi-Fi 6 1024 QAM, bande passante totale : 5952 Mbps (4804 Mbps sur la bande 5 GHz et 1148 Mbps sur la bande 2.4 GHz).**
  - **8 antennes externes.**
  - **Compatible Wi-Fi 802.11a/b/g/n/ac.**
  - **Port WAN 2.5 GbE (2.5G/2G/1G/100M).**
  - **8 ports LAN 1 GbE (1G/100M/10M).**
  - **Serveur VPN PPTP & OpenVPN.**
  - **Cryptage : 64/128-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK.**
  - **2 ports USB 3.0.**

Possède la fonction de band steering, c'est-à-dire que le routeur va faire en sorte que les appareils se connectent à la bande de fréquences la plus performante pour eux. Souvent, il s'agit de pousser les appareils bi-bandes (donc plutôt récents) à se connecter en 5 GHz.

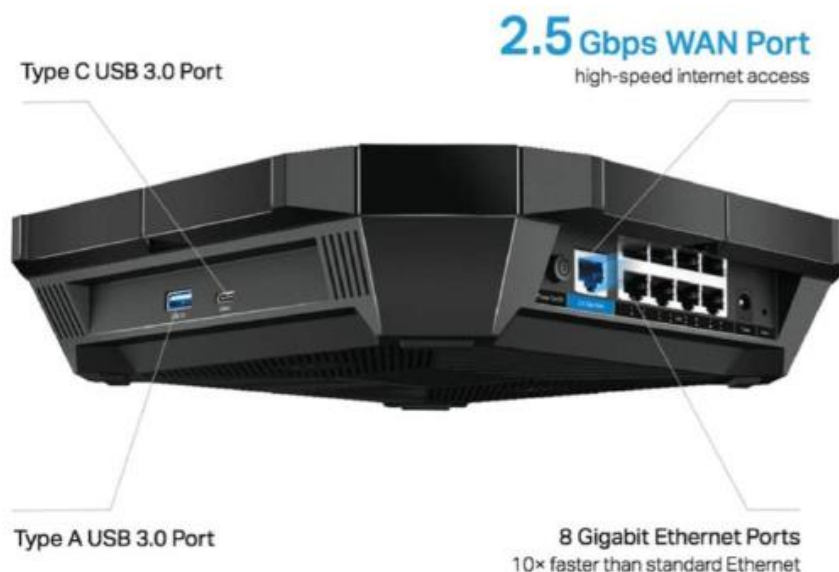


Figure III-1: - Routeur Wi-Fi 6 AX6000

#### ➤ Switch :

- **Modèle :** TP-LINK TL-SG1024D.
- **Caractéristiques techniques :**

Équipé de 24 ports 10/100/1000 Mbps. Les 24 ports sont compatibles Auto MDI/MDIX, nul besoin de se soucier des types de câbles. **TL-SG1024** est Plug & Play, il ne nécessite donc aucune installation logicielle. Chaque port peut être raccordé à d'autres switches pour étendre le réseau.

De plus le TL-SG1024D. Accroît considérablement la capacité réseau en utilisant une vitesse de transfert élevée pour échanger rapidement les dossiers les plus volumineux. Avec la fonction **full-duplex**, le TL-SG1024 supporte jusqu'à **2000 Mbps**. Ainsi, Les étudiants et personnel du département pourront transférer plus rapidement les fichiers gourmands en bande passante (des fichiers graphiques, CGI, CAD ou multimédia) instantanément sur le réseau.

Grâce à sa technologie innovante d'économie d'énergie, le TL-SG1024D permet de réduire de 20 %\* sa consommation d'énergie, ce qui en fait une solution écologique adaptée à notre réseau. Ce switch ajuste automatiquement sa consommation d'énergie en fonction de l'état de la liaison et de la longueur du câble

Mise hors tension des ports en veille Lorsqu'un ordinateur ou un périphérique réseau est éteint, le port correspondant sur un switch classique consomme encore beaucoup d'énergie. Le TL-SL1024D détecte automatiquement le statut de connexion de chaque port et réduit la consommation d'énergie des ports qui sont en veille. Gestion d'énergie selon la longueur de câble Idéal

Les fonctions automatisées de ce switch Gigabit assurent une installation rapide et facile. Aucune configuration n'est requise. La fonction Auto MDI/MDX permet de s'affranchir des câbles croisés. L'auto-négociation sur chaque port détecte la vitesse de connexion d'un appareil sur le réseau (10, 100 ou 1000 Mbps) et l'ajuste intelligemment pour une meilleure compatibilité et des performances optimales.

### ➤ **Adaptateur réseau sans fil**

- **Modèle :** TP-LINK TG-3468
- **Caractéristiques Techniques :**

#### **GÉNÉRAL**

- Type de périphérique : Adaptateur réseau.
- Format : Carte enfichable.
- Type d'interface (bus) : PCI Express x1.
- Révision des spécifications PCI : PCIe 1.0a.
- Bluetooth : 4.2

#### **RÉSEAUX**

- Ports : Gigabit Ethernet
- Technologie de connectivité : Filaire
- Type de câblage : Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
- Protocole de liaison de données : Ethernet, Fast Ethernet, Gigabit Ethernet
- Débit de transfert de données : 1 Gbits/s
- Protocole réseau / transport : TCP/IP, CSMA/CD
- Indicateurs d'état : Port mode duplex, liaison/activité
- Caractéristiques : Contrôle du flux, auto-négociation, wake on LAN (WOL), auto-uplink (MDI/MDI-X auto), mode semi-duplex, mode duplex intégral
- Normes de conformité : IEEE 802.3, IEEE 802.3u, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x

#### **EXTENSION/CONNECTIVITÉ**

- Interfaces : 1 x 1000Base-T - RJ-45
- Connecteurs compatibles : 1 x PCI Express x1

#### **LOGICIELS / CONFIGURATION REQUISE**

- Système d'exploitation requis : Microsoft Windows XP / Vista / 7 / 8 / 8.1 / 10

### ➤ **Amplificateur WiFi**

- **Modèle :** Netgear EX7300

***NETGEAR Répéteur WiFi Mesh (EX6250), Amplificateur WiFi AC1750, WiFi Booster, répéteur Wifi puissant avec itinérance Intelligente Maillée, jusqu'à 139 m<sup>2</sup> et 25 Appareils, compatible toutes Box .***

- **Caractéristiques Techniques :**

**Style: AC1750 Mesh**

- Netgear répéteur Wi-Fi mesh EX6250 couvre jusqu'à 139 m<sup>2</sup> et 25 appareils grâce à un amplificateur de signal Wi-Fi Dual Band AC1750 (jusqu'à 1 750 mbit/s) et à l'itinérance intelligente maillée..
- La technologie MESH permet de garder le même nom de wifi que l'actuel dans tout le département, cela pour une utilisation plus confortable.
- Couverture Wi-Fi élargie : offre une couverture Wi-Fi de plus de 139 m<sup>2</sup> et permet de connecter jusqu'à 25 appareils dans toute la maison (ordinateurs portables, smartphones, enceintes, caméras ip, tablettes, appareils iot, etc).
- Vitesse Wi-Fi AC1750 : offre des performances jusqu'à 1 750 mbit/s grce à la technologie Dual Band et à la technologie brevetée fastlane(tm), idéal pour les exigences du streaming de vidéos HD et des jeux vidéo en ligne.
- Compatibilité universelle : fonctionne avec tout routeur Wi-Fi, box internet et modem filaire avec Wi-Fi.
- Port Ethernet filaire : branchez simplement vos consoles de jeu, lecteurs multimédias ou autres appareils filaires sur le port Gigabit pour profiter d'une vitesse maximale.
- Sécurité : prend en charge les Protocoles de sécurité sans fil WEP et WPA/WPA2.

➤ **Les câbles Ethernet RJ45 et les connecteurs RJ45 :**

**Le câble à paire torsadées :**

Un câble à double paire torsadées (Twisted pair câble) décrit un modèle de câblage ou une ligne de transmission qui est constitué de deux brins de cuivre entrelacés en torsade et recouverts d'isolant. Cette configuration a pour but de maintenir précisément la distance entre le fil et de diminuer la diaphonie.

Dans ce projet nous proposons ceci :

- **Câble RJ45 Cat5 D-Link FTP.**
- **Câble RJ45 Cat6 D-Link STP.**
- **Noyaux RJ45 Cat5 Femelle FTP.**
- **Noyaux RJ45 cat6 Femelle STP.**
- **Connecteurs (jarretières) RJ45 Cat5.**
- **Connecteurs (jarretières) RJ45 Cat6.**

➤ **Système de refroidissement :**

**STYLE : PLATEAU DE VENTILATEURS RACKABLE, HORIZONTAL**

- Équipements destinés à optimiser le flux d'air.

- S'installe facilement dans toute armoire dotée de rails 19" standard.
- Trois ventilateurs de 160 m³/h assurent une circulation d'air efficace qui refroidit votre équipement.
- Compact : occupe seulement 1U d'espace utile.
- Les grilles de protection des pales évitent de mettre les doigts dans un ventilateur en marche.
- Finition noire.
- Prise secteur IEC C13 sur le panneau arrière.

***b) Ressources Logicielles :***

<b>Produit</b>	<b>Spécification</b>
<b>Système d'exploitation Debian</b>	V8.6 - AMD64 – Environnement serveur
<b>Système FreeBSD PfSense</b>	Pare feu/routeur – V 2.3.5 – AMD64
<b>Logiciel Pydio</b>	V8 - client
<b>Logiciel Pydio</b>	V8 Entreprise – serveur

## B. Evaluation Du Coûts :

Matériels	Marques	Quantités	Prix Unitaire (DZD)	Prix Total (DZD)
Point d'accès	Tenda i24	7	7400,00	51800,00
Routeur	Archer AX6000	1	55595,00	55595,00
Switch	TP-LINK TL-SG1024D	12	15000,00	180000,00
Adaptateur réseau sans fil	TP-LINK TG- 3468	120	2700,00	324000,00
Amplificateur Wifi	Netgear EX7300	1	16000,00	16000,00
Cables RJ45 CAT6 STP	D-Link	30	60,00	1800,00
Cables RJ45 CAT5 FTP	D-Link	500	45,00	22500,00
Noyaux RJ45 Cat5 Femelle	Shneider	320	25,00	8000,00
Noyaux RJ45 cat6 Femelle	Shneider	25	35,00	875,00
Connecteurs RJ45 Cat5	Shneider	200	15,00	3000,00
Connecteurs RJ45 Cat6	Shneider	25	25,00	625,00
Système de refroidissement	Plateau de ventilateurs rackable	1	12000,00	12000,00
<b>TOTAL</b>				<b>676195,00</b>

<b>Coûts matériels</b>	<b>676195.00 DZD</b>
<b>Coûts mains d'œuvre</b>	<b>2000 DZD / jour</b>

## C. Etude et configuration du serveur :

Un serveur DNS, ou serveur de noms, est utilisé pour résoudre une adresse IP en un nom d'hôte ou vice versa.

Vous pouvez configurer quatre types différents de serveurs DNS:

- *Un serveur DNS maître pour votre ou vos domaines, qui stocke les enregistrements faisant autorité pour votre domaine.*
- *Un serveur DNS esclave, qui repose sur un serveur DNS maître pour les données.*
- *Un serveur DNS de mise en cache uniquement, qui stocke les demandes récentes comme un serveur proxy. Il fait autrement référence à d'autres serveurs DNS.*
- *Un serveur DNS de transfert uniquement, qui renvoie toutes les demandes à d'autres serveurs DNS.*

- *fonctionnalités chroot*

La fonction chroot est exécutée avec le nom de l'utilisateur nommé, et elle limite également les fichiers nommés peuvent voir. Une fois installé, named est dupé en pensant que le répertoire / **var / named / chroot** est en fait le répertoire racine ou / . Par conséquent, les fichiers nommés normalement trouvés dans le répertoire / **etc** se trouvent plutôt dans le répertoire / **var / named / chroot / etc** , et ceux que vous vous attendez à trouver dans / **var / named** se trouvent en fait dans / **var / named / chroot / var / nommé**.

L'avantage de la fonction chroot est que si un hacker pénètre dans votre système via **un exploit BIND**, l'accès de l'hacker au reste de votre système est isolé aux fichiers sous le répertoire chroot et rien d'autre. Ce type de sécurité est également connu sous le nom de prison chroot.

## 1. Configurer le serveur DNS

Dans cet exemple, nous allons configurer un serveur DNS et tester du côté client.

Pour cet exemple, nous utiliserons trois systèmes, un serveur Linux, un client Linux et un client Windows.

Le rpm **bind** et **caching-nameserver** est requis pour configurer DNS. vérifiez-les pour l'installation si vous ne les trouvez pas, installez-les.

```
[root@Server ~]# rpm -qa bind*
bind-libs-9.3.3-10.el5
bind-chroot-9.3.3-10.el5
bind-devel-9.3.3-10.el5
bind-utils-9.3.3-10.el5
bind-libbind-devel-9.3.3-10.el5
bind-9.3.3-10.el5
bind-sdb-9.3.3-10.el5
[root@Server ~]# rpm -qa cach*
caching-nameserver-9.3.3-10.el5
cachedfilesd-0.8-2.el5
[root@Server ~]# _
```

Figure III-2 : Le rpm bind et caching-nameserver

Définissez le nom d'hôte sur **server.example.com** et l'adresse IP sur **192.168.0.254**

```
[root@Server ~]# cat /etc/sysconfig/network
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=Server.example.com

[root@Server ~]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:11:AD:E1
          inet addr:192.168.0.254  Bcast:192.168.0.255  Mask:
          inet6 addr: fe80::20c:29ff:fe11:ade1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:17981 (17.5 KiB)
          Interrupt:67 Base address:0x2000
```

Figure III-3: Définition du nom d'hôte et l'adresse IP

Le fichier de configuration principal du serveur DNS est **nommé.conf**. Par défaut, ce fichier n'est pas créé dans le répertoire **/var/named/chroot/etc/**. Au lieu de **named.conf**, un exemple de fichier **/var/named/chroot/etc/named.caching-nameserver.conf** est créé. Ce fichier est utilisé pour créer un serveur de noms de mise en cache uniquement. Vous pouvez également effectuer des modifications dans ce fichier après avoir changé son nom en **named.conf** pour configurer le serveur DNS maître ou vous pouvez créer manuellement un nouveau fichier **named.conf**.

Dans notre exemple, nous créons un nouveau fichier **named.conf**

```
[root@Server etc]# vi /var/named/chroot/etc/named.conf _
```

Figure III-4: Création du nouveau fichier "named.conf"

Nous utilisons les fonctionnalités chroot de bind afin que tous nos fichiers nécessaires soient situés dans le répertoire chroot. Définissez l'emplacement du répertoire sur **/var/named**. De plus, nous définirons l'emplacement des fichiers de zone avant et de zone de recherche inversée.

Faites l'édition exactement comme indiqué ici dans l'image

```
options {
    directory "/var/named/";
};

zone "example.com" {
    type master;
    file "example.com.zone";
    allow-transfer {192.168.0.1;};
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "0.168.192.in-addr.arpa.zone";
};
```

Figure III-5: l'édition

Enregistrez ce fichier avec : **wq** et quittez



## 2. Configurer le fichier de zone

Nous avons défini deux fichiers de zone **example.com.zone** pour la zone avant et **0.168.192.in-addr.arpa** pour la zone inverse. Ces fichiers seront stockés dans **/var/named/chroot/var/named/location**. Nous utiliserons deux exemples de fichiers pour créer ces fichiers.

Remplacez le répertoire par **/var/named/chroot/var/named** et copiez les exemples de fichiers sous le nom que nous avons défini dans **named.conf**

```
[root@Server named]# cd /var/named/chroot/var/named
[root@Server named]# cp localhost.zone example.com.zone
[root@Server named]# cp named.local 0.168.192.in-addr.arpa.zone
[root@Server named]# _
```

Figure III-6: mise à jour du répertoire

Ouvrez maintenant le fichier de zone de **transfert example.com.zone**

```
[root@Server named]# vi example.com.zone _
```

Figure III-7: ouverture d'un fichier zone

Par défaut, ce fichier ressemblera à ceci

```
$TTL      86400
@          IN SOA  @           root (
                                42      ; serial
                                3H      ; refresh
                                15M     ; retry
                                1W      ; expiry
                                1D      ; minimum

                                IN NS   @
                                IN A    127.0.0.1
                                IN AAAA  ::1
```

Figure III-8: le fichier zone

Modifiez ce fichier exactement comme indiqué dans l'image ci-dessous

```
$TTL      86400
@          SOA      example.com.  root (
                                42      ; serial
                                3H      ; refresh
                                15M     ; retry
                                1W      ; expiry
                                1D      ; minimum

@          NS       server.example.com.
@          NS       client1.client.com.
server     A         192.168.0.254
client1    A         192.168.0.1
client2    A         192.168.0.2
```

Maintenant, ouvrez le fichier de zone de recherche inversée **0.168.192.in-addr.arpa**

```
[root@Server named]# vi 0.168.192.in-addr.arpa.zone _
```

Figure III-9 : Ouverture fichier zone de recherche inversée

Par défaut, ce fichier ressemblera à ceci

```
$TTL      86400
@         IN      SOA      localhost. root.localhost. (
                                1997022700 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum

1         IN      NS       localhost.
1         IN      PTR      localhost.
```

Figure III-10: fichier zone de recherche inversée

Modifiez ce fichier exactement comme indiqué dans l'image ci-dessous :

```
$TTL      86400
@         IN      SOA      example.com. root.server.example.com. (
                                1997022700 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum

254      IN      NS       server.example.com
1        IN      PTR      server.example.com.
1        IN      PTR      client1.example.com.
2        IN      PTR      client2.
```

Figure III-11: Modification du fichier

Maintenant changez la propriété de ces fichiers de zone en groupe **nommé**

```
[root@Server named]# chgrp named example.com.zone
[root@Server named]# chgrp named 0.168.192.in-addr.arpa.zone
[root@Server named]# _
```

Figure III-12: modification de la propriété des fichiers

Maintenant, démarrez le service **nommé**

```
[root@Server named]# chkconfig named on
[root@Server named]# service named restart
Stopping named: [ OK ]
Starting named: [ OK ]
[root@Server named]# _
```

Figure III-13: Démarrage du service nommé

Si le service redémarre sans aucune erreur, cela signifie que vous avez configuré avec succès le serveur de noms maître.

### 3. Configurer le serveur esclave DNS

Pour cet exemple, nous utilisons trois systèmes, un serveur Linux, un client Linux et un client Windows.

Nous avons configuré le serveur DNS principal avec l'adresse IP de **192.168.0.254** et le nom d'hôte **server.example.com** sur le serveur Linux. Nous allons maintenant configurer le **serveur DNS esclave** sur les clients Linux

Pour configurer le serveur DNS esclave, allez sur le système client1.

Testez d'abord la connectivité du serveur DNS par des commandes ping et vérifiez le nombre de tours par minute nécessaire. Le rpm **bind** et **caching-nameserver** est requis pour configurer DNS. vérifiez-les pour l'installation si vous ne les trouvez pas, installez-les.

```
[root@Server ~]# rpm -qa bind*
bind-libs-9.3.3-10.el5
bind-chroot-9.3.3-10.el5
bind-devel-9.3.3-10.el5
bind-utils-9.3.3-10.el5
bind-libbind-devel-9.3.3-10.el5
bind-9.3.3-10.el5
bind-sdb-9.3.3-10.el5
[root@Server ~]# rpm -qa cach*
caching-nameserver-9.3.3-10.el5
cachedfilesd-0.8-2.el5
[root@Server ~]# _
```

Figure III-14: Le rpm bind et caching-nameserver

Définissez le nom d'hôte sur **client1** et l'adresse IP sur **192.168.0.1** et créez un nouveau fichier **named.conf**

```
[root@Client1 ~]# vi /var/named/chroot/etc/named.conf _
```

Nous utilisons les fonctionnalités **chroot** de bind afin que tous nos fichiers nécessaires soient situés dans le répertoire chroot. Définissez l'emplacement du répertoire sur **/var/named**. Comme nous configurons le **serveur esclave**, nous n'avons pas besoin de définir l'emplacement des fichiers de base de données de zone. Le fichier de base de données de zone ne peut être créé et modifié que sur le serveur maître. Un **serveur esclave** n'a copié que depuis le serveur maître.

Faites l'édition exactement comme indiqué ici dans l'image dans **named.conf**

```
options{
    directory "/var/named/";
};
zone "example.com" IN {
    type slave;
    masters {192.168.0.254;};
    file "slave/example.com.zone";
};
```

Enregistrez ce fichier avec : **wq** et quittez

Redémarrez maintenant le service nommé. Il devrait être démarré sans aucune erreur.

```
[root@Client1 ~]# service named restart
Stopping named: [FAILED]
Starting named: [ OK ]
[root@Client1 ~]# _
```

Figure III-15: la fin de la configuration avec succès

C'est fait, la configuration du Serveur DNS maître et client concrétisée avec succès le serveur DNS maître et client. Maintenant, nous allons configurer le client DNS et le tester avec le serveur DNS.

## 4. Configuration de base du système

### a) Introduction

Les systèmes basés sur le noyau linux utilise des archives qui sont appelés paquets ou parfois (paquetages). Ces paquets, qui comprennent des fichiers compressés qui offrent des informations et des procédures nécessaires à l'installation d'un logiciel sur le system d'exploitation en s'assurant de la cohérence fonctionnelle du système ainsi modifié pour les besoins des logiciels.

### b) Démarrage de la machine

On a démarré le serveur Debian, et vue que nous avons configuré la carte réseau et installer un serveur de connexion distante (ssh), il nous suffit d'y s'y connecter via un client ssh comme il en existe de toute sorte, dans notre cas nous avons utilisé Putty, un client ssh très connus et rependu dans le monde du réseau, qui est installer sur un ordinateur client du même réseau que le serveur en question.

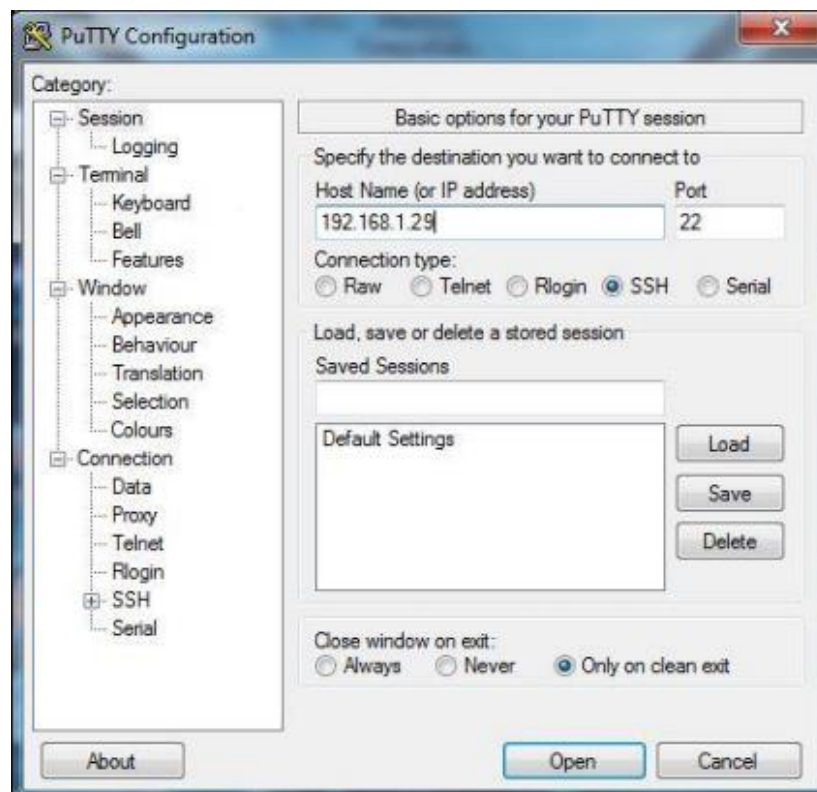


Figure III-16: établissement d'une connexion au serveur via PuTTY

Une fois la connexion établie, Putty nous offre un terminale (console de commande), qui nous a permis de nous identifier pour que nous puissions effectuer les modifications nécessaires pour l'installation et le bon fonctionnement du serveur Pydio, mais pour cela il nous a fallu nous y connecter en tant que Root (administrateur) du système pour que nous ayons l'autorité suffisante et pouvoir modifier ce dernier.

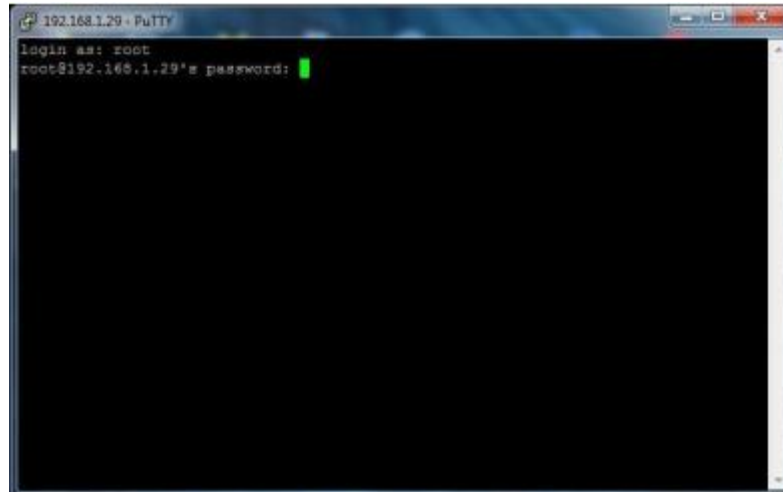


Figure III-17 : authentification de l'administrateur

### **c) Installation des paquets nécessaires**

Puis nous avons entamé l'installation des paquets nécessaire qui nous ont permis de faire fonctionner les fonctionnalités et options de Pydio, pour cela nous avons installé des paquets et librairies php, apache2-php, mysqlq-php

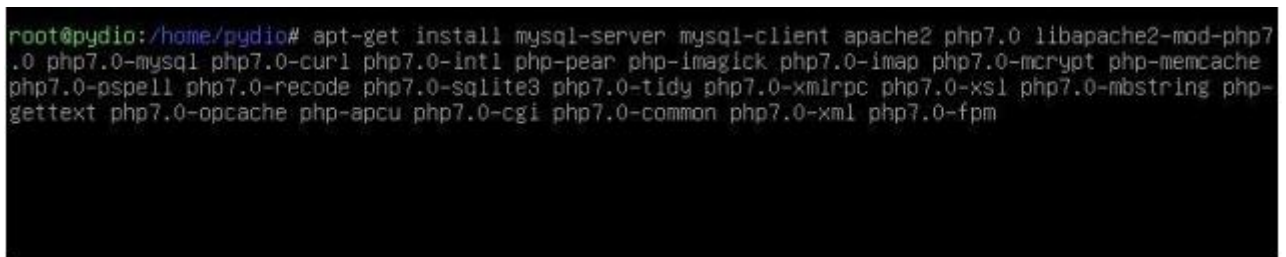


Figure III-18 : installation des prérequis pour Pydio

### **d) Configuration et activation des paquets :**

Puis nous avons entamé l'activation des composants tels que PHP7.0-cgi, proxy-fcgi et la configuration des paquets et serveurs tels que MySQL-server, apache2 ..., nous avons aussi changé le répertoire que le serveur apache peut atteindre et nous lui avons attribué l'autorisation nécessaire.

```

root@pydio: /home/pydio
root@pydio:/home/pydio# a2enmod proxy_fcgi setenvif
Considering dependency proxy for proxy_fcgi:
Module proxy already enabled
Module proxy_fcgi already enabled
Module setenvif already enabled
root@pydio:/home/pydio# a2enconf php7.0-fpm
Conf php7.0-fpm already enabled
root@pydio:/home/pydio# systemctl reload apache2
root@pydio:/home/pydio# a2enmod proxy_fcgi setenvif
Considering dependency proxy for proxy_fcgi:
Module proxy already enabled
Module proxy_fcgi already enabled
Module setenvif already enabled
root@pydio:/home/pydio# a2enconf php7.0-fpm
Conf php7.0-fpm already enabled
root@pydio:/home/pydio# systemctl reload apache2
root@pydio:/home/pydio# mysql_secure_installation

```

Figure III-19 : configuration d'apache-php

### e) Configuration et préparation du serveur web :

Pour préparer notre serveur web (apache2) à offrir un accès au serveur de gestion de fichier, nous avons créé un fichier de configuration en XML pour le serveur web (apache) « **2int.local.conf** », dans ce fichier nous avons bien évidemment désigner l'adresse et le port d'écoute du serveur mais aussi le répertoire qui sera exploité par ce dernier.

```

<VirtualHost *:443>
    ServerName pydio.2int.local
    ServerAdmin webmaster@localhost
    DocumentRoot /home/pydio/public_html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    Alias /log "/var/log/"
    <Directory "/var/log/">
        Options Indexes MultiViews FollowSymLinks
        AllowOverride None
        Order deny,allow
        Deny from all
        Allow from all
        Require all granted
    </Directory>

    Alias /public_html "/home/pydio/public_html"
    <Directory "/home/pydio/public_html">
        Options Indexes MultiViews FollowSymLinks
        AllowOverride None
        Require all granted
    </Directory>
</VirtualHost>

```

Figure III-20 : configuration d'apache2

### f) Configuration de la base de données (MySQL)

Nous avons commencé par nous connecter à notre base de données pour pouvoir ajouter un utilisateur, une base de données et une table dédiée au serveur Pydio.



```

root@pydio:/home# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 5
Server version: 10.1.26-MariaDB-0+deb9u1 Debian 9.1

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create user pydio@localhost identified by 'password';
Query OK, 0 rows affected (0.01 sec)

MariaDB [(none)]> create database pydio;
Query OK, 1 row affected (0.01 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON pydio.* to 'pydio'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.01 sec)

MariaDB [(none)]> exit_

```

Figure III-21 ; configuration de la base de données

### **g) Téléchargement de Pydio (gestion et partage de fichier)**

Lorsque nous avons fini la mise en place et la configuration des paquets et serveur requis pour Pydio nous somme enfin passer au téléchargement de ce dernier sur son site officiel

« <https://download.pydio.com/pub/cells-enterprise/release/1.0.0/linux-amd64/pydio-cells-enterprise-1.0.0-linux-amd64.zip> » avec un outil de Debian qui est « **wget** »

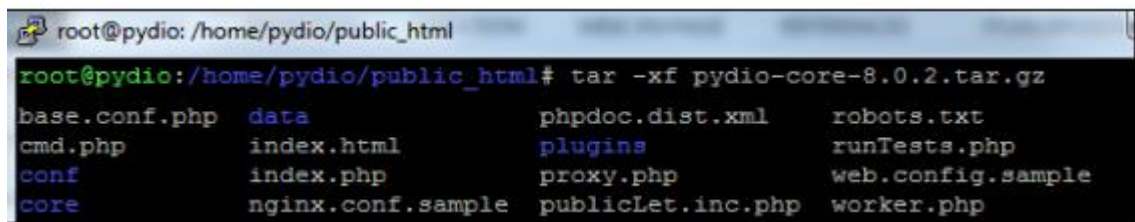
```

root@pydio:/home/pydio# wget https://download.pydio.com/pub/cells-enterprise/release/1.0.0/linux-amd64/pydio-cells-enterprise-1.0.0-linux-amd64.zip
--2018-05-31 14:37:20-- https://download.pydio.com/pub/cells-enterprise/release/1.0.0/linux-amd64/pydio-cells-enterprise-1.0.0-linux-amd64.zip
Résolution de download.pydio.com (download.pydio.com)... 62.210.29.232
Connexion à download.pydio.com (download.pydio.com) [62.210.29.232]:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 86018645 (82M) [application/zip]
Sauvegarde en : « pydio-cells-enterprise-1.0.0-linux-amd64.zip »
-cells-enterprise-1.0.0- 1%[ ] 1,26M 210KB/s eta 9m 50ss

```

Figure III-22: téléchargement de Pydio

Puis nous avons procédé à la décompression des fichiers qui compose Pydio grâce à une commande (**tar**) qui est disponible sur la distribution Debian



```

root@pydio: /home/pydio/public_html
root@pydio:/home/pydio/public_html# tar -xf pydio-core-8.0.2.tar.gz
base.conf.php  data          phpdoc.dist.xml  robots.txt
cmd.php        index.html    plugins          runTests.php
conf          index.php    proxy.php       web.config.sample
core          nginx.conf.sample  publicLet.inc.php  worker.php
  
```

Figure III-23: décompression des fichiers qui compose Pydio

Après que nous ayons extrait les composant de Pydio nous avons attribué la propriété et l'autorité nécessaire au serveur web pour qu'il dispose du répertoire de Pydio .



```

root@pydio:/home# chown -R www-data:www-data pydio/public_html;chmod -R 777 /home/pydio/public_html/
  
```

Figure III-24: délégation de propriété et attribution des autorisations à apache2



## IV. Etude et configuration des postes client :

### A. Configurer le client DNS Windows

Maintenant, allez sur le système Windows XP et testez la connectivité du serveur DNS. Et définissez l'adresse **IP DNS** dans les propriétés de la carte LAN.

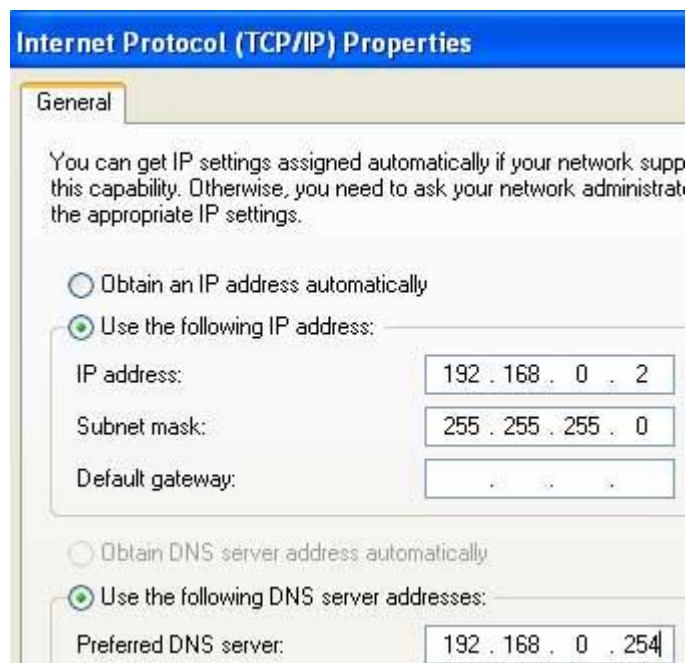


Figure IV-1: configuration de l'adresse IP

Maintenant, allez sur l' **invite de commandes** et envoyez un ping à partir d'un autre client par nom pour tester le **DNS** .

```

C:\>ping client2

Pinging client2 [192.168.0.2] with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>_

```

Figure IV-2: Test du DNS

Vous pouvez également vérifier le serveur DNS par la commande **nslookup**

```

C:\>nslookup 192.168.0.254
Server:  server.example.com
Address: 192.168.0.254

Name:    server.example.com
Address: 192.168.0.254

C:\>

```

Figure IV-3 : vérification du serveur DNS

Testez également en **envoyant une requête ping au serveur à partir du nom**

```

C:\>ping server.example.com

Pinging server.example.com [192.168.0.254] with 32
Reply from 192.168.0.254: bytes=32 time=2ms TTL=64
Reply from 192.168.0.254: bytes=32 time<1ms TTL=64
Reply from 192.168.0.254: bytes=32 time<1ms TTL=64
Reply from 192.168.0.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%)
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>_

```

```

[root@Client1 ~]# ping client2
PING client2.example.com (192.168.0.2) 56(84) bytes of data.
64 bytes from client2 (192.168.0.2): icmp_seq=1 ttl=128 time=16.3 ms
64 bytes from client2 (192.168.0.2): icmp_seq=2 ttl=128 time=0.383 ms

--- client2.example.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.383/8.348/16.313/7.965 ms
[root@Client1 ~]# _

```

Figure IV-4: Test avec la commande ping.

## B. Configurer les clients DNS Linux

Sur l'interface de ligne de commande, vous ne disposez d'aucune option pour définir l'adresse IP DNS dans la fenêtre de configuration du réseau. L'adresse IP du serveur DNS peut être définie à partir **du** fichier **/etc/resolv.conf**. Chaque ligne de serveur de noms représente un serveur DNS et la ligne de recherche spécifie les noms de domaine à essayer si seule la première partie d'un nom d'hôte est utilisée. Par exemple, si seul le nom client1 est utilisé comme nom d'hôte, **client1.example.com** sera également essayé si le fichier /etc/resolv.conf est configuré comme indiqué dans l'image ci-dessous sur le système.

Pour définir l'IP DNS, ouvrez le fichier **/etc/resolv.conf**

```

[root@Client1 ~]# vi /etc/resolv.conf _

```

Définissez l'ip du **serveur de noms** sur **192.168.0.254** et l'option de **recherche** sur **example.com**

```
search example.com
nameserver 192.168.0.254_
```

Après avoir enregistré le fichier `/etc/resolv.conf`, redémarrez le service réseau

```
[root@Client1 ~]# service network restart
Shutting down interface eth0: [ OK ]
Shutting down loopback interface: [ OK ]
Bringing up loopback interface: [ OK ]
Bringing up interface eth0: [ OK ]
[root@Client1 ~]# _
```

Utiliser `server.example.com` pour tester le serveur DNS

```
[root@Client1 ~]# dig server.example.com

; <<>> DiG 9.3.3rc2 <<>> server.example.com
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERR
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1,
;; QUESTION SECTION:
;server.example.com.          IN      A
```

Vérifiez maintenant en envoyant un Ping à un autre client à partir du nom

### C. Mise en place d'une plateforme de tests :

La réalisation de cette plateforme a été réalisé au travers du logiciel Cisco packet tracer.

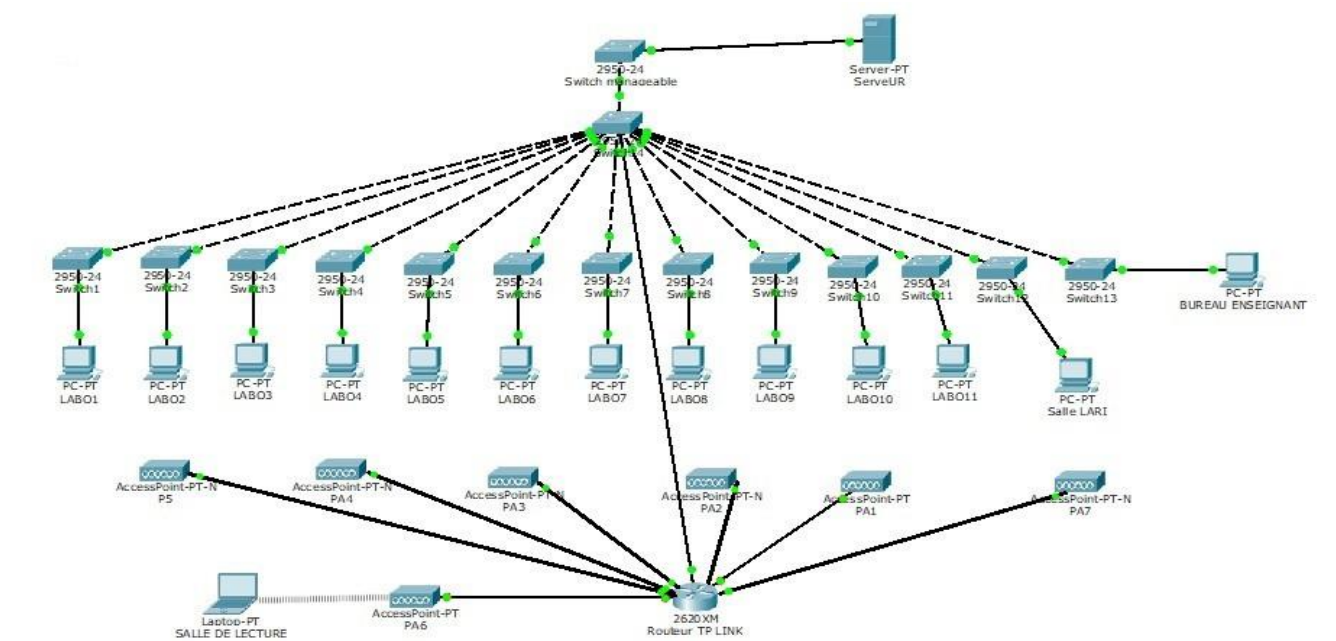


Figure IV-5: Plateforme de tests

*Le logiciel " Cisco packet tracer " ne permet pas de tester la connectivité entre un point d'accès et plusieurs terminaux à la fois.*

## D. Elaboration d'un devis :



Nom de la Société  
Adresse  
Code Postal - Ville  
Téléphone - Courriel

# Devis

Devis N° :  
Date : 03/06/2021

Client : Responsable du projet  
UMMTO ,département informatique  
1500 - TIZI OUZOU

Vendeur	Paiement	Livraison	Fin de validité
Nom - Prénom	CB / Chèque / Mandat	Le [date] par transporteur privé	[date]

Quantité	Description	Prix unitaire HT	Total HT
7	POINT d'ACCES TENDA i24	7 400,00 DA	51 800,00 DA
1	ROUTEUR AX6000	55 595,00 DA	55 595,00 DA
12	SWITCH TP-LINK TL-SG1024D	15 000,00 DA	180 000,00 DA
120	ADAPTATEUR RESEAU SANS FIL TP-LINK TG-3468	2 700,00 DA	324 000,00 DA
1	AMPLIFICATEUR WIFI NETGEAR EX7300	16 000,00 DA	16 000,00 DA
30	CABLES RJ45 CAT6 STP D-LINK	60,00 DA	1 800,00 DA
500	CABLES RJ45 CAT5 FTP D-LINK	45,00 DA	22 500,00 DA
320	NOYAUX RJ45 CAT5 FEMELLE D-LINK	25,00 DA	8 000,00 DA
25	NOYAUX RJ45 CAT6 FEMELLE D-LINK	35,00 DA	875,00 DA
200	CONNECTEURS RJ45 CAT5 D-LINK	15,00 DA	3 000,00 DA
25	CONNECTEURS RJ45 CAT6 D-LINK	25,00 DA	625,00 DA
1	PLATEAU DE VENTILATEUR RACKABLE	12 000,00 DA	12 000,00 DA
7	MAIN D'ŒUVRE	2 000,00 DA	14 000,00 DA
<b>TOTAL HT</b>			<b>690 195,00 DA</b>

Devis gratuit et sans engagement valable jusqu'au [date], pour plus d'informations téléphonez au : X XX XX XX XX

## V. Conclusion

---

**La démocratisation des réseaux WIFI a grandement simplifié le déploiement des infrastructures domestiques et professionnelles, offrir la possibilité de créer des réseaux locaux sans fils à haut débit pour peu que la station à connecter ne soit pas trop distante par rapport au point d'accès.**

**Au cours de ce projet, nous avons étudié la technologie WIFI en présentant ses différentes architectures et nous avons développé un outil de dimensionnement d'un réseau de transmission de données haut débit d'accès WIFI.**

**Lors de ce projet, nous avons proposés une infrastructure d'un réseau sans fil pour le département informatique et en étudiant ses techniques d'accès au support.**

**En fin, nous avons expliqué le processus général de dimensionnement de tel réseau en présentant les différentes étapes suivies pour effectuer le dimensionnement du réseau.**

**Le dimensionnement consiste à déterminer le rayon d'une cellule WI-FI, le nombre de point d'accès, le nombre de switches nécessaire ....**

# ANNEXE

## VI. Annexe 1 :

### **1. Configuration des points d'accès :**

**1-on va brancher le câble internet dans le LAN port de notre point d'accès et l'autre dans le port LAN du pc.**

**2-dans notre pc on accède au paramètre réseau internet→ Ethernet→ modifier les options d'adaptateur→ local area connection→ (clique gauche) propriété→ Internet Protocol version 4 (TCP/IPv4) → (clique gauche) propriété → utiliser l'adresse IP suivante on va lui donner une adresse IP Ex adresse IP : 192.168.0.9.**

**Masque sous réseau: 255.255.255.0 → ok.**

**3- dans un navigateur on va saisir l'adresse IP de notre point d'accès qu'on trouve derrière la boîte → on va saisir le nom et MDP par défaut admin.**

**4- dans quick setup on peut changer le nom de notre PA dans SSID, pour le mode de sécurité on choisit WPA2-PSK puis on change le mot de passe et on sauvegarde.**

**5- dans paramètre d'internet on change l'adresse IP par exemple on met 192.168.1.2180**

**Masque sous réseau: 255.255.255.0 passerelle par défaut 192.168.1.1 premier DNS 192.168.1.10**

**Optimisation d'internet on choisit pour une longue distance (10mbps full duplex) puis on sauvegarde.**

**On va se reconnecter avec la nouvelle adresse IP mais pour cela on doit d'abord revenir à la 2ème étape on change juste l'adresse IP par exemple 192.168.1.90**

**4- on va saisir la nouvelle adresse IP dans le mm navigateur → on accède à l'interface du notre point d'accès → dans Wireless (wifi) → SSID → 5GHz**

**5- on va mettre statuts et broadcast SSID à désactiver → sauvegarder. 6- on accède à paramétrage RF → on désactiver 5GHz0**

**7- on va refaire encore une autre fois la 2 ème étape mais cette fois-ci on va choisir dans propriété → obtenir une adresse IP automatiquement.**

**8- on va débrancher le câble de port Lan du pc et on va le brancher dans le port Lan du routeur.**

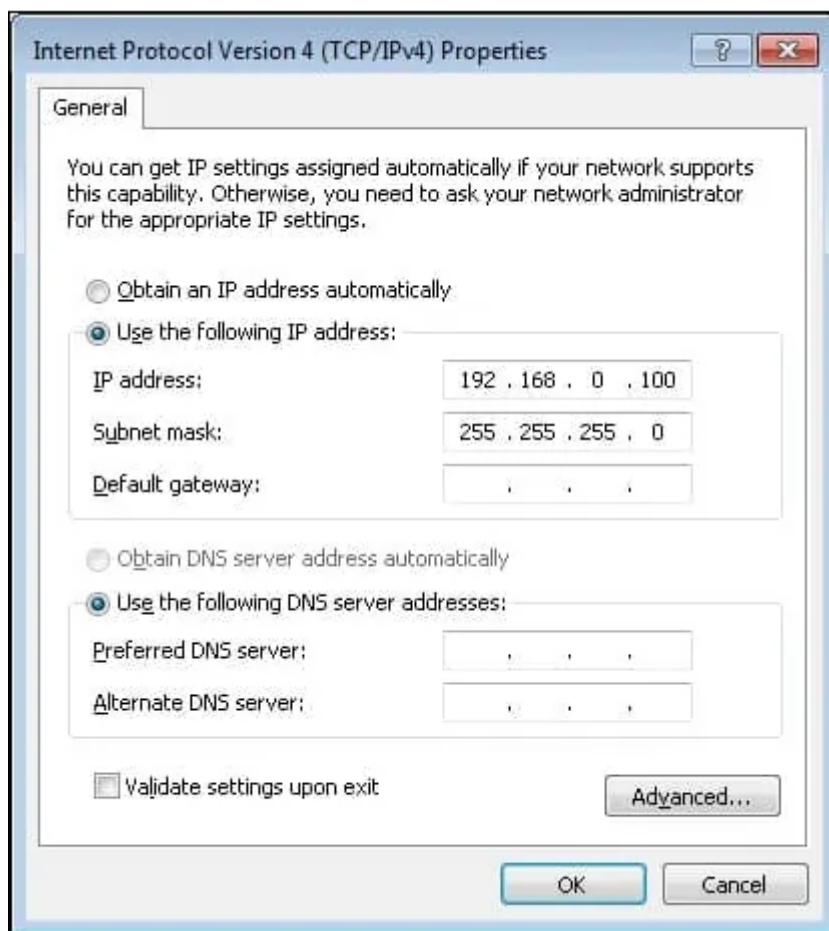
**9- connexion à notre réseau.**

### **2. Configuration Routeur :**



Configurez l'adresse réseau suivante sur votre ordinateur :

- IP - 192.168.0.100
- MASQUE RÉSEAU - 255.255.255.0



Allumez le TP-LINK AX6000 et attendez 1 minute.

Appuyez sur le bouton reset situé à l'arrière de votre équipement pendant 10 secondes.

Sur votre bureau, ouvrez une invite DOS et essayez de pinger l'adresse IP par défaut de l'équipement TP-LINK.

- IP : 192.168.0.1

```

1  C:\> ping 192 .168.0.1
2
3  Pinger 192 .168.0.1 avec 32 octets de données:
4  Réponse de 192 .168.0.1 : octets = 32 temps<1ms TTL = 128
5  Réponse de 192 .168.0.1 : octets = 32 temps<1ms TTL = 128
6  Réponse de 192 .168.0.1 : octets = 32 temps<1ms TTL = 128

```

Ouvrez votre navigateur et entrez l'adresse IP de votre routeur sans fil.

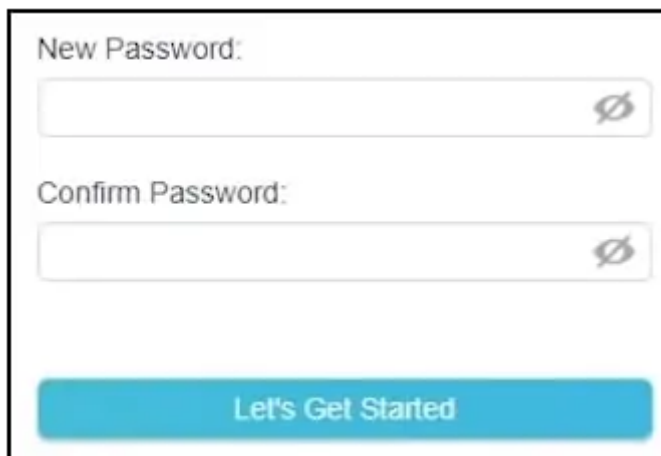
Dans notre exemple, l'URL suivante a été saisie dans le navigateur :

- <http://192.168.0.1>



L'interface web AX1800 doit être présentée.

Définissez un mot de passe de gestion .



Sur l'écran de connexion, saisissez le mot de passe de gestion.




Sélectionnez le bon fuseau horaire.



Sélectionnez la meilleure option pour votre connexion Internet.

Dans notre exemple, nous avons sélectionné l'adresse IP dynamique.



### Select Connection Type

Select your internet connection type. If you are not sure, try AUTO DETECT or contact your ISP (internet service provider) for assistance.

**AUTO DETECT**

☒ Dynamic IP  
Select this type if your ISP doesn't provide any information for internet connection.

☐ Static IP

☐ PPPoE

☐ L2TP

☐ PPTP

**BACK** **NEXT**

Cliquez sur le bouton Suivant.

Cliquez sur le bouton Suivant.



### Dynamic IP

Set the MAC address of your router. Use the default address unless your ISP allows internet access from only a specific MAC address.

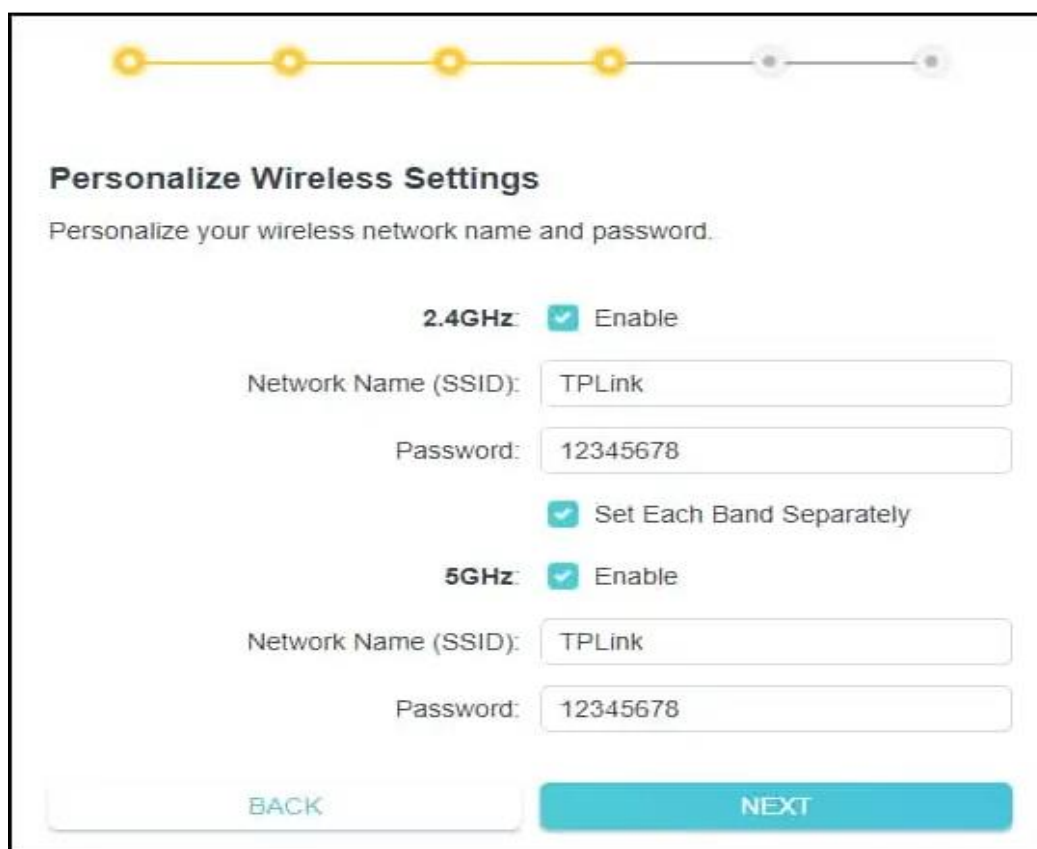
Router MAC Address:

00 - 0A - EB - 11 - 22 - DE

► Special ISP Settings (IPTV/VLAN)

**BACK** **NEXT**

Entrez un nom de réseau sans fil et le mot de passe souhaité.



The screen displays a progress bar at the top with six steps; the first four are highlighted in yellow, and the last two are grey. Below the progress bar, the title "Personalize Wireless Settings" is followed by the instruction "Personalize your wireless network name and password." There are two sections for wireless bands. The "2.4GHz" section has a checked checkbox "Enable", a "Network Name (SSID)" field with "TPLink", a "Password" field with "12345678", and a checked checkbox "Set Each Band Separately". The "5GHz" section also has a checked checkbox "Enable", a "Network Name (SSID)" field with "TPLink", and a "Password" field with "12345678". At the bottom, there are "BACK" and "NEXT" buttons.

**Personalize Wireless Settings**  
Personalize your wireless network name and password.

**2.4GHz:** ☒ Enable

Network Name (SSID): TPLink

Password: 12345678

☒ Set Each Band Separately

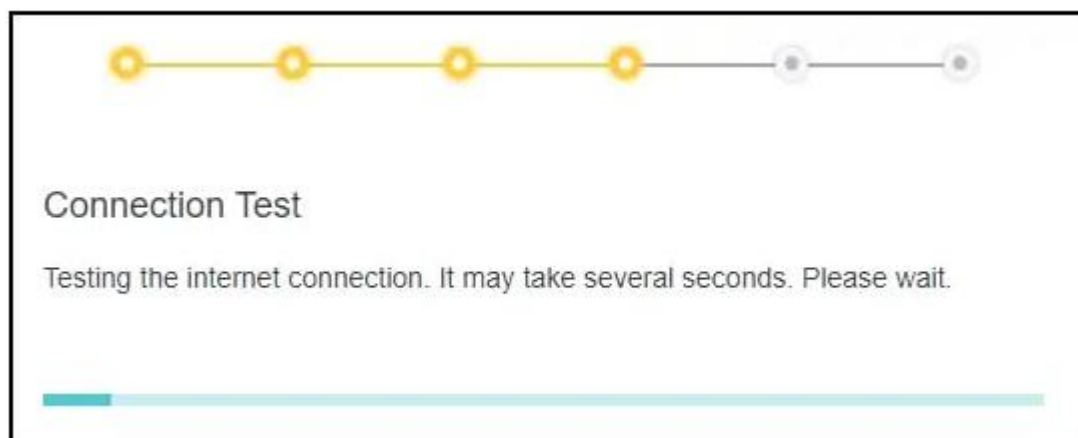
**5GHz:** ☒ Enable

Network Name (SSID): TPLink

Password: 12345678

BACK NEXT

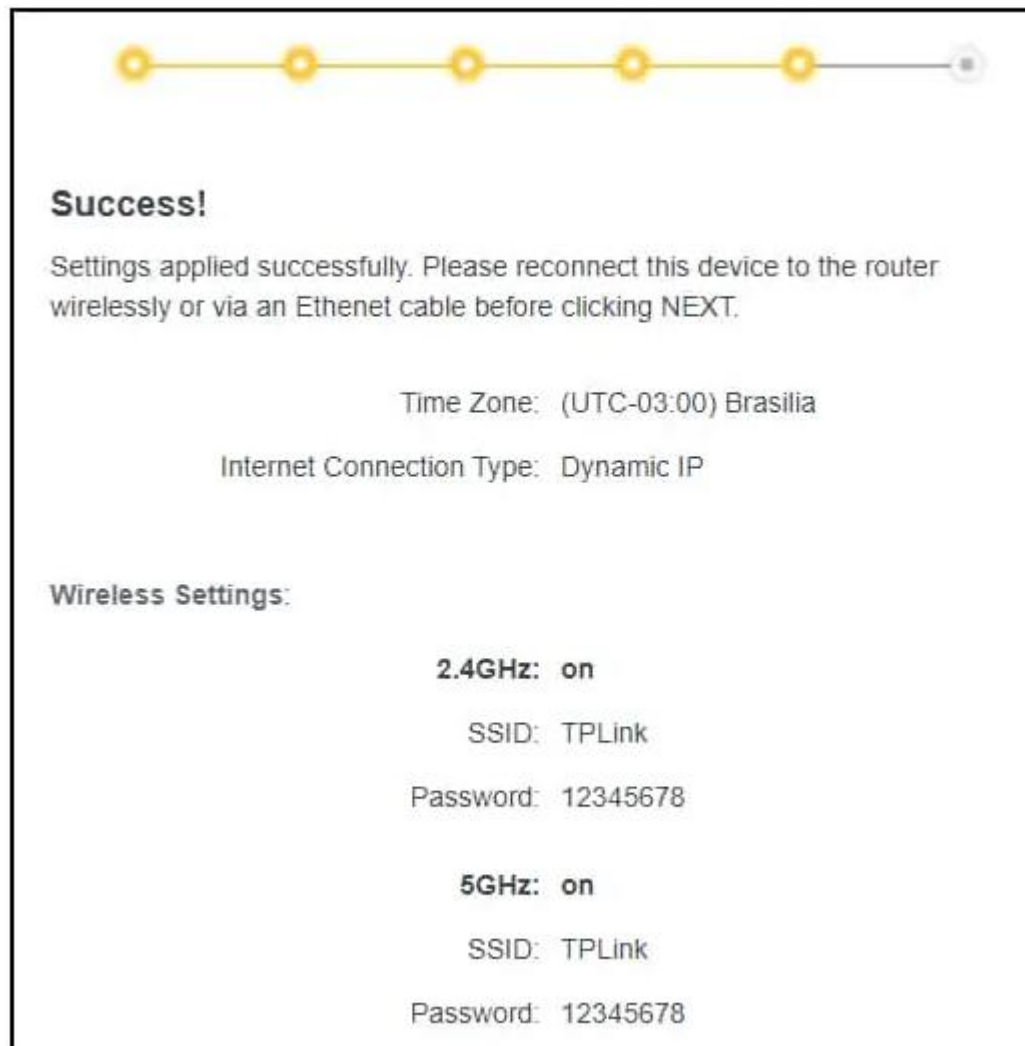
Testez la connexion Internet.



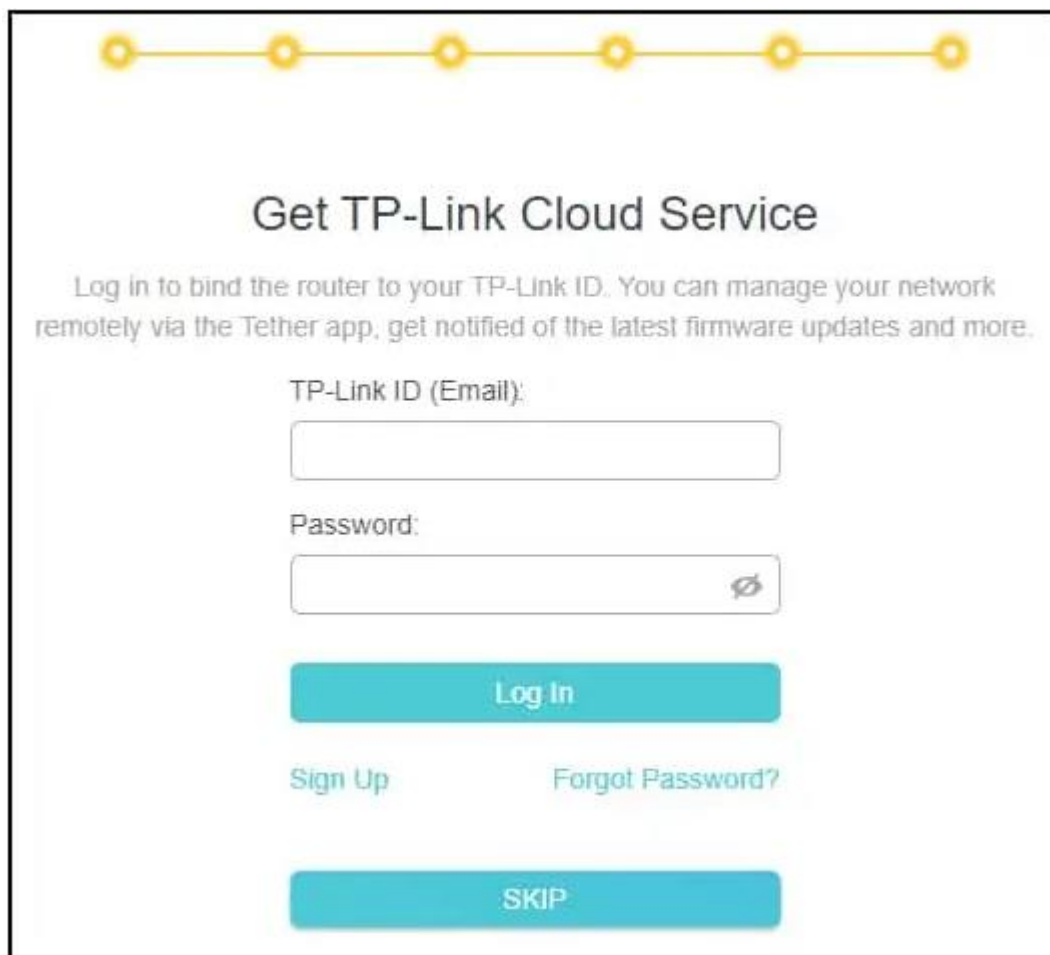
The screen displays a progress bar at the top with six steps; the first four are highlighted in yellow, and the last two are grey. Below the progress bar, the title "Connection Test" is followed by the instruction "Testing the internet connection. It may take several seconds. Please wait." At the bottom, there is a long, thin, light blue progress bar.

**Connection Test**  
Testing the internet connection. It may take several seconds. Please wait.

Sur l'écran récapitulatif, cliquez sur le bouton Suivant.



Cliquez sur le bouton ignorer



**Get TP-Link Cloud Service**

Log in to bind the router to your TP-Link ID. You can manage your network remotely via the Tether app, get notified of the latest firmware updates and more.

TP-Link ID (Email):

Password:

**Log In**

[Sign Up](#)      [Forgot Password?](#)

**SKIP**

Si vous devez modifier l'adresse IP de l'appareil, accédez à l'onglet Avancé en haut de l'écran.



Accédez au menu RÉSEAU et sélectionnez l'option LAN.



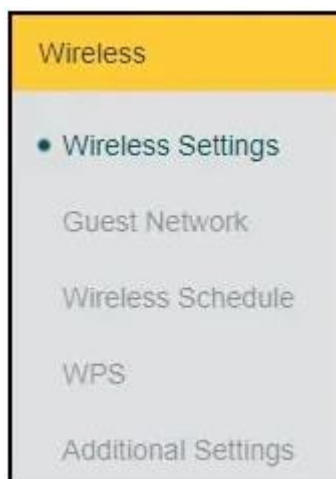
Entrez la configuration réseau souhaitée et cliquez sur le bouton Enregistrer.

MAC Address:	00-0A-EB-11-22-DD
IP Address:	<input type="text" value="192.168.0.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

Si vous devez modifier la configuration sans fil, accédez à l'onglet Avancé en haut de l'écran.



Accédez au menu SANS FIL et sélectionnez l'option PARAMÈTRES SANS FIL.



Entrez la configuration sans fil souhaitée et cliquez sur le bouton Enregistrer.

**Smart Connect:** ☐ Enable ?

**2.4GHz:** ☒ Enable Sharing Network

Network Name (SSID):  ☐ Hide SSID

Security:  ▼

Version:  ▼

Encryption:  ▼

Password:

Transmit Power:  ▼

Channel Width:  ▼

Channel:  ▼

Mode:  ▼