République Algérienne Démocratique et Populaire Ministre de l'Enseignement Supérieur de la Recherche Scientifique

Université Abderrahmane Mira de Bejaia

Faculté des Sciences Exactes

Département d'Informatique

Mémoire De Fin De Cycle

En vue de l'obtention d'un diplôme de Master professionnel en informatique

Option : **A**dministration et **S**écurité des **R**éseaux

Thème

Conception et Réalisation d'une application mobile pour la configuration des modems sous Android

---

Réalisé par :

HANIFI Mohamed Fouad

HAMMOUCHE Ouail

Soutenu devant le jury composé de :

Examinateur: Mr MOKTEFI Mohand

Examinateur: Mr MEHAOUED Kamel

Encadrant : Mme El BOUHISSI Houda

Remerciements

Louange à Dieu, le miséricordieux, sans lui rien de tout cela n'aurait pu être.

Nous tenons tout d'abord à remercier Mme Elbouhissi Houda pour l'honneur qu'elle nous a fait en acceptant de nous encadrer. Ses conseils précieux ont permis une bonne orientation

Dans la réalisation de ce modeste travail.

Nos remerciements s'adressent aux enseignants de notre département en particulier ceux qui se sont montrer présent et à notre écoute et sans oublier le membre de la commission Du jury qui évalueront notre travail.

Nous tenons à remercier vivement tous ceux et celles qui nous ont accompagné tout au long de ce parcours, pour les conseils avisés qu'ils nous ont donné, a la sollicitude Dont ils ont fait preuve à notre égard, et les documents et outils mis gracieusement à notre disposition.

Nos remerciements les plus vifs vont particulièrement à nos parents.
Enfin, merci à tous ceux qui ont contribué de près ou de loin à la réalisation de ce mémoire.

Dédicace

Je dédie ce modeste travail ***A mes parents*** *qui ont beaucoup sacrifié pour moi et qui continuent d'en faire pour me voir réussir. Avec tous mes sentiments de respect, d'amour et de reconnaissance, pour tous les sacrifices déployés pour m'élever dignement et assurer mon éducation dans les meilleures conditions. Que dieu les protègent.*

À ***mon grand-père*** *aucun hommage ne pourrait être à la hauteur de l'amour dont il ne cesse de me combler. Que dieu l'accueil dans son vaste paradis.*

À mes profs qui m'ont soutenu tout au long de mon parcours d'étude. Avec tous mes sentiments de respect, d'amour et de reconnaissance.

À mes chères collègues de travail, « Lounis lwendaji », « Babi », « Allouache », « Jugo » et « Abdeslam » et tous les autres

À mes chers amis « Habib, Bilal »

À Mon Binôme « Ouail » et à toute sa famille. Et à tous ceux qui ont contribué de près ou de loin pour ce projet soit possible, je vous dis merci.

Fouad.H

Dédicace

Nous dédions notre travail à nos très chers parents pour leurs patiences, leurs amours leurs Soutiens et leurs encouragements tout le long de notre cursus D'études

.

À nos frères et sœurs qui n'ont cessé d'être pour nous des exemples de Persévérance, pour leurs encouragements et leurs aides.

À tous les membres de nos familles qui nous ont soutenus.

À nos amis(e) et nos camarades qui ont contribué de près ou de loin.

Ouail.H

Table des matières

Table des matières

Table des matières

Table des matières

Liste des Figures

Liste des Tableaux

Introduction Général

Les réseaux informatiques sont devenus des éléments stratégiques pour les entreprises et administrations. Alors que de nombreuses activistes reposent sur les réseaux informatiques, il n'est plus acceptable que le mauvais fonctionnement d'un élément du réseau perturbe les utilisateurs. Les administrateurs sont chargés de veiller au bon fonctionnement des réseaux informatiques. Les systèmes d'administration de réseaux constituent leur principal outil pour la configuration, la surveillance et la maintenance des divers équipements informatiques constituant le réseau. Plusieurs plates-formes d'administration de réseaux sont commercialisées. Ce sont pour la plupart des systèmes propriétaires fondes sur la technologie client/serveur et fonctionnant sur une architecture matérielle et un système d'exploitation donnes

De nos jours, les appareils mobiles hébergent de nombreuses applications directement téléchargées et installées à partir d'un "Store" d'applications mobiles. L'existence d'une telle quantité d'applications pour une multitude d'objectifs impose une énorme surcharge sur les utilisateurs, qui doivent sélectionner, installer, supprimer et exécuter les applications appropriées. En outre, Ces applications servent à des fins spécifiques et sont supprimées ou oubliées, la plupart du temps, après la première utilisation. De plus, ces applications ne tiennent pas compte du monde des objets connectés en raison de leur architecture monolithique mise en œuvre pour fonctionner sur des appareils individuels. La solution proposée est d'offrir une nouvelle façon de répondre aux besoins de l'utilisateur de façon dynamique et distribuée. Une évolution continue des applications (en cours d'exécution) en ajoutant, supprimant, et déplaçant des fonctionnalités sur les appareils utilisés par l'utilisateur. Elle permet, aussi, de modifier le mode d'interaction en distribuant les exécutions sur plusieurs appareils en fonction des besoins de l'utilisateur. Pendant que l'utilisateur se déplace dans son environnement, l'application détecte des événements environnementaux et construit des situations contextuellement décrites. Ainsi, ce travail vise à offrir un nouveau type d'application mobiles capables de détecter, de formuler et de comprendre le contexte des utilisateurs puis réagir en conséquence.

Chapitre 1

Les Technologie mobiles

1.1 Introduction

L'objet de ce chapitre est de poursuivre notre réflexion sur les projets de développement de systèmes d'exploitation pour smartphones. En le reliant aux projets concrets de développement de systèmes d'exploitation mobiles, ce premier point renvoie aux systèmes Symbian et BlackBerry qui ont connus un certain succès mais sont désormais en mauvaise posture. Le second point met face à face les différentes stratégies, afin de voir les conditions industrielles de leur réussite, puis plus particulièrement nous aborderons l'influence des partenariats industriels sur l'évolution de la plateforme. Ce second point nous permettra d'avoir un premier aperçu des enjeux économiques relatifs à l'évolution stratégiques des projets de systèmes d'exploitation mobile. C'est le cas de Symbian qui passe d'une organisation sous forme de consortium ouvert à différents fabricants de terminaux, à une fondation « open source » pour finalement revenir dans le giron de Nokia. de manière plus prospective, nous pouvons aussi y voir la tension subie par Google, visant à donner à Android une structure organisationnelle moins ouverte

1.2 Les différents systèmes d'exploitation mobiles :

Un système d'exploitation mobile est un système d'exploitation conçu pour fonctionner sur un appareil mobile.

Le système d'exploitation n'est rien de plus qu'une interface entre des applications pour les usagers finals (software) et une infrastructure physique (hardware). Seulement, cette représentation d'où l'intérêt d'une granularité assez fine. L'Illustration 1 donne un aperçu des différents niveaux de granularité que l'on peut adopter en étudiant un système logiciel et met en avant l'imbrication hiérarchique de ces différents niveaux, de la ligne de code au système d'exploitation [1].

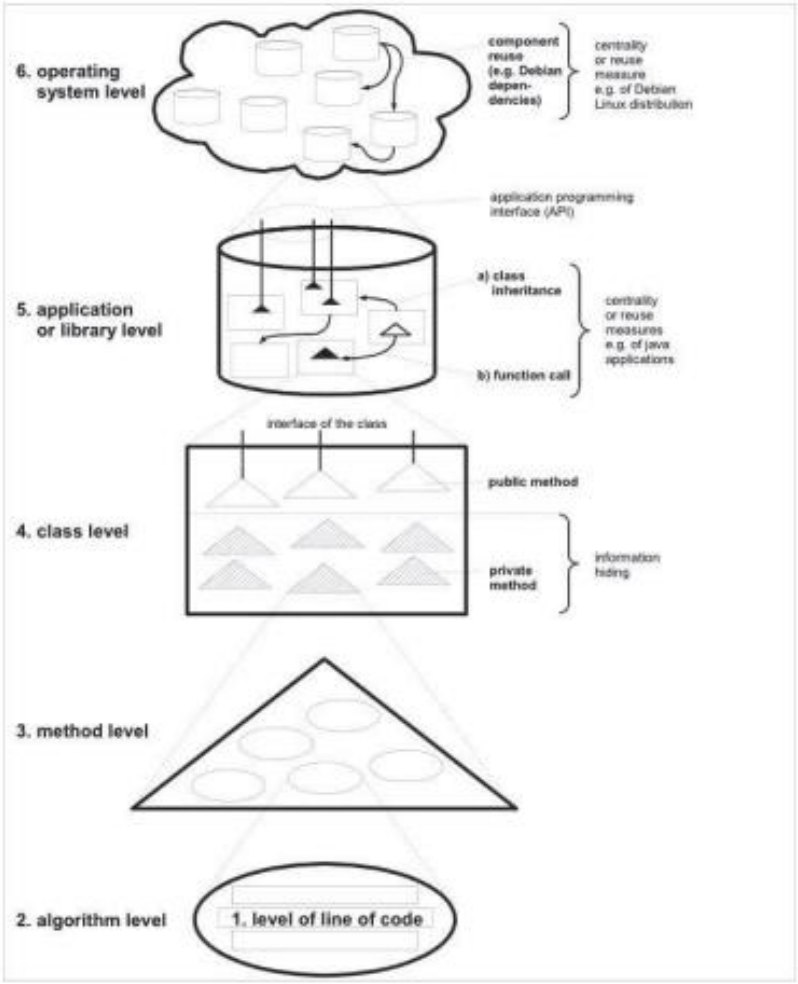


Figure 1.1: *Hiérarchie par niveaux des modules d'un système logiciel*

Voici donc les quatre OS les plus populaires :

1.2.1 Ios

Nous allons commencer par Apple, non pas parce que ses appareils sont les meilleurs ou parce qu'il détient la plus grande part de marché, mais parce qu'Apple a provoqué une révolution sur le marché. Cela a changé la façon dont les utilisateurs voient les appareils mobiles et la navigation Web mobile, et c'est la raison pour laquelle de nombreux développeurs (web ou non) ont tourné leur attention vers le monde mobile. Apple, une société d'ordinateurs de bureau bien connue, est entrée dans le monde mobile avec un appareil révolutionnaire : l'iPhone.

iOS, anciennement iPhone OS, le « i » d'iOS étant pour iPhone d'où la minuscule, est le système d'exploitation mobile développé par Apple pour plusieurs de ses appareils. Il est dérivé de macOS dont il partage les fondations (le noyau hybride XNU basé sur le micro-noyau Mach, les services Unix et Cocoa, etc.). iOS comporte quatre couches d'abstraction, similaires à celles de macOS : une couche « Core OS », une couche « Core Services », une couche « Media » et une couche « Cocoa »[2,Note 1]. Le système d'exploitation occupe au maximum 3 Go de la capacité mémoire totale de l'appareil, selon l'appareil.

1.2.2 BlackBerry OS

Research in Motion (RIM) était le fabricant canadien des appareils BlackBerry, des appareils mobiles axés sur le fait d'être toujours connectés avec les technologies push. La société a été rebaptisée "BlackBerry" au début de 2013, abandonnant le nom de RIM pour l'avenir. Les premiers utilisateurs étaient principalement des utilisateurs d'entreprise qui devaient rester connectés aux intranets et aux réseaux d'entreprise : puis les appareils sont apparus sur de nouveaux marchés, devenant populaires auprès des adolescents et instantanés. RIM avait l'habitude d'appeler tous ses appareils des « smartphones », mais d'autres ne les considéraient pas toujours comme faisant partie de cette catégorie.

Pendant des années, RIM a eu peu d'appareils destinés au marché de masse ; la plupart d'entre eux avaient des claviers QWER et n'étaient pas conçus pour les jeux. Beaucoup de ces appareils avaient des périphériques d'entrée propriétaires, comme une molette de défilement ou un pavé tactile, bien que certains appareils tactiles aient été lancés au cours des dernières années, offrant aux utilisateurs plus de support multimédia et de jeu.

1.2.3 Windows phone

Microsoft a lancé son nouveau système d'exploitation avec des sociétés telles que HTC, LG et Samsung, mais il n'a pas obtenu trop de parts de marché. Un accord spécial avec Nokia a changé cela, offrant une distribution beaucoup plus large de Windows Phone dans le monde à partir de 2012. La plupart des analystes indépendants concluent que dans les années suivantes, iOS, Android et Windows Phone seront probablement les trois principales plates-formes du marché. La première version du système d'exploitation Windows Phone était la 7.0 (suivant Windows Mobile 6,5). Cela a été suivi par la première grande étape : Windows Phone 7.5,

également connu sous le nom de Mango, qui prenait en charge le multitâche et HTML5 dans Internet Explorer 9. Le système d'exploitation a les mêmes restrictions qu'iOS lorsqu'il s'agit de fournir un Utilisez la plate-forme et masquez certains éléments de bas niveau, tels que le système de fichiers, l'installation d'applications à partir de sources inconnues ou le véritable multitâche. Les appareils Windows Phone incluent des services et des applications liés à Microsoft, tels que les services Office, Internet Explorer et Bing. Les applications sur les appareils Windows Phone ne peuvent être bloquées que via le magasin Windows officiel. Architecture et un Ul optimisé pour une meilleure personnalisation, y compris Kid's Corner, qui offre un moyen sans souci pour que vos enfants jouent avec votre téléphone. Tous les appareils Windows Phone 8 incluent le Windows Phone Store, anciennement connu sous le nom de Windows Marketplace,

1.2.4 Android

Android est un système d'exploitation open source basé sur Linux, créé et maintenu par un groupe de sociétés et d'opérateurs de logiciels et de matériel appelé Open Handset Alliance. Google le maintien principalement, il est donc parfois connu sous le nom de « système d'exploitation Google Mobile ». Comme pour tout logiciel open source, n'importe quel fabricant pourrait théoriquement supprimer tous les éléments spécifiques à Google du système d'exploitation avant de l'installer sur ses appareils. Cependant, au moment de la rédaction de cet article, aucun fournisseur ne l'a fait, c'est pourquoi chaque appareil Android est très " Compatible avec Google

1.3 Plateforme Android

Android est une plate-forme, pas un fabricant. Par conséquent, il peut sembler ne pas correspondre à cette liste. C'est le cas, cependant, si nous développons un site Web pour un appareil Android, nous n'avons pas besoin de trop nous soucier de l'identité du fabricant. En effet, la plate-forme Android est suffisamment puissante pour laisser la marque et le modèle à la deuxième place lorsque nous parlons de fonctionnalités de développement [2].

1.3.1 Versions

Au moment de la rédaction de ce mémoire, le système d'exploitation Android est disponible en plusieurs versions. Un appareil ne peut généralement mettre à jour son système d'exploitation qu'une ou deux fois, car chaque fabricant (et parfois les opérateurs) doit créer sa propre version d'Android à partir du code source de Google. Cela signifie qu'à tout moment, nous pouvons trouver sur le marché des appareils exécutant au moins trois versions principales de l'OS qui sont bloqués sur cette version et ne recevront pas de mise à jour. Connaître la version du système d'exploitation sera très utile pour déterminer quelles fonctionnalités du navigateur sont disponibles. Malheureusement, la documentation sur les fonctionnalités du navigateur Android n'est pas complète, bien que (comme nous le verrons dans le chapitre suivant) Google Chrome semble

des formes pour l'avenir résolvent certains de ces problèmes pour l'avenir. Chaque version Android est connue par son numéro et aussi par un nom de code qui est toujours un dessert, commençant par les lettres successives de l'alphabet. Dans le tableau 1vous verrez une liste des versions d'Android qui ont été publiées ou qui doivent être publiées

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.3%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.2%
4.2.x		17	1.5%
4.3		18	0.5%
4.4	KitKat	19	6.9%
5.0	Lollipop	21	3.0%
5.1		22	11.5%
6.0	Marshmallow	23	16.9%
7.0	Nougat	24	11.4%
7.1		25	7.8%
8.0	Oreo	26	12.9%
8.1		27	15.4%
9	Pie	28	10.4%

Tab1.1 : différente version Android [3]

1.3.2 L'Architecture d'Android :

Android est basé sur un kernel linux 2.6.xx, au-dessus du kernel il y a "le hardware abstraction layer " qui permet de séparer la plateforme logique du matériel. Au-dessus de cette couche d'abstraction on retrouve les librairies C/C++ utilisées par un certain nombre de composants du système Android. Au-dessus des librairies on retrouve l'Android Runtime, cette couche contient les librairies cœurs du Framework ainsi que la machine virtuelle exécutant les applications. Au-dessus la couche "Android Runtime" et des librairies cœurs on retrouve le Framework permettant au développeur de créer des applications. Enfin au-dessus du Framework il y a les applications. L'image ci-dessous décrit l'architecture complète d'Android :

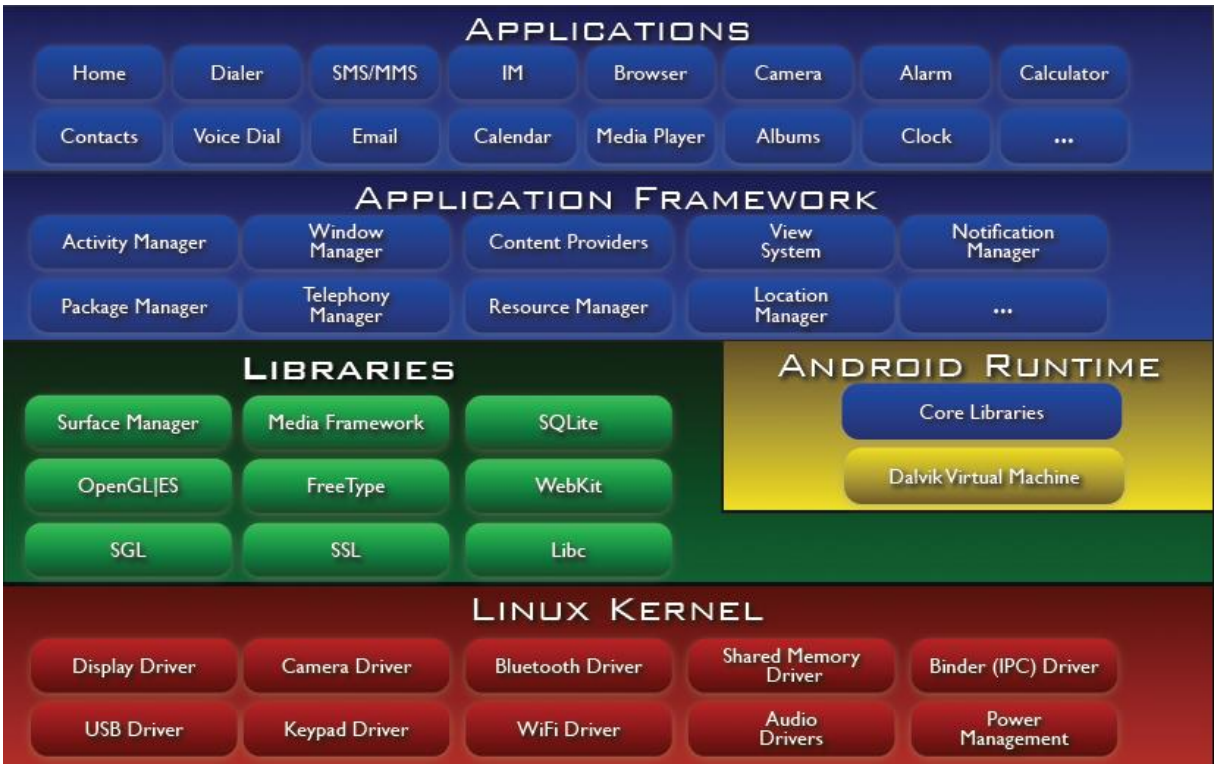


Figure1.2 : *l'architecture complète d'Android [4]*

1.4 Les outils de développement

Android Les différents outils de développement Android sont :

- **Le SDK Android**

Le Kit de développement logiciel Android (Android SDK) contient les outils nécessaires pour créer, compiler et déployer les applications Android. La plupart de ces outils sont en ligne de commande.

- **Le débogueur « ADB »**

Le SDK Android contient un débogueur appelé « Android debug bridge » ou aussi « adb », qui permet de connecter un appareil Android virtuel ou réel, dans le but de gérer le périphérique ou de déboguer votre application.

- **Les IDE « Android Développer Tools » et « Android Studio »**

Google propose deux environnements de développement intégrés (IDE) pour développer de nouvelles applications.

a) Eclipse

Les outils de développement Android sont basés sur l'IDE Eclipse. ADT est un ensemble de composants (plug-ins), qui étendent l'IDE Eclipse avec des capacités de développement Android.

b) Android Studio

Google propose également cet IDE appelé pour la création d'applications Android quel que soit le terminal sous-jacent (smartphone, tablette, montre, TV…) et qui est basé sur l'IDE IntelliJ

- **La machine virtuelle Dalvik Dalvik**

est une machine virtuelle incorporée dans le système d'exploitation Android. Destinée à permettre l'exécution simultanée de plusieurs applications sur un appareil de faible capacité (peu d'espace mémoire et peu de puissance de calcul).

- **Le runtime Android (ART**)

Les dernières versions d'Android introduisent une nouvelle machine, le runtime Android. le moteur qui permet l'exécution des applications pour Android.[5]

1.5 Cycle de vie d'une activité

Voici un diagramme qui explique le cycle de vie d'une activité sous Android :

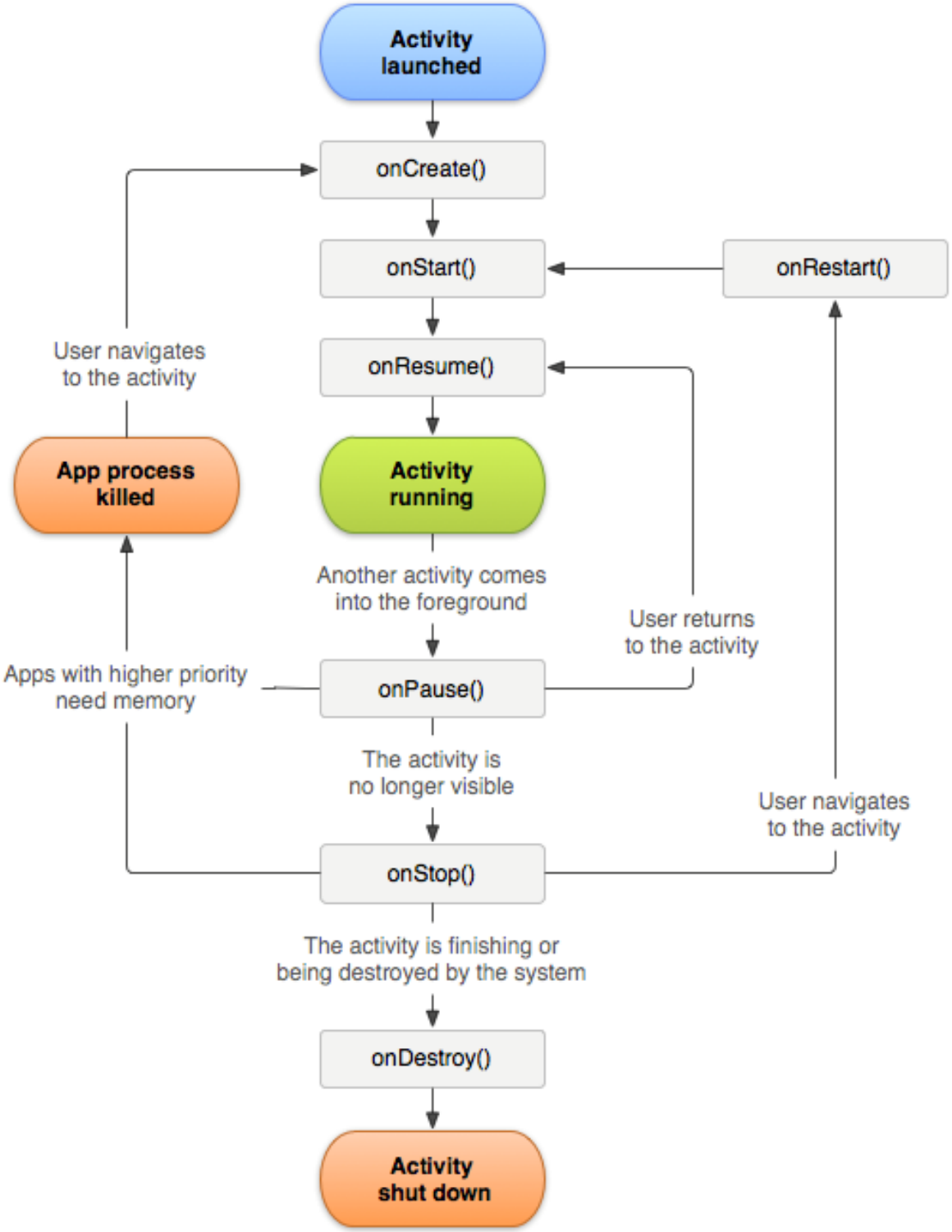


Figure 1.3 : *le cycle de vie d'une activité sous Android [6]*

Lorsque notre application est lancée, l'activité est chargée et la méthode onCreate() est lancée. Cette méthode va nous permettre d'initialiser votre activité. Il sera aussi possible de restaurer un précédent lancement de notre application qui aurait été interrompu (bundle, par exemple lors de la rotation de l'écran). Suite à cette méthode, onStart() sera lancée.

onStart() est lancée tout de suite après le onCreate() lorsque l'activité va devenir visible à l'utilisateur. Vous allez pouvoir charger des données, ...Le système pourra ensuite lancer onResume() ou onStop().

onResume() est lancée lorsque notre application est passée en avant plan. Nous pourrons donc (re)lancer nos threads, ... Le système pourra ensuite lancer onPause()

onPause() est lancée lorsqu'une autre activité va s'afficher à l'avant plan. C'est le moment de sauver toutes les données/informations saisies par l'utilisateur pour l'activité courante. En effet, le système peut décider par la suite de mettre fin à votre activité par exemple à cause d'un manque de mémoire. Par conséquent, le système pourra soit lancer soit onResume() pour remettre votre activité en avant plan ou onStop().

Conclusion

Dans ce chapitre, nous avons étudié la plateforme Android en voyant son historique, ses versions, son architecture et ses outils de développements.

Chapitre 2

Généralités sur les réseaux informatiques

2.1 Introduction

Un réseau informatique est constitué d'un ensemble de systèmes informatiques interconnectés les uns avec les autres grâce à des équipements et supports de communications. L'objectif est de permettre à plusieurs machines de communiquer entre elles à fin d'assurer des échanges d'informations et un partage de ressources matérielles ou de données. Du point de vue de l'utilisateur, le réseau doit être le plus transparent possible : ses applications doivent être capables de communiquer toutes seules avec le reste du réseau, sans l'intervention humaine.

2.1.1 Les différents types de réseaux :

On classe les différents réseaux selon leurs tailles, leurs vitesses de transfert ainsi que leurs étendues, donc on parlera de [7] :

Réseau personnel (PAN), Réseau local (LAN), Réseau métropolitain (MAN), Réseau étendu (WAN).

Topologie des réseaux : On peut différencier deux types de topologies, la topologie physique et la topologie logique.

2.1.1 Les modèles de références :

2.1.1.1 Le Modèle OSI :

L'ISO[1] (International Standardization Organization) a normalisé sa propre architecture sous le nom d'OSI (Open Systems Interconnection). L'architecture OSI permet l'interconnexion des réseaux hétérogènes. Ce modèle est composé de 7 couches (niveaux). Les services des couches supérieures peuvent intervenir sur chaque couche immédiatement inférieure**.**

[1] ISO (International Standardization Organisation) organisme dépendant composé de 140 organismes nationaux de normalisation, a développé un modèle de référence appelé modèle OSI.

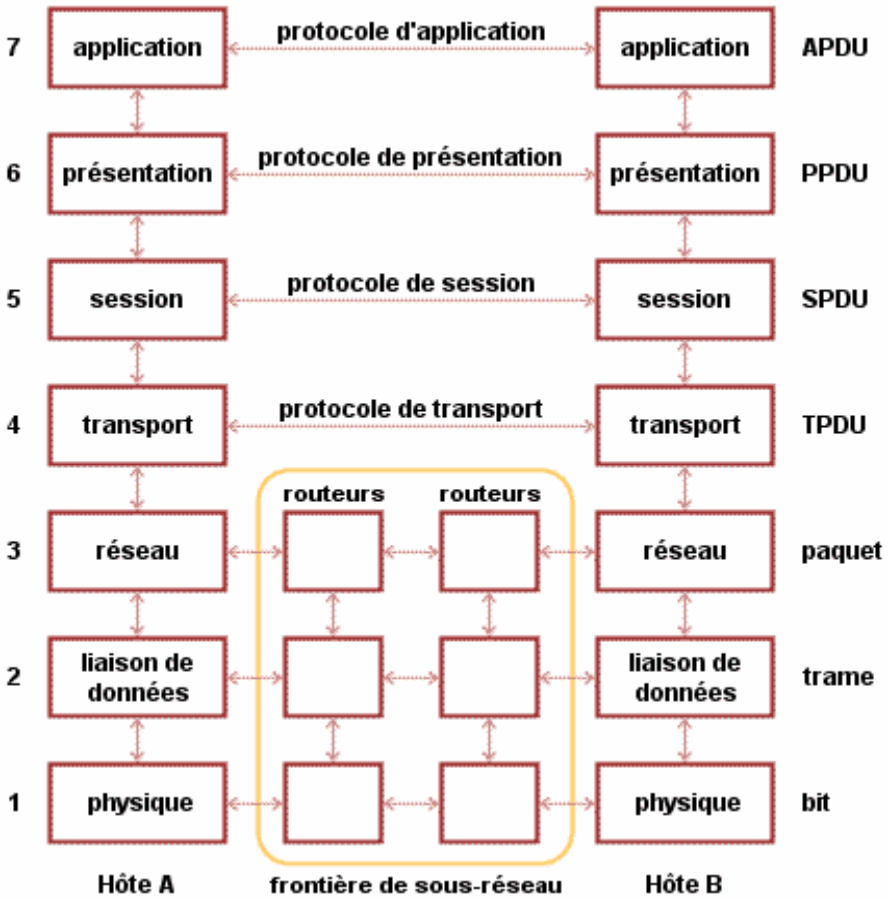


***Figure 2.1**: modèle OSI [8]*

2.2 Internet et intranet

2.2.1 Internet

Internet est un système mondial d'interconnexion de réseau informatique, utilisant un ensemble standardisé de protocoles de données. C'est donc un réseau de réseaux, composé de millions de réseaux aussi bien publics, privés, universitaires, commerciaux et gouvernementaux dont leur pile de protocoles est compatible avec la pile TCP/IP. Internet transporte un large spectre d'information et permet l'élaboration d'applications et de services variés comme le courrier électronique, la messagerie instantanée et le World Wide Web.

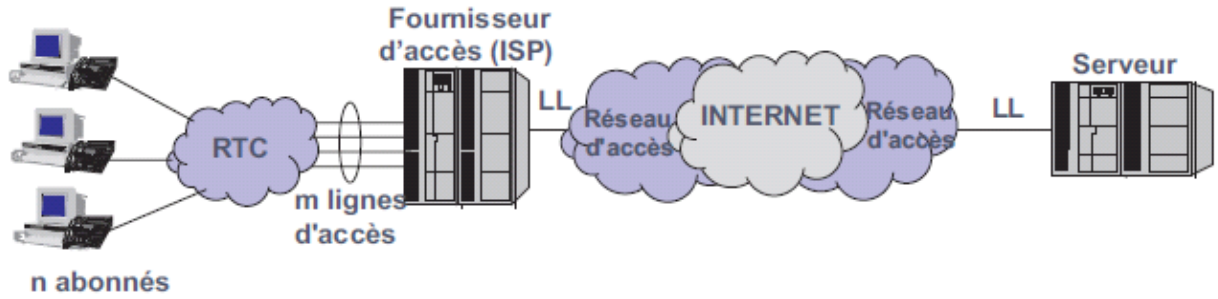


Figure 2.2: *L'acheminement des données jusqu'au serveur*

L'accès à Internet peut être obtenu grâce à un fournisseur d'accès à Internet (FAI) via divers moyens de communication électronique : soit filaire (réseau téléphonique commuté (RTC), ADSL[2], fibre optique jusqu'au domicile) , soit sans fil (par satellite,3G[3]).

2.2.2 Intranet

Intranet est un petit réseau d'entreprise qui a accès à Internet. Il consiste à utiliser les standards client-serveur de l'internet (en utilisant les protocoles TCP/IP).

Les Intranets sont principalement utilisés en tant que système d'information générale. En effet, cette technologie permet de regrouper en un seul endroit une quantité non négligeable de données, que ce soit des informations sur les clients, sur les fournisseurs, une gestion de stock, un centre de documentation, une messagerie électronique, etc., le tout commun à l'ensemble de l'entreprise ou de l'organisation. Cela permet d'avoir un accès centralisé et cohérent à la mémoire de l'entreprise. On parle ainsi de *capitalisation de connaissances*. De cette façon, il est généralement nécessaire de définir des droits d'accès pour les utilisateurs de l'intranet aux documents, donc une authentification de ceux-ci afin de leur permettre un accès personnalisé à certains documents.

Et voici quelques-unes des fonctions que peut réaliser un intranet [9] :

- Mise à disposition d'informations sur l'entreprise,
- Mise à disposition de documents techniques,
- Moteur de recherche de documentations,

[2] ADSL: Asymmetric Digital Subscriber Line. Technique de transmission qui permet, via modem adapté, d'utiliser une partie de la bande passante des lignes téléphoniques ordinaires.

[3] 3G : c'est la troisième génération (3G) désigne une génération de normes de téléphonie mobile

- Un échange de données entre collaborateurs,
- Annuaire du personnel,
- Gestion de projet, aide à la décision, agenda, ingénierie assistée par ordinateur,
- Messagerie électronique,
- Forum de discussion, liste de diffusion, chat en direct,
- Visio-conference,
- Portail vers internet.

2.2.2.1 Équipements d'interconnexion d'un intranet

Un réseau local est constitué d'équipements reliés par un ensemble d'éléments matériels et logiciels. Les principaux équipements matériels d'interconnexion mis en place dans les réseaux locaux sont [10] :

- Carte réseau : Elle est employée pour faire communiquer un ordinateur avec d'autres éléments, tels que des serveurs, des imprimantes ou même des PCs.
- Répéteur : C'est un élément qui régénère et augmente le signal pour le transmettre d'un réseau à un autre. Il agit au niveau 1(physique) du modèle OSI.
- Pont (Bridge) : Est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole pour n'en former qu'un seul réseau logique. Le pont travaille au niveau logique (couche 2 du modèle OSI).
- Routeur : Un routeur opère au niveau de la couche réseau du modèle OSI(niveau 3). Ils permettent de relier des réseaux sur de longues distances et à examiner l'adresse réseau pour prendre des décisions de routage.
- Commutateur (Switch) : Équipement de niveau 2 (couche liaison de données) du modèle OSI. Les commutateurs sont généralement utilisés pour réorganiser un réseau, isoler des serveurs, segmenter des réseaux.
- Passerelle (Gateway) : Les passerelles permettent de relier des réseaux locaux de types différents, par exemple un réseau local et Internet. En effectuant le routage, l'ensemble du réseau local peut accéder à Internet par l'intermédiaire de la passerelle.

2.3 Protocole IP :

Le protocole IP (Internet Protocol) est un protocole de communication de réseau informatique, il est de niveau 3 du modèle OSI et du modèle TCP/IP. Il assure ainsi sans connexion, un service non fiable de délivrance de datagrammes IP, car il n'existe aucune garantie pour que les datagrammes IP arrivent à la destination. Certains peuvent être perdus, dupliqués, retardés, altérés ou remis dans le désordre. Le mode de transmission est non connecté car IP traite chaque datagramme indépendamment de ceux qui le précédent et le suivent :

<table>
<tr><td>Ver</td><td>Let</td><td>Type de service</td><td colspan="2">Langueur table</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment ofset</td></tr>
<tr><td colspan="2">Durée de vie</td><td>Protocole</td><td colspan="2">Cheksum d’en-téte</td></tr>
<tr><td colspan="5">Adresse source</td></tr>
<tr><td colspan="5">Adresse destination</td></tr>
<tr><td colspan="5">Option + bourage</td></tr>
</table>

Tab2.1 : structure d’un datagramme ip

Description de quelques champs :

Ver : Spécifie la version du protocole IP (la version courante est la 4, d'où son nom d'IPv4).

LET : Représente la longueur de l'en-tête sur 4 bit, l'unité étant le mot de 32 bits.

Type de service : Codé sur 8 bits, il donne une indication sur la qualité de service souhaitée, qui reste cependant un paramètre abstrait. Le Type de Service sert à préciser le traitement effectué sur le datagramme pendant sa transmission à travers Internet.

Longueur totale : Donne la taille du datagramme, en-tête plus les données.

Identification, Flags et Fragment Offset : Ces mots sont prévus pour contrôler la fragmentation des datagrammes.

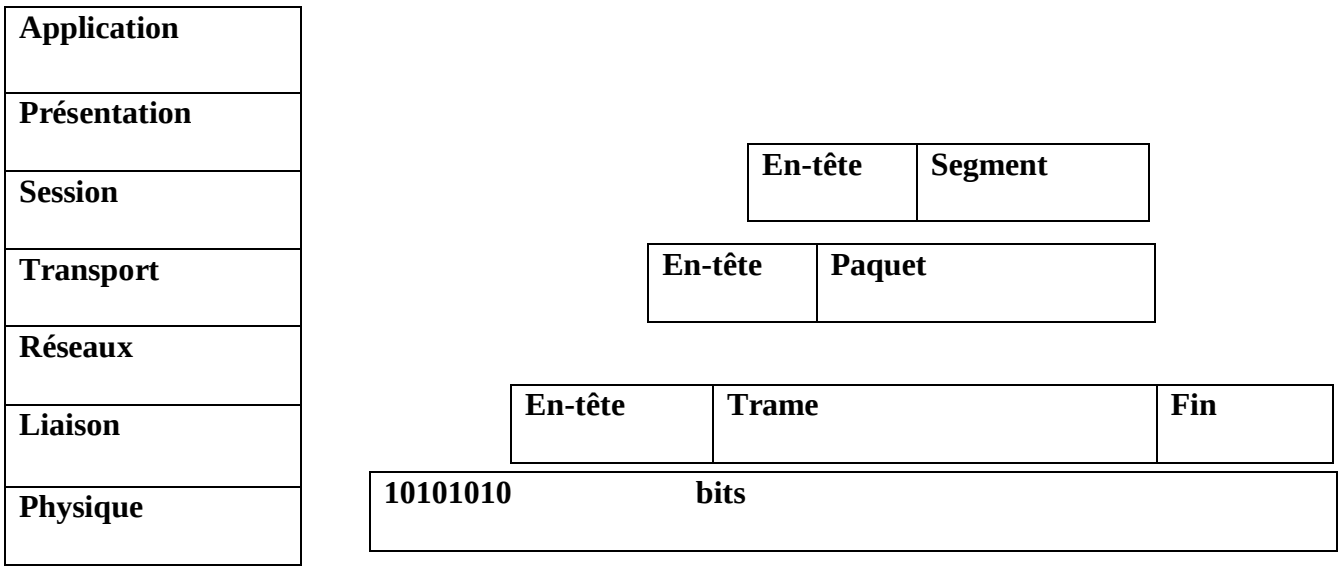
Duré de vie : C'est le temps de vie pour un datagramme sur le net.

Protocole : Sert à identifier le format et le contenu des données.

Checksum d'en-tête : Ce champ contient une valeur codée sur 16 bits qui permet de contrôler intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission.

2.3.1 L'encapsulation IP :

Le paquet est l'unité d'information de base transféré via le réseau. Le paquet de base consiste en un en-tête avec les adresses des systèmes émetteurs et récepteurs, ainsi qu'un corps, ou champ de données, avec les données à transférer. Lorsque le paquet parcourt la pile de protocoles TCP/IP, les protocoles de chaque couche ajoutent ou suppriment des champs de l'en-tête de base. Lorsqu'un protocole sur le système émetteur ajoute des données à l'en-tête du paquet, le processus s'appelle encapsulation de données. De plus, chaque couche possède un terme différent pour le paquet modifié, comme indiqué dans la figure suivante :



Tab 2.2 l'encapsulation ip des données

A chaque niveau, le paquet de données change d'aspect, car on lui ajoute un en-tête, ainsi les appellations changent suivant les couches :

- Le paquet de données est appelé message au niveau de la couche Application :

- Le message est ensuite encapsulé sous forme de segment dans la couche Transport.

- Le segment une fois encapsulé dans la couche Internet prend le nom de datagramme.

- Enfin, nous parlons de trame au niveau de la couche Liaison de donnée

2.3.2 Protocole TCP :

Le protocole TCP (Transport Control Protocol) est un protocole qui procure un service de flux d'octets orienté connexion et fiable. Les données transmises par TCP sont encapsulées dans des datagrammes IP.

Le terme orienté connexion signifie que les applications dialoguâtes à travers TCP sont considérées l'une comme un serveur, l'autre comme un client, et qu'elles doivent établir une connexion avant de pouvoir dialoguer.

La fiabilité fournie par TCP consiste à remettre des datagrammes, sans perte, ni duplication, alors même qu'il utilise IP qui lui est un protocole de remise non fiable. Ceci est réalisé à l'aide de la technique générale de l'accusé de réception.

<table>
<tr><td colspan="7">Port source</td><td>Port destination</td></tr>
<tr><td colspan="8">Numéro de séquence</td></tr>
<tr><td colspan="8">Accusé de réception</td></tr>
<tr><td>Data ofset</td><td>réservé</td><td>Urg</td><td>Ack</td><td>Psh</td><td>Rst</td><td>Syn</td><td>Fin</td><td>Fenétre</td></tr>
<tr><td colspan="7">Cheksum</td><td>Pointeur données urgents</td></tr>
<tr><td colspan="7">Option</td><td>Bourrage</td></tr>
</table>

Tab 2.3 : structure d'un datagramme TCP

Les principaux protocoles et applications de l'environnement TCP/IP sont **:**

- **HTTP :** *HyperText Transport Protocol*, assure le transfert de fichiers hypertextes entre un serveur Web et un client Web **;**
- **FTP :** *File Transfer Protocol*, est un système de transfert de fichiers à distance (transfert, suppression, création...) ;
- **TELNET** : *TELetypewriter NETwork protocol* (ARPA) ou *TERminaL NETwork protocol*, système de terminal virtuel, permet l'ouverture de sessions avec des applications distantes.
- **SMTP :** *Simple Mail Transfer Protocol*, offre un service de courrier électronique.
- **TFTP** *Trivial FTP*, est une version allégée du protocole FTP.
- **DNS** : *Domain Name System*, est un système de bases de données réparties assurant la correspondance d'un nom symbolique et d'une adresse Internet (adresse IP).
- **ICMP** : Internet Control and error Message Protocol, permet la signalisation de la congestion, la synchronisation des horloges et l'estimation des temps de transit... Il est utilisé par l'utilitaire Ping qui permet de tester la présence d'une station sur le réseau.

2.3.3 Protocole UDP :

Le protocole UDP (User Data Protocol) utilise IP pour acheminer, d'un ordinateur à un autre, en mode non fiable des datagrammes qui lui sont transmis par une application. UDP n'utilise pas d'accusé de réception et ne peut donc pas garantir que les données ont bien été reçues. Il ne réordonne pas les messages si ceux-ci n'arrivent pas dans l'ordre dans lequel ils ont été émis et il n'assure pas non plus le contrôle de flux.

<table>
<tr><td colspan="2">Adresse ip source</td></tr>
<tr><td colspan="2">Adresse ip destination</td></tr>
<tr><td>Port udp source</td><td>Prt udp destination</td></tr>
<tr><td>Longueur</td><td>cheksum</td></tr>
<tr><td colspan="2">Donnée
<table><tr><td>Octet de bourrage</td></tr></table></td></tr>
</table>

Tab 2.4 : structure d'un datagramme UDP

2.3.4 Protocole ICMP :

Le protocole ICMP (Internet Control Message Protocol) gère les informations relatives aux erreurs de transmission. ICMP ne corrige pas les erreurs, mais signale aux autres couches que le message contient des erreurs. Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour signaler une erreur (appelé Delivery Problem). Les messages d'erreur ICMP sont transportés sur le réseau sous forme de datagramme, comme n'importe qu'elle donnée. Ainsi, les messages d'erreur peuvent eux-mêmes être sujet d'erreurs.

Voici à quoi ressemble un message ICMP encapsulé dans un datagramme IP:

<table>
<tr><td>En-téte</td><td>Message icmp
<table><tr><td>Type
(8 bits)</td><td>Code
(8 bits)</td><td>Cheksum
(16 bits)</td><td>message
(taille varriable)</td></tr></table></td></tr>
</table>

Tab 2.5 : Message ICMP

2.3.5 Protocole TFTP

Le but du protocole TFTP (Trivial File Transfer Protocol) est de permettre le transfert de fichiers entre deux machines en réseau via UDP/IP. Une machine est serveur de fichiers et les clients peuvent télécharger ou fournir des fichiers à ce serveur. Aucune authentification n'est nécessaire ! Il est souvent utilisé pour le transfert de fichiers de configuration ou d'erreurs vers/en provenance des équipements du réseau (routeurs, hub...).

2.3.6 Protocole DNS :

Chaque ordinateur directement connecté à Internet possède au moins une adresse IP propre. Cependant, les utilisateurs ne veulent pas travailler avec des adresses numériques du genre 172.16.8.2 mais avec un nom de domaine ou des adresses plus explicites.

Ainsi, il est possible d'associer des noms en langage courant aux adresses numériques grâce à un système appelé DNS (Domain Name System).

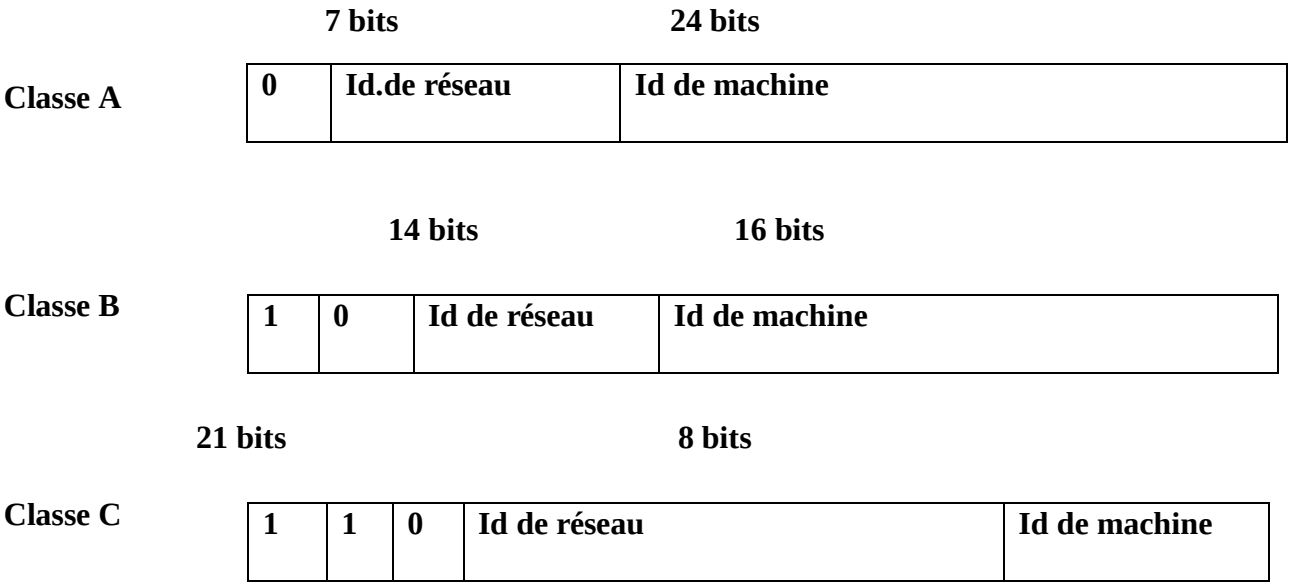
2.4 L'adressage Internet :

Principe

Chaque ordinateur du réseau Internet dispose d'une adresse IP (IPv4 pour être précis) unique codée sur 32 bits. Plus précisément, chaque interface dispose d'une adresse IP particulière. En effet, un même routeur interconnectant 2 réseaux différents possède une adresse IP pour chaque Interface de réseau. Une adresse IP est toujours représentée dans une notation décimale pointée constituée de 4 nombres (1 par octet) compris chacun, entre 0 et 255 et séparés par un point . Plus précisément, l'adresse se décompose en deux parties : l'adresse de réseau (id. de réseau), attribuée par l'administration d'Internet, et l'adresse de la machine dans le réseau (id. de machine), choisie par l'administrateur du réseau local. Toutes les machines d'un même organisme auront donc des adresses dont la partie adresse réseau sera identique.

2.4.1 Classes de réseau :

Afin d'offrir toute la flexibilité requise par des réseaux d'ampleurs différentes (petits à grands réseaux), il existe trois classes d'adressage IP, soient les classes A, B et C, (voir la figure suivante) :



Tab 2.6 les trois classes de l'adresse ip

Classes supplémentaires qui ne sont pas utilisées pour accéder à l'Internet, soient Il existe deux classes supplémentaire les classes D et E. Adresse de classe D est une adresse de multidiffusion, les bits de l'octet le plus significatif débutent par 1110.

Adresse de classe E est une adresse réservée pour des tests et expérimentations, les bits d'une adresse de classe E est une adresse ou l'octet le plus significatif débute par 1111.

2.4.2 Adresses privées :

Un certain nombre de ces adresses IP sont réservées pour un usage interne aux entreprises, elles ne doivent pas être utilisées sur l'Internet où elles ne seront de toute façon pas routées. Il s'agit des adresses suivantes :

Classe	**Plage d'adresse interne**
A	**10.0.0.0----10.255.255.255**
B	**172.16.0.0----172.31.255.255**
C	**192.168.0.0----192.168.255.255**

Tab 2.7 : adresses ip privées

2.4.3 Adresses de diffusion (broadcast) :

L'adresse de diffusion permet à une machine d'envoyer un paquet à toutes les machines d'un réseau. Elle adresse est celle obtenue en mettant tous les bits de la partie machine à 1.

2.4.4 Sous-réseaux :

L'adresse réseau attribuée par l'administration Internet à une entreprise permet à cette dernière de relier un certain nombre de machines, selon la classe de réseau. Il est de plus possible de répartir les machines en sous-réseaux. Il suffit pour cela de réserver un ou plusieurs bits de la partie adresse machine pour désigner le sous-réseau, les autres bits étant l'adresse de la machine

Un sous-réseau est défini par un masque. C'est une suite de bits dont les premiers sont à 1 (ceux qui correspondent à la partie réseau et sous-réseau de l'adresse) et les derniers à 0 (partie machine de l'adresse)

2.3 La norme 802.1Q :

La norme 802.1Q est née en 1998 pour répondre à un besoin de normalisation sur le transport des VLANs. La principale fonction de la norme est de transporter les VLANs sur le réseau, pour permettre à deux machines d'un même VLAN de se communiquer à travers un nombre non défini d'équipements réseaux. Selon la norme IEEE 802.10, l'étiquetage de trames (méthode de distribution des ID de VLAN aux autres switchs) est la meilleure façon de mettre en oeuvre des LAN virtuels. La méthode d'étiquetage des trames VLAN a été développée spécialement pour les communications commutées.

Cette méthode place un identificateur unique dans l'en-tête de chaque trame au moment où celle-ci est acheminée dans le backbone du réseau. L'identificateur est interprété et examiné par chaque switch avant tout broadcast ou transmission à d'autres commutateurs, routeurs ou équipements de station d'extrémité. Lorsque la trame quitte le backbone du réseau, le commutateur retire l'identificateur avant de transmettre la trame à la station d'extrémité cible.

Description de la norme :

Elle définit, en premier lieu, l'ajout de 2 octets dans la trâme Ethernet. Ces deux octets ajoutent plusieurs champs pour répondre à plusieurs besoins. La norme définit alors sur la trame Ethernet le champ VPID à 0x8100 pour désigner la trame 802.1Q.

Canonical Format Identifier (CFD) : Un champ protocole a

Pouvoir utiliser le 802.10 aussi bien sur Ethernet que sur Token Ring.

• **Priorité :** 3 bits utilisés pour coder 8 niveaux de priorité (de 0 à 7). On se sert de ces 8 eaux pour fixer la priorité des trames d'un VLAN par rapport à d'autres (exemple d'utilisation :

On un VLAN sur lequel on utilise la visioconférence (nécessitant beaucoup de bande nous favorisons un VLAN sur lequel on utilise passante) par rapport à un VLAN où l'on ne fait qu'envoyer et recevoir des mails)

• **VLAN ID (VID):** Le champ VID permet de fixer un identifiant sur 12 bits, c'est le champ d'identification du VLAN auquel appartient la trame.

Conclusion

Ce chapitre nous a permis de mieux cerner les notions de bases sur les réseaux, d'avoir une idée sur les différents types de réseaux ainsi que les différentes topologies et aussi d'éclaircir la notion de couche dans le modèle OSI et le modèle TCP / IP. Nous avons fini par une présentation de l'internet et surtout de l'intranet qui est le domaine de notre travail.

Dans le prochain chapitre, nous aborderons la sécurité des réseaux informatiques qui compte actuellement parmi les sujets les plus importants au sein d'une entreprise ou dans les réseaux informatiques.

Chapitre 3

La sécurité des réseaux

I. La sécurité des réseaux

3.1 Introduction

Notre dépendance vis à vis des ordinateurs est de plus en plus prononcée et l'informatique est devenue pour l'entreprise un outil obligatoire de gestion, d'organisation, de production et de communication. De ce fait les données mises en œuvre par le système d'information, les échanges internes et externes, la garde d'archives et d'informations personnelles sont exposés aux actes de malveillance de différentes natures. Ce qui a poussé nombreuses industries d'émerger dans le domaine de la sécurité informatique et des réseaux afin d'analyser leurs systèmes de façon correcte et d'élaborer des solutions adaptées à leurs besoins opérationnels. Dans ce chapitre, nous parlerons alors des principes de la sécurité des réseaux ainsi que de quelques solutions proposées.

3.2 Les principes de la sécurité informatique

3.2.1 Terminologies de la sécurité informatique

- **Vulnérabilité :** C'est une faille de sécurité dans un ou plusieurs systèmes, qui peut être exploitable ou non.
- **Attaque (exploit) :** Elle représente le moyen d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité.
- **Contre-mesure :** C'est une procédure ou technique permettant de résoudre une vulnérabilité ou d'empêcher une attaque spécifique.
- **Menace :** C'est un adversaire déterminé capable de monter une attaque exploitant une vulnérabilité.
- **Politique de sécurité :** Elle définit un certain nombre de règles, de procédures permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation.

3.3 Les objectifs de la sécurité

La sécurité informatique, d'une façon générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. La sécurité vise généralement ses objectifs :

- **La confidentialité :** Protection de données émises sur le réseau compréhensibles seulement par des entités autorisées.
- **Authentification :** Garantie que les données reçues proviennent bien de l'entité émettrice.
- **Intégrité :** Garantie que les données reçues n'ont subi aucune modification lors du transport dans le réseau.
- **Non répudiation** : C'est la propriété qui assure la preuve de l'authenticité d'un acte.

3.4 Les différents types d'attaques réseau

Vu que l'informatique est un domaine très vaste, alors le nombre de vulnérabilités présentes sur un système peut donc être important. Ainsi, on ne doit pas s'étonner si les attaques visant ces failles soient à la fois très variées et très dangereuses. Et pour cela, dans un premier temps, nous allons analyser ce que nous appelons « *anatomie d'une attaque* », puis dans un second temps, nous présenterons les différentes techniques d'attaques et observerons leurs déroulements.

3.4.1 Anatomie d'une attaque

Aussi nommés « les 5 P », ces verbes anglophones forment le squelette de toute attaque informatique : Probe, Penetrate, Persist, Propagate, Paralyze. Et voilà en détail chacune de ces étapes [11]:

- **Probe** : Consiste en la collecte d'informations, et cette collecte peut s'effectuer de plusieurs manières.
- **Penetrate** : C'est l'utilisation des informations récoltées pour pénétrer un réseau.
- **Persist** : Afin de pouvoir se ré-infiltrer ultérieurement, il est donc nécessaire de créer un compte avec des doigts de super utilisateur.
- **Propagate** : ça consiste à observer ce qui est accessible et disponible sur le réseau local.

- **Paralyse** : Sur cette étape, le pirate peut utiliser le serveur pour mener une attaque sur une autre machine, détruire des données ou encore endommager le système d'exploitation dans le but de planter le serveur.

3.4.2 Les techniques d'attaques réseaux

Si une personne mal intentionnée veut acquérir des ressources, il existe un grand nombre d'attaques qui lui permet de les appropriées, de les bloquer ou de les modifier.

Certaines requièrent plus de compétence que d'autres. Ces attaques ont plusieurs types à savoir :

a) Les attaques passives (Écoute du réseau)

Consistent à écouter sans modifier les données ou le fonctionnement du réseau, on site par exemple :

i. Le sniffing des mots de passe et des paquets :

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

ii. Le scanning :

Un scanner est un programme qui permet de savoir quels ports sont ouverts sur une machine donnée. Les Hackers utilisent les scanners pour savoir comment ils vont procéder pour attaquer une machine.

b) Les attaques actives

Ces attaques consistent à modifier des données, à se glisser dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau, exemple :

i. L'attaque par déni de service

Les attaques par déni de service en anglais (Denial of Service, Dos) sont destinées à refuser des services à des hôtes légitimes qui essayent d'établir des connexions. Les attaques par déni de service sont utilisées par les pirates pour bloquer les réponses système.

ii. Le spoofing IP

C'est une technique qui permet à un pirate de transmettre à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate. Donc il s'agit d'une modification des paquets envoyés afin de faire croire au destinataire qu'ils proviennent d'une autre machine.

3.5 Quelques solutions de sécurité

3.5.1 Le firewall (pare-feu)

Le **firewall** est un logiciel ou un matériel qui joue le rôle d'une barrière entre nous et le monde extérieur.

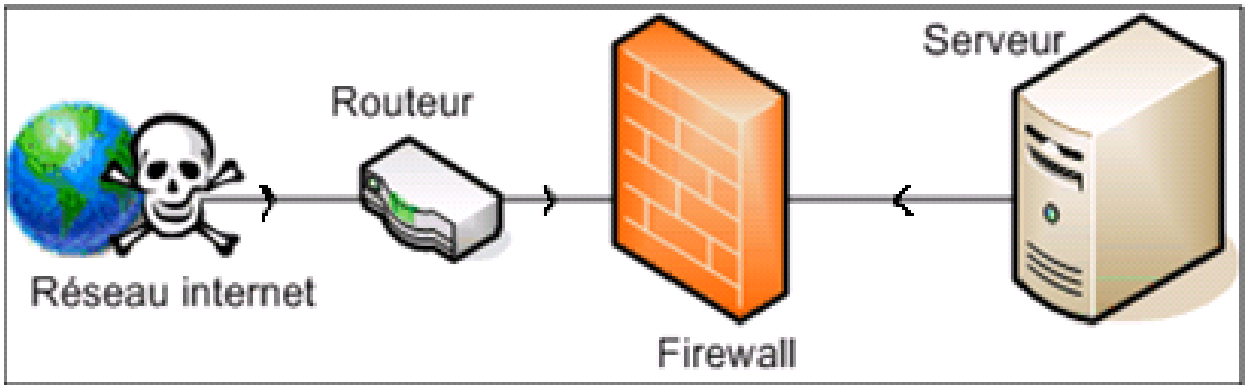


Figure 3.1 : *Architecture d'un Firewall*

Le pare-feu permet de filtrer les paquets de données échangés avec le réseau, donc il représente une *passerelle* filtrante comportant au minimum les interfaces réseau suivantes :

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

3.5.2 Contre quoi protège-t-il ?

Certains firewalls autorisent seulement le passage du courrier électronique. Ainsi, ils protègent contre toute autre attaque qu'une attaque basée sur le service de courrier. D'autres firewalls sont plus tolérants, ils bloquent uniquement les services reconnus comme étant dangereux.

En générale, les firewalls sont configurés pour empêcher tout accès non authentifiés du réseau externe. Ceci, plus qu'autre chose, protège les machines des réseaux internes contre les vandales qui essaient de s'y loger, mais laisse un accès libre aux utilisateurs s'ils veulent communiquer avec l'extérieur.

Les firewalls sont intéressants dans le sens ou ils constituent un point unique ou la sécurité peut être imposée. Tous les échanges passeront par lui. Des résumés de trafic, des statistiques sur ce trafic, ou encore toutes les connexions entre les deux réseaux pourront être données.

3.5.3 Contre quoi ne protège-t-il pas ?

Logiquement un firewall ne peut pas protéger contre des attaques qui ne passent pas par lui, ni contre les traitres et les idiots à l'intérieur de l'entreprise. Si un espion industriel décide de faire sortir des données, il y arrivera.

Les firewalls n'assurent pas parfaitement la protection contre les virus. Pour transférer des fichiers il y a différentes manières de les coder. Les utilisateurs doivent être vigilants et respecter un certain nombre de règles, la première est bien évidement de ne jamais ouvrir un fichier attaché à un mail sans être sûr de sa provenance, car un firewall ne pourra pas remplacer leurs attentions et leurs consciences.

3.5.4 Les différents types de firewalls

a. Les firewalls bridge

Ce sont des firewalls très répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus. Leurs interfaces ne possèdent pas d'adresse IP, et leur rôle consiste en la transmission des paquets d'une interface à une autre en leur appliquant des règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable pour un hacker. En effet, quand une requête ARP est émise sur le câble réseau, le firewall ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination.

b. Les firewalls matériels

Ils sont directement intégrés dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur avantage est la simplicité d'interaction avec les autres fonctionnalités du routeur.

Leurs niveaux de sécurité est de plus très bon. Néanmoins, il faut savoir que l'on est totalement dépendant du constructeur du matériel pour cette mise à jour, ce qui peut être, dans certains cas, assez contraignant. Enfin, seules les spécificités prévues par le constructeur du matériel sont implémentées. Cette dépendance induit que si une possibilité nous intéresse sur un firewall d'une autre marque, son utilisation est impossible. Il faut donc bien déterminer à l'avance son besoin et choisir le constructeur du routeur avec soin.

c. Les firewalls logiciels

Présents à la fois dans les serveurs et les routeurs, on peut les classer en :

- ***Les firewalls personnels :***

Ils sont généralement commerciaux et ils sont destinés pour sécuriser un ordinateur particulier. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

- ***Les firewalls plus « sérieux » :***

Ils sont généralement utilisés sous linux, car cet OS offre un niveau de sécurité élevé et un contrôle plus adéquat, en générale ils ont pour but d'avoir le même comportement que les firewalls matériels des routeurs, ils sont configurables à la main. Le plus courant est iptables (anciennement ipchains), qui utilise directement le noyau linux.

3.5.6 Fonctionnement d'un système firewall

Un système firewall contient un ensemble de règles prédéfinies permettant :

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

Ces règles permettent la mise en œuvre d'une méthode de filtrage dépendant de la **politique de sécurité** adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées,
- Soit d'empêcher les échanges qui ont été explicitement interdits.

Sans nul doute la première méthode est la plus sûre, mais toutefois elle impose une définition précise et contraignante des besoins en communication. [9]

3.5.7 Les différents types de filtrages

a. Le filtrage simple de paquet « *stateless packet filtering »*

C'est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet en effectuant une analyse sur les en-têtes de chaque paquet de données (*datagramme*) échangé entre une machine du réseau interne et une machine du réseau externe, ces paquets transitent par le firewall et possèdent les en-têtes suivants :

- L'adresse IP de la machine émettrice. (Identification de la machine émettrice).
- L'adresse IP de la machine réceptrice. (Identification de la machine cible).
- Le type de paquet (TCP, UDP, ICMP … etc.).
- Le numéro de port[4] .

Cela nécessite de configurer le Firewall ou le routeur par des règles de filtrages, généralement appelées des ACL (Access Control Lists).

Le tableau ci-dessous donne des exemples de règles de firewall :

Régles	**Action**	**Ip source**	**Ip destination**	**Protocol**	**Port source**	**Port destination**
1	Accept	192.168.10.20	194.154.192.3	Tcp	Any	25
2	Accept	Any	192.168.10.3	Tcp	Any	80
3	Accept	192.168.10.0/24	Any	Tcp	Any	80
4	Deny	Any	Any	Any	Any	Any

Tab 3.1 : Exemple de règles du firewall

Les ports reconnus (dont le numéro est compris entre 0 et 1023) sont associés à des services courants (les ports 25 et 110 sont par exemple associés au courrier électronique, et le port 80 au Web). La plupart des dispositifs firewall sont au minimum configuré de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables.

b. Le filtrage de paquet avec état *« stateful inspection»*

L'amélioration par rapport au filtrage simple, est la conservation de la trace des sessions et des connexions dans des tables d'états internes au Firewall. Le Firewall prend alors ses décisions en fonction des états de connexions, et peut réagir dans le cas de situations

[4] Un port : est un numéro associé à un service ou une application réseau.

protocolaires anormales. Ce filtrage permet aussi de se protéger face à certains types d'attaques DoS.

Il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de filtrage dynamique de paquets est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions entre le client et le serveur.

Un dispositif pare-feu de type « stateful inspection » est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu ; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

Si le filtrage dynamique est plus performant que le filtrage de paquets basique, il ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications. Or ces vulnérabilités représentent la part la plus importante des risques en termes de sécurité.

Une fois que l'accès à un service a été autorisé, il n'y a aucun contrôle effectué sur les requêtes et réponses des clients et serveurs.

c. Le filtrage applicatif « ou pare-feu de type proxy »

Le filtrage applicatif est comme son nom l'indique est réalisé au niveau de la couche Application. Ce type de filtrage est appelé généralement « passerelle applicative » (ou *« proxy »*) car les requêtes sont traitées par le Proxy par exemple une requête de type Http sera filtrée par un processus proxy Http. Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse toutes les règles protocolaires des protocoles qu'il doit filtrer.

Donc le pare-feu proxy est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif.

Le premier problème qui se pose est la finesse du filtrage réalisé par le proxy. Il est extrêmement difficile de pouvoir réaliser un filtrage qui ne laisse rien passer, vu le nombre de protocoles de niveau 7. En outre le fait de devoir connaître les règles protocolaires de chaque protocole filtré pose des problèmes d'adaptabilité à de nouveaux protocoles.

3.6 Architecture DMZ

Quand certaines hôtesses du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, etc.), on est souvent appelé à créer une nouvelle interface vers un réseau différent, qui est accessible de l'extérieur ainsi que du réseau interne, et cela sans risquer de nuire à la sécurité de l'entreprise. Et c'est ce qu'on appelle *« zone démilitarisé »* (notée DMZ pour DeMilitarized Zone) pour désigner cette zone isolée qui contient des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile.

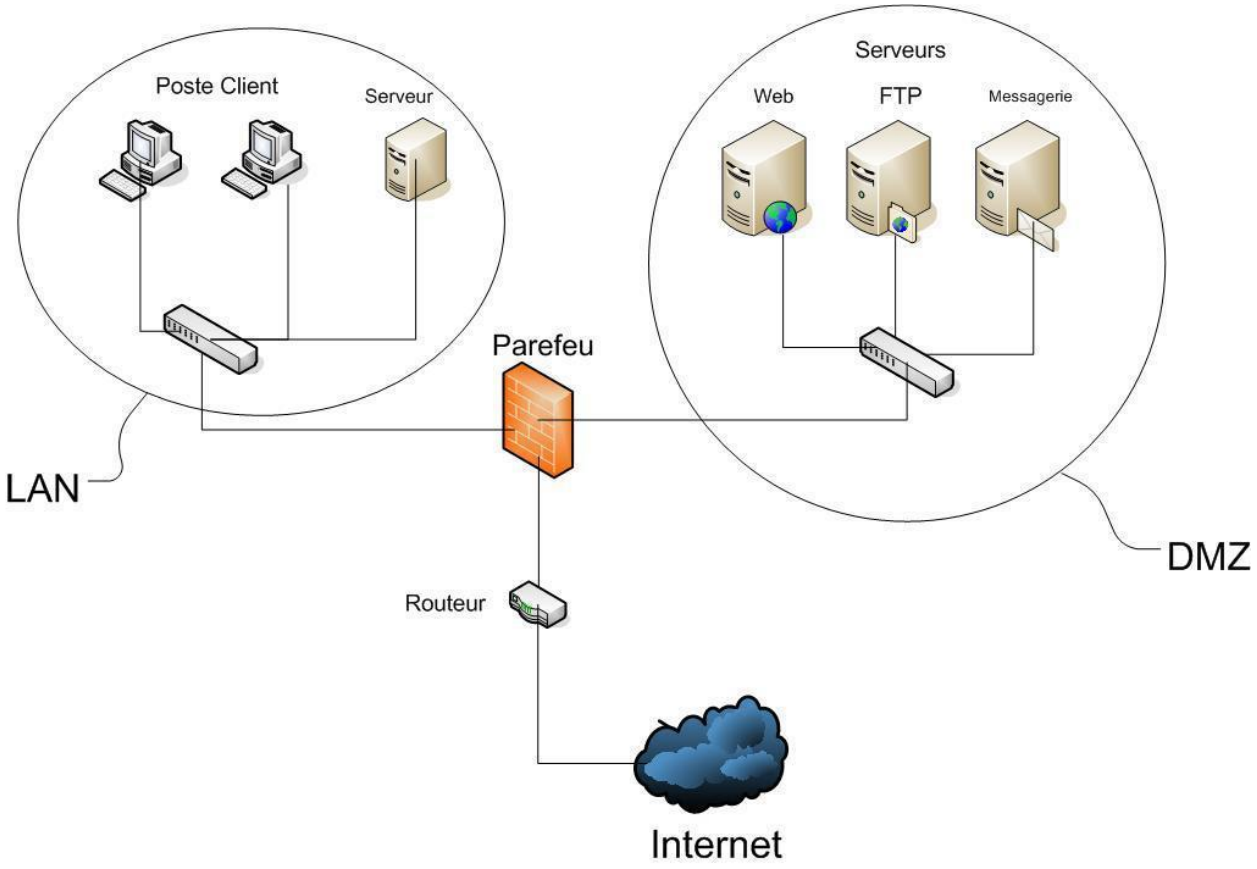


Figure 3.2 : *Architecture DMZ*

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Autorisation du trafic du réseau externe vers la DMZ,
- Interdire le trafic du réseau externe vers le réseau interne,
- Autorisation du trafic du réseau interne vers la DMZ,
- Autorisation du trafic du réseau interne vers le réseau externe,

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise [9].

3.7 La cryptographie

La cryptographie permet de se protéger contre de nombreuses faiblesses de sécurité et de contrôler la sécurité des systèmes d'information. Cette science peut cependant être aussi utilisée par les auteurs de virus afin de renforcer leur caractère nocif. La cryptographie permet d'assurer l'authenticité, l'intégrité et la confidentialité des données.

3.7.1 La Cryptographie Symétrique

Elle est basée sur une clé unique partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages.

3.7.2 La Cryptographie Asymétriques (à clé publique)

Contrairement à la cryptographie symétrique, la cryptographie asymétrique utilise deux clés : un est privé et n'est connue que par l'utilisateur, l'autre est publique et donc accessible par tout le monde.

3.8 Les systèmes de détection d'intrusions (IDS)

Un système peut subir plusieurs attaques, il est donc nécessaire d'avoir un logiciel spécialisé capable de surveiller les données qui transitent sur ce système, et qui peut réagir si des données semblent suspectes. Les systèmes de détection d'intrusions (IDS) conviennent parfaitement pour réaliser cette tâche [11].

3.8.1 Les différentes sortes d'IDS

Les IDS se caractérisent par leur domaine de surveillance. Celui-ci peut se situer au niveau d'un réseau d'entreprise, d'une machine hôte, d'une application…, il existe trois sortes distinctes d'IDS :

a. La Détection d'Intrusion Réseau (N-IDS) *(Network Based Intrusion Detection System)*

Le rôle essentiel d'un IDS réseau est l'analyse et l'interprétation des paquets circulant sur ce réseau. Les N-IDS assurent la sécurité au niveau du réseau en utilisant principalement des capteurs qui sont souvent des hôtes dont leur seule tâche est l'analyse du trafic réseau et d'envoyer une alerte à une console sécurisée. Ils agissent de manière invisible ce qui les rend difficile à localiser et à atteindre par un attaquant. Les capteurs peuvent être placés avant ou après le pare-feu, ou encore dans une zone sensible que l'on veut spécialement protéger.

b. La détection d'Intrusion basée sur l'hôte H-IDS (*Host Based Intrusion Detection System)*

Ils analysent seulement l'information concernant cet hôte. Ces systèmes n'ont pas à contrôler le trafic du réseau mais uniquement les activités d'un hôte donné, ce qui leur donne une grande précision sur les types d'attaques subies.

c. Détection d'Intrusion basée sur une Application

Les IDS basés sur les applications sont un sous-groupe des IDS hôtes (H-IDS), mais on les mentionne séparément. Ces IDS sont mis entre l'utilisateur et son application donc contrôlent l'interaction entre un utilisateur et un programme. Puisqu'ils opèrent ainsi il est facile de filtrer tout comportement notable.

3.9 Les VLANs (Virtual Local Area Network)

Le commutateur (switch) a pour fonction de permettre la cohabitation de différents sous-réseaux physiques, qui ne communiquent pas nécessairement entre eux, sur le même équipement.

Pour atteindre cet objectif, le principe du VLAN (Virtual LAN) a été créé. À la base, un port du commutateur est assigné à un VLAN particulier et seuls les ports du même VLAN peuvent s'échanger de l'information.

Il existe plusieurs méthodes de construction de VLAN :

- **VLAN par port** : il est défini en associant chaque VLAN à un port du commutateur. Son avantage, c'est qu'il est facile d'emploi. L'inconvénient est qu'on ne définit qu'un seul VLAN par port.
- **VLAN basée sur l'adressage MAC** : il s'agit de dire quelles adresses MAC (adresses physiques) appartiennent à tel VLAN. L'avantage est que des stations sur un même port peuvent être sur des VLAN différents. L'inconvénient, c'est la difficulté de manipulation des adresses MAC.
- **VLAN par sous-réseau** (niveau 3) : il s'agit de définir, en utilisant les adresses IP *(Internet Protocol*), un VLAN par sous réseau. Cela permet une configuration plus facile. De plus, des stations sur un même port peuvent appartenir à des VLAN différents.
- **VLAN par Protocole** : est obtenu en associant un réseau virtuel par type de protocole du réseau (par exemple TCP/IP), regroupant ainsi toutes les machines utilisant le même protocole dans un même VLAN.

3.10 Les listes de contrôles d'accès (ACL)

Une ACL est une liste de règles permettant de filtrer ou d'autoriser du trafic sur un réseau en fonction de certains critères (IP source, IP destination, port source, port destination, protocole. Une ACL permet de soit autoriser du trafic (permit) ou de le bloquer (deny). Il est possible d'appliquer au maximum une ACL par interface et par sens (input/output). Une ACL est analysée par l'IOS de manière séquentielle. Dès qu'une règle correspond au trafic, l'action définie est appliquée, le reste de l'ACL n'est pas analysé. Toute ACL par défaut bloque tout trafic. Donc tout trafic ne correspondant à aucune règle d'une ACL est rejeté.

II. La sécurité dans les routeurs

1. Architecture d'un routeur

À l'instar d'un ordinateur personnel, un routeur par exemple de type CISCO est équipé d'un system d'exploitation nommé **IOS** (Internet Operating System). IOS fournit des fonctionnalités qui permettent à un routeur Cisco d'envoyer et de recevoir du trafic tel que les fonctions de routage et un accès fiable et sécurisé aux ressources du réseau.

Cette plate-forme logicielle est proposée aux clients sous la forme d'images. Ces images sont chargées sur un routeur avant de commencer le processus de configuration.

Chaque routeur possède les mêmes composants de base qu'un ordinateur standard. Il est doté d'un processeur (UC), de mémoire, ainsi que de diverses interfaces d'entrée / sortie.

1.1. Composants internes

Tous les routeurs Cisco ont une architecture interne qui peut être représentée par [12] :

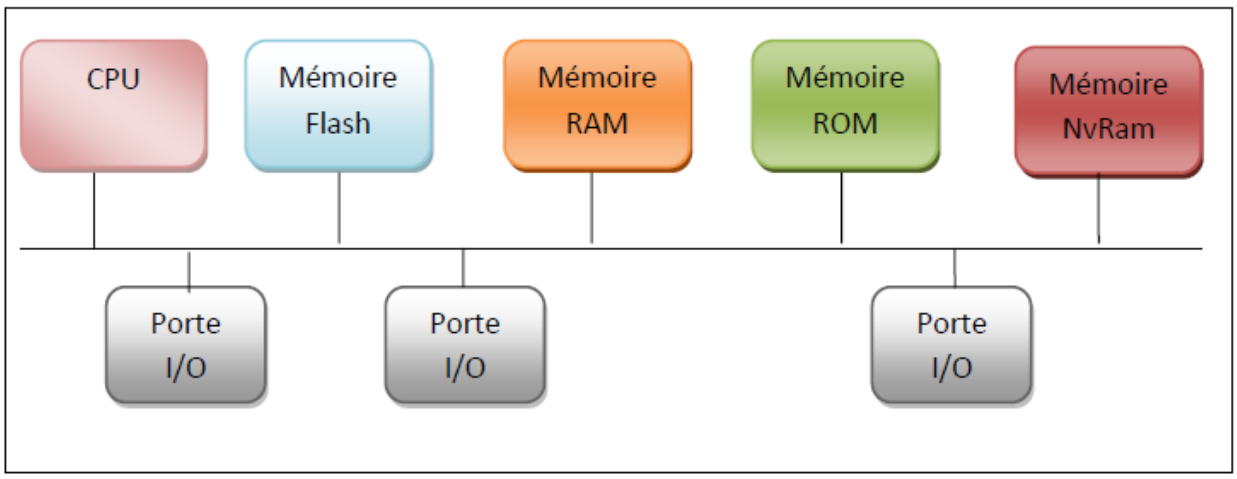


***Figure 3.3** : Composants internes d'un routeur*

- **Mémoire NvRam : (***Non-Volatile Random Access Memory*), c'est la Ram non volatile, elle est utilisée comme emplacement de stockage pour le fichier de configuration du routeur au démarrage. Elle solutionne le problème de la coupure de l'alimentation, puisqu'elle conserve les données.
- **Une mémoire ROM :** Contient le *BootStrap,* la séquence de démarrage du routeur. Cette mémoire n'est utilisée qu'au démarrage du routeur.
- **Une mémoire RAM :** Elle est utilisée par le système d'exploitation pour maintenir les informations durant le fonctionnement. Elle peut contenir les tampons, les tables de routage, la table ARP, la configuration mémoire et un nombre important d'autres choses. Et comme c'est de la RAM, lors de la coupure de l'alimentation, elle est effacée.
- **Une mémoire FLASH :** La mémoire flash représente une sorte de ROM effaçable et programmable, sur beaucoup de routeurs, la mémoire flash est utilisée pour maintenir une image IOS.
- **Unité centrale (CPU) :** L'unité centrale, ou le microprocesseur, est responsable de l'exécution du système d'exploitation (chez Cisco, c'est IOS) du routeur.
- **Les portes I/O** : l'interfaçage vers le monde extérieur est important. Chaque routeur possède des interfaces LAN qui sont en général des ports Ethernet et des interfaces WAN incluant des ports séries.

1.2. Composants externes

Les composants externes d'un routeur sont constitués d'un certain nombre de ports (console, auxiliaire), de slots (NM, WIC), d'interfaces (LAN, WAN), une alimentation et un interrupteur.

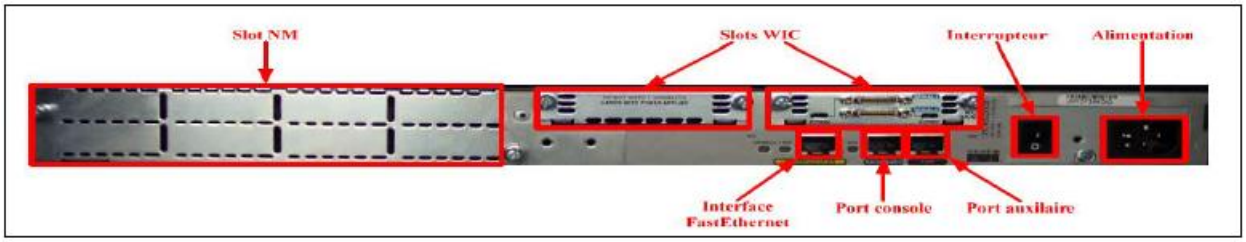


Figure 3.4 : Vue arrière d'un routeur Cisco

2. Fonction de routage dans les routeurs

Les routeurs assurent la fonction du routage, qui représente une façon de déterminer le trajet optimal des données entre l'expéditeur et le destinataire. Le routage est basé sur un algorithme lié au protocole de routage. L'algorithme prend en considération la durée moyenne de transmission, la charge du réseau, la longueur totale du message. Il permet au trafic provenant d'un réseau local d'atteindre sa destination après avoir traversé plusieurs réseaux intermédiaires.

2.1. Table de Routage

Les routeurs disposent de tables de routage IP. Cette table contient des informations sur les destinations et la manière de les atteindre. Une entrée de table de routage contient la destination et le routeur de prochain pas (next hop) pour transmettre le datagramme.

2.2. Type de Routage

2.2.1 Routage statique

Le routage statique consiste à construire dans chaque nœud, une table indiquant pour chaque destination, l'adresse du nœud suivant. Cette table est construite par l'administrateur du réseau lors de configuration du réseau et à chaque changement de topologie.

2.2.2 Routage dynamique

Le routage dynamique utilise un protocole de routage dont le principe est la diffusion périodique sur le réseau des informations de routage. Les équipements de routage échangent leurs informations de routage et mettent à jour leurs tables de routage. Pour faciliter le travail de ces protocoles de routage, il a été nécessaire de hiérarchiser la topologie d'Internet. Ce réseau est composé de systèmes autonomes (AS5) ayant chacun sa propre politique de routage interne, et communiquant entre eux via un protocole de routage externe [10].

2.3. Protocole de Routage

Le protocole de routage définit la manière dont les routeurs s'échangent des informations afin de déterminer la meilleure route vers une destination. Il existe deux familles de protocoles de routage ; les protocoles de routage Internes (IGP), et les protocoles de routage externes (EGP). [13]

2.4. Choix d'un protocole de routage

Il existe beaucoup de protocoles, en choisir un est relativement facile. Pour des réseaux locaux, RIP est le plus courant. OSPF n'est pas encore largement disponible.

Pour un protocole extérieur, on a rarement le choix du protocole. Deux systèmes autonomes qui échangent des informations doivent utiliser le même protocole. Ce choix est souvent EGP même si BGP se diffuse de plus en plus.

3. Vulnérabilité des routeurs

Comme les routeurs sont des passerelles vers d'autres réseaux, ils constituent des cibles évidentes et sont soumis à une variété d'attaques. Voici quelques exemples des différents problèmes de sécurité rencontrés :

- **La configuration**

Un routeur est semblable à un ordinateur dans lequel il y a plusieurs services permis par défaut. Beaucoup de ces services sont inutiles et peuvent être utilisés par un attaquant pour la collecte d'informations ou pour l'exploitation.

- **Gestion du Routeur**

Le contrôle de l'accès à un routeur par des administrateurs est une tâche importante.

Il y a deux types d'accès :

- **L'accès local**

L'accès local implique une connexion directe à un port de console sur le routeur avec un terminal ou un ordinateur portable,

- **L'accès à distance Il** représente généralement la permission Telnet, pendant l'accès à distance, les mots de passes Telnet sont envoyés en clair sur le réseau, donc une écoute sur le réseau suffit pour les connaître.

Ces failles peuvent être à l'origine des différentes attaques qui visent à prendre contrôle sur le routeur, ce qui veut dire prendre le contrôle sur l'acheminement des données dans le réseau.

4. Les routeurs et leurs rôles dans la sécurité des réseaux

Les routeurs peuvent jouer un rôle dans la garantie de la sécurité des réseaux. Ils exécutent beaucoup de travaux différents dans les réseaux modernes.

Les routeurs remplissent les rôles suivants :

- Filtre les utilisateurs ;
- Fournir un accès aux segments de réseau et aux sous-réseaux.

4.1. Filtrage des paquets

Le filtrage des paquets contrôle l'accès à un réseau en étudiant les paquets entrants et sortants, et en les transmettant ou en les stoppant en fonction de tests prédéfinis.

Un routeur filtre les paquets lors de leur transmission ou de leur annulation conformément aux règles de filtrage. Lorsqu'un paquet accède à un routeur de filtrage, certaines informations de son en-tête sont extraites. Conformément aux règles de filtrage, le routeur décide alors si le paquet peut être transmis ou rejeté. Le filtrage des paquets fonctionne sur la couche réseau du modèle OSI (Open Systems Interconnection) ou sur la couche Internet de TCP/IP.

Un routeur de filtrage des paquets, en tant que périphérique de couche 3, se réfère aux règles pour déterminer s'il doit autoriser ou refuser le trafic en fonction des adresses IP source

et de destination, du port source, du port de destination et du protocole des paquets. Ces règles sont définies en fonction des listes de contrôle d'accès.

Conclusion

Nous avons vu en premier lieu dans ce chapitre les principes de la sécurité, les terminologies, les objectifs fixés par la sécurité, les mécanismes d'une attaque. En deuxième lieu nous avons présenté quelques solutions qui permettent d'assurer une politique de sécurité efficace tel que le firewall, la cryptographie, les IDS, les Vlans et enfin les listes de contrôle d'accès.

Chapitre 4

Etude préalable

4.1 Introduction

Le recours a la modélisation est une étape indispensable pour le d'enveloppement, car elle permet d'anticiper, de prévoir et d'étudier les informations d'un système. ` Nous avons opté pour l'UML comme langage de modélisation et la démarche de développement UP (Unified Process). Nous introduirons dans ce chapitre l'étude détaillée et la modélisation conçue en termes de diagramme approprie

❖ Présentation du projet

Le projet à réaliser s'intitule « Conception et réalisation d'une application mobile Android pour la configuration des modem routeur » Une application mobile qui a comme but de faciliter Aux utilisateurs la gestion de leur réseau local avec la possibilité de configurer le modem routeur avec toute facilité

4.2 Problématique

Pour la bonne gestion d'un réseau local, les utilisateurs doivent avoir l'accès totale aux données qui circule via leur wifi, et évité les conflits des adresse IP, la non-reconnaissance de l'appareil connecté…etc.

Comment l'utilisateur pourra-t-il gérer son réseau local ?
La configuration du routeur sera-t-il plus facile avec cette application ?

Cependant, il existe quelques difficultés pour accomplir cette tâche, nous pourrons citer :

- Les coupures d'internet
- L'information confidentiel fournis par l'actel (Algérie télécom)
- La méthode de l'authentification
- L'étendu du réseau local
- Le model et la plateforme du périphérique a configurer
- Réalisation d'une interface assez basic et plus facile pour une certaine catégorie d'utilisateur accessible à tous

4.3 Objectif de travaille

Pour la réalisation de ce travail on va prendre n'importe quel routeur, et notre but sera de créer une application mobile pour la configuration des modems (router wifi) permettra à l'utilisateur de :

1. Gérer à distance.
2. Gagner du temps.
3. Configurer l'adresse IP.
4. Changer le mot de passe.
5. Gérer les utilisateurs.
6. Information wifi.

4.3.1 Idée générale sur notre application

C'est une application qui nous permet de configurer un modem / routeur WiFi et de contrôler ses paramètres en tant qu'administrateur, en général, il contient tous les outils qui permettent vous gérez et contrôlez et configurez n'importe quel routeur. Surveiller et mesurer tout ce qui le concerne.

Détection automatique de la page de configuration du routeur WiFi, quelle qu'elle soit 192.168.1.1 ou 192.168.0.1 ou 192.168.1. Ou 10.0.0, l'application ouvrira automatiquement la page de configuration du routeur et vous fera gagner du temps, vous pouvez configurer votre routeur et modifier ses paramètres facilement en quelques clics.

- **Qui utilise votre WiFi :** L'application analysera le réseau pour vous et détectera qui est connecté à votre routeur, par l'adresse IP et l'adresse MAC.
- **Générateur de mot de passe** : Un outil pour créer un mot de passe fort aléatoire, qui vous aidera à protéger votre connexion WIFI.

4.4 Les besoins spécifiques

Comme les bonnes questions représentent la moitié de la réponse dans la plupart des domaines, en informatique une bonne spécification des besoins et primordiale en effet elle représente le travail le plus délicat et le plus significatif. Mais elle même repose sur une bonne spécification des besoins qui n'est autres que la question que doit se poser tout développeur au

début de son travail qu'est-ce qu'on veut réaliser, cette phase consiste à mieux comprendre le contexte du système, il s'agit de déterminer les fonctionnalités et les acteurs et d'identifier les cas d'utilisation initiaux.

4.5 Identifications des besoins

4.5.a Les besoins techniques

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

• **La rapidité du traitement** : en effet, vue le nombre d'utilisateur d'internet de nos jours il est impérativement nécessaire que la durée d'exécution des traitements s'approche le plus possible du temps réel, pour accédés à l'information demandé.

• **La performance** : une application doit être avant tout performante c'est-t-à-dire à travers ces fonctionnalités, elle doit répondre à toutes les exigences des usagers d'une manière optimale.

• **La convivialité** : la future application doit être facile à utiliser. En effet les interfaces utilisateur doivent être conviviales, c'est à dires simple, ergonomiques et adaptes à l'utilisateur.

• **La confidentialité** : vu que les données manipulées par notre application sont critiques, nous devons garantir une sécurité optimale. Ainsi, les droits d'accès au système doivent être attribués, afin d'assurer la sécurité des données.

4.5.b Les besoins fonctionnels

Ces derniers représentent la principale fonctionnalité du system. Ces besoins proviennent généralement des utilisateurs du système. Cette application devra permettre la : `

- Configurer l'adresse IP.
- Changer le mot de passe Wifi
- Gérer les périphériques connectés
- Sécuriser le réseau local

4.6 Identifications des acteurs

• L'utilisateur : ce dernier est lui-même l'administrateur il possède le droit d'accéder aux différentes interfaces de l'application

4.7 Diagramme de cas d'utilisation

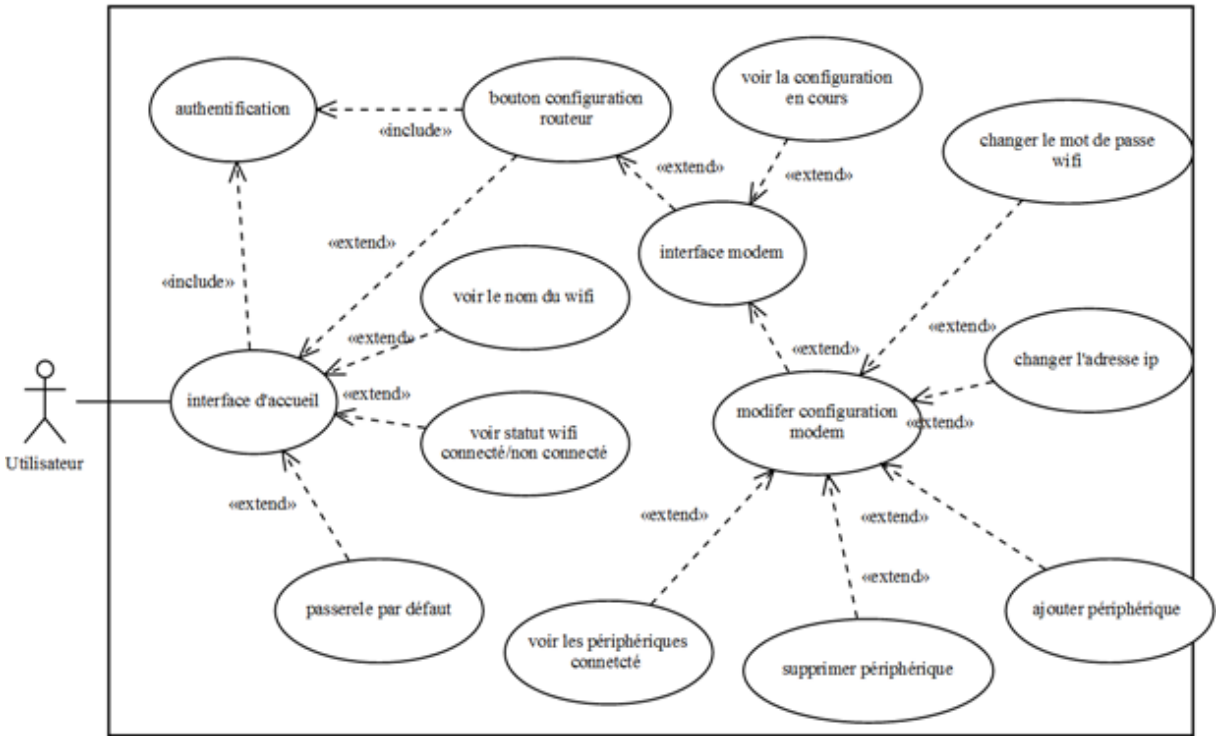


Figure 4.1 : *le diagramme de cas d'utilisation*

4.8 Les diagrammes de de séquence

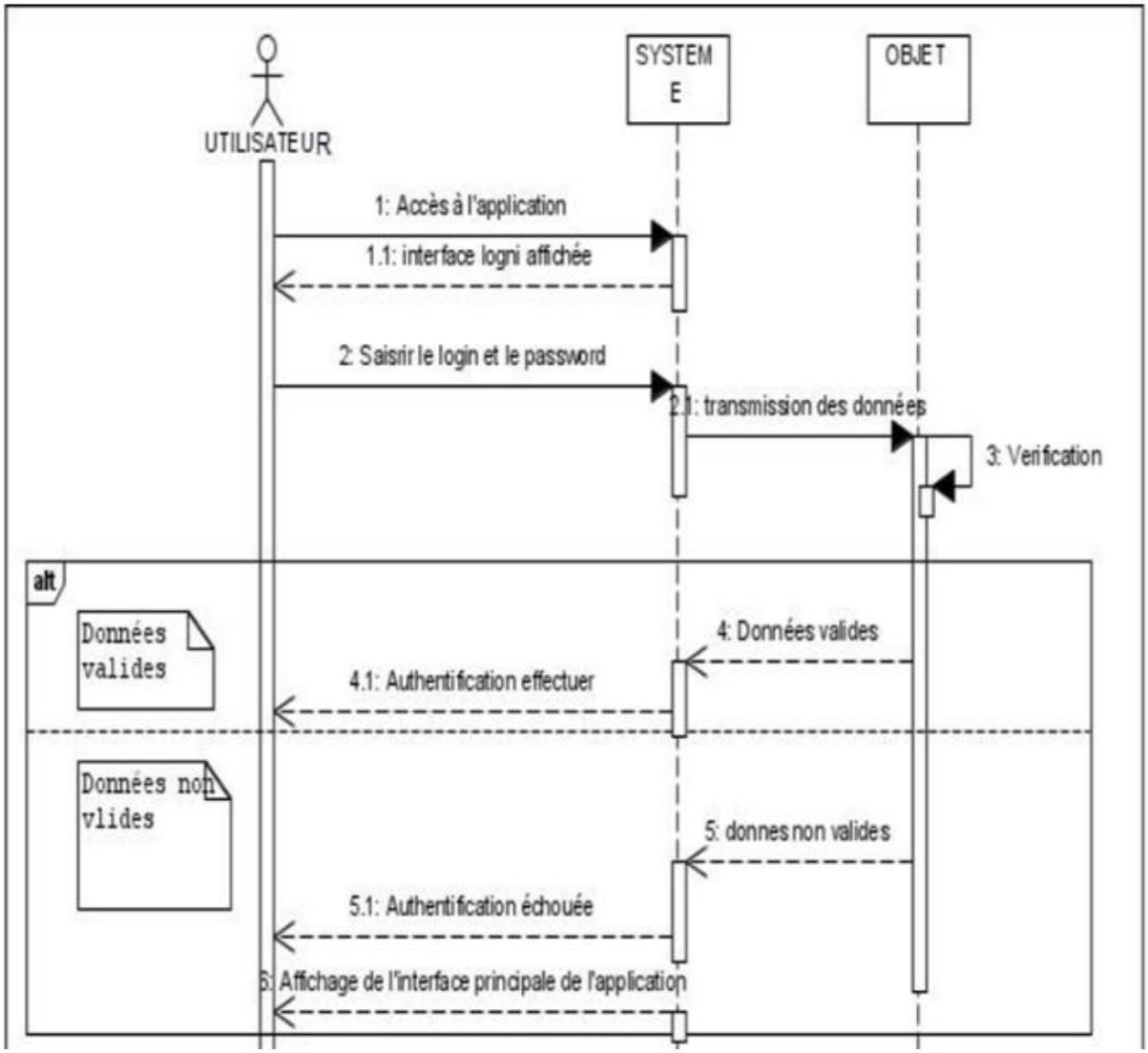


Figure 4.2 : *Le diagramme de séquence*

Conclusion

Dans ce chapitre nous avons présente l'analyse et la conception de notre application en utilisant le langage de modélisation UML. ´ Apres avoir définit la solution proposée, nous allons passer à la réalisation de cette solution, qui sera l'objectif du prochain chapitre.

Chapitre 5

Réalisation

Réalisation

5.1 Introduction

La réalisation représente l'étape qui suit immédiatement la phase de conception. C'est l'aboutissement final de notre projet et c'est la raison d'être du projet lui-même.

Dans ce chapitre nous allons présenter dans un premier lieu l'environnement matériel et logiciel de développement, par la suite, nous décrirons la phase d'implémentation en nous basant sur quelques interfaces.

5.2 Environnement de travail

5.2.1 Environnement matériel

Pour la réalisation de notre projet, nous avons À utiliser un ordinateur HP caractérisé par :

- Système d'exploitation : Windows 10.
- Processeur : Intel R Core(TM) i5 4300U 2.40 GHz.
- Mémoire vive : 8 Go.
- Disque Dur : 750 Go.

5.2.2 Environnement logiciel

a) Le language :

JAVA : « Java est un langage de programmation orienté objet, développé par Sun Microsystems. Il permet de créer des logiciels compatibles avec de nombreux systèmes d'exploitation (Windows, Linux, Macintosh, Solaris). Java donne aussi la possibilité de développer des programmes pour téléphones portables. » [14]

Figure 5.1 : *logo java*

b) Les outils

Android Studio : Android Studio est un environnement de développement intégré (IDE) pour le développement sur la plateforme Android. Il a été annoncé en mai 2013. Android est disponible librement sous la licence Apache 2.0. Basé sur le logiciel IDEA de JetBrains 'IntelliJ', Android Studio est conçu spécifiquement pour le développement Android. Il est disponible en téléchargement sur les systèmes d'exploitation ; Windows, Mac OS et Linux.[15]

Android Studio permet principalement d'éditer les fichiers Java et les fichiers de configuration d'une application Android. Il propose aussi des outils pour gérer le développement d'applications multilingues et permet de visualiser la mise en page des différents types et tailles d'écrans avec des résolutions variées simultanément [16].

Figure 5.2 : *Logo android studio*

Java Development Kit (JDK) : « Le Java Development Kit (JDK) désigne un ensemble de bibliothèques logicielles de base du langage de programmation Java, ainsi que les outils avec lesquels le code Java peut être compilé, transformé en bytecode destiné à la machine virtuelle Java. »[17]

Figure 5.3 : *Logo JDK*

Android Software Development Kit (SDK) : Le SDK est un ensemble d'outils que met à disposition Google afin de nous permettre de développer des applications pour Android. Il est disponible pour Windows, MacOs X et linux et inclut des outils ainsi qu'un émulateur Android pour exécuter des applications.[18]

Figure 5.4 : *Logo SDK*

5.3 Structure de l'application

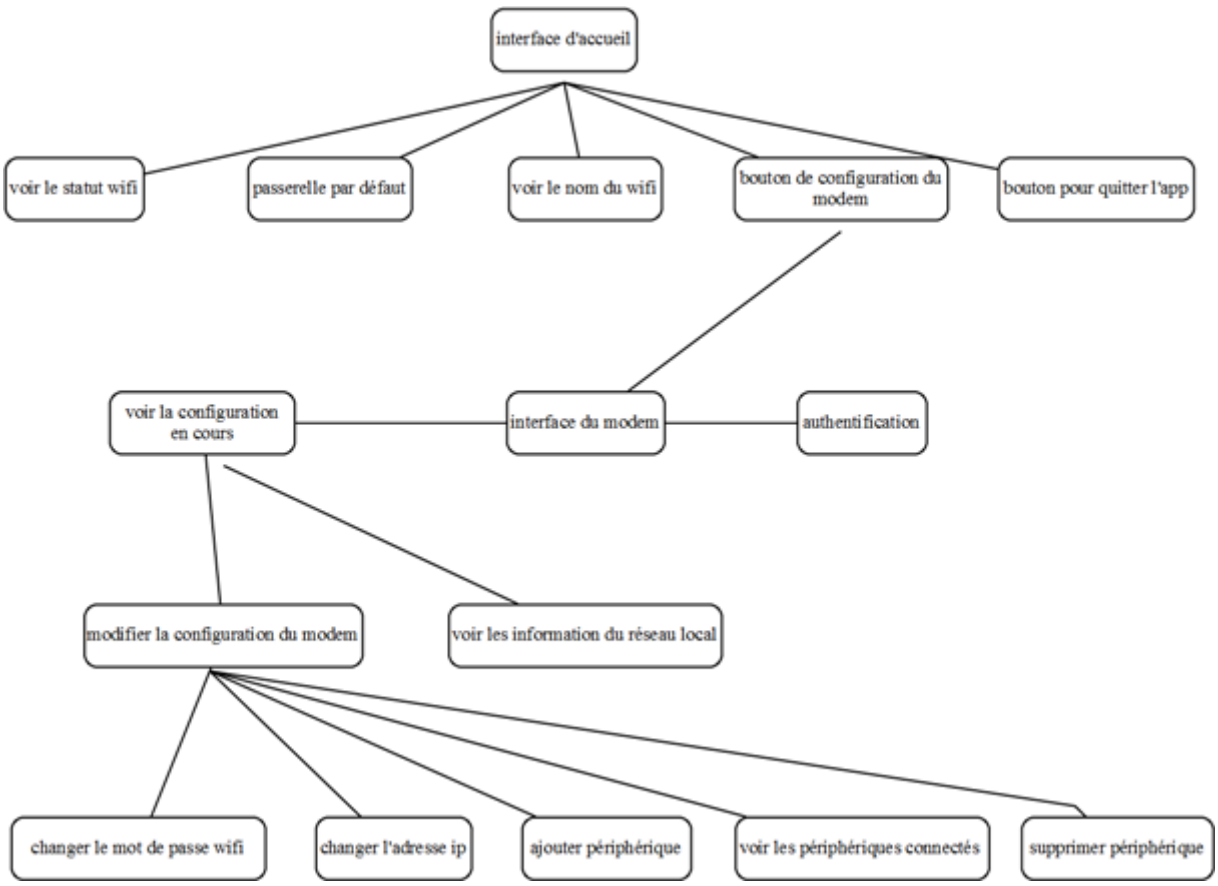


Figure 5.5 : *plan de l'application*

5.4 Captures d'interfaces de l'application

Dans ce chapitre, nous fournirons toutes les interfaces de notre application :

La (Figure) illustre l'Interface du logo de l'application. Cette page dure trois secondes au maximum

Figure 5.6 : *Logo de l'application*

Lorsque l'application se lance, l'interface d'accueil comme présenté sur la (Figure 5.7) ci-dessous se lance et affiche des informations sur le wifi (id) et le statut (connecté/non connecté), la passerelle par défaut avec le Botton de configuration du routeur et dans le haut on peut voir l'entête Home (accueil) deux buttons à droite et à gauche, un pour quitter l'application et l'autre pour plus d'information sur l'application

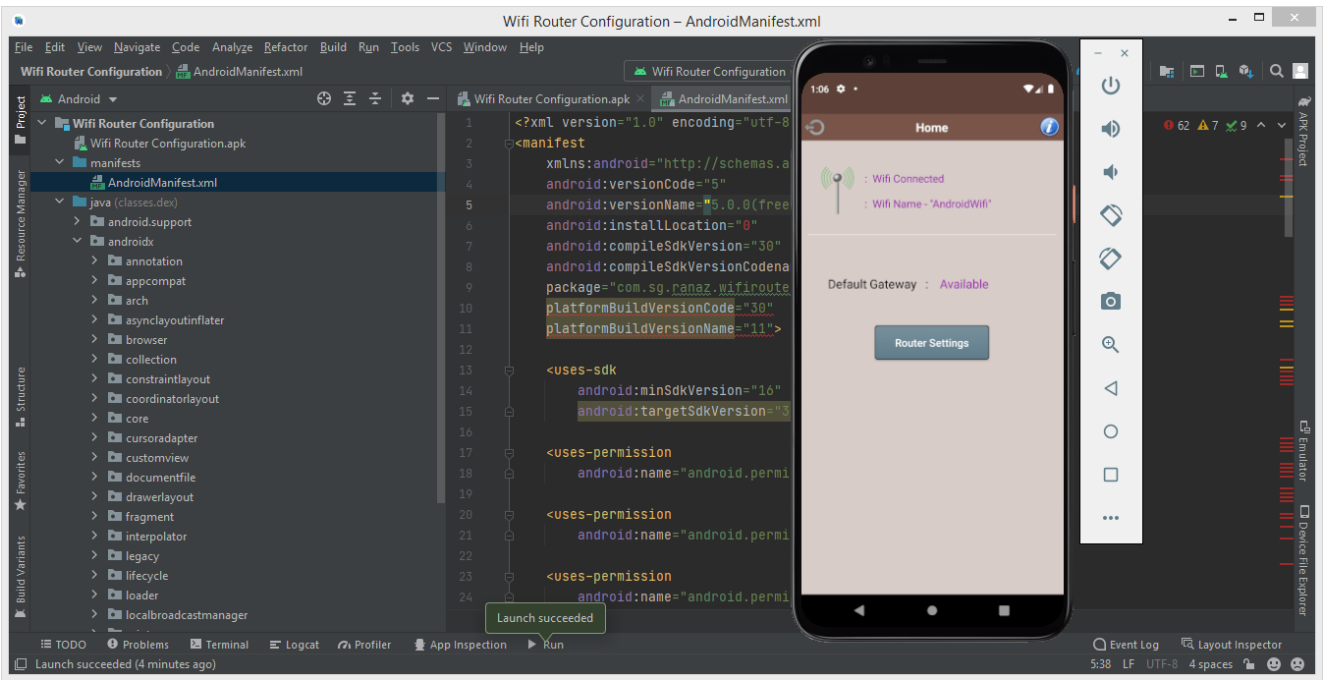


Figure 5.7 : *interface d'accueil de l'application*

Lorsque l'utilisateur clique sur le bouton de "router setting", une interface de modem qui est installé à domicile s'ouvre, il faut introduire le nom d'utilisateur et le mot de passe du routeur, ces informations généralement sont prédéfinies sur le dos du boitier du routeur pour mesure de sécurité.

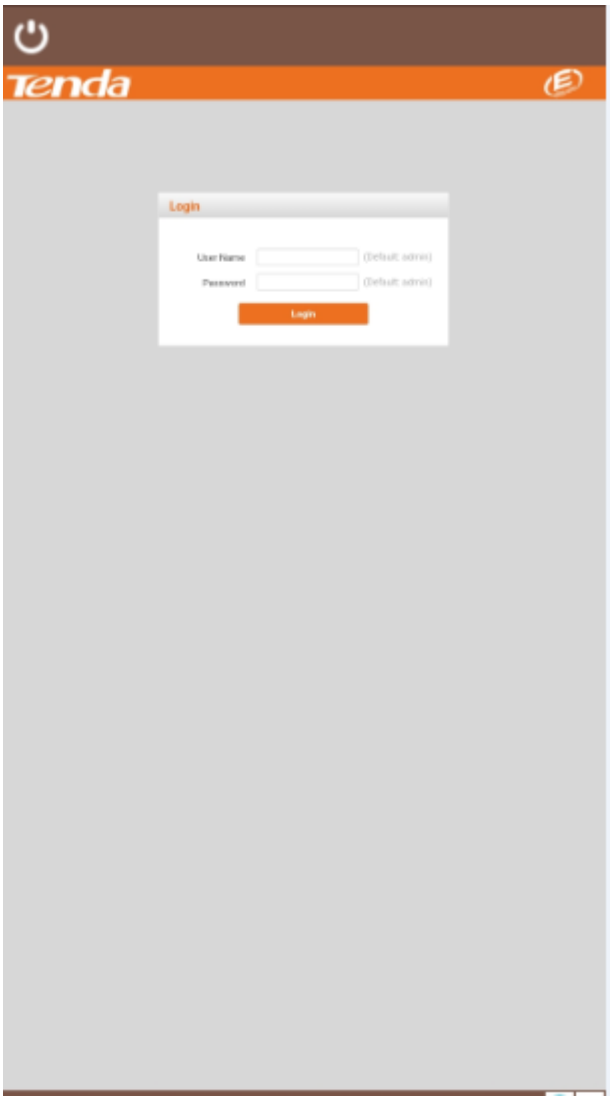


Figure 5.8 : *interface d'authentification du routeur*

Après avoir saisis le nom de l'utilisateur et le mot de passe l'interface du modem s'affiche avec la configuration en cours, et on peut ensuite accéder à tous les fonctionnalités du routeur.

Figure 5.9 : *la configuration en cours du routeur*

Dans cette interface on pourra faire des modifications sur notre réseau local, comme :

- Modifier son adresse ip.
- Allouer des adresses ip.
- Ajouter des périphériques.
- Limiter la vitesse et la bande passante.
- Sécurisé l'accès (wps).

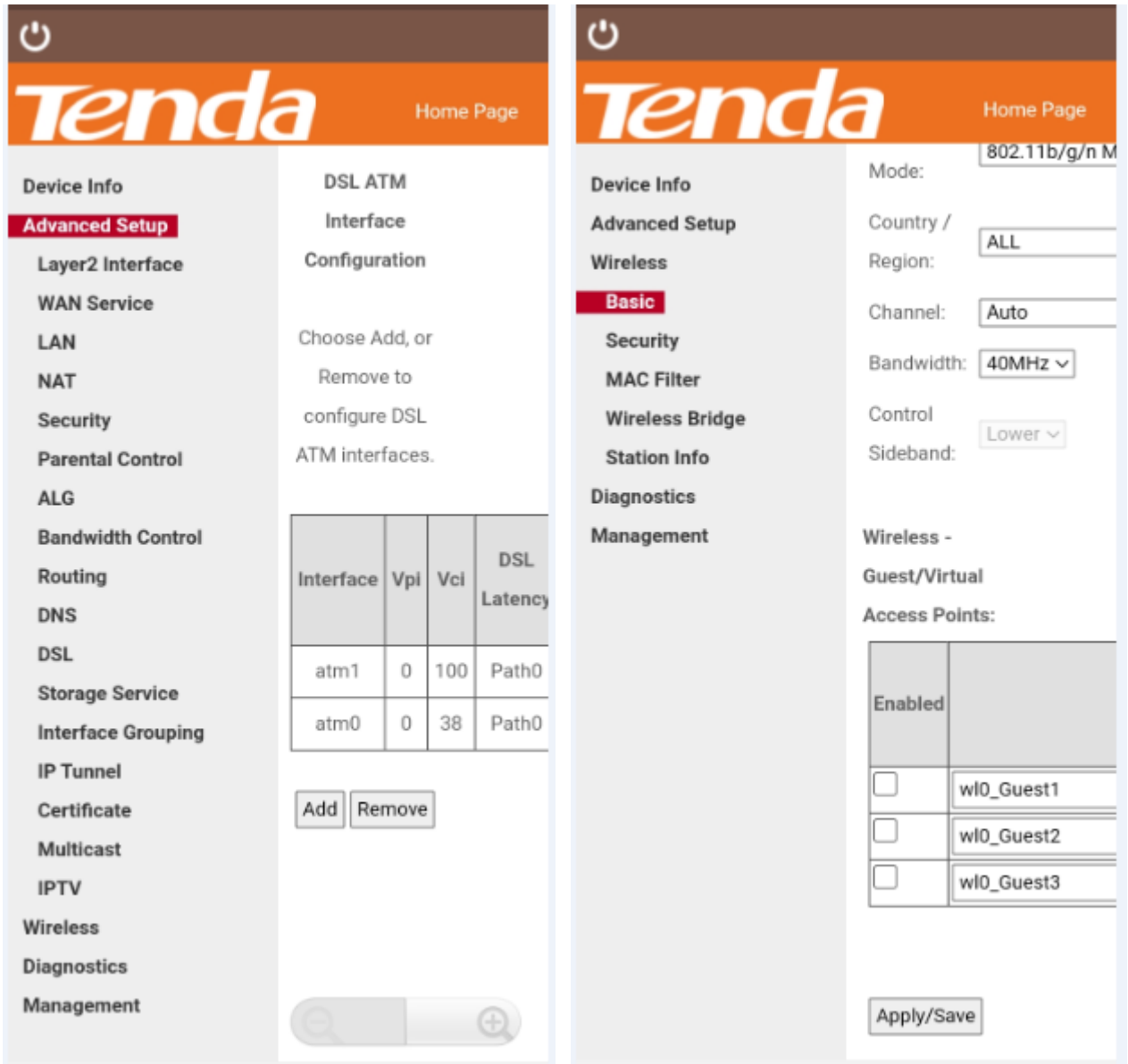


Figure 5.10 : *les fonctionnalités du routeur*

Conclusion

La phase de réalisation est l'étape la plus importante dans le cycle de vie d'une application. Dans ce chapitre, nous avons décrit brièvement le processus de réalisation de notre application en spécifiant l'environnement, les outils et les langages de développement associés à notre système. En effet, nous avons achevé l'implémentation tout en respectant la conception élaborée.

Conclusion générale

Face à l'importance de la disposition et la disponibilité de l'internet dans nos domiciles, nous avons étudié, conçu et réalisé à travers de ce travail un système (application) mobile qui permet d'aider les utilisateurs à gérer leur réseau local à travers leur modem routeur et à surveiller la sécurité de la connexion wifi. Il permet aussi à l'utilisateur de modifier la configuration du modem et gérer son réseau a sa guise, modifier le mot de passe wifi et le nom du wifi changer son adresse IP, ajouter des périphériques manuellement dans la table de routage du routeur, voir les périphériques connectés au wifi, limiter la bande passante, attribuait un nombre pour tous les périphériques et organiser leur canal d'écoute, et d'autre fonctionnalité qu'un routeur peut avoir vis-à-vis çà plateforme et marques.

Nous avons parlé dans le premier chapitre de la technologie mobile et de l'application mobile et de leurs types et nous nous sommes familiarisés avec le système Android et dans le deuxième chapitre nous nous sommes familiarisés avec le réseau informatique et ses différentes topologies et protocoles et de normes. Dans le troisième chapitre nous avons également parler du rôle important que joue la sécurité dans un réseau informatique, et l'importance de la protection contre les attaques et menaces qui viennent de l'internet. Dans le quatrième chapitre, Nous avons introduit des étapes de création d'applications, avec des examens des besoins et des modèles de cas Utilisation et fonctionnalité. Dans le cinquième chapitre nous sommes passés au côté pratique, qui consiste à créer l'application avec un examen des photos de la plupart des écrans d'application avec explication

Bien que notre application ne soit pas encore finie, nous avons l'intention de la compléter et l'améliorer en terme design (ergonomie), et augmenter les fonctionnalités de connexion tel que scanner le wifi, calculer la vitesse du débit, et améliorer une méthode pour générer les mots de passe wifi pour une sécurité optimal, ajouter d'autres langues à l'application afin d'attirer un grand nombre d'utilisateurs, et déploiement de l'application sur Play store.

Bibliographie

[1] « https://fr.wikipedia.org/wiki/Syst%C3%A8me_d%27exploitation_mobile » consulté le 18/07/2021

[2] « https://sites.google.com/site/androidtraitementimage/plateforme-android » consulté le 10/08/2021

[3] « https://www.nextpit.fr/repartition-smartphones-version-android » consulté le 10/08/2021

[4] « http://www-igm.univ-mlv.fr/~dr/XPOSE2008/android/archi_comp.html » consulté le 11/08/2021

[5] « https://www.appstud.com/fr/guides/agence-mobile/app088/ » consulté le 11/08/2021

[6] « https://mathias-seguy.developpez.com/tutoriels/android/comprendre-cyclevie-activite/ » consulté le 11/09/2021

[7]] Moussa DAVOU, Mise en place d'un Intranet au Ministère de l'Économie et des Finances, Mémoire d'ingénieur de conception en informatique, Université Polytechnique Bobo- Dioulasso, Janvier 2001.

[8] « https://www.frameip.com/osi/ » consulté le 11/08/2021

[9] « http://www.commentcamarche.net » Encyclopédie Informatique, Comment ça Marche, consulté le 12/08/2021

[10] « http://www.resoo.org » TCP/IP Internet/Intranet/Extranet, consulté 12/08/2021

[11] « https://dbprog.developpez.com/securite/ids/ » David BURGERMEISTER, Jonathan KRIER, Les Systèmes de Détection d'Intrusions, consulté le 14/08/2021

[12] « http://fr.wikibooks.org » 14/08/2021

[13] « http://cpham.perso.univ-pau.fr/ENSEIGNEMENT/PAU-UPPA/IRES-L3/Routage-IP.pdf » C. Pham , Université de Pau et des Pays de l'Adour, consulté le 14/08/2021

[14] « http://www.futura-sciences.com/tech/definitions/internet-java-485 » consulté le 20/08/2021

[15] « http://www.zdnet.fr/actualites/android-studio-une-version-10-pour-l-ide-de-google-39811025.html » consulté le 20/08/2021

[16] « http://tvaira.free.fr/dev/android/android-installation.html ». consulté le 21/08 /2021

[17] « http://www.commentcamarche.net/contents/559-java-introduction » consulté le 21/08/2021

[18] « https://www.techopedia.com/definition/4220/android-sdk » consulté le 22/08 /2021

Résumer

Devenue nécessaire l'informatique a prouvé son utilité et son efficacité dans les domaines des recherches mais aussi dans la vie quotidienne jusqu'à l'avenir indétournable car elle apporte des solutions efficaces aux nombreux problèmes rencontrés régulièrement comme la configuration des réseaux locaux et la gestion totale de ce dernier, réaliser une application sous réseau pour la gestion du réseau local (LAN).

Ce travail est le projet de fin d'cycle, et son but est de développer une application mobile pour aider les utilisateurs gérer leur réseau local, et configurer leur routeur. Nous avons commencé par un une partie théorique qui consiste à expliquer le fonctionnement d'un réseau et le system Android, suivie d'une conception architecturelle de la solution envisagée. Pour l'implémentation, nous avons utilisé l'environnement de développement intégré Android Studio, java-Sdk Android et l'émulateur Android

Mots clés : Application Android, Routeur, wifi, sécurité, Réseau.

Abstract

Computing has become necessary and has proven its usefulness and efficiency in the fields of research but also in daily life until the inevitable future because it provides effective solutions to the many problems encountered regularly such as the configuration of local networks and management. total of the latter, create a sub-network application for the management of the local area network (LAN).

This work is end of study project, and this aim is to develop a mobile application to help users manage their local network, and configure their router. We started with a theoretical part, which consisted in explaining the functioning of a networking and the Android system, followed by an architectural design of the envisaged solution. For the implementation, we used the Android Studio integrated development environment, Android java-Sdk and the Android emulator.

Keywords: Android application, Router, WIFI, security, Network