MINISTERE DES ENSEIGNEMENTS SECONDAIRE, SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE(MESSRS)

.....

SECRETARIAT GENERAL(SG)

.....

UNIVERSITE POLYTECHNIQUE DE BOBO-DIOULASSO(UPB)

.....

ECOLE SUPERIEURE D'INFORATIQUE(ESI)

MINISTERE DE LA SANTE(MS)

.....

SECRETARIAT GENERAL(SG)

.....

CENTRE HOSPITALIER UNIVERSITAIRE SANOU SOURO DE BOBO-DIOULASSO(CHUSS)

.....

HOPITAL DE JOUR(HDJ)

MEMOIRE DE FIN DE CYCLE POUR L'OBTENTION DU DIPLOME D'INGENIEUR DE TRAVAUX INFORMATIQUES

Option : RESEAUX ET MAINTENANCE INFORMATIQUES

Thème :

Etude et mise en place d'un réseau informatique sécurisé à l'hôpital de jour du Centre Hospitalier Universitaire Sanou Souro de Bobo-Dioulasso

Présenté et soutenu par :

- **DIALLO Azise Oumar**
- **TALL Hamadoun**

Maître de stage :

Dr BADO Guillaume

Expert et Ingénieur en SIS

Superviseur :

Dr MALO Sadouanoua

Enseignant à l'ESI

Année académique 2009-2010

Table des matières

DEDICACES

DIALLO Azise Oumar

Je dédie le présent document:

A ma mère qui m'a toujours encouragé dans mes études, et m'a toujours apporté son amour et son soutien infaillible.

A la mémoire de mon père. Que la terre lui soit légère et que son âme repose en paix.

TALL Hamadoun

Je dédie ce document à mes chers parents et particulièrement à mon frère ainé TALL Abdoulaye pour m'avoir toujours encouragé et soutenu dans mes études.

REMERCIEMENTS

Nous remercions :

- l'École Supérieure d'Informatique et les intervenants professionnels qui dispensent les cours à l'ESI pour avoir assuré notre formation ;
- Monsieur MALO Sadouanouan, notre superviseur et personne grâce à qui nous avons obtenus ce stage à l'HDJ ;
- Docteur Adrien Bruno SAWADOGO, chef de service de l'HDJ pour nous avoir acceptés au sein de son service;
- Docteur BADO Guillaume, notre maitre de stage pour nous avoir guidés tout au long de ces trois mois mais aussi pour son accueil et la confiance qu'il nous a accordé dès notre arrivée dans le service ;
- Monsieur TAPSOBA Achille responsable informatique de l'HDJ pour sa parfaite collaboration ;
- Docteur KABORE Firmin ainsi que l'ensemble du personnel de l'HDJ pour leur accueil sympathique et leur coopération professionnelle durant ces trois mois de stage;
- Nos parents, tuteurs et les personnes qui d'une manière ou d'une autre ont contribué à notre formation et à faire de ce stage une réussite.
- Nos amis et camarades de classe pour leur solidarité et leur sympathie pendant notre formation.

Que chacun trouve ici un motif de satisfaction et puisse **DIEU** tout puissant rendre à chacun au centuple ses bienfaits.

SIGLES ET ABREVIATIONS

ACL: Access Control List

ARV : Antiretroviraux

CHUSS : Centre Hospitalier Universitaire Sanou Souro

CSMA/CD : Carrier Sense Multiple Access/ Collision Detection

DEA : Diplôme d'Étude Approfondie

DHCP : Dynamics Host Control Protocol

EAP: Extensible Authentification Protocol

ESTHER : Ensemble pour une Solidarité Thérapeutique Hospitalière En Réseau

FAI : Fournisseur d'Accès à Internet

GIP : Groupement d'Intérêt Publique

HDJ : Hôpital De Jour

HTTP /s: Hyper Text Transfer Protocol /secure

IEC: International Electrotechnical Commission

IEEE: Institute of Electrical and Electronics Engeneers

IP: Internet Protocol

ISO: International Organization of Standardization

LDAP: Lightweight Directory Access Protocol

LDIF: Ldap Data Interchange Format

MAC: Media Access Control address

MB: Mega Bite

MYSQL: My Structured Query Language

NAS: Network Access Server

OSI: Open Systems Interconnection

PC : Personal Computer

RADIUS: Remote Access Dial In User Service

RAM : Random Access Memory

RC4: Rivest Cypher 4

RFC: Request For Comments

SIDA : Syndrome de l'Immuno Déficience Acquise

SSL : Secure Sockets Layer

TCP: Transmission Control Protocol

TLS: Transport Layer Security

UDP: User Datagram Protocol

UIT: Union Internationale des Télécommunications

VIH : Virus de l'Immunodéficience Humaine

WEP: Wired Equivalent Privacy

Wi-Fi: Wireless Fidelity

WPA: Wi-Fi Protected Access

AVANT – PROPOS

L'École Supérieure d'Informatique (ESI) est un établissement public d'enseignement supérieur et de recherche de l'Université Polytechnique de BOBO-DIOULASSO (UPB).

Créée en 1991 pour accompagner le pays dans son ambition de former des cadres moyens et supérieurs dans le domaine des Nouvelles Technologies de l'Information et de la Communication (NTIC), l'ESI forme des ingénieurs de travaux informatiques en trois(03) ans, des ingénieurs de conception informatique en cinq (05) ans et des étudiants de niveau DEA informatique. Au niveau du cycle des Ingénieurs de Travaux, l'ESI offre des formations en Analyse Programmation (AP) et en Réseaux et Maintenance Informatiques (RéMI).

Dans l'optique de mieux outiller les étudiants en fin de cycle, l'ESI, les confronte aux réalités et aspects pratiques de la profession d'informaticien en alliant à la formation théorique un stage pratique obligatoire de douze (12) semaines pour les ingénieurs de travaux.

C'est à cet effet que nous avons été reçus à l'HDJ du CHUSS de Bobo-Dioulasso, du 26 aout au 26 novembre 2010 pour un stage pratique en réseaux et maintenance informatiques au cours du quel nous avons développé un projet de fin de cycle dont le présent document tient lieu de rapport.

Introduction générale

La performance du système d'information d'une entreprise est d'une importance capitale pour son efficacité et son bon fonctionnement. La recherche de cette performance entraine de plus en plus l'utilisation d'un système informatique pour la gestion quotidienne des informations. C'est dans cette optique que nous avons été accueillis à l'Hôpital De Jour pour étudier et mettre en place un réseau informatique sécurisé.

Fruit de notre travail à l'HDJ, notre rapport s'articulera autour des principaux points suivants:

La présentation de la structure d'accueil, partie dans la quelle nous allons présenter l'HDJ, son système informatique et faire une étude de notre thème en abordant sa problématique, ses objectifs et la démarche à suivre ;

La sécurité d'un réseau informatique, où nous allons évoquer les différentes solutions permettant de sécuriser un réseau informatique câblé et Wi-Fi puis choisir la solution idoine à mettre en place;

La mise en œuvre des solutions retenues. Dans cette partie, nous allons procéder à la configuration des solutions choisies pour le réseau câblé ainsi que le réseau Wi-Fi puis faire une évaluation des coûts que ces solutions choisies pourront engendrer.

1ère partie : présentation de la structure d'accueil

Chapitre I : Présentation de l'HDJ

I-Historique

Avant la création de l'HDJ, les statistiques ont montré que sur trente(30) personnes admises au service des maladies infectieuses du CHUSS de Bobo-Dioulasso, environ vingt (20) étaient souffrantes du VIH/SIDA.

Vue cet état des faits, le Docteur Adrien Bruno SAWADOGO, actuel chef de service de l'HDJ a émis l'idée de la création d'un centre de prise en charge des personnes vivants avec le VIH/SIDA .Il constitua ainsi un dossier qui fut analysé positivement lors d'une conférence annuelle à Paris. Par ailleurs, sous la bannière de la croix rouge et avec le soutien financier de la fondation Jacqueline DEYTOUT, un Centre de Traitement Ambulatoire(CTA) avait été bâti depuis 2000, mais sans avoir ouvert ses portes au public. Après la conférence, les locaux de ce CTA ont été rétrocédés au service de maladies infectieuses pour l'ouverture d'un hôpital de jour. C'est ainsi que l'Hôpital du jour du CHSSU a ouvert ses ports au puplic le 25 Juillet 2005 dans la ville de Bobo-Dioulasso.

II-Présentation générale

L'HDJ est un détachement du CHUSS de Bobo-Dioulasso chargé de la prise en charge et du suivie des personnes infectées par le VIH/SIDA. Cette structure est soutenue dans son fonctionnement par le programme ESTHER et la Mairie de Paris à travers le partenariat entre l'Hôpital Tenon (AP-HP) et le CHUSS de Bobo-Dioulasso.

II-1- Mission et objectifs

Pour réussir sa mission, l'HDJ s'est fixé les objectifs suivants :

- Le dépistage ;
- Le traitement des infections opportunistes ;
- La prise en charge des personnes vivant avec le VIH/SIDA ;
- Le soutien social, psychologique et nutritionnel des personnes infectées ;
- L'Assurance de la formation dans les centres décentralisés ;
- La contribution aux activités de ces centres décentralisés ;
- Et la promotion de la recherche dans son domaine d'action.

II-2- Partenaires

Ce centre dispose d'un certain nombre de partenaires parmi lesquels on a :

Les partenaires techniques qui sont:

- Hôpital TENON de PARIS (clinique) ;
- Le Centre Hospitalier Universitaire de MONTPELLIER (biologie).

Les partenaires financiers, à savoir:

- La Mairie de Paris ;
- Le groupement d'intérêts publics ESTHER.

II-3-Structuration

L'HDJ est constitué d'une administration (chef de service, gestionnaire et secrétaire) chargé des questions administratives et de cinq (5) unités de traitement qui se pressentent comme suit:

- **L'accueil**

Cette unité s'occupe de l'accueil et de l'enregistrement des patients puis est également chargée de la programmation des rendez-vous de consultations et des examens biologiques des patients.

- **La consultation d'observance**

Elle assure l'éducation thérapeutiques des patients et le suivi de la bonne prise des ARV par ces derniers.

- **Le laboratoire**

C'est là que tous les examens biologiques sont effectués.

- **La consultation médicale**

Dans cette unité, les médecins assurent le suivi des patients vis-à-vis de l'évolution de leur état de santé. Ils leur délivrent aussi des bulletins d'examen et des ordonnances pour les ARV. A cet effet ils utilisent le logiciel « ESOPE » pour ce suivi.

- **La pharmacie**

La pharmacie de l'HDJ s'occupe de la distribution des ARV aux patients à l'aide d'un logiciel appelé « LOGONE ». Mais d'une manière générale elle est chargée de la gestion des produits de cet hôpital.

Par ailleurs toutes les unités sont surveillées par un major et le chef de service.

II-4-Organigramme

L'organigramme de l'HDJ se présente comme suit :

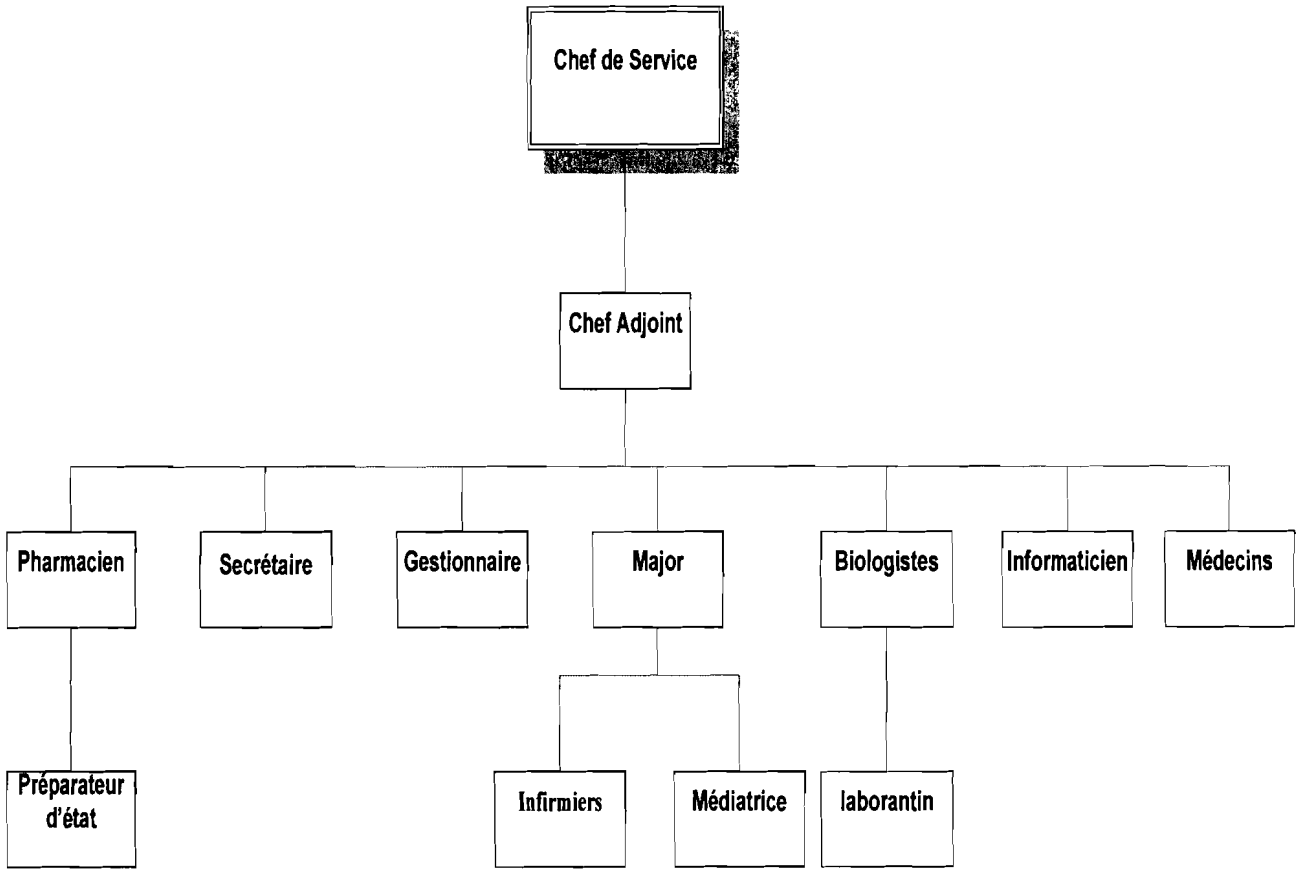


Figure1 : Organigramme de l'HDJ

Chapitre II : Le système informatique de l'HDJ

Vu le nombre important de patients à consulter et surtout pour faciliter la gestion de l'information les concernant, l'HDJ dispose d'un réseau informatique composé d'un réseau câblé et d'un réseau Wi-Fi. Ce réseau informatique encore embryonnaire utilise un certain nombre de matériel et logiciels informatiques pour la gestion quotidienne des patients.

I- Le parc informatique

I-1- Environnement client

L'HDJ dispose d'un parc informatique composé :

- De quatorze (14) ordinateurs de bureau équipés de processeur Pentium 4 tous protégés par des onduleurs ;
- De dix huit(18) ordinateurs portables dont les seize (16) appartiennent au personnel;
- Une(01) imprimante réseau et quatre (03) imprimantes simple.

Il faut également noter la présence circonstancielle d'ordinateurs portables(en dehors des 18 ci-dessus mentionnées) au sein du parc informatique de l'hôpital, apportés et utilisé par des stagiaires ou des médecins en mission au sein de la structure.

Mémoire Ram	Capacité disque dur	Caractéristiques Processeur
512 – 1024MB	80 - 160 Go	1,8 - 3 GHz

Tableau 1: Caractéristiques des ordinateurs de l'HDJ

I-2- Environnement serveur

L'HDJ ne dispose pas encore de serveurs, cependant la structure a un besoin assez pressant d'un serveur pour héberger un certain nombre de logiciels partagés comme ESOPE. Notre étude prendra en compte cette préoccupation.

I-3-Le matériel d'interconnexion

Les équipements d'interconnexion représentent le cœur du réseau dans une architecture. S'ils sont mal dimensionnés, ils pourront avoir des effets négatifs sur le trafic du réseau, pouvant entrainer la détérioration de celui-ci. Dans notre cas d'étude, l'infrastructure du réseau

de l'HDJ étant embryonnaire, ne comporte qu'un commutateur (D-LINK DES 1024D) de 24 ports pour l'interconnexion des différents clients et un modem routeur (NETGEAR DG834G) intégrant le point d'accès du Wi-Fi et permettant l'accès à internet. De par leur fonction, ces équipements ne permettent pas de segmenter le réseau par la technologie VLAN ou de sous-réseau. Cette insuffisance sera prise en compte dans notre étude.

Equipements	caractéristiques	Nombre	Rôle
Modem-Routeur	NETGEAR DG834G	01	Pour l'accès à internet
Switch	D-Link DES 1024D	01	Pour interconnecter les ordinateurs

Tableau 2 : les équipements d'interconnexion de l'HDJ

II- Les logiciels

Le principal système d'exploitation utilisé par les machines au sein de l'HDJ est Windows XP pour les ordinateurs de bureau et Windows vista pour les ordinateurs portables. Pour suivre convenablement les patients au sein des différentes unités de l'hôpital, un certain nombre de logiciels et de programmes sont utilisés, il s'agit:

- du logiciel « **ESOPE** » utilisé par les médecins pour l'enregistrement des patients à la consultation médicale. C'est ainsi qu'on désignera l'identifiant d'un patient par un numéro appelé numéro ESOPE.
- un programme ACCESS dénommé le **<<planificateur>>** utilisé au niveau de l'accueil pour la saisie des informations sur les patients et la planification des rendez-vous.
- Un autre programme ACCESS appelé ***<<EXOAPP>>*** utilisé au niveau de l'observance pour la saisie des informations sur les patients ainsi que la saisie des différents approvisionnements en ARV.
- un logiciel appelé « **LOGONE** » est utilisé au niveau de la pharmacie pour la délivrance des ARV aux patients, mais ce logiciel ne satisfaisant pas la gestion, un fichier EXCEL est également utilisé pour compléter cette gestion pharmaceutique.

III-Le réseau de l'hôpital

III-1- Présentation du réseau

Dans le souci de faciliter le partage d'information entre les différentes unités de l'hôpital (accueil, consultation d'observance, consultation médicale, pharmacie et laboratoire), un réseau informatique local a été installé et deux solutions ont été utilisées pour sa mise en place:

- un câblage filaire avec une topologie physique en étoile utilisant des câbles UTP (Unshielded twisted pair) catégorie 5 pour la liaison entre les ordinateurs de bureau et le Switch (D-Link DES 1024D);
- et un réseau sans fil (Wi-Fi) avec un seul point d'accès fournissant une vitesse théorique de 54Mbits/s destiné aux ordinateurs équipés d'une carte Wi-Fi (IEEE 802.11), particulièrement les portables. Le Wi-Fi est utilisé principalement pour l'accès à internet.

Tous les ordinateurs de bureau fonctionnent en réseau avec une topologie étoile à travers le Switch qui est relié au modem routeur (NETGEAR DG834G) pour l'accès à internet.

III-2- Architecture du réseau

La figure2 ci-dessous présente la topologie physique du réseau de l'HDJ:

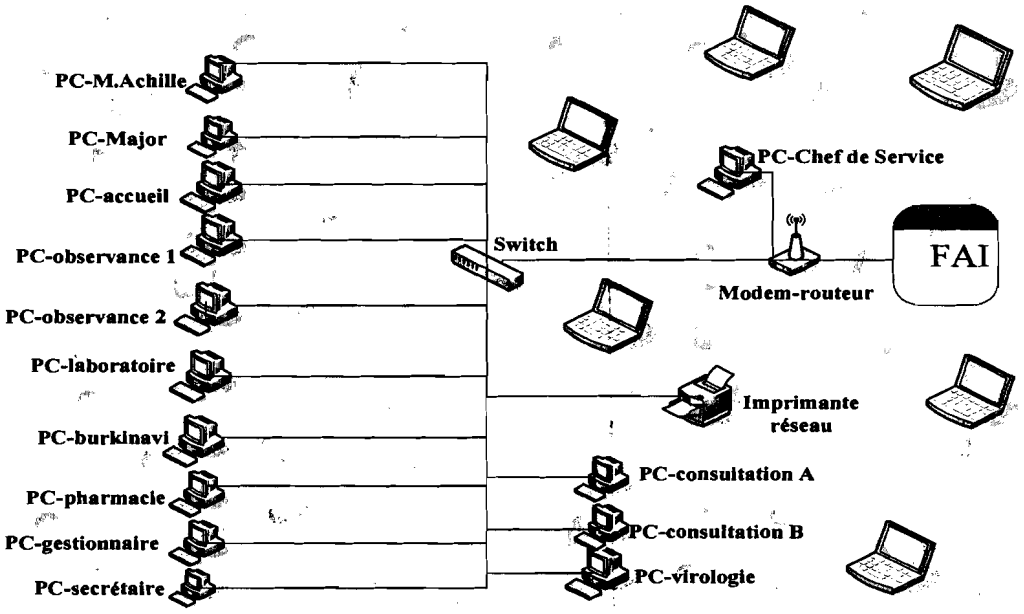


Figure2: Topologie physique du réseau de l'HDJ

III-3- La politique de sécurité du réseau en place

La politique de sécurité utilisée est le cryptage des données circulant et le contrôle d'accès par le WEP au niveau du Wi-Fi.

Chapitre III : Analyse de l'existant et présentation du thème

I-Critique de l'existant

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

- Le positionnement (excentré) du point d'accès du Wi-Fi ne permet pas de couvrir toute la zone de l'hôpital, par conséquent certains médecins ne peuvent pas accéder à internet via Wi-Fi ;
- Le WEP utilisé pour la protection du Wi-Fi présente un certain nombre de limites, car seulement 40 bits ou 104 bits sont utilisés pour le chiffrement de données. La découverte de la clé peut être ainsi rapide si une attaque par force brute (essayer plusieurs possibilités de clés) est effectuée.
- Au niveau du réseau câblé, l'allocation des adresses se fait de façon dynamique sans une demande d'authentification, ce qui donne l'occasion à un individu quelconque de pouvoir accéder au réseau avec son ordinateur portable via un câble réseau d'un poste du réseau câblé;
- L'absence d'une segmentation du réseau en vlan ou en sous-réseau favorise l'action des utilisateurs pirates ;
- Absence d'un nom de domaine pour la structure;
- Absence d'un local technique approprié pour loger les équipements réseau (Switch, modem-routeur, serveur) ;
- Le branchement directe du PC du chef de service au modem-routeur, ce qui attribut une moitié de la connexion internet au PC du chef et les autres PCs devant partager le reste via le Switch ;
- Absence d'un administrateur réseau au sein de la structure ;
- L'absence d'un serveur principal pour héberger les différentes applications partagées sur le réseau.

L'étude de notre thème consistera donc à faire des propositions concrètes par rapport aux problèmes ci-dessus énumérés.

II- Spécification des besoins

Suite à l'étude critique de l'existant et aux échanges effectués avec le responsable informatique de l'HDJ, plusieurs besoins ont été relevés, à savoir:

- Besoin d'élargir la portée du rayonnement du Wi-Fi afin de couvrir toute la zone souhaité ;
- Besoin d'authentifier toute personne souhaitant se connecter au réseau Wi-Fi pour accéder à internet ;
- Besoin de crypter de façon efficace les données circulant sur le réseau Wi-Fi;
- Besoin de segmenter le réseau câblé en vlan ou en sous-réseau;
- Besoin de mettre en place un serveur pour les applications partagées (ESOPE, LOGONE) ;
- La nécessité d'avoir un local technique approprié pour les équipements réseaux ;
- La nécessité d'avoir un administrateur réseau.

III- Étude du thème

III-1- Problématique

L'HDJ dans le but de réussir sa mission doit garder un œil sur son système informatique, en particulier sur la sécurité de son réseau. Cependant malgré la présence d'un système de sécurité, d'énormes difficultés et des vulnérabilités existent, entre autre on a :

- L'adressage dynamique sans demande d'authentification au niveau du réseau câblée ;
- L'absence d'une segmentation du réseau en vlan ou en sous-réseau ;
- L'absence d'un système de gestion centralisée des utilisateurs ;
- La faiblesse du système de contrôler d'accès au réseau wifi ;
- La difficulté de sécuriser les communications sans fils ;
- L'absence d'un serveur pour les applications partagées.

Au regard de toutes ces difficultés rencontrées, l'HDJ souhaiterait mettre en place un système de gestion et de suivi plus efficace de son réseau. C'est ainsi qu'il nous a été proposé de réfléchir sur le thème:« **Etude et mise en place d'un réseau informatique sécurité à l'hôpital du jour du centre hospitalier universitaire Sanou Souro de Bobo-Dioulasso**»

III-2- Objectifs

Notre étude a pour objectif la conception et la mise en place d'un réseau sécurisé qui pourra répondre aux besoins énumérées plus haut. Ainsi nous pourrons:

- Segmenter le réseau en vlan ou en sous-réseau ;
- Contrôler et Authentifier les différents utilisateurs souhaitant accéder au réseau,
- Journaliser quotidiennement les informations sur les utilisateurs qui se connecter ;
- Positionner de façon adéquate le point d'accès du Wi-Fi ;
- Sécuriser les données qui transitent sur le réseau wifi,
- Planifier la mise en place d'un serveur central.

III-3- Démarche à suivre

Dans la suite de notre étude, nous allons identifier des solutions permettant de sécuriser un réseau local filaire et Wi-Fi en mettant l'accent sur le contrôle d'accès et la protection des données du réseau. Parmi les solutions proposées, nous dégagerons, une capable de répondre au mieux aux besoins du moment au niveau filaire et au niveau du Wi-Fi. Nous finirons par une mise en œuvre de la solution choisie.

2ème partie : Étude de la sécurité du réseau

Le réseau local est un ensemble de moyens, mettant en relation permanente des équipements terminaux (stations de travail, micro-ordinateurs, terminaux passifs) et des serveurs au moyen de liaisons, filaires ou non, à l'intérieur d'une zone entièrement sous la responsabilité de l'entreprise.

Un réseau local se caractérise par :

- son système de câblage (paire torsadée, fibre optique, coaxial),
- sa vitesse de transmission,
- sa méthode d'accès : contention Ethernet ou jeton (Token-ring),
- son logiciel de gestion (Windows NT, Netware, Lan-Serveur ...).

Pour assurer son fonctionnement ou ses interconnexions, le réseau a besoin d'équipements tels que les ponts ou passerelles, les routeurs, les commutateurs (switchs) et les concentrateurs (hubs). Ces équipements très sensibles sont installés dans des locaux spécifiques sécurisés couramment appelés "locaux techniques".

La sécurité est un sujet qui touche tous les composants du système d'information, y compris l'environnement (local technique) et les utilisateurs. Elle couvre généralement trois principaux objectifs:

- l'intégrité : garantir que les données sont bien celles qu'on croit être ;
- La confidentialité : donner l'accès aux ressources aux seules personnes autorisées ;
- La disponibilité : maintenir le bon fonctionnement du système informatique.

La suite de notre étude consistera donc à trouver les éléments nécessaires pour garantir l'intégrité, la confidentialité, et la disponibilité du réseau informatique de l'HDJ.

Chapitre I : Sécurité des éléments physique d'un réseau local

L'analyse physique du réseau local se décline selon les composantes suivantes : les locaux techniques, les éléments terminaux et les liaisons.

I-Les locaux techniques et leur contenu

Les locaux techniques sont des points essentiels du réseau local, sans lesquels il ne peut fonctionner correctement. Ils présentent un point de vulnérabilité important dans la mesure où ils abritent un nombre d'appareils sensibles (hubs, routeurs, etc.) et sur lesquels pèsent des menaces importantes (écoute, piratage, etc.). Ils sont intégrés dans un ensemble de bâtiments délimités géographiquement répondant à des règles d'organisation particulières et à des contraintes spécifiques en matière de sécurité (accessibilité, usage unique ou compatible, moyens de surveillance, etc.). Ces locaux devront être alimentés en énergie électrique sécurisée, et éventuellement équipés d'une climatisation. Les câblages, courants forts et courants faibles, devront respecter les normes en vigueur. Au même titre que l'ensemble des éléments d'une entité, certaines menaces pèsent sur ces locaux. Entre autre on peut citer :

Type de Menace	Conséquences	Parades
Incendie	• Indisponibilité des équipements du local • Destruction des équipements • Indisponibilité partielle ou totale du réseau.	• Prévision d'un système de détection et protection contre l'incendie avec un retour d'alarme vers un poste permanent. • Vérification périodique de l'efficacité des équipements. • Affichage des consignes de sécurité encas d'incendie. • Affichage de consignes de sécurité spécifiques. • Information et formation aux moyens de secours du personnel amené à travailler dans les locaux techniques. • Exercices périodiques. • Exigence d' ''un permis de feu'' pour tous les travaux par points chauds dans les sites classés ou les installations.
Dégât des eaux	• Indisponibilité des équipements du local • Destruction des équipements • Indisponibilité partielle ou totale du réseau.	• Étude approfondie préalable du risque eau. • Installation de système de prévention (sonde hygrométrique) avec remontée d'alarme vers un poste permanent. • Installation de système d'évacuation d'eau. • Prévision d'un système

		permettant la coupure automatique de l'électricité. • Nécessité d'un schéma des canalisations. • Localisation formalisée des robinets d'arrêts.
Intrusion	• Détérioration des équipements et/ou du local. • Déconnexion, débranchement ou inversion de câble. • Pose de sonde d'écoute. • Dysfonctionnement des équipements et/ou du réseau. • Vol de matériel	• Prévision d'un accès sécurisé (clé, badge, etc.) avec au besoin un enregistrement des accès et une remontée automatique d'alarme vers un poste permanent. • Prévision d'un système de repérage des câbles ainsi qu'un schéma du câblage. • Identification des équipements au moyen de plaques inviolables, de système de tatouage, de plombage, etc. • Détection d'ouverture (portes, fenêtres, etc.). • Éviter, si possible, l'utilisation des locaux techniques partagés dans les immeubles intelligents

Tableau3 : Les principales menaces et parades associées des locaux techniques

II-Les éléments terminaux du réseau local

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

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

Tableau4 : Les principales menaces et parades associées des éléments terminaux

III-Les liaisons

Les liaisons servent à véhiculer l'information entre les éléments actifs du réseau contenus soit dans les locaux techniques, soit dans le poste de travail de l'utilisateur (exemple : carte modem). Les liaisons peuvent être des éléments internes (câbles, fibre optique, ondes, laser, infrarouges, etc.). Ces liaisons sont présentes dans tous les locaux de l'entreprise (bureau, entrepôt, couloirs) ce qui les rend faciles d'accès et donc difficile à sécuriser. De plus, elles sont en perpétuelle évolution. Il est souhaitable d'éviter que les chemins de câbles soient dans des endroits non protégés.

Menace type	Conséquences	Parades
Coupure accidentelle ou volontaire de câbles (sabotage).	Isolement de tout ou partie du réseau local.	• Réduction des risques du blocage du réseau par une architecture sécurisée en boucle et une redondance de la topologie. • Protection des chemins de câbles (capot, scellement, mise sous pression, etc.). • Plan de câblage à jour. • Repérage des câbles. • Contrôles périodiques des câbles. • Utilisation d'outils d'analyse des câbles.
Erreur de manipulation (déconnexion accidentelle).	• Dysfonctionnements. • Isolement de tout ou partie du réseau local.	• Plan de câblage à jour. • Repérage des câbles. • Formation du personnel de maintenance. • Contrôle des interventions des sous traitants.

Tableau5: Les principales menaces et parades associées des liaisons

Toutes ces recommandations et préconisations ne dispensent pas, bien au contraire, de faire une étude sécuritaire de contrôle d'accès logique.

Chapitre II : Les équipements d'interconnexion

Un réseau peut être divisé en unités plus petites appelées segments.

Chaque segment utilise le mode d'accès CSMA/CD et assure le trafic entre les utilisateurs sur le segment. Il constitue également son propre domaine de collision.

La segmentation permet alors de réduire significativement la congestion. On distingue la segmentation physique et celle logique.

I- Segmentation Physique

I-1- Segmentation à l'aide des ponts

Les ponts sont des équipements de couche 2 qui transmettent des trames de données en fonction de l'adresse MAC. Les ponts lisent l'adresse MAC de l'émetteur des paquets de données reçus sur les ports entrants pour découvrir les équipements de chaque segment. Les adresses MAC sont ensuite utilisées pour créer une table de commutation qui permet au pont de bloquer les paquets qu'il n'est pas nécessaire de transmettre à partir du segment local.

Bien que le fonctionnement d'un pont soit transparent pour les autres équipements, l'utilisation d'un pont augmente de dix à trente pour cent la latence d'un réseau. Cette latence résulte du processus de prise de décision qui a lieu avant l'envoi d'un paquet. Un pont est considéré comme un équipement de type Store-and-Forward, car il doit examiner le champ d'adresse de destination et calculer le code de redondance cyclique (CRC) dans le champ de séquence de contrôle de trame avant l'envoi d'une trame. Si le port de destination est occupé, le pont peut stocker temporairement la trame jusqu'à ce que le port soit de nouveau disponible.

1-2- Segmentation LAN à l'aide de routeurs

Les routeurs assurent la segmentation des réseaux en ajoutant un coefficient de latence de 20 à 30 % sur un réseau commuté. Cette latence accrue est due au fonctionnement d'un routeur au niveau de la couche réseau qui utilise l'adresse IP pour déterminer le meilleur chemin vers le nœud de destination.

Dans la segmentation LAN, les ponts et les commutateurs assurent la segmentation au sein d'un réseau ou d'un sous-réseau. Les routeurs assurent la connectivité entre les réseaux et les sous réseaux.

En outre, les routeurs n'envoient pas de broadcast, tandis que les commutateurs et les ponts doivent transmettre des trames de broadcast.

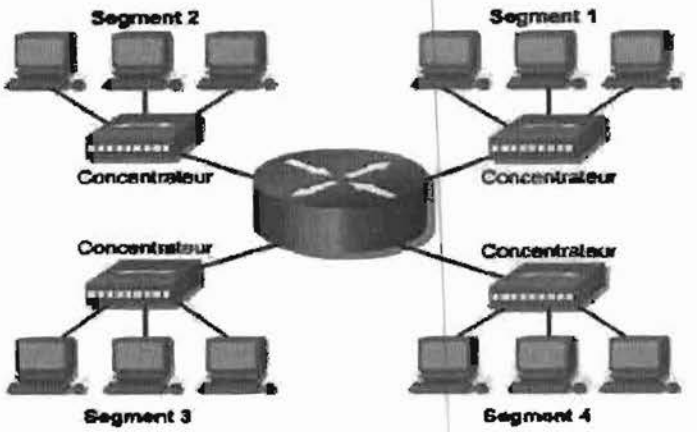


Figure3 : Réseau segmenté par routeur

I-3- Segmentation LAN à l'aide de commutateurs

La commutation LAN réduit les pénuries de bande passante et les goulots d'étranglement sur le réseau, comme ceux qui se produisent entre plusieurs stations de travail et un serveur de fichiers distant. Un commutateur divise un réseau LAN en micro segments afin de réduire la taille des domaines de collision. Cependant, tous les hôtes connectés au commutateur restent dans le même domaine de broadcast.

Dans un LAN Ethernet commuté parfait, les nœuds d'émission et de réception opèrent comme s'ils étaient les seuls nœuds du réseau. Lorsque ces deux nœuds établissent une liaison, ou circuit virtuel, ils accèdent au maximum de bande passante disponible. Ces liaisons offrent un débit plus important que les LAN Ethernet connectés via des ponts ou des concentrateurs.

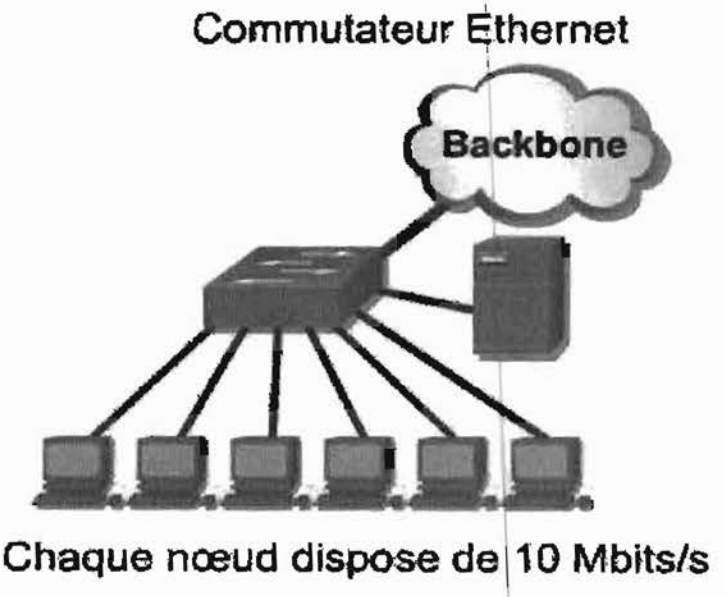


Figure 4: Réseau segmenté par commutateur

II-Segmentation Logique, la solution VLAN

II-1- Généralités

Par définition, un VLAN (Virtual Local Area Network) Ethernet est un réseau local virtuel (logique) utilisant la technologie Ethernet pour regrouper les éléments du réseau (utilisateurs, périphériques, etc.) selon des critères logiques (fonction, partage de ressources, appartenance à un département, etc.), sans se heurter à des contraintes physiques (dispersion des ordinateurs, câblage informatique inapproprié, etc.).

Les VLAN offrent un certain nombre de propriétés à savoir :

- Un support de transferts de données allant jusqu'à 1Gb/s,
- La couverture d'un ou plusieurs bâtiments,
- Ils peuvent s'étendre au niveau d'un réseau plus large,
- L'appartenance d'une station à plusieurs VLAN simultanément.

C'est un sous réseau de niveau 2 construit à partir d'une technologie permettant de cloisonner des réseaux par usage de filtres de sécurité. Cette technologie balise le domaine de broadcast auquel ces machines appartiennent de telle sorte que le trafic intra-domaine ne puisse pas être vu par des tiers n'appartenant pas à ce domaine de broadcast.

II-2- Avantages Offerts par les VLANs

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

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

- **La flexibilité de segmentation du réseau.** Les utilisateurs et les ressources entre lesquels les communications sont fréquentes peuvent être regroupés sans devoir prendre en considération leur localisation physique. Il est aussi envisageable qu'une station appartienne à plusieurs VLANs en même temps,
- **La simplification de la gestion.** L'ajout de nouveaux éléments ou le déplacement d'éléments existants peut être réalisé rapidement et simplement sans devoir manipuler les connexions physiques dans le local technique,
- **L'augmentation considérable des performances du réseau.** Comme le trafic réseau d'un groupe d'utilisateurs est confiné au sein du VLAN qui lui est associé, de la bande passante est libérée, ce qui augmente les performances du réseau;
- **Une meilleure utilisation des serveurs réseaux.** Lorsqu'un serveur possède une interface réseau compatible avec le VLAN, l'administrateur a l'opportunité de faire

appartenir ce serveur à plusieurs VLAN en même temps. Cette appartenance à de multiples VLAN permet de réduire le trafic qui doit être routé (traité au niveau du protocole de niveau supérieur, par exemple IP) de, et vers ce serveur; et donc d'optimiser ce trafic. Tout comme le découpage d'un disque dur en plusieurs partitions permet d'augmenter les performances (la fragmentation peut être diminuée) de son ordinateur, le VLAN améliore considérablement l'utilisation du réseau,

- **Le renforcement de la sécurité du réseau.** Les frontières virtuelles créées par les VLAN ne pouvant être franchies que par le biais de fonctionnalités de routage, la sécurité des communications est renforcée,
- **La technologie évolutive et à faible coût.** La simplicité de la méthode d'accès et la facilité de l'interconnexion avec les autres technologies ont fait d'Ethernet une technologie évolutive à faible coût quelles que soient les catégories d'utilisateurs,
- **La régulation de la bande passante.** Un des concepts fondamentaux des réseaux Ethernet est la notion d'émission d'un message réseau vers l'ensemble (broadcast ou multicast) des éléments connectés au même commutateur (hub/Switch). Malheureusement, ce type d'émission augmente sérieusement le trafic réseau au sein du composant de connexion. Même si les vitesses de transmission ne cessent d'augmenter, il est important de pouvoir contrôler ce gaspillage de capacité de trafic (bande passante). Ici encore, le VLAN offre à l'administrateur les moyens de réguler l'utilisation de la capacité de trafic disponible au sein de l'infrastructure.

II-3- La technique des VLANs

Pour réaliser des VLANs, il faut tout d'abord des commutateurs spéciaux de niveau 2 du model OSI qui supportent le VLAN.

Ces produits combinent tous les avantages des solutions précédentes :

- Partitionnement en plusieurs domaines de broadcast
- Affectation d'un ou plusieurs ports à un VLAN depuis une console centrale (amélioration de la bande passante par la fonction de commutation)
- Adaptation de la vitesse du Switch à la capacité du réseau
- Regroupement des VLAN sur un même segment backbone (réseaux distants avec des Vlan commun de bout en bout)
- Gestion d'une bonne étanchéité entre VLAN

On distingue généralement trois techniques pour construire des VLAN, en fonction de leurs méthodes de travail, nous pouvons les associer à une couche particulière du modèle OSI :

II-3-1 VLAN de niveau 1 ou VLAN par port

On affecte chaque port des commutateurs à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par sa connexion à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN.

Les ports des Switchs sont associés à des VLANs (Figure 5) :

- Ports 1,2 et 3 appartiennent au VLAN 1
- Ports 4,5 et 6 au VLAN 2
- Ports 7 et 8 au VLAN 3

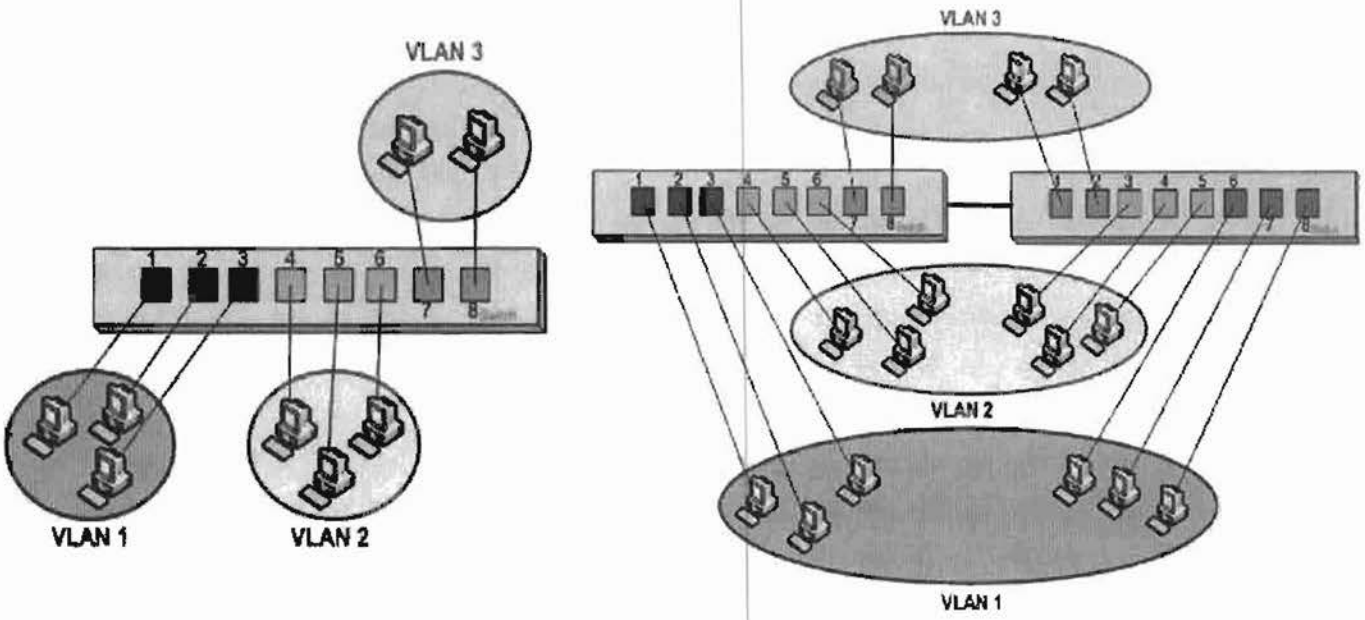


Figure5 : Vlan par port

II-3-2- VLAN de niveau 2 ou VLAN MAC

On affecte chaque adresse MAC à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminé par son adresse MAC. En faite il s'agit à partir de l'association Mac/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN.

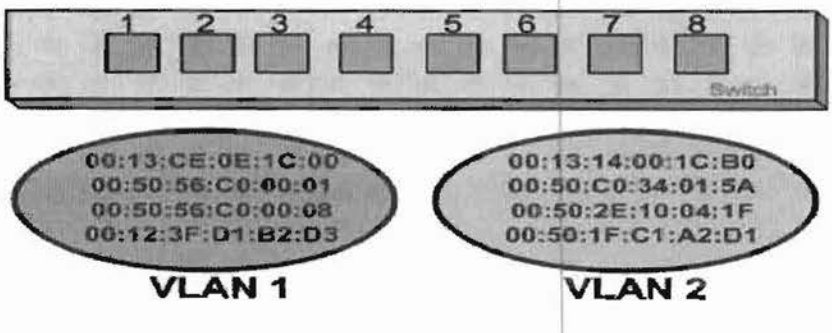


Figure6 : **Vlan par adresse MAC**

II-3-3- VLAN de niveau 3 ou VLAN d'adresses réseaux

On affecte un protocole de niveau 3 ou de niveau supérieur à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par le protocole de niveau 3 ou supérieur qu'elle utilise. En faite il s'agit à partir de l'association protocole/VLAN d'affecter dynamiquement les ports des commutateurs a chacun des VLAN.

II-4- Principe de fonctionnement des VLANs

Comment transporter et reconnaitre à l'arrivée sur un même segment physique, des trames issues de plusieurs VLANs ?

II-4-1- L'étiquetage

L'étiquetage consiste à marquer toutes les trames sortantes du commutateur avec le numéro du VLAN d'appartenance.

Le commutateur suivant peut alors repérer les trames et les diriger vers le VLAN correspondant.

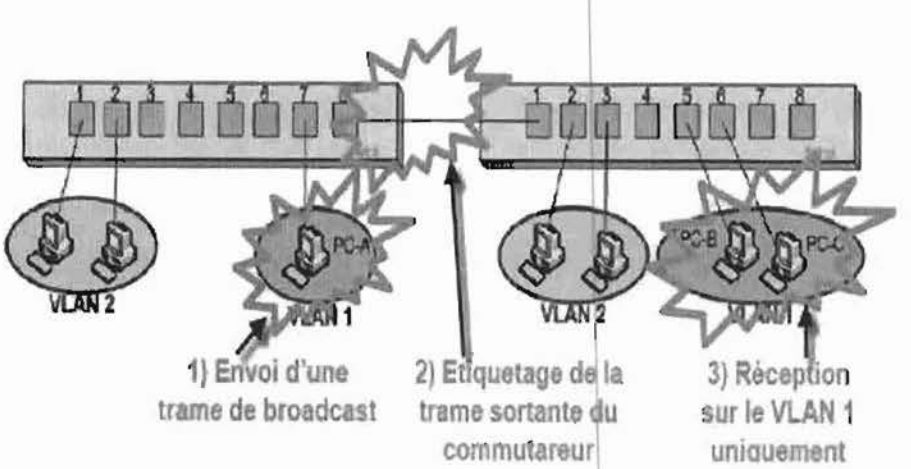


Figure7 : Étiquetage

II-4-2- La trame Ethernet classique

La figure8 nous montre une trame Ethernet classique sans VLANs

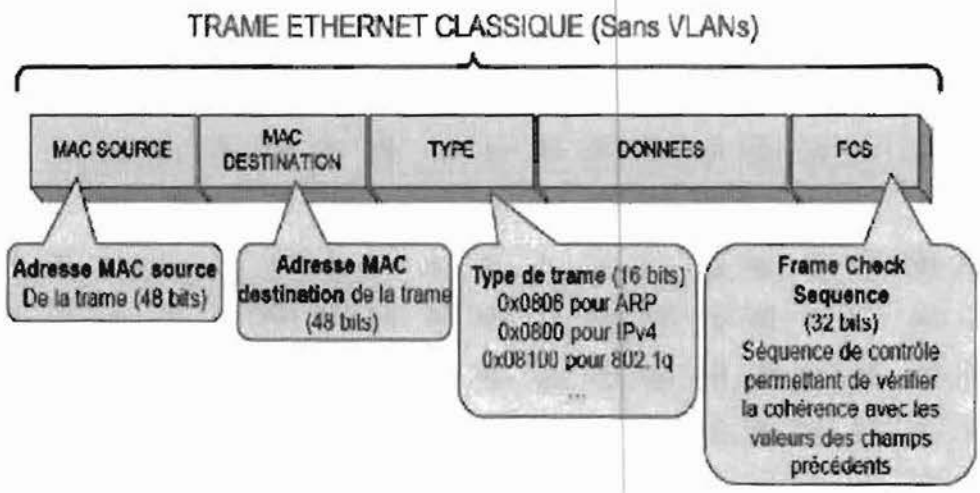


Figure8 : Trame Ethernet classique

II-4-3- La trame Ethernet 802.1q

L'étiquetage se fait grâce à la norme 802.1q (dot1.q) et Les trames ont un champ supplémentaire comme indiquées sur la figure9.

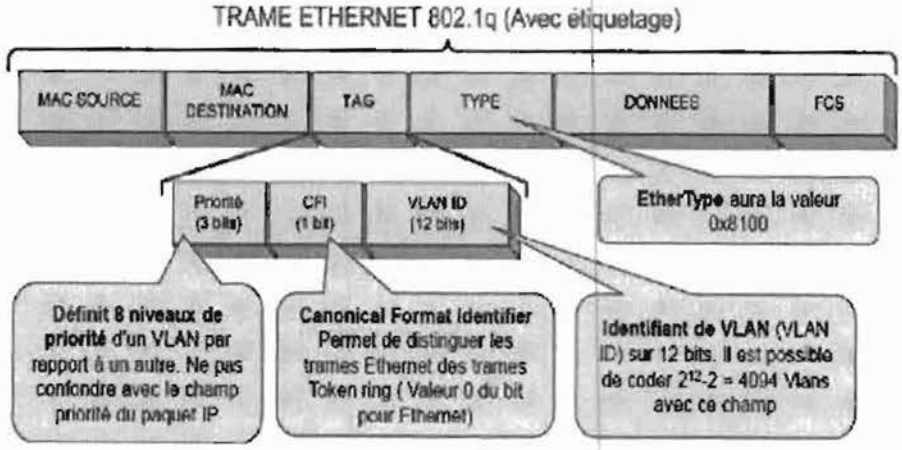


Figure9 : Trame Ethernet 802.1q

Chapitre III : La sécurité du réseau Wi-Fi

I-Généralités sur le Wi-Fi

I-1- Définition

La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fils (Wi-Fi). Le nom Wi-Fi (contraction de Wireless Fidelity) correspondait initialement au nom donné à la certification délivrée par la Wi-Fi alliance, autrefois connu sous le nom de WECA (Wireless Ethernet Compatibility Alliance), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau Wifi est en réalité un réseau sans fils répondant à la norme 802.11.

Cette norme 802.11 est définie sur les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- La couche physique, proposant trois types de codages de l'information ;
- La couche liaison de donnée, constituée de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support connu sous l'acronyme MAC.

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet des règles de communication entre les différentes stations.

I-2- Les normes du Wi-Fi

Il existe plusieurs normes de Wi-Fi, cependant les plus utilisées sont les suivantes :

- **802.11a,** cette norme est baptisée *Wi-Fi 5* et permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 11 canaux radio dans la bande de fréquence des 5 GHz. Il s'agit d'une bande de fréquence peu utilisée : les interférences seront donc moindres que dans la bande de fréquence 2.4 GHz (bande de fréquence utilisée par la plupart des autres normes Wi-Fi). Cependant cette norme est interdite en extérieur.

- **802.11b,** elle propose un débit théorique de 11 Mbps (contre 6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.
- **802.11g,** Il s'agit d'une évolution de la norme 802.11b. Elle permet d'obtenir un haut débit (54 Mbps théoriques, contre 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b. C'est la norme la plus utilisée actuellement.

I-3- Types et Mise en place d'un réseau wifi

Il existe deux modes de déploiement d'un réseau Wi-Fi :

- Le mode « Ad-Hoc » : c'est un mode de fonctionnement qui permet de connecter directement les ordinateurs équipés d'une carte réseau Wi-Fi, sans utiliser un matériel tiers tel qu'un point d'accès. Ce mode est idéal pour interconnecter rapidement des machines entre elles sans matériel supplémentaire.

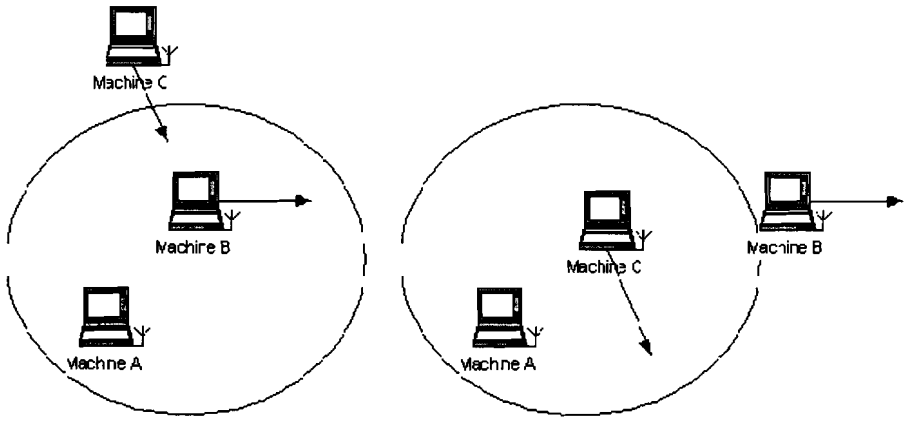


Figure10: Schéma d'un réseau Wi-Fi de type Ad-Hoc

- Le mode infrastructure : c'est un mode de fonctionnement qui permet de connecter les ordinateurs équipés d'une carte réseau Wi-Fi entre eux via un ou plusieurs points d'accès qui agissent comme des concentrateurs. Il est essentiellement utilisé en entreprise. La mise en place d'un tel réseau oblige de poser à intervalle régulier des points d'accès dans la zone qui doit être couverte par le réseau.

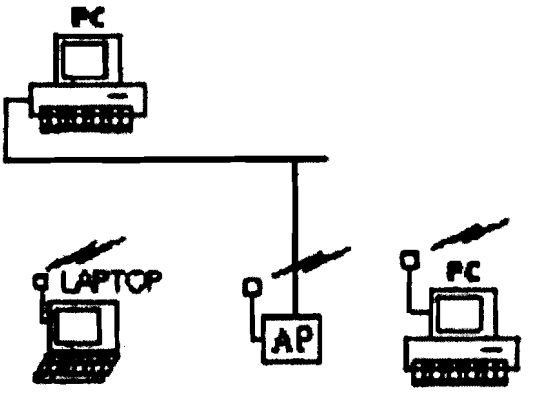


Figure11 : Schéma d'un réseau Wi-Fi de type infrastructure

La mise en place d'un réseau wifi est beaucoup moins compliquée que celle d'un réseau filaire. Cependant la sécurité reste encore un problème nécessitant une attention particulière.

II-Sécurité du Wi-Fi

La sécurisation du réseau Wi-Fi passera d'abord par le bon positionnement du (ou des) point(s) accès afin de couvrir toute la zone souhaitée. Avant de prendre en compte la disponibilité, la confidentialité et l'intégrité des données circulant sur le réseau.

II-1- Les solutions de cryptage de donnée circulant sur le réseau

II-1-1- Le WEP

Pour remédier aux problèmes de confidentialité des échanges sur un réseau sans fil, le standard 802.11 intègre un mécanisme simple de chiffrement de données, le WEP. Ce cryptage travaille avec l'algorithme RC4 pour chiffrer les données et utilise des clés statiques de 64 ou 128 voire 152 bits suivant les constructeurs.

Le principe du WEP consiste à définir une clé sécrète qui doit être déclarée au niveau de chaque adaptateur sans fil du réseau ainsi que sur le point d'accès. La clé sert à créer un nombre pseudo-aléatoire d'une longueur égale à la longueur de la trame. Chaque élément du réseau voulant communiquer entre eux doit connaître la clé secrète qui va servir au cryptage WEP. Une fois mis en place, toutes les données transmises sont obligatoirement cryptées. Il assure ainsi l'encryptage des données durant leur transfert ainsi que leurs intégrités.

Avantages : Le WEP permet un cryptage des données transitant sur le réseau et limite l'accès au réseau à un certain nombre d'individus.

Comme limite, il ya un certain nombre de vulnérabilité, à savoir :

- Contre la confidentialité, du fait de la réutilisation de la suite chiffrée, de la faiblesse du RC4 et d'une possible fausse authentification ;
- Contre l'intégrité du fait de la capacité à modifier les paquets et d'en injecter des faux.

II-1-2- Le WPA

Une autre solution de sécurisation des données et d'accès au réseau sans fil est le WPA. Il signifie Wi-Fi Protected Access. Il repose sur un protocole d'authentification et un algorithme de cryptage, TKIP (Temporary Key Integrety Protocol).TKIP permet une génération aléatoire de clés et la modification de ces dernières plusieurs fois par seconde. On distingue deux modes de fonctionnement du WPA :

- Le **WPA personnel** : il se base sur l'utilisation d'une clé partagée appelée PSK (Pre-Shared Key) entre le point et les postes clients. Cette clé n'est pas prédéfinie comme au niveau du WEP, c'est plutôt une passphrase (phrase secrète) qui est saisie et ensuite traduite en PSK par un algorithme de hachage.
- Le **WPA entreprise** : il se base ici sur l'utilisation d'une infrastructure d'authentification 802.1x (serveur RADIUS par exemple) et d'un point d'accès.

Avantages: il est difficile de déterminer la clé utilisée au niveau du WPA car l'algorithme TKIP en plus de la génération périodique de clés de chiffrement, utilise aussi 48bits pour l'initialisation. Aussi, un vérificateur de données permet de vérifier l'intégrité des informations reçues pour être sûr que personne ne les a modifiées. Il permet également d'utiliser une clé par station connectée au réseau sans fil.

Limites: Quelques problèmes subsistent tout de même à ce protocole et notamment l'attaque de type « déni de service ». En effet, si quelqu'un envoie au moins deux paquets chaque seconde utilisant une clé de cryptage incorrecte, alors le point d'accès sans fil « tuera » toutes les connexions utilisateurs pendant une minute. C'est un mécanisme de défense pour éviter les accès non-autorisés à un réseau protégé, mais cela peut bloquer tout un réseau sans fil. Il ya également l'absence d'un meilleur protocole de cryptage tel que AES (Advanced Encryption Standard).

II -1-3- Le WPA-802.1x

Cette version du cryptage WPA nécessite l'utilisation d'un serveur Radius pour le processus d'authentification. Chaque utilisateur (client sans fil) doit avoir un identifiant d'utilisateur sur le serveur Radius, et cet appareil doit avoir un identifiant de client sur le serveur Radius. Les transmissions de données sont cryptées à l'aide d'une clé générée automatiquement.

II-1-4- Le WPA2

Outre les solutions citées ci-dessus, il existe une autre solution de sécurisation poussée proposée par la norme 802.11i. Le WPA2 s'appuie sur l'algorithme de chiffrement comme le WPA mais supporte l'AES (Advanced Encryption Standard) au lieu du RC4. Il faut noter que l'AES est un algorithme de chiffrement plus sûr. En plus d'assurer le cryptage et l'intégrité des données, le WPA 2 offre d'autres fonctionnalités que sont le « **key caching** » et la « **pré-authentification** ».

- **Key caching** : l'utilisateur a la possibilité de conserver la clé PMK (PairwiseMaster Key) afin de la réutiliser lors des prochaines transactions avec le même point d'accès(PA). La clé PMK, une variante de la clé PSK est gérée par le PMKID (Pairwise Master Key Identifier) qui n'est d'autre qu'un hachage entre la clé PMK, l'adresse MAC du point d'accès et du client mobile, et une chaîne de caractères. La clé PMK est identifiée de façon unique par le PMKID.
- **Pré-authentification** : l'utilisateur a la possibilité de s'identifier avec un PA sur le quel il est probable qu'il se connecte dans le futur. Ceci se fait par la redirection des trames d'authentification générées par le client et envoyées au PA actuel vers son PA futur grâce au réseau filaire.

Avantages : le WPA2 offre une sécurité et une mobilité plus efficaces grâce à l'authentification du client où qu'il soit. Aussi une forte intégrité et une forte confidentialité sont offertes grâce à un mécanisme de distribution dynamique de clés.

En plus il permet une flexibilité grâce à une ré- authentification rapide et sécurisée.

Limites : le fait qu'une station puisse se connecter à plusieurs points d'accès en même temps accroît de manière significative le temps de charge. Le WPA2 engendre des coûts supplémentaires pour les entreprises car pour son utilisation il faut un équipement spécifique tel qu'une puce cryptographique dédiée pour les calculs exigés par l'AES.

II-2-Les solutions de Contrôle d'accès

L'utilisateur qui souhaite se connecter au réseau doit d'abord signaler sa présence avant de se faire connaître ou reconnaître par le ou les serveur(s) chargés de le faire. On appelle solution de contrôle d'accès ou méthode d'authentification, la manière dont procède l'utilisateur pour se faire reconnaître ou se faire authentifier par le serveur d'authentification. On dénombre plusieurs procédés parmi lesquels on peut citer :

II-2-1- Le filtrage des adresses MAC

Cela consiste à définir au niveau de notre point d'accès les adresses des équipements qui sont autorisés ou non à accéder au réseau. En rappel, une adresse MAC est un numéro unique propre à chaque carte réseau composé de 12 chiffres hexadécimaux groupés par paires et séparés par des tirets. La liste des équipements définis au niveau du point d'accès autorisés ou non au réseau est appelée ACL.

Cette solution a certes des avantages mais aussi des limites :

Avantages : avec cette solution, l'usurpation des adresses MAC est difficile car on ne peut pas a priori connaître l'adresse MAC. Aussi on peut changer l'adresse IP sans toucher l'adresse MAC. Cependant on distingue plusieurs limites.

Limites: cette solution n'est pas adaptée au grand réseau car la collecte d'adresse MAC est fastidieuse. En cas de changement de carte réseau, il faut aussi changer la configuration initiale du système de filtrage. Aussi, on peut facilement redéfinir l'adresse MAC par voie logicielle (exemple **smac**). Enfin, le protocole 802.11b/g n'encrypte pas les trames où apparaissent ces adresses MAC.

II-2-2- Le standard 802.1x

II-2-2-1- Définition

Le 802.1x est un standard mis au point par IEEE en juin 2001. Il permet de contrôler l'accès au réseau local et cela dans le but d'authentifier tout utilisateur désirant s'y connecter. Cette authentification intervient avant tout mécanisme d'auto configuration comme le DHCP.

Pour son fonctionnement trois entités interviennent:

- le système souhaitant s'authentifier ou **supplicant** dont l'objectif est de pouvoir accéder aux ressources contrôlées par le point d'accès et celles disponibles sur le réseau ;
- le système authentificateur qui contrôle une ressource disponible via le point d'accès physique du réseau appelé PAE (Port Access Entity), il joue le rôle de mandataire entre le suppliciant et le serveur d'authentification ;

- le serveur d'authentification qui se charge de gérer l'authentification proprement dite en dialoguant avec le supplicant.

II-2-2-2- Principe de fonctionnement

Le supplicant se connecte au réseau par l'intermédiaire d'un PAE contrôlé par le système authentificateur, ce PAE est divisé en deux ports logiques : un port non contrôlé et un port contrôlé. Le port non contrôlé est un port toujours accessible (toujours fermé). Il permet l'échange entre le serveur d'authentification et le supplicant pour l'authentification. Le port contrôlé peut prendre deux états (ouvert ou fermé). Ces états sont contrôlés par une variable appelée **Authcontrolled Port Control.** Cette variable peut être positionnée à trois valeurs définissant ainsi l'état du port. On a la valeur **Force Unauthorised** qui définit l'état ouvert quelque soit le résultat de l'authentification. La valeur **Force Authorised** qui définit l'état fermé quelque soit le résultat de l'authentification. Et enfin la valeur **Auto** qui définit soit l'état ouvert si l'authentification échoue, soit l'état fermé si l'authentification réussit.

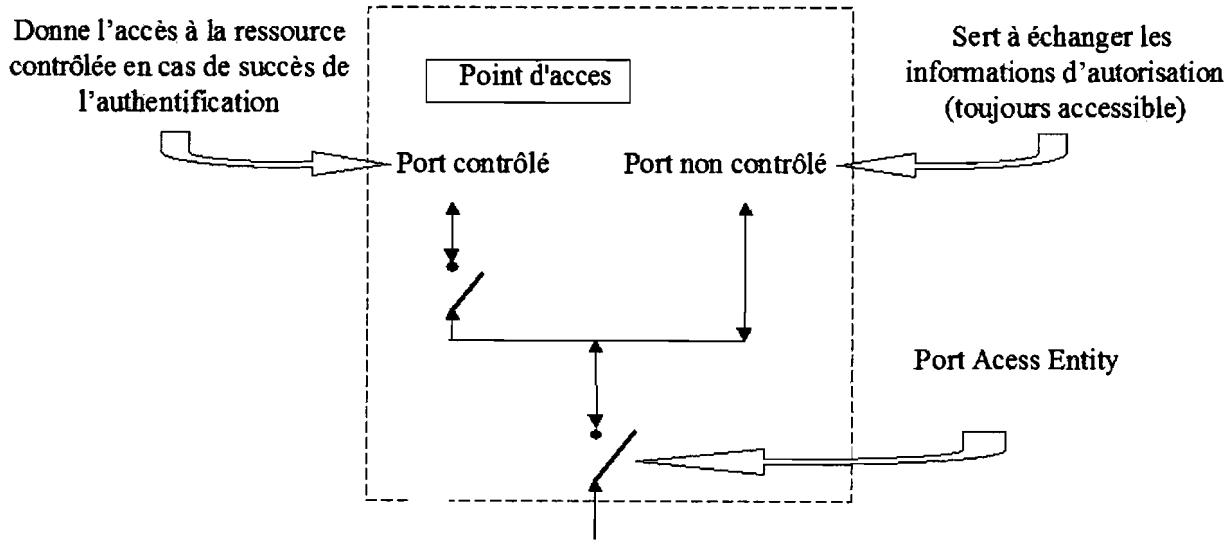


Figure12 : l'état des différents ports

La communication entre le serveur et le supplicant se fait grâce au protocole EAP.
Ce protocole supporte plusieurs méthodes d'authentification, dont les plus utilisés sont :

- **EAP-MD5** (**M**essage **D**igest **5**) : méthode définie dans la RFC 3748, elle repose sur le protocole CHAP (**C**hallenge **H**andshake **A**uthentification **P**rotocol) avec le hash MD5. Le principe du CHAP est le suivant : le serveur commence par envoyer un défi au client ainsi qu'un compteur qu'il incrémente à chaque fois qu'il lance un défi. Le client doit alors passer le compteur, son mot de passe, et le défi au travers d'un algorithme de

hachage (MD5 habituellement). Le résultat appelé hash est une séquence de bits pseudo-aléatoires. Le hash est envoyé au serveur qui peut effectuer un calcul et vérifier si le résultat concorde avec celui du client. Cet algorithme évite donc que le mot de passe soit transféré et évite qu'un pirate ne répète une authentification réussie (le défi change). Mais il ne permet pas au client de s'assurer l'identité du serveur.

- **EAP-TLS** : il est défini dans la RFC 2716 et se repose sur l'identification par certificat. Son utilisation nécessite la création et l'installation d'un certificat électronique (avec sa clé correspondante) sur le serveur d'authentification ainsi que des certificats distincts (avec leurs clés privés) sur les postes clients. Lors donc du dialogue EAP, le client et le serveur s'échangent et vérifient leurs certificats en suivant le protocole TLS (Transport Layer Security). L'authentification est très sûre et mutuelle avec EAP-TLS. Cependant son déploiement est assez lourd à gérer.
- **EAP-PEAP** : il a été développé par Cisco et Microsoft et est généralement appelé PEAP (Protected EAP). Son principe différant de quelque peu d'EAPTLS, est le suivant: le serveur demande soit l'identité du client, soit un certificat venant de celui-ci. Le client n'est pas obligé de révéler sa véritable identité ni même de fournir un certificat. Seul le serveur doit prouver son identité en fournissant un certificat au client. Plutôt de s'arrêter à la négociation TLS, PEAP va jusqu'à établir complètement le tunnel TLS. Au sein de celui-ci, une négociation complète a lieu. Il faut noter ici que le client fournit son identité et sa preuve d'identité a l'aide d'une des méthodes d'EAP au serveur. Une fois que l'identification EAP « interne » se termine avec un paquet de succès ou d'échec, le tunnel TLS est fermé et le serveur renvoie un paquet de succès ou d'échec au client en claire cette fois-ci. Sans cela le contrôleur d'accès ne saura pas qu'il faut laisser le client ou non car toute l'identification interne était cryptée. Le PEAP n'imposant pas de déployer un certificat sur le poste de chaque client, sa mise en œuvre peut être assez simple tout en offrant un niveau de sécurité très important. Cependant l'utilisation d'une méthode interne reposant sur un mot de passe peut le rendre vulnérable à des attaques de dictionnaires.
- **EAP-TTLS** : il est aussi appelé TTLS et présente beaucoup de points communs avec PEAP. Les différences notées sont les suivantes :

- Il a été crée par la société **F**unk **S**oftware
- Il n'est pas intégré dans Windows
- Il autorise tout type d'identification interne et pas seulement EAP (PAP par exemple).

- Dans les paquets TTLS, il est possible de rajouter des paires d'attribut/valeur (AVP). La possibilité que le serveur et le client puissent utiliser des AVP s'avère intéressante car les AVP peuvent transporter des informations supplémentaires (paramètres de configuration) en plus de celles liées à l'authentification.

II-3- Le portail captif

II-3-1- Définition

Le portail captif est une méthode d'authentification forçant un client http à afficher une page web spéciale. Cette page indique les informations que l'utilisateur doit entrer afin de se connecter à Internet. Les informations demandées sont généralement le nom du compte d'utilisateur et le mot de passe.

II-3-2- Principe de fonctionnement

Le fonctionnement du portail captif peut s'illustre à travers le schéma suivant:

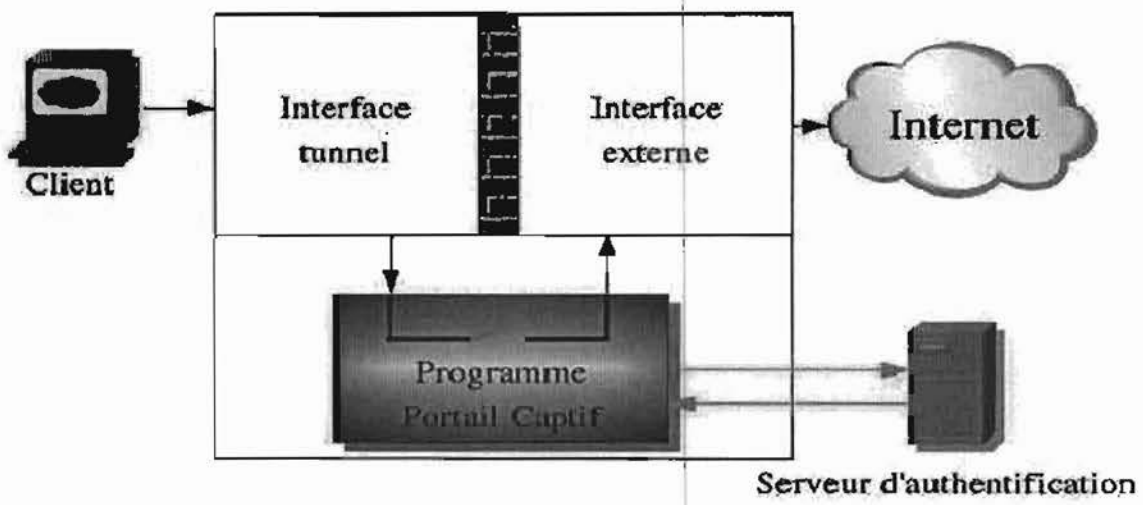


Figure13 : schéma illustratif du fonctionnement d'un portail captif

Tout d'abord, l'utilisateur se connecte à un réseau local. Pour toute tentative de connexion à internet, l'utilisateur est renvoyé vers une page web spéciale appelée portail captif. Celle-ci indique les informations nécessaires que l'utilisateur doit entrer afin d'obtenir la connexion à Internet. Ces informations seront transmises vers un serveur d'authentification (exemple RADIUS) par le portail captif. Si les informations sont exactes du point de vue du serveur, l'utilisateur se voit afficher la page web demandée. Sinon une erreur est retournée et une

nouvelle authentification est demandée. L'ensemble des informations échangées entre le portail captif et le serveur est sécurisé dans un tunnel HTTPS.

Nous pouvons retenir qu'un tunnel est une sorte de canal virtuel où les données échangées à travers un protocole réseau peuvent être encapsulées dans un autre qui est situé sur la même couche ou sur une couche supérieure du modèle en couche. Dans le cadre d'un portail captif plusieurs services et protocoles sont mis en œuvre parmi lesquels nous pouvons citer :

- le protocole https pour permettre une communication sécurisée entre le client et le serveur ;
- le protocole IP pour l'adressage des machines et l'acheminement des données ;
- le protocole SSL (Secure Sockets Layer) devenu TLS (Transport Layer Secure en 2001) pour la transmission des paramètres de connexion ;
- le protocole EAP pour l'établissement d'accès à un réseau pour l'utilisateur ;
- le protocole LDAP pour l'interrogation et la modification des services de l'annuaire au niveau du serveur d'authentification.

Il existe plusieurs types de portail captif.

II-3-3- Les différents portails captifs

On distingue plusieurs types de portail captifs, parmi les quels on a :

- **Le Nocat**

Le Nocat est un portail web captif destiné à la sécurisation du partage d'une connexion sans fil en redirigeant l'utilisateur vers une page web d'authentification lors d'une tentative de connexion à internet. Le Nocat intègre des modules nécessaires à sa bonne mise en œuvre à savoir :

- le NocatSplah qui est le portail captif ;
- le NocatAuth qui est l'application d'authentification ;
- le Splah Server qui est un service permettant de générer des formulaires appelés «Splash Pages » lors de la première connexion au réseau d'un utilisateur.

Nous pouvons retenir que ces modules peuvent être installés sur une même machine ou sur des machines différentes.

- **Le Wifidog**

Tout comme les autres, il permet l'authentification de l'utilisateur avant toute connexion à Internet. Il est constitué de deux parties : la passerelle et le serveur d'authentification.

- La passerelle est la partie installée sur le point d'accès. Elle est appelée **Wifidog Gateway** et chargée de rediriger l'utilisateur vers une page web d'authentification.

- Le serveur d'authentification est la partie installée sur un serveur externe joignable des passerelles. Nommé **Wiffidog Authentification Server**, il est chargé de valider ou pas les authentifications et de faire suivre la demande de l'utilisateur.

➢ **Le Talweg**

Le principe de base de talweg est identique à celui des autres portails captifs cités ci-dessus. Cependant une différence existe. Talweg dépose un cookie de session (temps de session) sur le navigateur. La navigation reste possible tant que ce cookie est présent sur le navigateur.

➢ **Le chillispot**

Tout comme Nocat, chillispot est un portail captif open source. Il propose deux modes d'authentification, à savoir, le mode *UAM* et le mode *WPA 802.1x*

- Le mode UAM (Universal Access Method) fonctionne de la manière suivante :une fois connecté au point d'accès, une adresse IP est automatiquement attribuée à l'utilisateur par Chillispot qui joue le rôle de serveur DHCP. Ensuite toute demande de connexion à Internet est interceptée et envoyée au serveur Web qui lui affiche une page d'authentification (login/password). Les informations d'authentification sont envoyées à un serveur d'authentification (RADIUS par exemple) pour vérification. Une fois la vérification terminée, le serveur confirme l'authentification et dans ce cas l'utilisateur reçoit sa page web demandée. Ou il la rejette et dans ce cas une nouvelle authentification est demandée à l'utilisateur. Nous pouvons retenir que la vérification, consiste à s'assurer que l'utilisateur est connu et autorisé à accéder à Internet.
- Le mode WPA 802.1x fonctionne comme suit : l'authentification s'effectue au niveau du point d'accès. Dès que l'utilisateur tente de se connecter au réseau, une page d'authentification lui est affichée. Ensuite les données d'authentification sont envoyées à chillispot qui joue le rôle de proxy d'authentification. Chillispot à son tour achemine ces informations au niveau du serveur pour authentification. Dans tous les deux cas, chillispot ne laisse passer que les sites et les protocoles autorisés par l'administrateur réseau.

III- Les services nécessaires pour une authentification ou contrôle d'accès

III-1- Un serveur d'authentification

Un serveur d'authentification est l'élément chargé de gérer le processus de communication entre lui et le client. Il permet au client de s'authentifier et d'accéder ou non aux services réseaux demandés. On distingue plusieurs serveurs d'authentification dont les plus connus sont RADIUS, DIAMETER.

III-1-1- RADIUS

III-1-1-1- Définition

Le Remote Authentication Dial-In User Service (RADIUS) est un protocole développé par Livingston Enterprise devenu une norme de fait décrite par les RFC 2865 et 2866. Il s'appuit sur l'architecture client/serveur. Son rôle est de fournir des services d'authentification, d'autorisation et de gestion des comptes pour l'accès réseau à distance.

III-1-1-2- Principe de fonctionnement

Le principe de fonctionnement du serveur radius est basé sur un scénario similaire à celui-ci :

- Un utilisateur envoie une requête au NAS (point d'accès) pour demander une connexion
- NAS achemine la demande au serveur RADIUS
- Le serveur RADIUS consulte la base de données d'authentification afin de connaître le type de scénario d'authentification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'authentification est demandée à l'utilisateur.

Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :

- **ACCEPT** : l'authentification a réussi ;
- **REJECT** : l'authentification a échoué ;
- **CHALLENGE** : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « **challenge** ») ;
- Il existe une autre réponse appelée **CHANGE PASSWORD** où le serveur

RADIUS demande à l'utilisateur un nouveau mot de passe. Change password est un attribut VSA (**V**endor-**S**pecific **A**ttributes), c'est-à-dire qu'il est spécifique à un fournisseur, et dans ce cas, c'est un attribut de Microsoft, celui de MS-Chapv2 pour être plus précis. Il n'appartient pas aux attributs radius standard définis dans la RFC 2865.

Suite à cette phase dite d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

Le schéma suivant récapitule les éléments entrant dans le fonctionnement du serveur RDIUS :

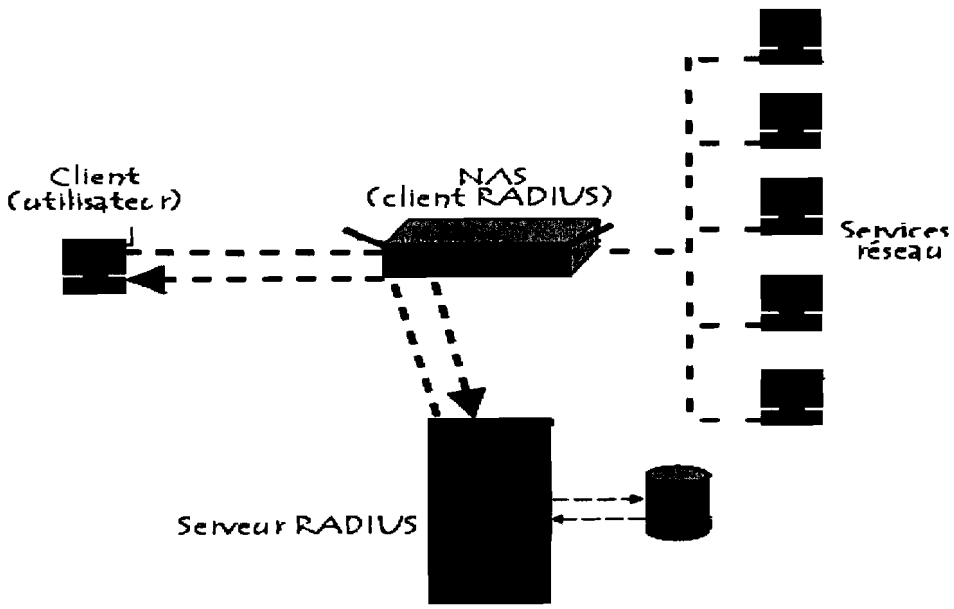


Figure14: Schéma illustratif du fonctionnement de RADIUS

Les transactions entre le client et le serveur RADIUS sont authentifiées au moyen d'un secret qui n'est "jamais" envoyé sur le réseau. Il est en fait chiffré avec l'algorithme MD5, puis un OU exclusif (XOR) avec le mot de passe de l'utilisateur est appliqué (transaction dans le sens client-->serveur). Dans l'autre sens, le serveur chiffre le secret en le concaténant avec un ensemble de paramètres, le tout étant "haché" avec MD5.

Notons aussi que le serveur Radius peut faire office de proxy vers d'autres serveurs

III-1-2- DIAMETER

Le serveur Diameter est présenté comme le successeur du serveur RADIUS, il a été crée pour pallier à un certain nombre de problèmes rencontrés au niveau de RADIUS. En effet il permet de remédier à un certains nombre de problèmes tels que :

- l'utilisation du protocole UDP, qui est un protocole de transport n'assurant pas de fiabilité ;
- le manque de mécanisme de redondance standard ;
- la limite de taille pour certains paramètres, par exemple la longueur d'un attribut n'est codée que sur un octet, ce qui limite les attributs à 256 caractères.

Il a été défini par la RFC 3588 mais est encore à sa phase embryonnaire. Son fonctionnement est similaire à celui de Radius.

IV-2- Système de stockage des données d'authentification

Le système de stockage des données d'authentification peut être une base de données ou un annuaire. Il permettra de stocker par exemple les coordonnées des différents utilisateurs souhaitant se connecter au réseau ainsi que le matériel utilisé au sein du réseau. Aussi il permettra de garder une trace des différents utilisateurs qui se sont connectés au réseau. Quelques éléments ont retenu notre attention, ce sont :

III-2- MySQL

III-2-1- Définition

Une base de données est un espace de stockage d'informations à consulter. Cette base de données doit être créée et gérée. MySQL est l'un des systèmes de gestion de bases de données relationnelles permettant cela. En effet il permet d'héberger des bases de données et l'obtention de l'information par une requête formulée dans un langage quasi naturel qu'est SQL (Structured Query Language se traduit en français par langage de requêtes structurées).

III-2-2- Fonctionnement

MySQL est un gestionnaire de base de données. Il manipule toutes les instructions adressées à la base de données. Recevant les requêtes, il les interprète et les exécute puis renvoie un message contenant le résultat de cette exécution. L'une des spécificités de Mysql est de faire fonctionner une même base de données avec plusieurs moteurs. En effet chaque table peut utiliser un moteur différent au sein d'une base. Ce qui permet d'optimiser l'utilisation de chaque table. Le moteur est le composant central d'un système de gestion de base de données. Il permet la lecture, le contrôle, et l'enregistrement puis le tri des informations dans une base de données.

III-3- Open LDAP

III-3-1- Définition

LDAP connu sous l'acronyme Light Weight Directory Access Protocol est un protocole permettant d'interroger des bases d'informations appelées annuaires. C'est une version améliorée du protocole DAP pour fonctionner avec le modèle TCP/IP qui fut utilisé dans les services d'annuaire X500 du modèle OSI. Dans un premier temps LDAP s'est contenté d'être l'interface pour TCP/IP à des annuaires X500.

X500 désignant l'ensemble des normes informatiques pour les services d'annuaires définis par l'UIT. Mais seule la partie X509 concernant l'authentification est utilisée actuellement. Depuis 1995, LDAP peut gérer les bases de façon autonome (standalone LDAP).Étant un protocole, son rôle est de présenter des informations.

Un serveur LDAP agit en tant qu'intermédiaire entre une source de données et un client. Ainsi, il définit quelques conventions, notamment l'organisation des données qu'il présente sous forme hiérarchique, mais aussi un format d'échange standard.

III-3-2- La notion d'annuaire

Un annuaire est un système de stockage de données. Il est dérivé des bases de données hiérarchisées et permet de conserver des données pérennes, c'est-à-dire des données n'étant que peu mises à jour (historiquement sur une base annuelle d'où le nom annuaire). L'ensemble des fonctionnalités et caractéristiques est regroupé en plusieurs modèles :

- **Le protocole LDAP**, il a pour rôle de présenter des données. Il définit comment se passe la communication entre client/serveur. Il fournit à l'utilisateur des commandes pour se connecter ou se déconnecter, pour rechercher, comparer, créer, modifier ou effacer des entrées. Il est également utilisé dans la communication serveur-serveur, pour permettre à plusieurs serveurs d'échanger leur contenu et de les synchroniser, ou de créer entre eux des liens permettant ainsi de relier des annuaires les uns aux autres.
- **Le modèle de nommage**, il définit la manière dont les éléments (informations) sont stockés et organisés dans l'annuaire. Chaque élément de l'annuaire est appelé « entrée ». Une entrée est constituée d'un ensemble d'attributs. Chaque attribut possède un nom, un type et une ou plusieurs valeurs. Cela constitue une différence entre LDAP et les bases de données classiques.
- **Le modèle fonctionnel**, Il définit les différents services fournis par l'annuaire. Plusieurs types d'opérations peuvent être effectués tels que:

- Rechercher une entrée suivant certains critères ;
- S'authentifier ;
- Ajouter une entrée ;
- Modifier une entrée ;
- Renommer une entrée ;
- Comparer des entrées ;
- Supprimer un objet.

La recherche nécessite des outils particuliers pour faciliter l'accès à l'annuaire.

- **Le modèle informationnel**, Il définit les types de données stockées parmi les quels nous distinguons les attributs, les classes d'objets et les schémas.
- **Le modèle de sécurité,** Il définit les droits d'accès aux différentes ressources. LDAP fournit un grand nombre de mécanismes de sécurité. Il s'agit en fait de mécanismes et protocoles pouvant être mis en œuvre pour assurer la protection des accès à l'annuaire ainsi que la protection des flux de données. Les principaux sont :

- L'authentification simple ou « binding » qui fournit des fonctionnalités d'authentification minimales ;
- Le mécanisme SASL (**S**imple **A**uthentification and **S**ecurity **L**ayer) qui est une structure d'authentification pour les protocoles ;
- TLS (Transfert Layer Security) qui est utilisé avec LDAP afin de garantir l'intégrité et la confidentialité des échanges dans une communication entre applications LDAP. Il permet ainsi de garantir la protection des données en transit sur le réseau lors des opérations LDAP ;
- Le contrôle d'accès à la base qui est une règle d'accès (ACL) aux données utilisées afin d'assurer les aspects de sécurité tels que la confidentialité et l'intégrité, lorsque des entrées de l'annuaire sont accédées et manipulées.

- **Le modèle de duplication**

La réplication : certains serveurs LDAP, dont OpenLDAP, permettent de manière native, de mettre en place un annuaire répliqué. Un annuaire dit "maître" envoie alors, par le biais du format LDIF, toutes les modifications effectuées sur un annuaire "esclave". L'avantage d'une telle opération est d'une part permettre une meilleure montée en charge pour de gros annuaires car il est possible de rediriger le client vers l'un ou l'autre des annuaires répliqués, d'autre part cela permet de disposer d'une copie conforme du premier annuaire, utile en cas de crash (attention, toute opération est reportée de l'annuaire maître vers l'esclave, donc ceci est non valable en cas de mauvaise manipulation).

La distribution (les referrals): la distribution est un mécanisme qui va permettre de faire pointer un lien vers un autre annuaire pour une branche particulière. Ceci va permettre de déléguer la gestion de cette branche, un peu au sens DNS (**D**omain **N**ame **S**erver) lorsqu'on délègue la gestion d'un domaine.

Chapitre IV:Comparaison et choix des différentes solutions à mettre en place

Dans cette partie nous allons passer en revue les différentes solutions proposées pour le réseau câblé ainsi que pour le Wi-Fi en faisant des comparaisons afin de choisir un système qui répondra mieux aux exigences suivantes:

- Le besoin actuel ;
- Les compétences requises ;
- La facilité de mise en œuvre ;
- Le coût que cela peut engendrer.

I-Au niveau du réseau câblé

I-1- Comparaison des différentes solutions

Segmentation physique		
Méthode	**Avantages**	**Limites**
Pont	• Intégrité des données transportées • Stockage temporaire des trames	• Temps de latence élevé • Ne peu pas connecter plusieurs machines à la fois
Routeur	• Connectivité entre les réseaux et les sous réseaux • Intégrité des données transportées	• Temps de latence élevé • Pas de broadcast

Commutateur	• Réduction des pénuries de bande passante et les goulots d'étranglement sur le réseau, • Un commutateur divise un réseau LAN en micro segments afin de réduire la taille des domaines de collision. • Débit important	• Tous les hôtes connectés au commutateur restent dans le même domaine de broadcast

Tableau4 : Comparaison de la segmentation physique

Types de VLANs	Description
VLAN niveau 1 **Basé sur le port**	• Configuration la plus courante • Ports affectés individuellement à un ou plusieurs VLANs • Facile à mettre en place • Couplé à DHCP, les VLAN par ports offrent une bonne flexibilité • Les interfaces de gestion des Switchs permettent une configuration facile
VLAN niveau 2 **Basé sur l'adresse MAC**	• Rarement utilisé • L'adresse MAC détermine l'appartenance à un VLAN • Les Switchs s'échangent leurs tables d'adresses MAC ce qui peut ralentir les performances I Difficile à administrer, à dépanner et à gérer.
VLAN niveau 3 **Basé sur le protocole**	• Pas utilisé aujourd'hui à cause de la présence de DHCP • L'adresse IP (sous-réseau) détermine l'appartenance à un VLAN

Tableau6 : de comparaison des VLANs

I-2- Choix d'une solution

Le réseau câblé de l'HDJ est un réseau commuté Ethernet 10-100 Mb/s. La solution de **segmentation LAN à base de commutateurs,** en implémentant le **VLAN de niveau 1** (segmentation logique du réseau) améliora considérablement la sécurité de notre réseau. Cette solution est attrayante du point de vue gestion de parc informatique et de bande passante. Elle pourra répondre à notre besoin d'optimisation du réseau de l'HDJ dans l'utilisation de ses services (voix/données/images).

II-Au niveau du réseau Wi-Fi

II-1- Comparaison des différentes solutions proposées

Méthodes d'accès et protocole de sécurisation des données		
Méthode	**Avantages**	**Limites**
WEP	Cryptage des données au sein du Réseau	• clé statique • le nombre de bits utilisés pour le cryptage est non élevé, donc facilement Crackable
WPA	• Utilisation de passphrase • Clé dynamique	Très sensible à l'attaque « déni de service »
WPA-802.1x	• Les données sont cryptées à l'aide d'une clé générée automatiquement ; • Utilisation d'un serveur RADIUS.	
WPA2	Sécurité et mobilité plus efficaces grâce a l'authentification du client où qu'il soit.	• Temps de charge élevé à cause de la possibilité de se connecter a plusieurs points d'accès • Supporté par peu de matériels

Tableau7 : Comparaison des méthodes d'accès et protocole de sécurisation des données

Méthodes d'authentification		
Méthode	**Avantages**	**Limites**
Filtrage d'adresses MAC	Limite l'accès réseau à un certain nombre d'individus	Mise en place très fastidieuse pour un vaste réseau
Standard 802.1x		
EAP-MD5	Défi dynamique	Impossibilité de s'assurer de l'identité du serveur
EAP-PEAP	Mise en œuvre simple tout en offrant un minimum de sécurité	Vulnérable aux attaques de dictionnaires
EAP-TLS	Authentification sûre et mutuelle	Mise en œuvre assez lourde
EAP-TTLS	Possibilité d'ajouter des AVP dans les paquets TTLS	Vulnérable aux attaques de dictionnaires

Tableau8: Comparaison des méthodes d'authentification

Portails captif		
Type	**avantages**	**limites**
Nocat	• Simplicité d'installation • Possibilité de régler le débit • Supporte beaucoup de protocoles Réseau	• Pas de sécurité d'authentification ni de communication • Ne permet pas la gestion des Utilisateurs
Wifidog	• Adapté à une communauté pour un contrôle poussé • Sécurité d'authentification • Supporte beaucoup de protocoles réseau	• Pas de sécurité de communication • Consommation réseau très élevée
Talweg	• Sécurités d'authentification et communication • Bonne gestion des utilisateurs	• Consommation réseau très élevée • Supporte peu de protocoles Réseau
Chillispot	• Sécurité d'authentification • Adapté aux grands réseaux • Bonne gestion des utilisateurs	• Perte au niveau de la bande passante et consommation des ressources systèmes ; • Pas de sécurité de communication.

Tableau9 : Comparaison des portails captifs

Serveurs d'authentifications		
Type	**Avantages**	**Limites**
RADIUS	Toute une communauté se penche sur les problèmes rencontrés	Utilisation du protocole UDP qui n'est pas très fiable
Diameter	Correction de certaines limites de radius	Absence de documentation

Tableau10: Comparaison des serveurs

Système de stockage de données d'authentification		
	Avantage	**Limites**
LDAP	Très performant en lecture	Moins performant en écriture
MYSQL	Très performant en écriture	Moins performant en lecture

Tableau11: comparaison du système de stockage

II-2- Choix des différentes solutions à mettre en place

Après la comparaison des différentes solutions ci-dessus effectuées, nos choix se sont finalement portés sur les solutions suivantes :

Pour l'accès au réseau wifi et la sécurisation des communications sans fils nous avons choisi le **WPA-802.1x**. Comme méthode d'authentification nous avons choisi le portail captif et particulièrement sur le **chillispot** car il oblige toute personne souhaitant accéder au réseau wifi de s'authentifier par conséquent seule les personnes autorisées par l'administrateur à accéder au réseau pourront le faire. Cette méthode d'authentification est beaucoup sécurisée. Le serveur d'authentification Radius avec sa version open source **freeradius** qui est le plus utilisé est celui que nous avons choisi. De plus, associé à l'annuaire **OpenLDAP** et à la base de données **MySQL** qui vont permettent respectivement, de stocker les informations des utilisateurs, et journaliser leurs accès au réseau wifi. Toutes ces configurations ont été effectuées sur un système d'exploitation **Debian lenny (5.0)**. Notre choix s'est porté sur ce système non seulement à cause de sa stabilité mais aussi du fait qu'il est plus sécurisé et dédié à l'administration réseau.

3ème partie: Mise en œuvre des solutions retenues

Chapitre I: Au niveau du réseau câblé

I-Planification du déploiement des VLANs

Une bonne mise en œuvre des solutions nécessite une bonne planification de déploiement.

Dans cette phase, nous allons lister le matériel et les différents protocoles nécessaires à la mise en place de la solution.

Il est aussi important de noter les différentes contraintes qui peuvent être rencontrées :

- garder les adresses IP serveurs et imprimantes identiques. Pour des raisons d'administration et d'accès externes à certains serveurs ;
- le service rendu à l'utilisateur doit être interrompu le moins longtemps possible pendant les heures de travail ;
- la bascule dans les réseaux virtuels doit se faire avec moins d'effort possible pour l'équipe réseau et assistance utilisateurs confondues.

Matériels	Quantité
Switch Cisco 2960	1
Modem Routeur	1
Serveur Radius	1

Tableau12 : Matériels utilisés

Dans cette nouvelle architecture, nous avons segmenté le réseau par la mise en œuvre des VLANs de niveau 1, c'est-à-dire que chaque VLAN se verra attribuer un ou plusieurs ports physique du commutateur. Aussi nous allons procéder au déplacement du modem-routeur qui est en même temps le point d'accès du Wi-Fi. Et enfin le poste du Chef de Service ne sera plus directement connecté au modem-routeur ce qui permettra d'avoir un bon débit de connexion à l'internet. Dans cette nouvelle infrastructure, nous disposons d'un commutateur sur lequel sont repartis les différents vlan. Le switch hopijo_sw accueil la liaison internet.

L'agrégation de lien implémenté permet de gérer les différents débits des différents VLANs ; des ACL sont prévus pour gérer la sécurité entre vlan et dans le réseau local.

Nous avons un sous-réseau par VLAN.

La passerelle par défaut, est l'équipement qui interconnecte les différents VLANs, donc ici chaque station des différents VLANs aura pour passerelle, la passerelle qui sera configuré sur le switch hopijo_sw.

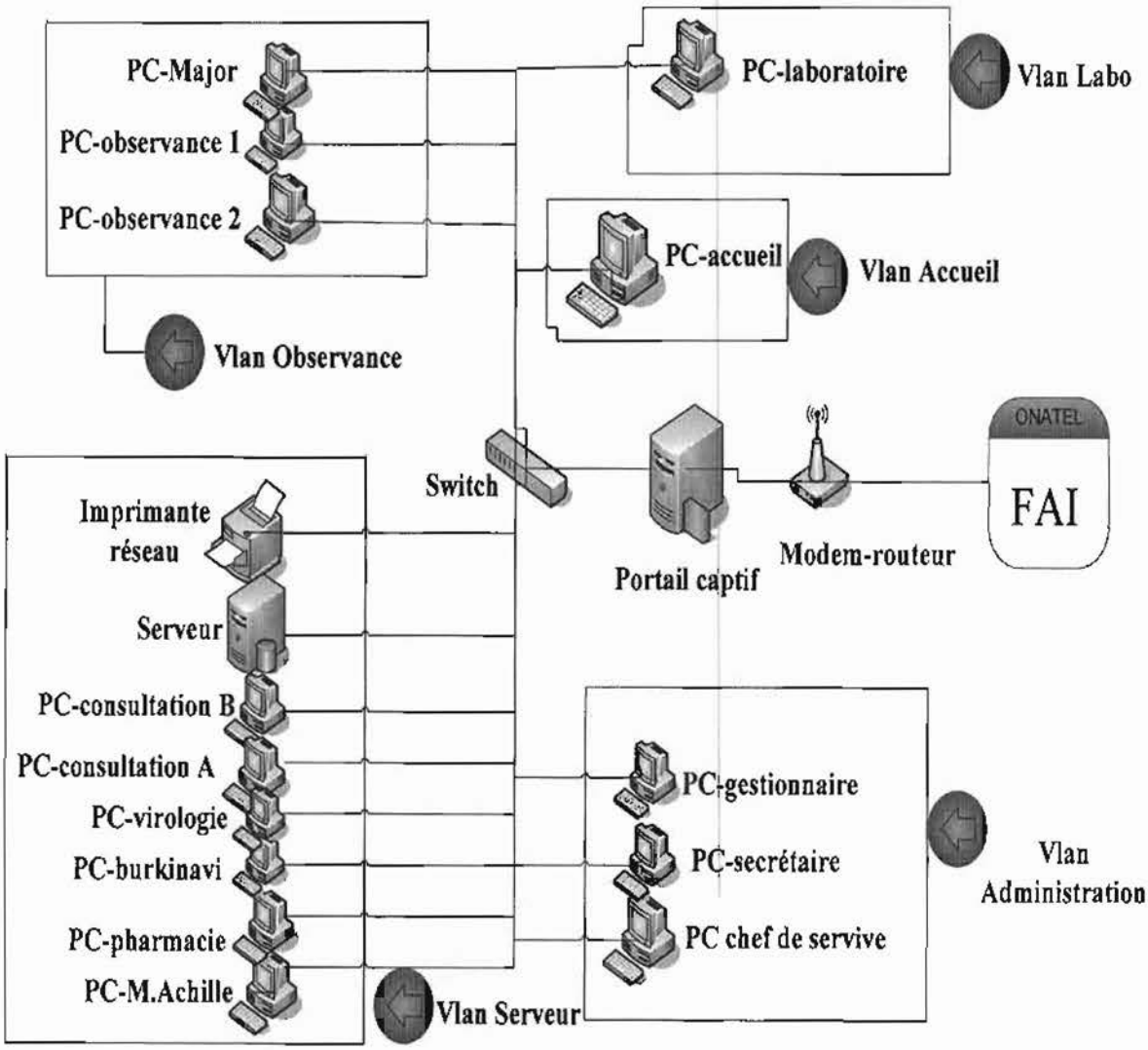


Figure15 : Architecture déploiement

II-Les différents VLANs à implémenter

Après analyse, nous avons défini cinq (05) VLANs repartis comme suit :

- **VLAN Serveur : Vlan10**

Ce Vlan contient l'imprimante réseau et les serveurs de production et de base de données. Il permettra de séparer les flux d'impressions du reste du trafic,

- **VLAN Administration: Vlan 20**

Dans ce Vlan, nous retrouverons toutes les machines de l'Administration, à savoir celle du Chef de Service, de la Secrétaire et de la Gestionnaire,

- **VLAN Observance: Vlan 30**

Ce Vlan est destiné aux médecins de l'HDJ qui échangent beaucoup d'information entre eux,

- **VLAN Labo: Vlan 40**

Ce Vlan est destiné aux chercheurs de la section Laboratoire,

- **VLAN Accueil: Vlan 50**

Ce Vlan est destiné aux utilisateurs n'ayant pas de carte Wi-Fi souhaitant se connecter dans la salle réunion.

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

II-1- Attribution des ports du Switch aux différents VLANs

Après identification des utilisateurs destinés à échanger des données entre eux, nous avons procéder à l'attribution des ports du switch aux différents du VLANs (Tableau13). Ainsi chaque ordinateur connecté à un port du switch sera assigné à son VLAN correspondant.

Matériels	Port Attribués	N° VLAN
Hopijo_sw	2, 3, 4, 5, 6, 7, 8,9	VLAN 10
	10, 11,12	VLAN 20
	13, 14,15	VLAN 30
	16,17	VLAN 40
	18, 19, 20	VLAN 50

Tableau13 : Les différents ports du Switch associés aux VLANs

II-2- L'adressage

Suite à l'attribution des ports du switch aux VLANs, nous avons données des adresses de sous-réseaux aux différents VLANs comme indiqué dans le tableau ci-dessous.

VLAN	N° VLAN	Sous-réseaux	Passerelles par défaut
Serveur	10	192.168.2.0	192.168.1.1
Administration	20	192.168.3.0	192.168.1.1
Observance	30	192.168.4.0	192.168.1.1
Labo	40	192.168.5.0	192.168.1.1
Accueil	50	192.168.6.0	192.168.1.1

Tableau14 : Adresses des sous-réseaux des différents Vlans

III-Eléments fonctionnels du VLAN

III-1- Les normes

Les VLANs seront mis en œuvre via ces deux normes :

- **802.1q** (Etiquetage de trames)
- **ISL** (Encapsulation de trames)

La norme ISL est une Technologie propriétaire CISCO. Grâce à cette norme nous pourrions :

- Créer un lien «Trunk» qui véhicule le trafic entre les différents VLANs
- Associer un port à un ou plusieurs VLANs
- Choisir les VLANs à véhiculer avec le «pruning»

III-2- Le protocole 802.3ad

L'agrégation de liens (également appelé *link aggregation* ou *port trunking*) est définie dans la norme IEEE 802.3ad ; elle permet d'augmenter la bande passante disponible entre deux stations Ethernet en autorisant l'utilisation de plusieurs liens physiques comme un lien logique unique. Ces liens peuvent exister entre 2 commutateurs ou entre un commutateur et une station. Avant cette norme, il était impossible d'avoir plusieurs liens Ethernet sur une même station,

sauf si ces liens étaient reliés à des réseaux ou des VLANs différents. L'agrégation de liens apporte les avantages suivants :

- La bande passante peut être augmentée à volonté, par pallier. Par exemple, des liens Fast Ethernet additionnels peuvent augmenter une bande passante entre deux stations sans obliger le réseau à passer à la technologie Gigabit pour évoluer ;
- La fonction de « load balancing » (équilibrage de charge) peut permettre de distribuer le trafic entre les différents liens ou au contraire de dédier une partie de ces liens (et donc de la bande passante) à un trafic particulier ;
- La redondance est assurée automatiquement : le trafic sur une liaison coupée est redirigé automatiquement sur un autre lien.

IV-Présentation du matériel d'interconnexion

L'implémentation de notre solution doit se faire à travers des équipements de constructeur. Donc ce choix doit tenir compte de certaines compétences techniques d'une part et d'autre part de l'évolution du réseau car chaque constructeur dispose de sa technologie qui diffère les uns des autres. Mais ils ont des commandes standard en commun.

L'interconnexion du réseau de l'HDJ est basée sur le commutateur Cisco catalyst série 2960 habilité à faire du VLANs, d'où le choix de ce constructeur. Le Switch catalyst utilisées dans notre cas est le **2960T-24**.

V-Installation de switch

Le déploiement de switchs dans un réseau se fait en deux étapes : la connexion physique et la configuration.

V-1- Connexion physique

Dans notre cas, le switch a été placé dans un coffret fermé à clé et branché à un onduleur.

V-2- Configuration du switch

La configuration d'un switch se fait entre autre par CLI (Command Line Interface).

L'accès au CLI se fait par console. Le port console permet de se connecter au CLI du switch même si celui-ci n'est pas déjà en réseau. Tout switch Cisco a un port console qui est physiquement un port RJ-45.

Un câble console relie un PC (via le port série ou USB) au switch (via le port console).

Une fois que le PC est physiquement connecté au port console du switch, il faut installer et configurer un émulateur de terminal sur celui-ci. Les émulateurs de terminaux intègrent les supports pour Telnet et SSH qui permettent de configurer un switch via le réseau.

V-2-1- Configuration de mot de passe et de nom du switch

Pour configurer le mot de passe et attribuer un nom au switch, on procède comme suit :

Switch> enable

Switch#configure terminal

Switch(config)#enable secret passwd

Switch(config)#hostname hopijo_sw

hopijo_sw(config)#line console 0

hopijo _sw(config-line)#password passwd

hopijo _sw(config-line)#login

hopijo _sw(config-line)#exit

hopijo _sw#write

V-2-2- Configuration de l'adresse IP du switch

La configuration de l'adresse IP du switch se fait comme suit :

hopijo _sw#configure terminal

hopijo _sw(config)#interface vlan 1

hopijo _sw(config-if)#ip address 192.168.0.2 255.255.255.0

hopijo _sw(config-if)#no shutdown

hopijo _sw(config-if)#exit

hopijo _sw(config)#ip default-gateway 192.168.0.1

V-2-3- Configuration des VLANs statiques

V-2-3-1- Création de VLAN

On créé un vlan en saisissant les commandes suivantes :

hopijo _sw #vlan database

hopijo _sw (vlan)#vlan no_vlan name nom_vlan ou

hopijo _sw (vlan)#exit

hopijo _sw #configure terminal
hopijo _sw (config)#vlan no_vlan
hopijo _sw (config-vlan)# name nom_vlan
hopijo _sw (config-vlan)#end

V-2-3-2- Association d'un port au VLAN créé

Pour associer un port quelconque à un vlan donné, on saisie les commandes suivantes :

hopijo _sw #configure terminal

hopijo _sw (config)#interface fastethernet0/5

hopijo _sw (config-if)#switchport mode access

hopijo _sw (config-if)#switchport access vlan no_vlan

Exemple : Configuration des VLANs statiques

Créer un VLAN

La création d'un vlan peux se faire par l'une des deux méthodes suivantes :

hopijo _sw # vlan database

hopijo _sw (vlan)# vlan 20 name Administration

hopijo _sw (vlan)# exit

oubien

hopijo _sw #configure terminal
hopijo _sw (config)#vlan 20
hopijo _sw (config-vlan)#name Administration
hopijo _sw (config-vlan)#end

Ajouter un port au VLAN 2

Pour ajouter un port dans le vlan2, on saisie les commandes suivantes :

hopijo _sw (config)# interface fastethernet0/10

hopijo _sw (config-if)# switchport mode access

hopijo _sw (config-if)# switchport access vlan 20

hopijo _sw (config-if)# end

Chapitre II : La configuration pour le réseau Wi-Fi

I- WPA-802.1x

La configuration du Wpa-802.1x se fait au niveau du point d'accès. L'interface du point d'accès est accessible via une page web avec l'adresse**192.168.0.1** puis on saisi le compte et le mot de passe de l'administrateur. Pour configurer le wpa-802.1x aller dans l'onglet **Paramètres sans fil** puis dans **options de sécurité** et cocher **Wpa-802.1X**

II-OpenLDAP

OpenLDAP sera installé sur la machine tournante sous Debian lenny. Le fichier principal de configuration de LDAP se nomme **slapd.conf**. Il se trouve dans **/etc/ldap/.** A ce fichier nous pouvons inclure un autre qui déterminera les droits de l'administrateur et des utilisateurs de l'annuaire. On pourra lui attribuer un nom judicieusement choisi, par exemple, **slapd.access.conf.** La page d'accueil de l'outil d'administration de OpenLDAP à savoir **phpldapadmin** se trouve en annexe1.

III-Freeradius et MySQL

Freeradius sera aussi installé sur Debian Lenny. Nous avons vu différentes manières de l'installer. Ce sont:

- Installation via l'archive freeradius-version-x.tar.gz disponible sur le site de FreeRADIUS puis méthode ;
- Installation par modification et compilation des paquets debian (.deb) ;
- Installation par un apt-get install freeradius directement

Il faut noter ici que le choix d'une des méthodes d'installation dépend du besoin ou non de certains modules surtout le module EAP qui ne se trouve pas dans le paquet fourni avec la Debian. Ainsi les deux premières méthodes permettent de l'avoir. Dans notre cas nous allons opter pour la première puis passer à l'installation. Pour tester si l'installation s'est bien passée, il suffit de saisir la commande **radiusd –X** et avoir comme résultat:

```
.....
Inclusion des fichiers de configuration nécessaire à freeradius
(clients.conf,ldap,...)
.....
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on proxy address * port 1814
Ready to process requests
```

Pour la configuration de freeradius, les fichiers à modifier sont les suivants :

- **/usr/etc/raddb/clients.conf**: c'est dans ce fichier que nous devons renseigner le ou les NAS qui communiqueront avec le serveur freeradius.
- **/usr/etc/raddb/radiusd.conf**: c'est le fichier de configuration principal de freeradius car il permet de faire appel à tous les autres fichiers de configuration. Mais il y a des versions de freeradius qui placent tous les autres fichiers de configuration dans radiusd.conf. Par la suite nous devons modifier la partie « journaux » et laisser le reste par défaut.
- **/usr/etc/raddb/modules/ldap**: dans ce fichier, il faut renseigner les informations de l'annuaire Openldap au serveur radius. Ces informations sont le login du compte administrateur, son mot de passe, le nom du serveur. Aussi nous avons ajouté l'attribut **dialupAccess=yes** et dé-commenter la ligne **access_attr = dialupAcess**.
- **/usr/etc/raddb/sites-enabled/default**: dans ce fichier, il faut spécifier à radius d'utiliser le protocole ldap pour authentifier un utilisateur. Quatre parties nous intéressent ici à savoir **authorize** (autoriser), **authenticate** (authentifier), **accounting (journalisation)** et **session**. De même nous devons commenté certaines lignes pour que ldap soit le seul à authentifier les utilisateurs.
- **/usr/etc/raddb/sites-enabled/inner-tunnel**: ce fichier est presque identique au fichier default, il n'est pas nécessaire d'effectuer de modification.

Les parties **accounting** et **session** permettront de faire la journalisation. Une table à laquelle nous intéressons est la table **radacct** de la base de données radius créée avec **MySQL**. En effet on pourra enregistrer un certain nombre de données telles que l'heure de connexion, l'identifiant, par quel NAS (borne), le nombre d'octets entrants/sortants, etc. Nous devrions crée une base de données appelée radius. Pour cela, nous allons installer le serveur MySQL. Après l'installation de MySQL, on va configurer freeradius pour communiquer avec cette base. Pour cela nous allons éditer le fichier **/usr/etc/raddb/sql.conf.** Dans ce fichier il faut indiquer au serveur radius les informations utiles pour se connecter à la base de données radius.

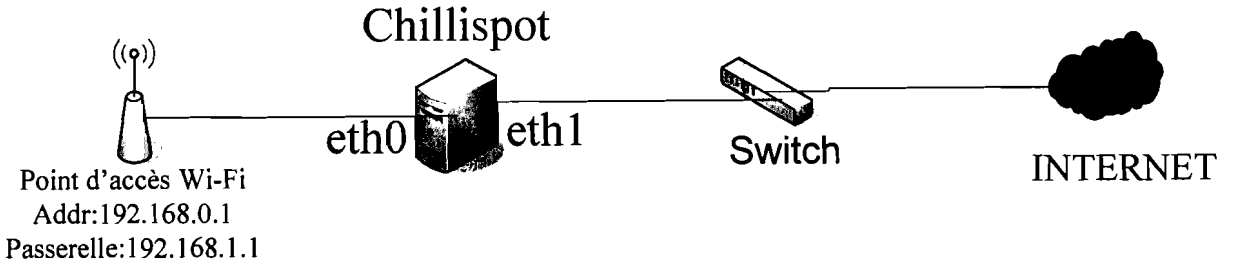
Pour l'administration de cette base, nous allons installer à cet effet l'outil **phpMyAdmin.** Voir la présentation de cet outil en annexe2.

Normalement notre serveur freeradius est prêt. Nous pourrons le relancé en mode debug (radiusd –X) pour vérifier les alertes. Pour qu'il se lance automatiquement au démarrage nous procéderons comme suit :

```
#cp /root/freeradius/freeradius-serveur-2.1.1/rc.radiusd /etc/init.d/
#update.rc.d rc.radiusd defaults
```

IV-Chillispot

Pour la mise en œuvre du chillispot, nous allons utiliser deux cartes réseaux comme indiquer sur la figure ci-dessous :



Eth0:192.168.1.1
Eth1: addresse dynamique

Figure16 : Schéma illustratif de la mise en place du chillispot

Par la suite nous allons fixer l'adresse de l'interface eth1. Le paquet chillispot ne se trouve pas dans les dépôts de Debian il faut donc télécharger le point deb sur le site http://www.chillispot.info. On pourra télécharger la version 1.0-4 puis l'installer sur notre Debian Lenny. Les fichiers de configuration de chillispot sont :

- **/usr/lib/cgi-bin/hotspotlogin.cgi** : Ce fichier contient le code du formulaire de la page d'accueil de chillispot. Il faut renseigner dans ce fichier le secret partagé entre le serveur UAM et le démon chillispot.
- **/etc/default/chillispot** : ce fichier permet d''activer chillispot car il ne l'est pas par défaut. Il suffit de remplacer la ligne ENABLED=0 par ENABLED=1
- **/etc/chilli.iptables :** ce fichier qui est la copie de **firewall.iptables** sert à définir les règles d'iptables du firewall. Il faut renseigner dans ce fichier les interfaces réseaux à savoir celles reliées au point d'accès et à Internet. Voir en Annexe3 Etape2 pour la configuration de ce fichier.

Nous devons ensuite activer le routage entre les interfaces réseau en saisissant la commande suivante:

#echo "1" > /proc/sys/net/ipv4/ip_forward

- **/etc/chilli.conf** : c'est le fichier principal de configuration de chillispot. Une partie de ce fichier peut être configurée lors de l'installation. Dans ce fichier il faut renseigner

beaucoup de paramètres à savoir le nom du domaine, l'adresse du serveur radius, l'adresse réseau où les clients seront placés avant et après l'authentification. La page d'authentification de chillispot doit être sécurisée par https. Nous devons configurer le serveur apache pour qu'il puisse fonctionner en mode sécurisé.

Pour cela nous avons besoin de générer les certificats pour le serveur apache. Il est à noter ici que les certificats sont délivrés par des autorités de certifications, mais pour des besoins d'expérimentation, nous allons nous même générer des certificats auto signés. Après cela il faut redémarrer chillispot en s'assurant qu'aucun autre serveur dhcp n'est lancé. On peut le faire en tapant la commande suivante:

#ifconfig eth1 0.0.0.0

#/etc/init.d/chilli stop

#/etc/init.d/chilli start

#/etc/chilli.iptables

Pour éviter d'avoir à taper ces mêmes commandes à tout moment, nous devons créer un script que nous placions dans **/etc/init.d/** pour permettre le lancement automatique au démarrage du système. Ainsi nous allons faire:

#vi /etc/init.d/script.sh et mettre les commandes listées ci-dessus

#update-rc.d script.sh defaults

Nous pourons ainsi tester chillispot avec une autre machine ayant une carte wifi. Celle-ci se connectera bien au réseau sans-fil. C'est à dire que la machine obtiendra une adresse du réseau 192.168.0.0/24. Ainsi lorsqu'elle tente d'ouvrir une page web, elle sera dirigée vers la page d'authentification. Voir en annexe2 les pages d'authentification présentées par le chillispot.

Évaluation des coûts

Désignation	Caractéristiques	Quantité	Prix unitaire	Montant
Ordinateur serveur	Pemtium4 ou supérieur	01	150.000	150.000
Carte réseau	Realtek pci 10/100Base TX Gigabit pci Express	01 01	5000 existante	5000
Point d'accès	Netgear **DG834G**	01	Existant	
Déplacement du point d'accès		01		25.000
Switch	Cisco catalyst série 2960T-24	01	Existant	
Système d'exploitation	Debian Lenny	-	Gratuit	
SGBD	MySQL	01	Gratuit	
Annuaire	Openldap	01	Gratuit	
Serveur Web	Apache2	01	Gratuit	
Firewall	iptables	01	Gratuit	
Portail captif	Chillispot	01	Gratuit	
Serveur d'authentification	Freeradius	01	Gratuit	
Nom de domaine	Hopijobobo.dyndns-pics.com	01	Gratuit	
Outils d'administration	Phpldapadmin	01	Gratuit	

php	phpmyadmin	01	gratuit	
Main d'œuvre	Ingénieurs de travaux informatiques	02	250.000	500.000
Coût total				680.000

Tableau17 : Évaluation des couts de mise en œuvre du projet

Conclusion générale

Ces trois(03) mois de stage à l'HDJ nous a permis d'abord de faire une étude détaillée du réseau informatique de l'hôpital de jour et de relever les différentes insuffisances présentée par le dit réseau. Ensuite, nous avons abordé différentes solutions permettant de faire faces à ces insuffisances, pour cela nous avons procédé à une étude comparée de l'efficacité de chacune de ces différentes solutions en vu de choisir la plus adéquate permettant de rendre le réseau beaucoup sécurisé. Enfin, nous avons pris en compte les besoins actuels de l'HDJ pour le fonctionnement de son réseau informatique sans oublier les insuffisances relevées par le réseau existant pour concevoir une nouvelle architecture du réseau qui est beaucoup sécurisé et plus fluide au échanges de données.

Ce stage à l'HDJ nous a également permis d'améliorer nos connaissances théorique et pratique acquises pendant ces années passées à l'ESI mais aussi de nous familiariser avec le monde professionnel.

Pour finir, nous pensons que la mise en œuvre de cette nouvelle architecture réseau que nous proposons est d'une importance capitale pour le bon fonctionnement du réseau informatique de l'HDJ. Évolutif, cette architecture pourra faire l'objet d'améliorations et de modification en fonction des besoins futur de la structure.

Bibliographie

http://www.memoireonline.com /

http://www.clusif.asso.fr

http://www.reseaucerta.org

http://chillispot.info/

http://www.ifi.auf.org/rapports/tpe-promo14/tpe-ewelle-richard.pdf

http://links.larsen-b.com/Rapport_de_stageV7_35.pdf

http://fr.wikipedia.org/wiki/Moteur_de_base_de_donnees

http://debian-facile.org/wiki/commande:..ion-reseau

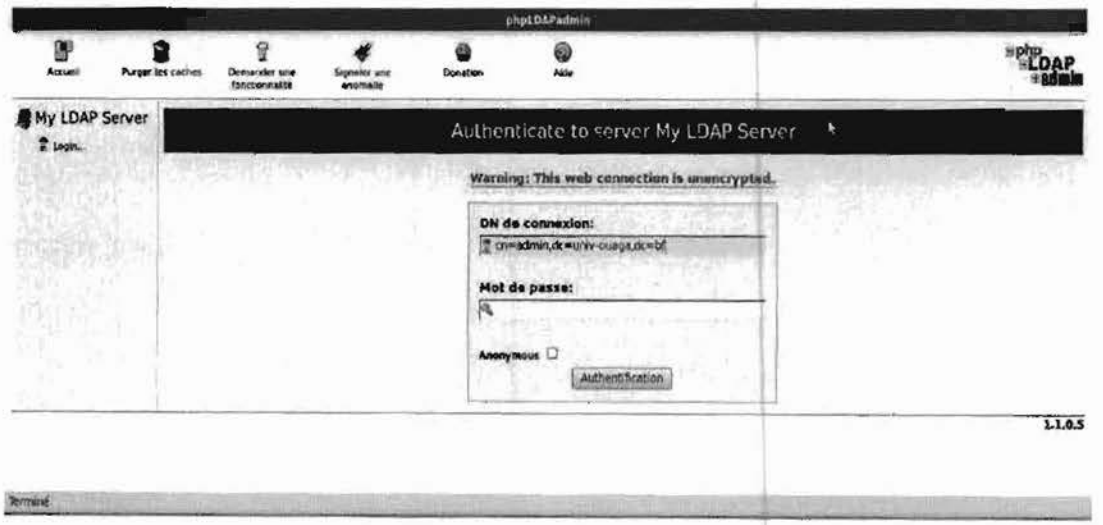
http://fr.wikipedia.org/wiki/Filtrage_par_adresse_MAC

DABRE M et ZOUGMORE G, mai 2010, Rapport de fin de cycle, Mémoire de fin de cycle en Réseaux et Maintenance Informatiques –ESI/UPB

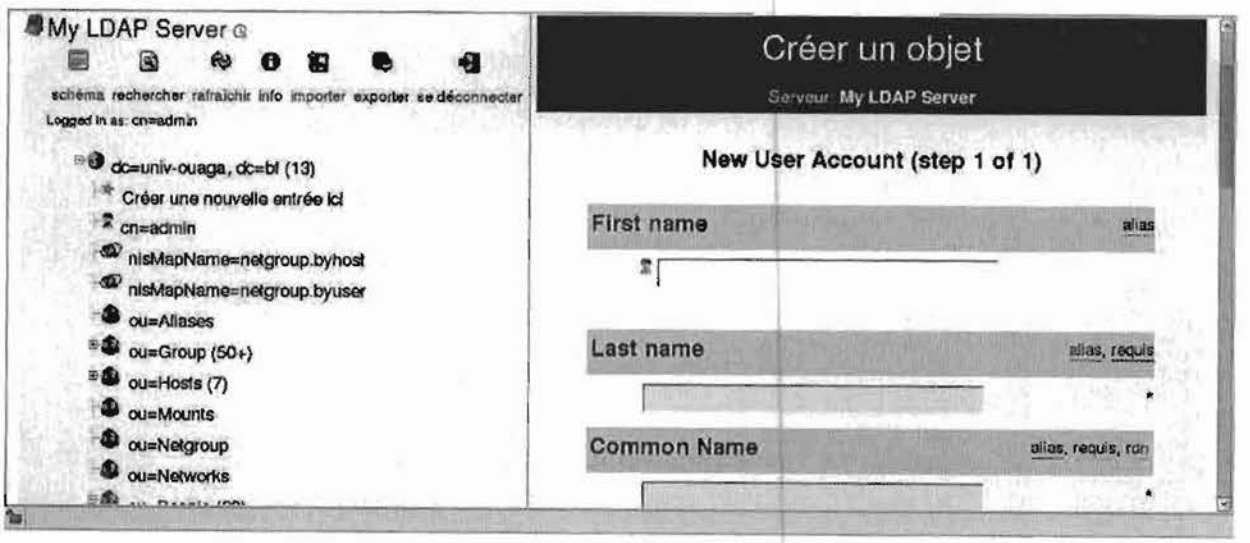
Annexes

Annexe1 : Pages d'accueil de l'outil d'administration phpldapadmin

La page d'accueil de l'outil phpldapadmin se présente comme suit :



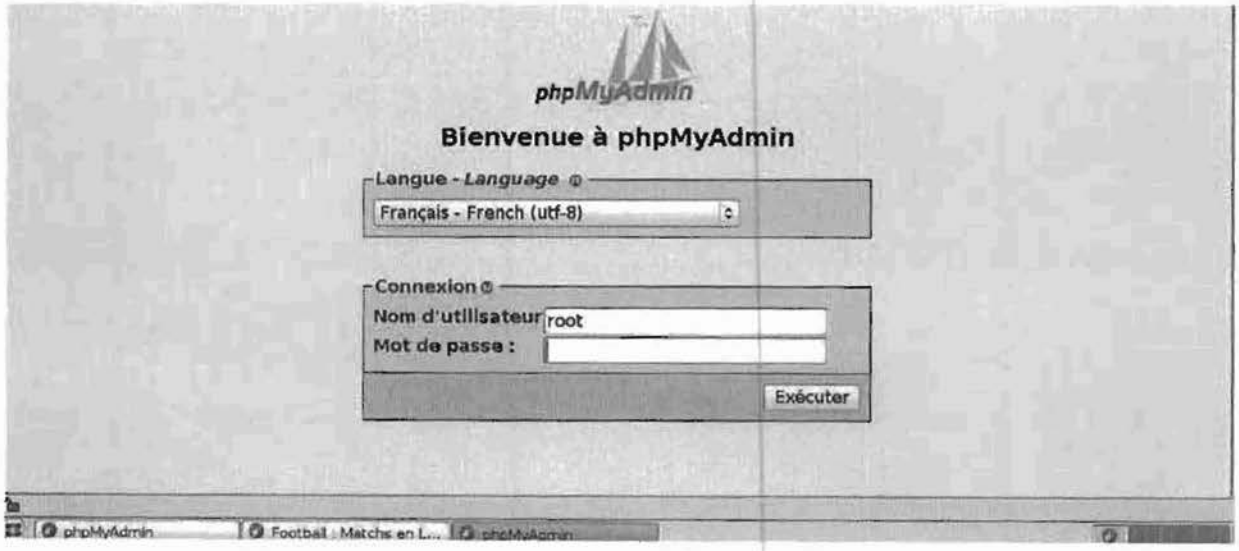
Après avoir se connecté on pourra créer un objet en cliquant sur **user account,** la page suite affiche :



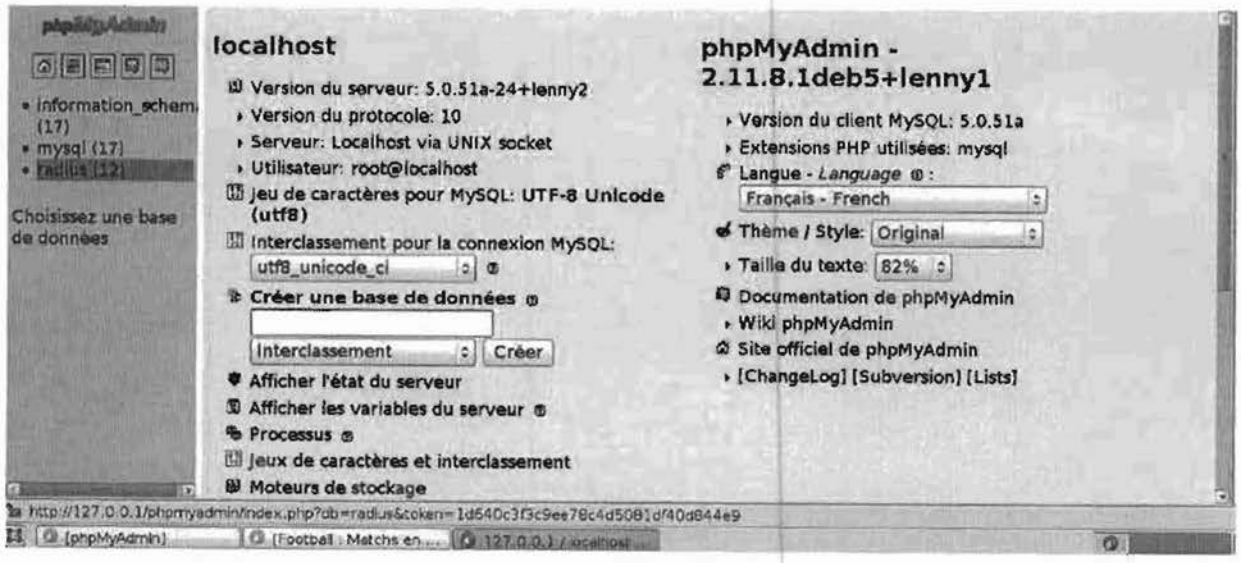
Il s'agira de remplir soigneusement les différents champs puis valider.

Annexe 2: Présentations des pages de l'outil PhpMyadmin

La page d'accueil de l'outil ressemble à ceci :

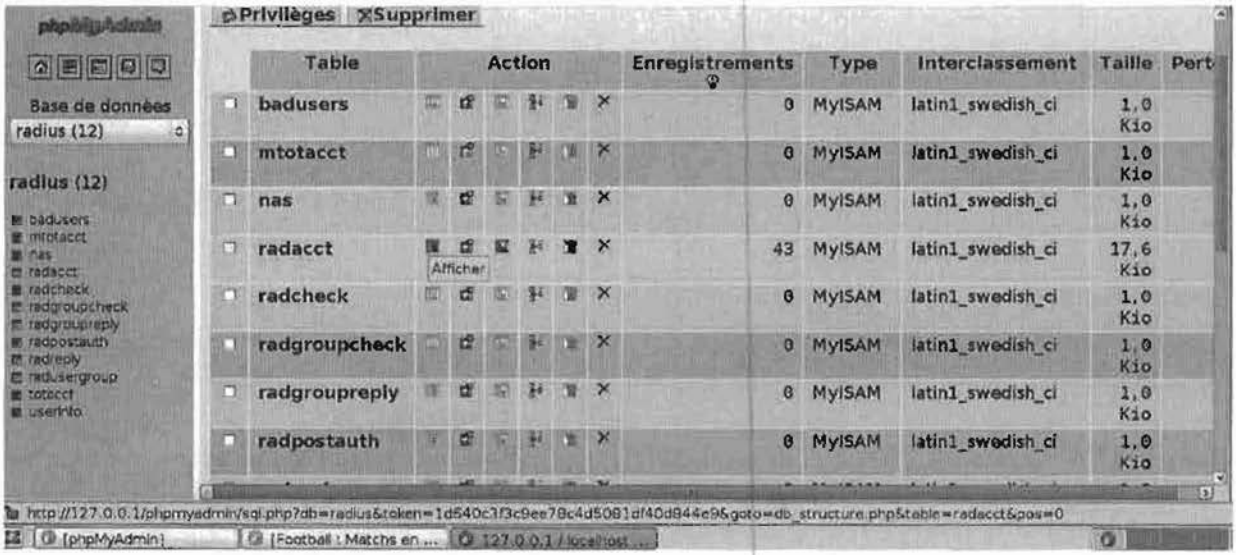


En cliquant sur **Exécuter**, la page qui apparaît montre les différentes bases de données existantes. Choisissez celle qui vous intéresse comme suit :



La page qui apparaîtra après le choix, nous présente les tables de la dite base.

Ici, on pourra choisir celle que nous voulons afficher, c'est la table **radacct** de la base de données **radius.**

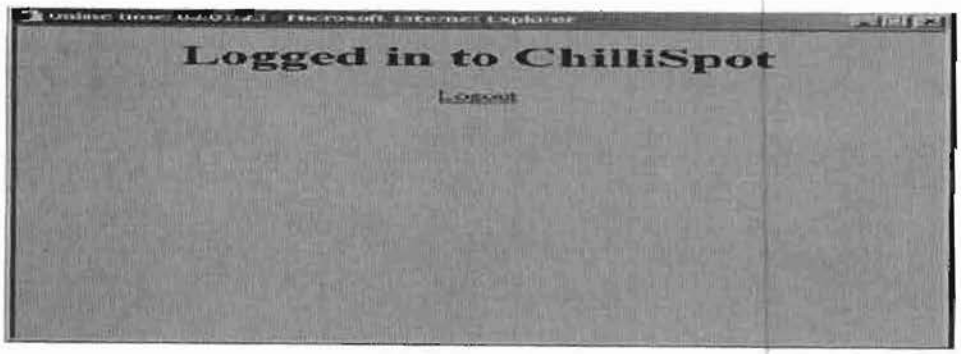


On pourra par la suite faire des enregistrements.

Annexe3 : Pages d'authentification présentées par le chillispot

La page d'accueil du chillispot lors d'une tentative de connexion se présente comme suit :

Si on entre le login et le mot de passe d'un utilisateur se trouvant dans l'annuaire ldap on doit obtenir la page suivante:



Au cas où l'utilisateur ne se trouve dans l'annuaire la page suivante nous sera affichée: