

UNIVERSITE D'ANTANANARIVO

ECOLE SUPERIEURE POLYTECHNIQUE

DEPARTEMENT TELECOMMUNICATION

MEMOIRE DE FIN D'ETUDES

en vue de l'obtention

du DIPLOME d'INGENIEUR

Spécialité : **TELECOMMUNICATION**

Option : **Radiocommunication**

par **RASATAMANANA Rado Nomeny**

**WIRELESS APPLICATION PROTOCOL
ET SON APPLICATION AVEC SIMPLE
MESSAGERIE**

Soutenu le Mercredi 02 Octobre 2002 , devant la Commission d'Examen composée de :

Président :

M. ANDRIAMIASY Zidora

Examineurs :

1. M. RATSIMBAZAFY Andriamanga
2. M. RANDRIANARISOA Joachim
3. M. RANDRIATSIRESY Ernest
4. M. RAMORASATA Joseph Raphaël

Directeur de mémoire :

M. RANDRIARIJAONA Lucien Elino

REMERCIEMENTS

Au terme de ce mémoire de fin d'études, je tiens à exprimer mes sincères gratitude à toutes les personnes suivantes :

A Monsieur ANDRIAMIASY Zidora, enseignant chercheur à l'Ecole Supérieure Polytechnique Antananarivo, qui a bien voulu présider cette soutenance,

A Monsieur RANDRIARIJAONA Lucien Elino, qui a apporté aides et conseils inestimables durant la période de la réalisation de ce travail ;

Veillez accepter ici ma très haute considération et mon humble remerciement.

J'adresse aussi mes vifs remerciements aux membres du jury, qui ont bien voulu examiner et juger le présent mémoire, composés de :

Monsieur RATSIMBAZAFY Andriamanga, enseignant à l'Ecole Supérieure Polytechnique Antananarivo ;

Monsieur RANDRIANARISOA Joachim, Directeur Informatique de MRSD ;

Monsieur RANDRIATSIRESY Ernest, enseignant à l'Ecole Supérieure Polytechnique Antananarivo ;

Monsieur RAMORASATA Joseph Raphaël, enseignant à l'Ecole Supérieure Polytechnique Antananarivo ;

Et également à :

Tous les enseignants du Département Télécommunications, qui ont assuré notre formation d'ingénieur pendant ces cinq années ;

Mes parents, qui n'ont cessé d'apporter leurs appuis moral et financier durant toutes ces années d'études que j'ai passées et durant la préparation de ce mémoire ;

Toute ma famille ;

Tous ceux qui ont contribué de près ou de loin à la réalisation de ce mémoire.

Gloire à Dieu !

TABLE DES MATIERES

LISTE DES FIGURES	vi
LISTE DES TABLEAUX	viii
GLOSSAIRE	Erreur ! Signet non défini.
INTRODUCTION	1

1^{ère} PARTIE : ETUDE THEORIQUE

Chapitre I. TECHNOLOGIES RADIO DE TRANSMISSION DE DONNEES : GSM -

GPRS - UMTS	3
I.1. Le système GSM	3
I.1.1. Présentation	3
I.1.2. Le principe de base	3
I.1.2.1. Principaux objectifs du concept cellulaire	4
I.1.2.2. Mode de transmission	4
I.1.2.3. Type de modulation	5
I.1.2.4. Multiplexages	5
I.1.2.5. Les bandes fréquences utilisées par le système GSM	6
I.1.3. Architecture d'un réseau GSM	6
I.1.3.1. Les différentes sortes de couches	6
I.1.3.2. Infrastructure d'un réseau GSM	7
I.2. Les systèmes GPRS et UMTS	11
I.2.1. Le système GPRS : General Packet Radio System	11
I.2.1.1. Généralité	11
I.2.1.2. Architecture du réseau GPRS	12
I.2.1.3. Les types de services offerts par GPRS	13
I.2.2. Le système UMTS : Universal Mobile Telecommunication System	14
I.2.2.1. Présentation	14
I.2.2.2 L'architecture du réseau UMTS	14
I.2.2.2.1 La structure du réseau cœur de l'UMTS	15
I.2.2.2.2 Le réseau d'accès UTRAN	18
I.2.2.3. Les services offerts par l'UMTS	21
I.2.2.4. Les objectifs de l'UMTS	22
I.2.2.5. Caractéristiques techniques	22
I.2.2.6. L'interopérabilité GSM-UMTS	23

I.3 Passage du système GSM vers le système UMTS	23
CHAPITRE II. INTERNET et INTRANET	26
II.1. L’Intranet	26
<i>II.1.1. Intranet en quelques mots</i>	<i>26</i>
<i>I.1.2. L’architecture Intranet</i>	<i>26</i>
<i>I.1.3. Les principales fonctions de l’Intranet</i>	<i>27</i>
II.2. Internet	28
<i>II.2.1. Présentation</i>	<i>28</i>
<i>II.2.2. Modèle d’architectures TCI/IP</i>	<i>29</i>
<i>II.2.3. Infrastructures</i>	<i>30</i>
<i>II.2.4. Les protocoles Internet</i>	<i>32</i>
II.2.4.1. Le protocole IP	32
II.2.4.2. Le protocole de contrôle de transmission (TCP)	32
II.2.4.3. Protocole de Transfert HyperTexte (HTTP)	33
II.2.4.4. Le protocole de transfert de fichier FTP	33
II.2.4.5. Le protocole de transfert simple de courrier SMTP	33
II.2.4.6. Le protocole de bureau de poste POP	33
II.2.4.7. Le protocole d’accès au message électronique IMAP	33
<i>II.2.5. Services disponibles sur l’Internet</i>	<i>34</i>
II.2.5.1. Les services de base	34
II.2.5.2. Les services d’information	34
Chapitre III. LA TECHNOLOGIE WAP	36
III.1. Définition et présentation	36
III.2. Architecture	37
<i>III.2.1. Le terminal WAP</i>	<i>38</i>
<i>III.2.2. La passerelle WAP ou serveur proxy WAP</i>	<i>40</i>
III.2.2.1. Définition et rôles	40
III.2.2.2. Les différents emplacements de passerelle WAP	41
<i>III.2.2.2.1. Passerelle WAP chez l’opérateur</i>	<i>41</i>
<i>III.2.2.2.2. Passerelle chez un fournisseur</i>	<i>41</i>
<i>III.2.2.2.3. Passerelle WAP en interne</i>	<i>43</i>
III.2.2.3. Impératives techniques des passerelles WAP	43
III.2.2.4. Fonctionnement de la passerelle WAP	45
<i>III.2.3. Le serveur d’application WAP</i>	<i>45</i>
III.2.3.1. Structure	45
III.2.3.2. Qu’est - ce qu’un serveur Web standard ?	46
III.2.3.3. Concept d’URL	46

III.2.4. Le réseau opérateur	47
III.2.5. Fonctionnement de la transaction	48
III.3. La structure du protocole WAP	49
III.3.1. La couche application : Wireless Application Environment (WAE)	50
III.3.1.2. Structure et présentation	50
III.3.1.2. Fonctions de la couche WAE	51
III.3.2. La couche session : Wireless Session Protocol (WSP)	51
III.3.2.1. Structure et présentation	51
III.3.2.2. Caractéristiques de la couche WSP	52
III.3.3. La couche transaction : Wireless Transaction Protocol (WTP)	52
III.3.3.1. Présentation de la couche transaction	52
III.3.3.2. Les avantages de la couche WTP	54
III.3.4. La couche sécurité : Wireless Transport Layer Security (WTLS)	55
III.3.4.1. Structure et présentation	55
III.3.4.2. Fonctions de la couche WTLS	55
III.3.5. La couche transport : Wireless Datagram Protocol (WDP)	56
III.3.5.1. Structure et présentation	56
III.3.5.2. Fonctions de la couche WDP	56
III.4. Les supports	57
III.5. Comparaison entre la pile WAP et la pile TCP/IP	58
III.6. Sécurité	59
III.6.1. Sécurité de « bout à bout »	59
III.6.2. le cryptage des données	61
III.7. Les compléments sur le WAP	62
III.7.1 Le protocole « PUSH »	62
III.7.2. Le protocole « WCMP » ou Wireless Control Message Protocol	64
III.8. Applications	65
 Chapitre IV. LE LANGAGE WML : Wireless Markup Language	68
IV.1. Définition et structure du langage WML	68
IV.2. Les principales fonctionnalités du WML	69
IV.3. La syntaxe du langage WML	69
IV.4. Eléments du langage	70
IV.5. Spécification du langage WML	71
IV.5.1. Les endtags	72
IV.5.2. Sensibilité à la casse	72
IV.5.3. Coder tous les caractères spéciaux	72

IV.5.4. Les différences du point de vue de l'utilisateur	73
IV.5.5. WML est parfaitement adapté au WAP	73
IV.5.6. La structure Card	74
Chapitre V. LE LANGAGE DE SCRIPT : WMLScript	75
V.1. Présentation	75
V.2. Intérêt du script et conseils d'utilisation	75
V.3. Conventions	76
Chapitre VI. LA TECHNOLOGIE WAP ENVERS LE MONDE	77
VI.1. Intégration du WAP dans le contexte économique actuel	77
VI.2. Perspectives de développement et évolutions envisageables	77
VI.3. Evolution de la technologie WAP à Madagascar	78
VI.4 L'avenir de la technologie WAP	79

2^{ème} PARTIE : APPLICATION SOUS LINUX

Chapitre I. ENVIRONNEMENT LINUX	80
I.1. Présentation	81
I.2. Pourquoi utilise-t-on Linux ?	81
I.3. Quels sont ses inconvénients par rapport aux autres systèmes d'exploitation ?	82
Chapitre II. SERVEUR APACHE	83
II.1. Présentation du serveur Apache	83
II.2. Qu'est-ce qu'on entend par type MIME ?	83
II.3. Installation de paquetage du serveur Web Apache et mise en relation avec PHP/MySQL	84
Définition 2.2.1	84
Définition 2.2.2	84
II.3.1. Méthode	85
II.3.1.1. Choix initiaux	85
II.3.1.2. Sélection des groupes de paquetages	85
II.3.2. Liste des paquetages à sélectionner	85
II.4. Les fichiers de configuration du serveur Apache	86
II.5. Lancement en mode autonome	87
II.5.1. Configuration du httpd.conf pour rendre Apache compatible WAP	87
II.5.2. Configuration pour httpd.conf avec la mise en relation Apache + PHP + MySQL	88

II.5.2.1. Utilisation du script PHP avec Apache	88
II.5.2.2. Utilisation de la base de données MySQL avec Apache	89
II.4.3. Lancement et relancement du serveur en mode autonome	89
Chapitre III. APPLICATIONS	91
But :	91
III.1 Présentation	91
III.2. Les formulaires	93
III.2.1 Principaux techniques d'élaboration de page WAP généré à partir du script PHP	93
III.2.2. Conception de site de simple messagerie	95
III.2.2.1. Formulaire de page d'accueil	95
III.2.2.2. Formulaire de page d'inscription	96
III.2.2.3. Formulaire de page d'authentification	97
III.2.2.4. Formulaire de page d'écriture d'un message	98
III.2.2.5. Formulaire de page de Consultation d'un message	99
III.3. Manipulation et résultats	100
III.3.1. Comment s'inscrire dans le site de simple messagerie « wap.tco5.edu »?	100
III.3.2. Authentification	101
III.3.3. Ecrire un message	103
III.3.4. Consulter un message	103
CONCLUSION	105

ANNEXES

ANNEXE A : Le protocole et transaction HTTP	105
ANNEXE B : Comparaison WTLS et SSL	107
ANNEXE C : Relation entre WML, XML et SGML	109
ANNEXE D : Configuration de base du serveur Apache	111
ANNEXE E. Installation d'Apache, de Php et de MySQL à partir des fichiers archives... 114	
BIBLIOGRAPHIE	117

LISTE DES FIGURES

<i>Figure 1.1.1.</i> Structure matérielle d'un réseau GSM	8
<i>Figure 1.1.2.</i> Interfaces du réseau GSM	10
<i>Figure 1.1.3.</i> Structure d'un réseau GPRS	12
<i>Figure 1.1.4.</i> Architecture du réseau UMTS avec les réseaux d'accès GSM et UTRAN	15
<i>Figure 1.1.5.</i> Constitution du réseau cœur de l'UMTS	16
<i>Figure 1.1.6.</i> Réseau d'accès UTRAN	19
<i>Figure 1.1.7.a.</i> Implémentations possibles du Node B	20
<i>Figure 1.1.7.b.</i> RNC et Node B en communication avec un terminal mobile	20
<i>Figure 1.1.8.a.</i> Evolution de la technologie des télécommunications sans fil	24
<i>Figure 1.1.8.b.</i> Migration des systèmes de deuxième génération vers UMTS	24
<i>Figure 1.2.1.</i> Structure d'un Intranet.....	27
<i>Figure 1.2.2.</i> Structure d'Internet.....	31
<i>Figure 1.3.1.</i> Structure d'un réseau WAP dans le cas général.....	38
<i>Figure 1.3.2.</i> Passerelle WAP chez l'opérateur	41
<i>Figure 1.3.3.</i> Passerelle WAP chez un fournisseur sans hébergement d'un site Web.....	42
<i>Figure 1.3.4.</i> Passerelle WAP chez un fournisseur avec hébergement d'un site Web	42
<i>Figure 1.3.5.</i> Passerelle WAP chez le client.....	43
<i>Figure 1.3.6.</i> Détail du fonctionnement de la passerelle.....	45
<i>Figure 1.3.7.</i> Schéma de principe d'un serveur Web.....	47
<i>Figure 1.3.8.</i> Echange d'informations à travers une passerelle lors d'une requête	49
<i>Figure 1.3.9.</i> Modèle de couches du protocole WAP	50
<i>Figure 1.3.10.</i> Connexion à sens unique sans acquittement	53
<i>Figure 1.3.11.</i> Connexion à sens unique avec acquittement.....	53
<i>Figure 1.3.12.</i> Connexion à double sens avec acquittement.....	54
<i>Figure 1.3.13.</i> Implémentation et performances de quelques supports	57
<i>Figure 1.3.14.</i> Comparaison entre les modèles de couches OSI et WAP	58
<i>Figure 1.3.15.</i> Comparaison entre la pile TCP/IP et la pile WAP	59
<i>Figure 1.3.16.</i> Représentation de type de sécurité « bout à bout »	60
<i>Figure 1.3.17.</i> Mécanisme de cryptage et de décryptage de données.....	62
<i>Figure 1.3.18.</i> Schéma simplifié des transactions « push » et « pull »	63
<i>Figure 1.3.19.</i> Représentation avec une passerelle « push ».....	63

<i>Figure 1.3.20.</i> Interaction du protocole WCMP dans la pile WAP	64
<i>Figure 1.4.1.</i> Différence entre les structures des documents Web et WAP	74
<i>Figure 2.3.1.</i> Arborescence des fichiers résidant dans « wap.tco5.edu »	92
<i>Figure 2.3.2.</i> Formulaire d'inscription.....	101
<i>Figure 2.3.3.</i> Formulaire d'authentification.....	102
<i>Figure 2.3.4.</i> Formulaire pour l'écriture d'un message	103
<i>Figure 2.3.5.</i> Formulaire pour l'écriture d'un message	104

LISTE DES TABLEAUX

<i>Tableau 1.1.1.</i> Traitement de la phonie dans le système GSM.....	5
<i>Tableau 1.1.2.</i> Modèle de couches d'un réseau GSM.....	6
<i>Tableau 1.1.3.</i> Tableau récapitulatif de l'évolution du système GSM vers l'UMTS	25
<i>Tableau 1.2.1.</i> Correspondance entre les modèles OSI à 7 couches et TCP/IP	30
<i>Tableau 1.3.1.</i> Caractéristiques de quelques outils de navigation WAP.....	39
<i>Tableau 1.3.2.</i> Structure d'information WCMP.....	65
<i>Tableau 2.2.1.</i> Types MIME utilisés par le WAP	84
<i>Tableau 2.3.1.</i> Codes de quelques caractères spéciaux.....	94

ABREVIATIONS

ASP : Active Server Page

AMRF : Accès Multiple à Répartition Fréquentiel

AMRT : Accès Multiple à Répartition dans le Temps

ASCII : American Standard Code for Information Interchange

AuC : Authentication Center

BRAN : Broadband Radio Access Network

BSC : Base Station Controller

BTS : Base Transceiver Station

CDMA : Code Division Multiple Access

CGI : Common Gateway Interface

CLNS : ConnectionLess Network Service

CONS : Connection Oriented Network Service

CS : Circuit Switched

CSD : Circuit Switched Data.

DNS : *Domain Name Server*

DTD : Document Type Definition

EDGE : Enhanced Data rates for Global Evolution

EIR : Equipment Identity Register

ETSI : European Telecommunications Standards Institute

FDD : Frequency Domain Duplex

FTP : File Transfer Protocol

GGSN : *Gateway GPRS Support Node*

GMSC : Gateway MSC

GMSK : Gaussian minimum shift keying

GPRS : General Packet Radio Service

GSM : global System for Mobil communications

HCSD : High Speed Circuit Switched Data

HLR : Home Location Register

HTML : HyperText Markup Language

HTTP : HyperText Transfer Protocol

IMAP : Internet Mail Application Protocol

IMEI : International Mobile Station Equipement Identity

IMSI : International Mobile Station Identity

IMT : International Mobile Telecommunications

IP : Internet Protocol

IRC : Internet Relay Chat

LA : Location Area

MIME : Multipurpose Internet Mail Extensions

MS : Mobile Station

MSC : Mobil Switching Center

OMC : Operation and Maintenance Center

OSI : Open System Interconnect

PCU : Packet Control Unit

PDA : Personal Digital Assistant

PDC : Personal Digital Cellular.

PDU : Protocol Data Unit.

PHP : Preprocessor Hyper Protocol

PPP : Point to Point Protocol

PS : Packet Switched

RAS : Remote Access Service

RNC : Radio Network Controller

RNIS : Réseau Numérique d'Intégration de Service

RRC : Radio Resource Control

RTC : Réseau Téléphonique Commuté

SDU : Service Data Unit

SGML : Standard Generalized Meta Language

SGSN : Serving GPRS Support Node

SIM : Subscriber Identity Module

SMS : Short Message Service

SMTP : Simple Mail Transfer Protocol

SRNC : Serving RNC

SSL : Secure Socket Layer

TCP : Transmission Control Protocol

TCI : Transmission Control Protocol

TDMA : Time Division Multiple Access

TIA : Telecommunications Industry Association

TDD : Time Domain Duplex

UMTS : Universal Mobile Telecommunication System

URL : Universal Resource Locator

UTRAN : UMTS Terrestrial Radio Access Network

VLR : Visitor Location Register

XML : Extensible Meta Language

WAP : Wireless Application Protocol

WAE : Wireless Application Environment

WTAIS : Wireless Telephony Application Interface Specification

WBXML : Wireless Binary XML

WCDMA : Wideband Code-Division Multiple-Access

WCMP : Wireless Control Message Protocol

WDP : Wireless Datagram Protocol

WIM : WAP Identity Module

WLAN : Wireless Local Area Network

WML : Wireless Markup Language

WSP : Wireless Session Protocol

WTP : Wireless Transaction Protocol

WTLS : Wireless Transport Layer Security

WWW : World Wide Web

INTRODUCTION

L'évolution technologique, qui est l'un des moteurs économiques de notre société, nous a amenés depuis quelques années à une nouvelle révolution, celle de l'Internet mobile. L'entrée dans le monde de l'information et de la communication a débuté par l'insertion progressive des téléphones fixes, des premiers postes radio et de télévision puis, quelques décennies plus tard s'est poursuivie par l'avènement de la micro-informatique et par la téléphonie mobile. L'engouement suscité tant auprès du grand public que des professionnels a fortement motivé les industriels à améliorer leurs offres et prestations.

Cette évolution technologique est née à partir de différentes découvertes dont l'onde radio vers l'an 1876 et de la Télégraphie Sans Fil (TSF). La compagnie Bell a su exploiter ces procédés et après des longues recherches, ils ont abouti à la première génération de système de télécommunication communément appelé AMPS (*Advanced Mobil Phone Service*). Quelques années plus tard, l'arrivée de la seconde génération de système de télécommunication fait son apparition : le système GSM (*Global System for Mobile Communication*) qui a innové les faiblesses de la première génération : système analogique, qualité moindre en terme de communication et jamais été normalisée. Ce système GSM était devenue un standard, surtout en Europe, en matière de communication mobile. Toutefois, ce système n'est pas encore à sa maturité surtout en terme de services offerts qui s'avèrent insuffisants pour certain public ciblé. Pour compléter cette défaillance, les industriels ont été amenés à faire évoluer la norme GSM en y ajoutant de nouvelles technologies plus performantes telles que le HSCSD (*High Speed Circuit Switched Data*), le GPRS (*Général Packet Radio Services*) et le EDGE (*Enhanced Data rates for GSM Evolution*) qui ont permis l'augmentation du débit d'échange d'information et la création d'une nouvelle génération de système de télécommunication offrant plus de gamme de services à haut débits. Ces différentes évolutions ont abouti, par la suite, au système appelé UMTS (*Universal Mobile Terrestrial System*).

Parallèlement, la montée des services proposés sur Internet - informations diverses, catalogues, achats en ligne - et son taux de pénétration en forte augmentation, plus facilement accessible, ont poussé les opérateurs en quête d'un nouveau genre de public à proposer un accès à Internet depuis les mobiles. C'est dans ce sens que le forum WAP a été créé afin d'harmoniser le développement

de cette nouvelle démarche. En décembre 1997, ce forum WAP était originairement formé par Nokia, Ericsson, Motorola et phone.com (Unwired Planete). L'objectif de cette collaboration était de développer un standard global pour le transfert de données sur les réseaux de téléphonie mobile afin de répondre aux besoins des usagers dans le domaine des télécommunications, de satisfaire une clientèle de plus en plus exigeante par la diversification des services offerts et de couvrir un marché en pleine globalisation. Cette association peut être rejointe par toute entreprise qui s'engage à respecter les spécifications décidées par le WAP (*Wireless Application Protocol*). C'est ainsi que le nombre de ses membres a augmenté régulièrement pour atteindre aujourd'hui environ plus de 90% des constructeurs des téléphones mobiles.

Le protocole Wireless Application Protocol est ainsi le résultat des efforts joints par les principaux acteurs industriels du monde sans fil afin de proposer une infrastructure standardisée pour le développement de services et la diffusion d'informations sur des terminaux sans fils. Grâce au protocole WAP, les possesseurs de téléphones mobiles plus récents vont pouvoir accéder à Internet et ses dérivés en commençant par l'Intranet et l'extranet. Il sera alors possible, à un client ou personnel d'un organisme, à n'importe quel endroit et moment, de consulter, par exemple, son compte bancaire, de vendre ou d'acheter des actions, de réserver une place de spectacle, de consulter la prévision météorologique ou de suivre des résultats sportifs, etc.

En conclusion à cette brève introduction, le présent mémoire, dont l'objet est la réalisation d'un projet de messagerie sur WAP, est divisé en deux grandes parties :

- La première partie est composée de cinq Chapitres qui couvrent dans son ensemble les descriptions des systèmes GSM, GPRS et UMTS suivies de la présentation de l'Internet et de l'Intranet. Cette première partie est terminée par une description exhaustive de la technologie WAP : son architecture, son protocole, ses supports, sa comparaison avec la pile TCP/IP, sa sécurité et ses applications.

- La seconde partie du mémoire concerne la présentation de l'application qui est l'aboutissement de notre travail en l'occurrence la messagerie par le biais du WAP. Cette application a été mise en oeuvre sous le système d'exploitation Linux en utilisant le serveur Apache en tant qu'hébergeur de site. Le langage de développement choisi pour la réalisation de l'application est le langage WML généré à partir du script PHP qui est en interaction avec une base de données sous MySQL.

1^{ère} PARTIE : ETUDE THEORIQUE

Chapitre I. TECHNOLOGIES RADIO DE TRANSMISSION DE DONNEES : GSM - GPRS - UMTS

I.1. Le système GSM [4] [5] [7] [9]

I.1.1. Présentation

GSM (*Global System for Mobile communications*) est une norme spécifiant un réseau de radiotéléphonie mobile à transmission numérique. GSM est une norme originale par rapport à d'autres normes (DECT, CT2/CAI, IS95,...) car elle spécifie l'ensemble du réseau de radiotéléphonie mobile et non pas uniquement l'interface radio. Cette norme permet en plus l'itinérance internationale, c'est-à-dire la possibilité pour un abonné d'utiliser un réseau étranger.

Un réseau GSM permet bien évidemment d'effectuer des appels téléphoniques mais aussi la transmission de données jusqu'à 9600 bit/s, la transmission de fax en groupe 3, l'accès à un réseau à commutation de paquet, le transfert de messages courts, et tous les services supplémentaires offerts sur les réseaux modernes (renvoi d'appels, signal d'appel, groupe fermé d'usagers...).

I.1.2. Le principe de base

Depuis la création du système GSM, le concept cellulaire occupe une place majeure dans la radiotéléphonie mobile de par le monde. Afin d'économiser le spectre hertzien, les opérateurs découpent leur zone de couverture en plusieurs entités hexagonales contiguës appelées « cellules » qui se voient allouer des fréquences de manière judicieuse. Une cellule est donc l'unité élémentaire pour structurer un territoire couvert par le réseau. Ainsi, des cellules suffisamment éloignées les unes des autres, peuvent réutiliser les mêmes fréquences sans aucun brouillage. La taille des cellules varie selon la zone couverte, elle peut aller de quelques centaines de mètres dans les zones urbaines où le trafic écoulé est très dense, à quelques dizaines de kilomètres dans les régions rurales. Chaque cellule est contrôlée par une station de base (BTS ou *Base Transceiver Station*) qui communique avec les différents terminaux mobiles (MS ou *Mobil Station*) présents dans cette cellule. Ce sont les fréquences allouées à chaque cellule qui sont utilisées entre la MS et la BTS pour communiquer.

En outre, des grandes innovations ont eu lieu dans le domaine de la Radiotéléphonie Mobile ; pour les normes GSM, trois majeures techniques sont introduites : l'utilisation du mode de

transmission numérique, des multiplexages des canaux radio, et du cryptage de l'information. Ceux-ci ont pour but de répondre aux besoins des utilisateurs, c'est-à-dire d'avoir une phonie de meilleure qualité, une augmentation du nombre d'abonnés servi par le réseau, une confidentialité des transmissions radio, un accès au RNIS, un contrôle de puissance d'émission et surtout afin d'offrir des nouveaux services de transmission (comme le texte, la télécopie, les images, etc.).

I.1.2.1. Principaux objectifs du concept cellulaire

- Utilisation de plusieurs fréquences
- Minimisation de la puissance de l'émetteur
- Réutilisation de fréquence

I.1.2.2. Mode de transmission

Le système GSM adopte le mode de transmission numérique de l'information. Cette technique dispose de nombreux traitements (voir *Tableau 1.1.1.*) qui s'avère être plus complexe que celle utilisée pour une transmission analogique, mais présente toutefois plus d'avantages.

Dans le système GSM, il faut tout d'abord numériser le signal avant de l'émettre. trois principales opérations sont alors nécessaires :

- l'**échantillonnage** : cette opération consiste à transformer un signal continu $s(t)$ à des tranches cadencées régulièrement dans le temps dont l'amplitude du signal à chaque instant t est alors prélevée.
- la **quantification** : Elle consiste à affecter une valeur aux amplitudes mesurées en fonction d'une certaine loi : « loi de correspondance ». Les lois de quantification utilisées sont quelques fois logarithmique afin de garantir une précision presque constante.
- le **codage** : le principe de codage consiste à attribuer une valeur numérique à un échantillon qui dépend du nombre de digits disponibles. La plage de variation du signal $s(t)$ est divisées en n intervalles. L'information voyageée dans le canal de transmission est donc la valeur codée sur n bits de chacun des échantillons. Le codage transforme la nature des informations à transmettre (physique $\Longrightarrow$ logique).

PHYSIQUE	LOGIQUE
Parole	
	Numérisation
	Codage
	Cryptage
Modulation	
Emission	
Transmission	
Réception	
Démodulation	
	Décryptage
	décodage
Synthèse	
Parole	

Tableau 1.1.1. Traitement de la phonie dans le système GSM

I.1.2.3. Type de modulation

Le système standard **GSM** utilise la modulation à déplacement minimal à filtre gaussien ou GMSK (*Gaussian minimum shift keying*) afin d'optimiser l'efficacité spectrale et de limiter les interférences avec les canaux adjacents.

I.1.2.4. Multiplexages

La norme GSM utilise deux types de multiplexage :

- Multiplexage temporel (AMRT : *Accès Multiple à Répartition dans le Temps*) qui consiste à partager le temps en plusieurs unités de base appelés «trames » qui sont des séquences invariables. Chaque trame se divise en 8 intervalles temporels « IT ». Ce multiplexage a donc pour but de multiplier par 8 le nombre de canaux de transmission possibles par unité de temps (un canal de communication ne transporte des données que dans un seul sens).

- Multiplexage fréquentiel (AMRF : *Accès Multiple à Répartition Fréquentiel*) qui consiste à partager les bandes disponibles en 124 sous-bandes ou canaux physiques de transmission radio utilisables simultanément (1 fréquence tous les 200kHz).

I.1.2.5. Les bandes fréquences utilisées par le système GSM

L'interface radio d'un réseau GSM est défini sur deux bandes à duplexage fréquentiel :

- 900 MHz pour le GSM : avec écart duplex de 45 MHz
 - o MS (*Mobile Station*) vers BTS (*Base Transceiver Station*): 890 à 915 MHz
 - o BTS (*Base Transceiver Station*) vers MS (*Mobile Station*): 935 à 960 MHz
- 1800 MHz pour le DCS : avec écart duplex de 75 MHz
 - o MS (*Mobile Station*) vers BTS (*Base Transceiver Station*): 1710 à 1785 MHz
 - o BTS (*Base Transceiver Station*) vers MS (*Mobile Station*): 1805 à 1880 MHz

I.1.3. Architecture d'un réseau GSM

I.1.3.1. Les différentes sortes de couches

Le modèle d'architecture des logiciels pour un réseau GSM est appelé «Open System Interconnect » ou **OSI** qui est reparti en 7 couches logicielles :

COUCHE APPLICATION
COUCHE PRESENTATION
COUCHE SESSION
COUCHE TRANSPORT
COUCHE RESEAU
COUCHE LIAISON
COUCHE PHYSIQUE

Tableau 1.1.2. Modèle de couches d'un réseau GSM

- **Couche Physique** : le logiciel de la couche physique émet et reçoit les données en provenance du support de transmission, il permet le transport des informations binaires. C'est au niveau de cette couche que l'on choisit le type de codage utile pour la transmission des données, le débit du canal de transmission, le type de transmission (synchrone ou asynchrone), le mode de transmission (analogique ou numérique) et le type de dialogue (point à point ou point à multipoint)

- **Couche Liaison** : elle permet l'empaquetage des trames, qu'elle reçoit de la couche inférieure, pour la couche supérieure. Elle contrôle et détecte les erreurs de transmission des trames reçus de la couche inférieure. Dans les réseaux locaux, cette couche règle le problème d'accès au réseau lorsque plusieurs utilisateurs souhaitent se connecter au réseau.

- **Couche Réseau** : elle détecte en permanence les stations présentes dans le réseau et enregistre leur adresse dans une table appelée «table de routage » pour chaque message émis. La table de routage est un tableau contenant toutes les stations du réseau et leur état. Lorsque la couche réseau reçoit les paquets venant de la couche inférieure, elle les réordonne afin d'assurer la séquentialité. La couche réseau gère aussi le contrôle de flux entre deux points.

- **Couche transport** : elle permet de garantir un transfert de données transparent entre deux entités de session. La couche transport offre un service communication aux couches supérieures et cinq classes de services à la couche session : classe 0 – 4.

- **Couche présentation** : qui gère la syntaxe utilisé pour structurer les données et la description de ces données.

- **Couche Application** : qui définit les interactions entre l'utilisateur et le système de communication. Elle offre un cadre d'accueil aux tâches.

I.1.3.2. Infrastructure d'un réseau GSM

- **Structure**

Le PLMN (*Public Land Mobile Network*) est l'équivalent du PSTN (*Public Switched Telephone Network* ou RTCP) pour les réseaux de téléphonie cellulaires. Le PLMN est composé de deux parties : le Sous-système Radio ou BSS et le Sous-système Réseau ou NSS.

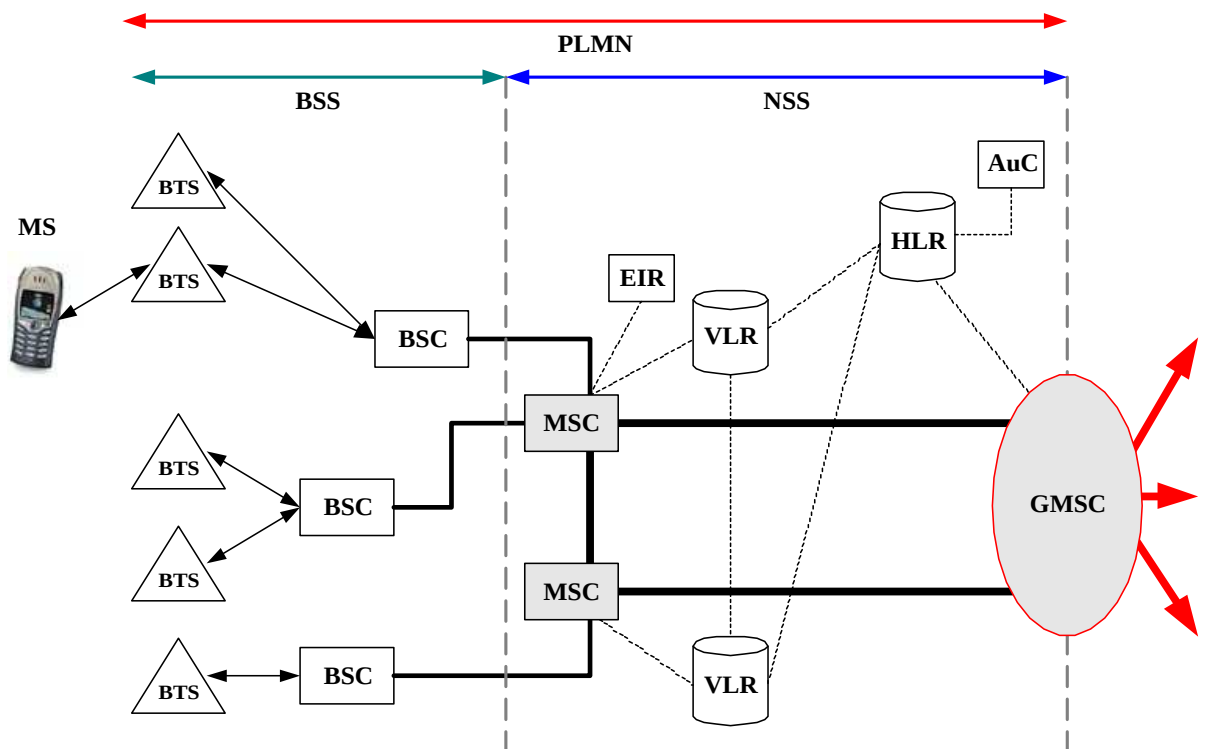


Figure 1.1.1. Structure matérielle d'un réseau GSM

- **Equipements**

Le BSS ou Sous-système Radio :

- o **MS** (*Mobil Station*) : c'est le poste d'abonné
- o La **BTS** (*Base Transceiver Station*) : elle regroupe le matériel d'émission – réception d'une ou plusieurs cellules (appelés TRX, Transceiver) et relie ainsi les stations mobiles avec l'infrastructure fixe du réseau. En effet, la BTS prend en charge la transmission radio (modulation/démodulation, égalisation, la mise en trame et en paquets élémentaires radio), gère toute la couche physique (Multiplexage TDMA, chiffrement, sauts de fréquences ...) et la couche liaison de données pour l'échange de signalisation entre les mobiles et l'infrastructure et enfin réalise l'ensemble des mesures radio nécessaires pour vérifier qu'une communication se déroule normalement.

o Le **BSC** (*Base Station Controller*) : le BSC commande un ensemble de stations radios BTS. Il gère la ressource radio, exploite les mesures effectuées par les BTS et les mobiles pour décider du hand-over. Le BSC permet aussi d'effectuer une concentration des circuits vers le MSC.

Le NSS ou Sous-système Réseau :

o **MSC** (*Mobile Switching Center*) : Le MSC est un commutateur téléphonique adapté pour supporter les fonctions mobiles :

- ❑ gestion des appels effectués par les mobiles présents dans la zone ;
- ❑ dialogue avec les bases de données pour accueillir les mobiles se présentant dans la zone ;
- ❑ fonction passerelle pour traiter les appels vers les mobiles (qui peuvent se trouver en un point quelconque) venant des abonnés téléphoniques voisins. Le MSC qui possède cette fonctionnalité est appelé G-MSC

o Le **VLR** (*Visitor Location Register*) : c'est une base de données relié a un MSC qui contient le profil des abonnés présents dans la zone du MSC et leur localisation précise.

o Le **HLR** (*Home Location Register*) : le HLR est une base de données qui contient les profils des abonnés et leur localisation approximative (identité du VLR associé). A partir du numéro d'un abonné, il est possible de retrouver les caractéristiques de l'abonné.

o **AuC** (*Authentication Center*) : Le centre d'authentification. C'est une base de données stockant les informations confidentielles :

- ❑ Algorithmes A3, A8
- ❑ Les enregistrements IMSI (*International Mobile Subscriber Identity*)
- ❑ Clef d'authentification Ki de chaque utilisateur.

o **OMC** (*Operation and Maintenance Center*) : Entité de gestion et d'exploitation du réseau. Elle regroupe la gestion administrative des abonnés et la gestion technique des équipements.

Elle autorise :

- ❑ La connexion de différentes BSS sur un même MSC.
- ❑ L'utilisation des différents MSC avec le même type de BSS.
- ❑ L'utilisation d'un même type de BSS dans n'importe quel PLMN.
- ❑ L'utilisation d'un même type de MSC dans n'importe quel PLMN.
- ❑ Une évolution séparée des technologies MSC, BSS, et O&M.
- ❑ Evolution vers des débits de codages de voie plus faibles.

I.2. Les systèmes GPRS et UMTS

I.2.1. Le système GPRS : General Packet Radio System [2] [8] [10] [11] [12] [13]

I.2.1.1. Généralité

La limitation du débit données pour GSM à 9.6 Kbps (TCH/F9.6) est un frein au développement des services de type Internet mobile et WAP (*Wireless Application Protocol*). Pour remédier à cela, les opérateurs ont élaboré un nouveau système appelé GPRS.

Le GPRS, qui constitue une évolution marquante du standard GSM, est essentiellement prévu pour la transmission des données en mode paquet sur les réseaux cellulaires actuels. Il est un système établi par l'ETSI (*European Telecommunications Standards Institute*) et permet de fournir, à des terminaux mobiles, l'accès à des services multimédia (décollage de l'Internet mobile). Ce système GPRS supporte un débit de transfert d'information élevé par rapport à celui du standard de la 2G (seconde génération de télécommunications mobiles). Par conséquent les opérateurs des réseaux ont besoin d'ajouter quelque nouvelle infrastructure pour faciliter ce service : deux types d'équipements sont rajoutés à l'infrastructure existante. De plus, les parties logicielles et l'interface A bis ont été modifiées.

Un service basé sur la commutation par paquet est un service qui exige " un temps minimum de transmission" pour l'envoi et la réception des données. En effet, lorsqu'une connexion est établie par un utilisateur, un canal n'est occupé que lorsque cet utilisateur fait une demande ou une

requête. Par contre, dans le cas de la méthode courant de connexion à la passerelle WAP (qui utilise la Commutation de Données en mode Circuit ou CSD, utilisé au système GSM), un canal est maintenu tout au long de la session même si l'utilisateur est actif ou non. Par conséquent, les solutions basées sur la commutation par paquet sont plus efficaces en terme de bande passante du réseau et de facturation de l'utilisateur. Cet usage effectif des ressources du réseau nécessite une plus large bande passante - en théorie 171.2 Kb/s. Cependant dans la pratique cette bande passante théorique n'est que rarement exploitée, en terme d'usage et de facturation, car la vitesse généralement utilisée et adaptée aux technologies utilisées semblent toujours inférieure.

I.2.1.2. Architecture du réseau GPRS

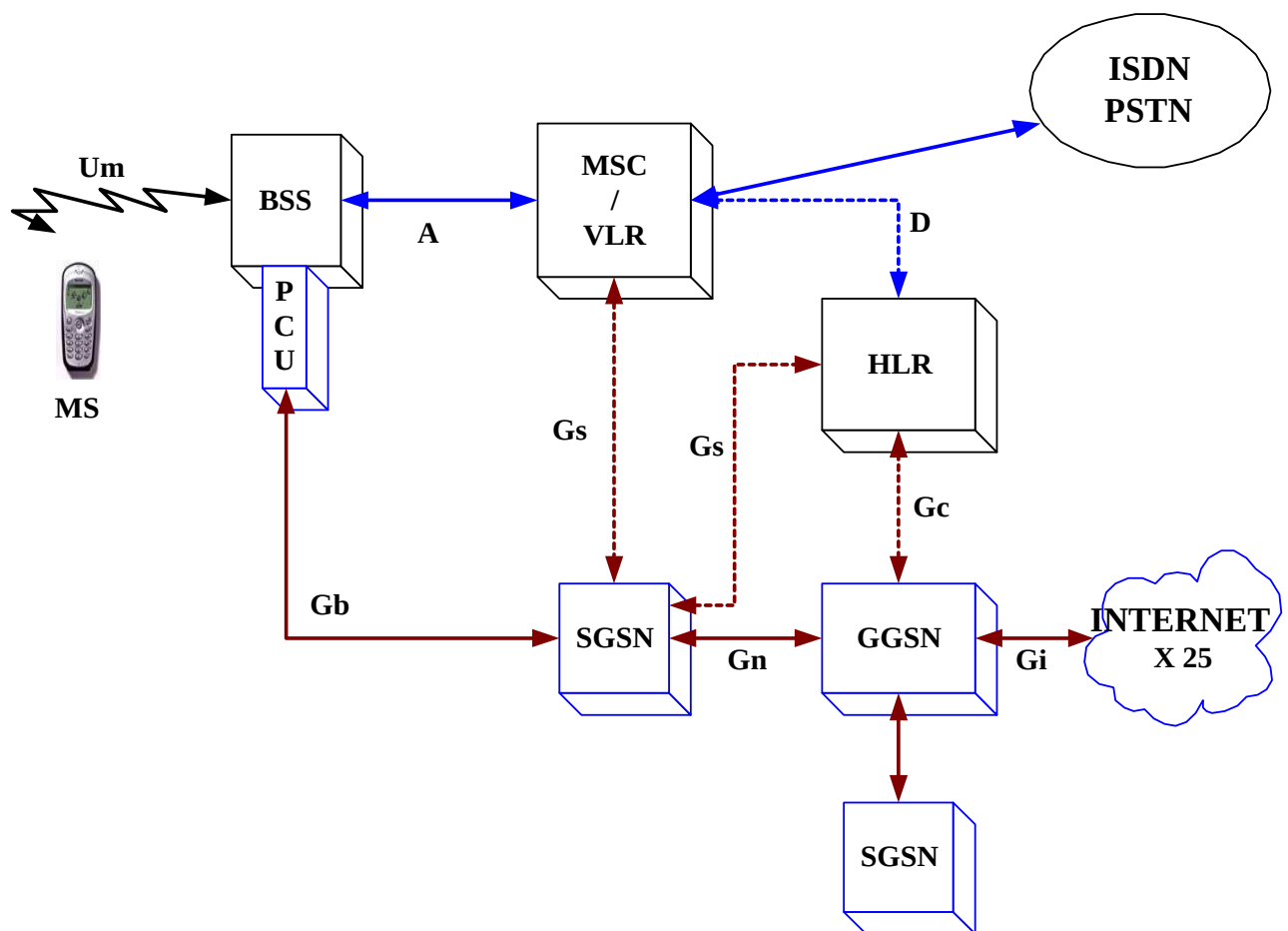


Figure 1.1.3. Structure d'un réseau GPRS

Nouveaux équipements :

❑ Le **PCU** (*Packet Control Unit*) : il assure la segmentation et l'assemblage des blocs de l'unité de paquet de données.

❑ Le **SGSN** (*Server GPRS support Node*) : c'est l'équivalent de MSC, il épargne l'emplacement du souscripteur.

Le SGSN assure les fonctions suivantes :

- o Management de la mobilité,
- o La gestion de la session (création d'un canal) ,
- o Facturation en volume

❑ Le **GGSN** (*Gateway GPRS support Node*) : c'est l'équivalent de GMSC, il permet l'interconnexion avec le réseau externe (IP/X 25). C'est-à-dire il dirige avec encapsulation les paquets IP en provenance de réseaux IP externes vers le SGSN.

I.2.1.3. Les types de services offerts par GPRS

Il y a deux types de services GPRS :

☞ Point à Point (PTP) :

o PTP (*Point to Point*) – CLNS (*ConnectionLess Network Service*) : pour ce type de service, les paquets sont indépendants, et peuvent prendre différents chemins sur le réseau (IP).

o PTP (*Point To Point*) – CONS (*Connection Oriented Network Service*) : pour cela, les paquets prennent le même chemin sur le réseau (X25).

☞ Point à Multipoint (PTM) :

o PTM-M : Multicast.

o PTM-G : Groupcall.

o PTM-IPM : IP-Multicast.

I.2.2. Le système UMTS : Universal Mobile Telecommunication System [2] [4] [14] [15] [16]

I.2.2.1. Présentation

L'UMTS est un standard qui fait parti des mobiles de la 3G (troisième génération des systèmes de télécommunication) à large diffusion, en terme couverture géographique, et dont le mode de transmission de données est basé sur la commutation par paquet. Il a été élaboré pour permettre aux usagers l'accès ultra-rapide aux services multimédia numériques (y compris les graphiques, la vidéo et le son, ainsi que l'accès ultra - rapide à Internet) jusqu'à 2 Mbit/s. Le système UMTS se présente comme un nouveau concept, qui a révolutionné à la fois les infrastructures radio, les infrastructures réseau, et les services offerts.

I.2.2.2 L'architecture du réseau UMTS

La modélisation du système UMTS est fortement inspiré de celui du GSM, il propose cependant une architecture et un découpage fonctionnel plus ouvert en séparant les fonctions liées à la technologie d'accès de celles qui ne dépendent pas du mode d'accès. Ce concept de séparation de la couche d'accès du reste du réseau accroît l'évolutivité de la norme UMTS. Cela permet, entre autres, de faire évoluer l'interface radio en minimisant les impacts sur les équipements du réseau.

Le réseau UMTS est composé de trois briques technologiques :

- ❑ le réseau cœur ou CN (*Core Network*) :
- ❑ le réseau d'accès ou UTRAN (*UMTS Terrestrial Radio Access Network*)
- ❑ le matériel de l'utilisateur ou UE (*User Equipment*)

L'interface entre les réseaux CN et UTRAN est appelée "Iu". Cette interface a été définie d'une manière aussi générique que possible afin d'ouvrir la connexion, en plus de l'UTRAN, à des réseaux d'accès de technologies différentes à celui du réseau cœur de l'UMTS.

Ainsi on pourra se connecter par exemple au SRAN (*Satellite Radio Access Network*) ou au BRAN (*Broadband Radio Access Network*), qui sont tous les deux des réseaux d'accès à large bande utilisant une technologie d'accès de type WLAN (*Wireless Local Area Network*).

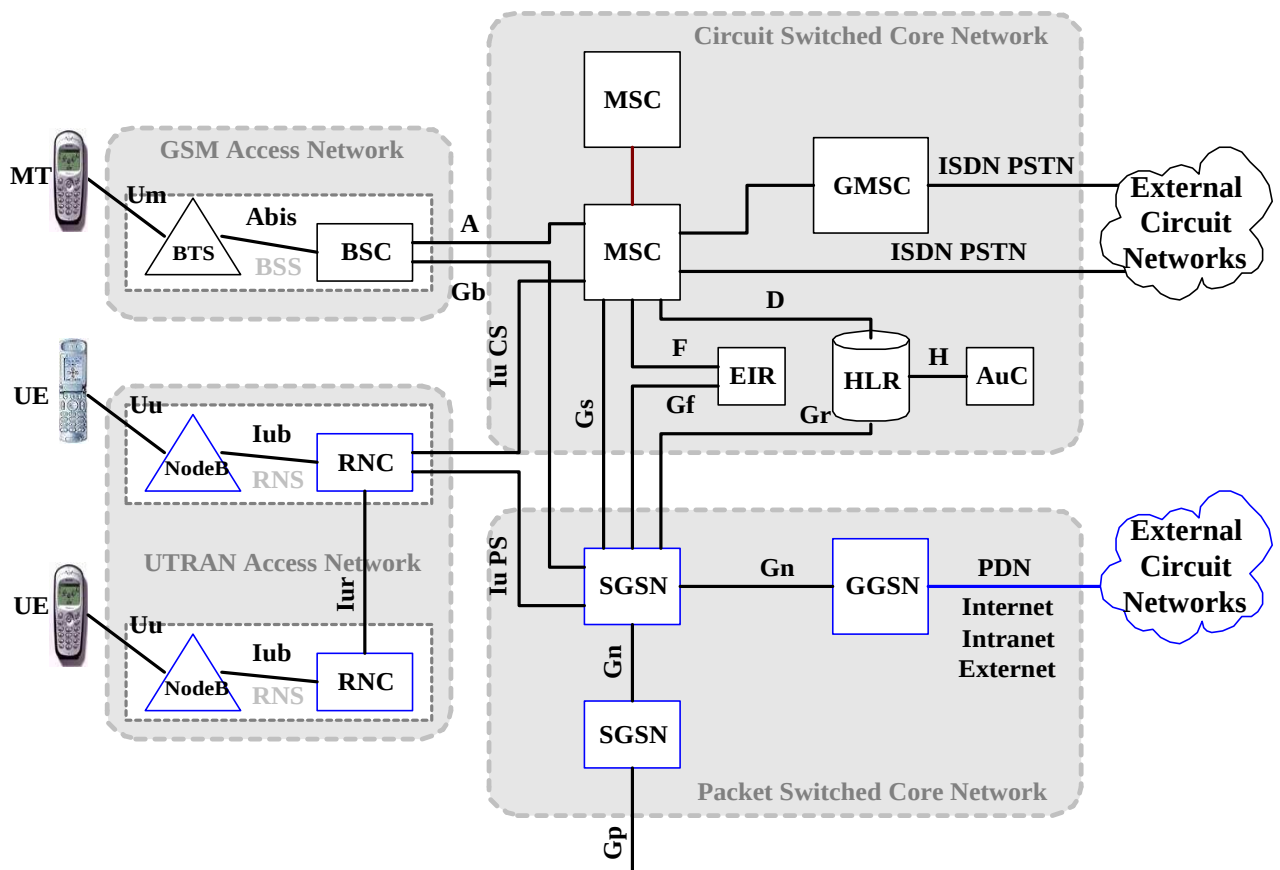


Figure 1.1.4. Architecture du réseau UMTS avec les réseaux d'accès GSM et UTRAN

1.2.2.2.1 La structure du réseau cœur de l'UMTS

Le réseau cœur permet d'aiguiller, de router, et de transiter le trafic de communication utilisateur. Il contient aussi les bases de données et les fonctions de gestion du réseau.

L'architecture du réseau cœur est basé sur le réseau GSM. Il est scindé en 2 sous-réseaux, classés selon le type de services qu'ils peuvent fournir :

- ❑ le CSCN (*Circuit Switched Core Network*) qui assure la transmission de données en mode circuit (utilisé pour la téléphonie);
- ❑ le PSCN (*Packet Switched Core Network*) : il assure la commutation de paquets (utilisé pour les données, Internet ...)

Ainsi les téléphones de 3^{ème} génération peuvent gérer simultanément une communication en mode paquet et circuit. Cette répartition permet de modéliser la notion de service dans le réseau cœur et lui donne la possibilité de créer ultérieurement d'autres services.

L'architecture du réseau cœur peut ainsi changer lorsque des nouveaux services et traits sont introduits. Par exemple, le Number Portability Data Base (*NPDB*) sera utilisé pour permettre aux utilisateurs de changer de réseau en gardant leurs anciens numéros de téléphone ; le Gateway Location Register (*GLR*) peut être utilisé pour optimiser le souscripteur qui manie entre les limites du réseau ; le MSC et Le VLR peuvent se fondre pour devenir un UMTS MSC.

Les éléments du réseau cœur sont répartis en 3 groupes, comme l'illustre la figure 1.1.5.

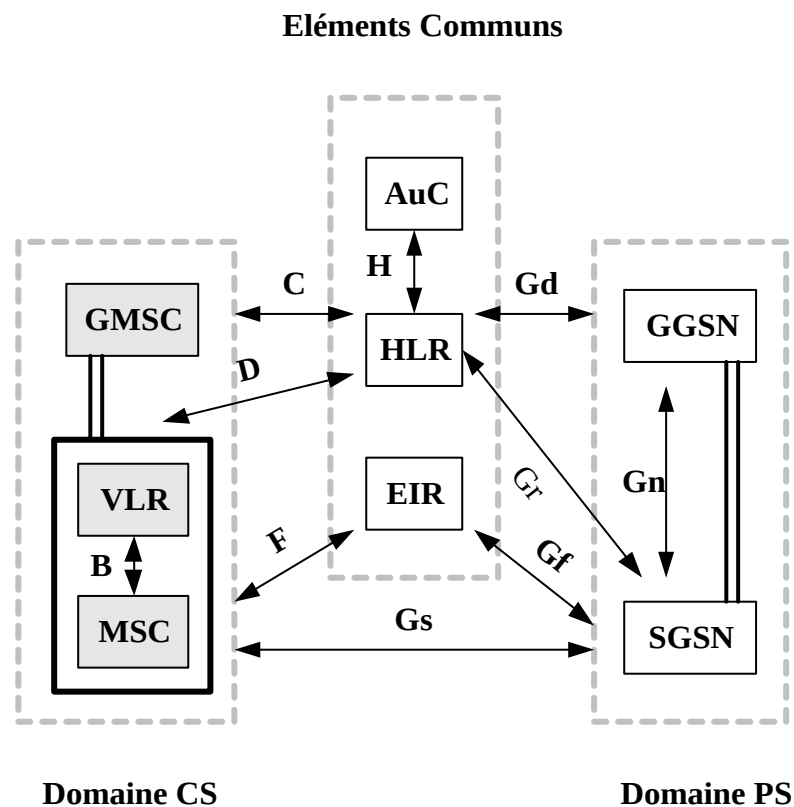


Figure 1.1.5. Constitution du réseau cœur de l'UMTS

Le groupe des éléments communs :

□ Le **HLR** (*Home Location Register*) : qui est la base de données contenant les informations relatives à l'abonné gérées par l'opérateur. Pour chaque abonné, le HLR mémorise les informations suivantes :

- les informations de souscription (abonnement, souscription à tel service, débit maximal autorisé, etc.)
- l'identité du mobile, ou IMSI (*International Mobile Station Identity*)
- le numéro d'appel de l'abonné.

□ Le **AuC** (*Authentication Center*) est un élément permettant au réseau d'assurer certaines fonctions de sécurité, telles que l'authentification de l'abonné et le chiffrement de la communication. Ces 2 fonctions de sécurité sont activées au début de l'établissement de l'appel avec l'abonné. En cas d'échec de l'une d'entre elles, l'appel est rejeté. L'AuC est couplé au HLR et contient pour chaque abonné une clé d'identification lui permettant d'assurer les fonctions d'authentification et de chiffrement.

□ L'**EIR** (*Equipment Identity Register*) est un équipement optionnel destiné à lutter contre le vol des terminaux mobiles. L'EIR est en fait une base de données contenant la liste des mobiles interdits (*black list*). L'identification du mobile se fait grâce à son IMEI (*International Mobile Station Equipment Identity*).

Le domaine CS comprend :

□ Le **MSC** (*Mobile-services Switching Center*) : c'est un commutateur de données et de signalisation. Il est chargé de gérer l'établissement de la communication avec le mobile.

□ Le **GMSC** (*Gateway MSC*) est un MSC un peu particulier servant de passerelle entre le réseau UMTS et le RTCP (*Réseau Téléphonique Commuté Public*). Lorsqu'on cherche à joindre un mobile depuis un réseau extérieur à l'UMTS, l'appel passe par le GMSC qui effectue une interrogation du HLR avant de router l'appel vers le MSC dont dépend l'abonné.

❑ Le **VLR** (*Visitor Location Register*) est une base de données attachée à un ou plusieurs MSC. Le VLR est utilisé pour enregistrer les abonnés dans une zone géographique appelée LA (*Location Area*). Le VLR contient des données assez similaires à celles du HLR et mémorise, pour chaque abonné, plusieurs informations telles que l'identité temporaire du mobile (pour limiter la fraude liée à l'interception et à l'utilisation frauduleuse de l'IMSI) ou la zone de localisation (LA) courante de l'abonné.

Le domaine PS comprend :

❑ Le **SGSN** (*Serving GPRS Support Node*) qui joue le même rôle que le VLR, c'est-à-dire la localisation de l'abonné mais cette fois sur une RA (*Routing Area*).

❑ Le **GGSN** (*Gateway GPRS Support Node*) a une fonction identique au GMSC pour la partie qui s'occupe la commutation en mode paquet du réseau, en jouant le rôle de passerelle vers les réseaux à commutation de paquets extérieurs (Internet public, un Intranet privé, etc.).

1.2.2.2.2 Le réseau d'accès UTRAN

Le concept retenu en 1998 par l'ETSI se dénomme UTRAN, qui est un compromis entre deux modes : FDD-WCDMA et TDD-WCDMA. C'est une solution mixte qui permet une utilisation complète des bandes des fréquences allouées par l'IMT-2000. En effet, les fréquences appariées devront être traitées en mode FDD-WCDMA tandis que les non-appariées devront être traités en mode TDD-WCDMA (*Wideband Code Distributed Multiple Access*)

Le réseau d'accès UTRAN est composé de Node B qui est équivalent de GSM BTS et de Radio Network Controller (RNC) qui est l'équivalent de GSM BSC. Une nouveauté avec le concept UTRAN est l'utilisation des nouveaux types de modulation : le Frequency Domain Duplex (FDD) et le WCDMA (*Wideband Code-Division Multiple-Access*) qui propose des débits allant de 384kbit/s à 2 Mbit/s. Ce nouveau concept permet d'offrir une plus haute efficacité du système quelque soit les conditions de la région : couverture urbaine, etc. et d'utiliser une porteuse de bande passante 5 MHz.

La figure suivante illustre les éléments du réseau d'accès UTRAN:

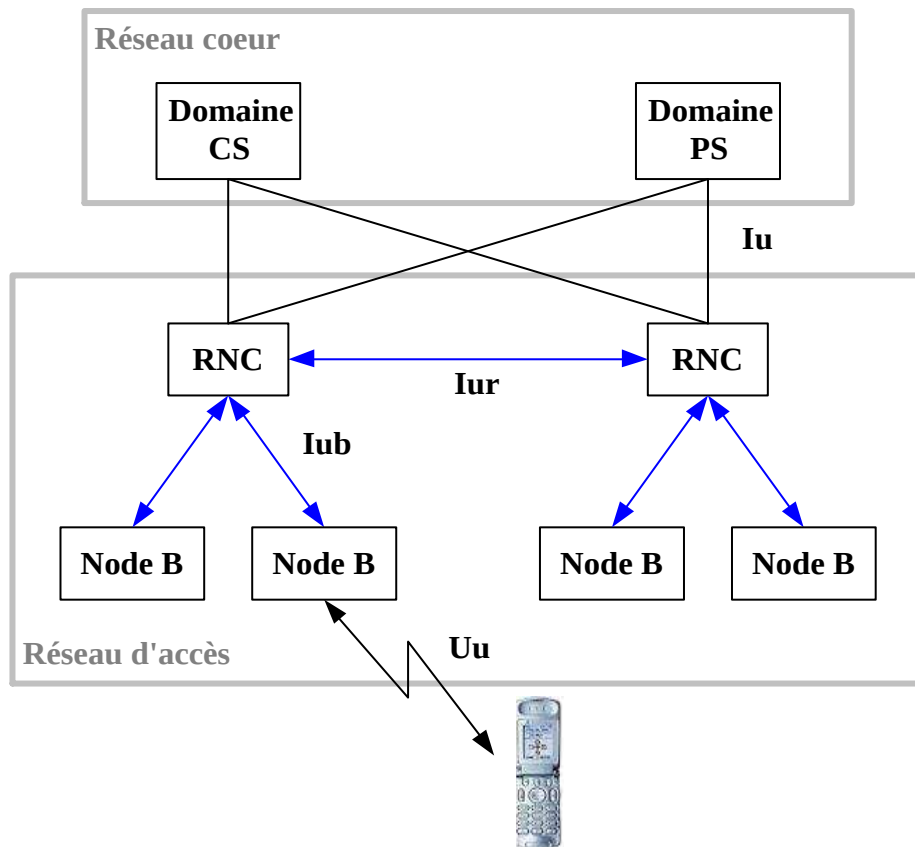


Figure 1.1.6. Réseau d'accès UTRAN

□ le **Node B** : son rôle principal est d'assurer les fonctions de réception et de transmission radio pour une ou plusieurs cellules de l'UTRAN (Figure 1.1.7.a.), c'est l'équivalent de la BTS pour le GSM. A savoir, il s'occupe des fonctions suivantes :

- Transmission et Réception
- Modulation et Démodulation
- Codage du canal physique par CDMA

□ le **RNC (Radio Network Controller)** : son rôle principal est le routage des communications entre le Node B et le réseau cœur. Lorsqu'un mobile est en communication (figure 1.1.7.b.), une connexion RRC (*Radio Resource Control*) est établie entre le mobile et un RNC de l'UTRAN. Le RNC en charge de cette connexion est appelé SRNC (*Serving RNC*). Lorsque l'utilisateur se déplace dans le réseau, il peut être conduit à changer de cellule en cours de communication, et peut même se retrouver dans une cellule faisant partie d'un Node B ne dépendant plus de son SRNC. On

appelle alors *controlling RNC* le RNC en charge de ces cellules distantes. D'un point de vue RRC, le RNC distant est appelé *drift RNC*. Les données échangées entre le *serving RNC* et le mobile transitent par les interfaces Iur et Iub. Le *drift RNC* joue donc le rôle de simple routeur vis-à-vis de ces données.

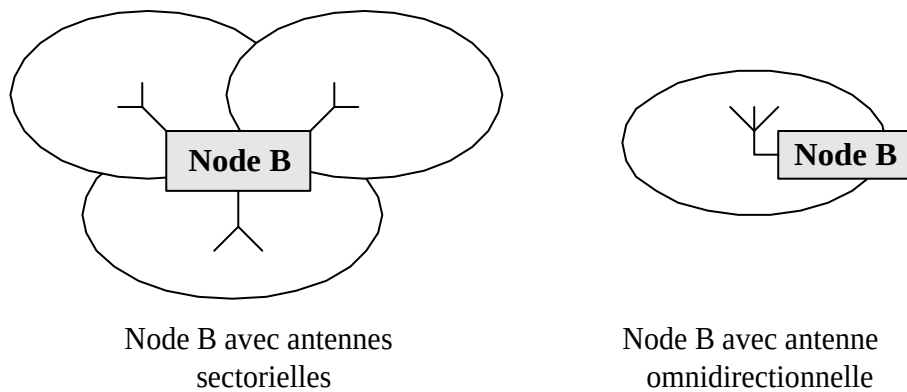


Figure 1.1.7.a. Implémentations possibles du Node B

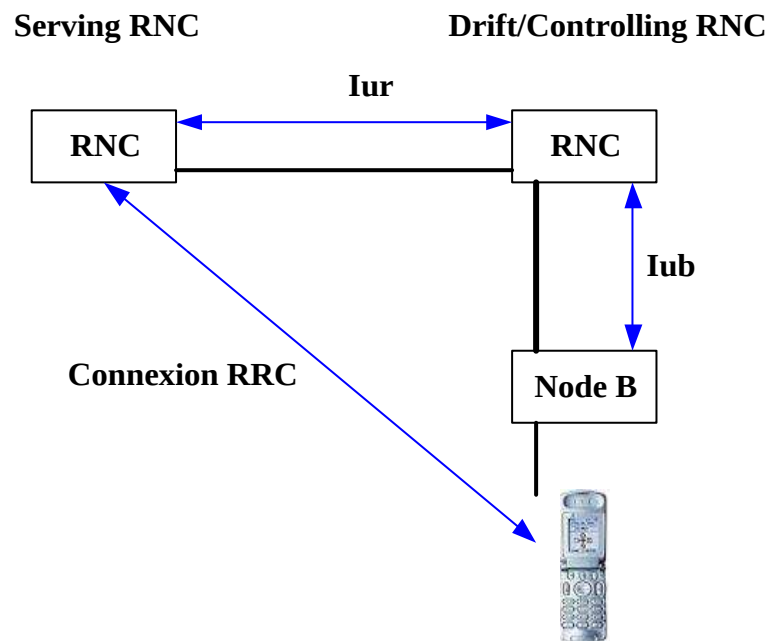


Figure 1.1.7.b. RNC et Node B en communication avec un terminal mobile

I.2.2.3. Les services offerts par l'UMTS

Les utilisateurs des systèmes de 3ème génération pourront bénéficier de nombreux services: certains sont des améliorations des systèmes existant actuellement sur les GSM, d'autres seront totalement révolutionnaires. Le consommateur pourra choisir les services auxquels il aura accès à partir de son terminal.

- Le téléphone mobile : à ce sujet, les prédictions les plus optimistes ont cours dans les milieux financiers.
- Le visiophone de poche : c'est l'une des plus spectaculaires innovations de la 3ème génération. Les terminaux portables de la 3^{ème} génération seront dotés d'une sorte de mini-écran de télévision permettant de voir l'interlocuteur avec lequel on dialogue. Dans la même lignée, on mentionnera la possibilité de faire des vidéo-conférences.
- Le communicateur personnel pour gérer son agenda qui a déjà eu un beau succès.
- Messagerie et fax rapides, fonctions existant déjà sur certains téléphones portables de la deuxième génération et qui seront plus rapides.
- Accès à l'Intranet : innovation majeure de la 3ème. Une telle innovation ne sera pas sans comporter des risques au niveau de la protection des données : on sait toutes les difficultés des grandes sociétés actuelles de se protéger contre l'intrusion inopinée des "hackers" sur son réseau
- Accès à Internet : à nouveau nous touchons ici un atout essentiel (et peut-être même le plus important) pour le développement, tant auprès du grand public que du public professionnel, du marché de la 3^{ème} génération.
- Le marché des jeux ordinateurs sera également visé par les promoteurs des portables de la 3ème génération.

Le portable de la troisième génération deviendra donc un véritable bureau mobile, pour peu que les obstacles mentionnés plus hauts soient en partie au moins contournés.

I.2.2.4. Les objectifs de l'UMTS

- L'UMTS doit répondre à un marché de masse pour les services de communication sans fil
- Offrir un service de mobilité universelle
- Offrir des services à débit élevé et de qualité de service proche de celle des réseaux filaires :
 - o 144 kbits/s en environnement extérieur,
 - o 384 kbits/s en environnement urbain extérieur,
 - o 2 Mbits/s usager quasiment immobile et proche de l'antenne d'émission de la cellule.
- Fournir une compatibilité avec le service de télécommunications personnelles universelles UPT qui gère la mobilité des clients sur l'ensemble des réseaux filaires et radioélectriques

I.2.2.5. Caractéristiques techniques

- A propos d'interface radio, il peut supporter une large gamme de services différents, c'est-à-dire l'interface radio supporte un débit d'information d'au moins 2Mbits/s.
- Pour le réseau UMTS, le changement de cellules se fait de façon transparente : aucune pertes de données, ni coupure perceptible pour l'utilisateur. Le réseau cellulaire des standards de la 3G (*troisième Génération des systèmes de télécommunication*) est en effet multicouche ; il se développe par l'interaction entre :
 - o Des macrocellules (0.5 à 10km de rayon) pour la couverture globale.
 - o Des microcellules (50 à 100m de rayon) pour la couverture des zones à forte densité de trafic.
 - o Des picocellules (5 à 50m de rayon) pour les zones à l'intérieures des bâtiments.

- Il y a une transopérabilité de l'interface radio de la 3G avec celui de la 2G en utilisant des terminaux bimodes GSM/3G à bas coût (largeur de porteuse multiple de 200kHz, utilise des débits délivrés d'une horloge commune avec celle du GSM :13 ou 26MHz).

- Bandes de fréquences utilisées par l'UMTS :

- o Bandes appariées : (1920-1980)MHz et (2110-2170)MHz : ces deux bandes sont utilisables en mode FDD (*Frequency Domain Duplex*). Mais seule la première peut être utilisée en mode TDD (*Time Domain Duplex*) afin de permettre l'acheminement d'un trafic asymétrique pour les services UMTS.

- o Bandes non appariées : (1900-1920)MHz et (2010-2025)MHz, qui sont utilisables seulement en mode TDD.

I.2.2.6. L'interopérabilité GSM-UMTS

Les normes de deuxième génération permettent une couverture presque globale des territoires. Trois types de cellules sont utilisées: des macrocellules de 15 km de rayon environ, des microcellules de 500m de rayon, et des picocellules de 100m. L'UMTS, parce qu'il opère à une fréquence plus élevée et avec des débits à la fois variables et importants, nécessite des cellules plus petites que les macrocellules actuelles, qui pourraient être de quelques centaines de mètres. Cela conduira à un réseau au coût plus élevé, coûteux en infrastructures. L'UMTS se développera probablement, dans un premier temps, dans des îlots de couverture, (milieu urbain, centres d'affaires, indoor, essai bientôt à Monaco) et se généralisera par un déploiement graduel, permettant des investissements incrémentaux. La troisième génération va donc s'adosser aux infrastructures de la deuxième génération pour s'assurer une couverture maximale, les services UMTS seront accessibles, à haut débit dans les îlots UMTS, et en mode dégradé, lorsque le mode GSM prendra le relais. Cela implique une interopérabilité maximale avec le GSM, de façon transparente, et des terminaux multimodes GSM-UMTS pour passer d'îlots en îlots en respectant la continuité de service.

I.3 Passage du système GSM vers le système UMTS

Afin d'augmenter les débits et de relier confortablement les mobiles à Internet, plusieurs technologies entrent dès aujourd'hui en lice : HSCSD (*High Speed Circuit Switched Data*), GPRS

(Général Packet Radio Services) et EDGE (Enhanced Data rates for Global Evolution), en attendant la téléphonie mobile de troisième génération, l'UMTS (Universal Mobile Telecommunication System).

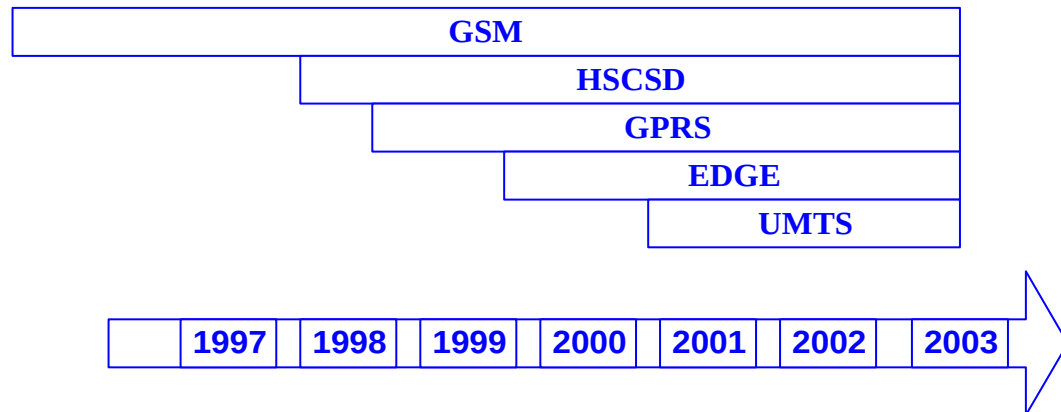


Figure 1.1.8.a. Evolution de la technologie des télécommunications sans fil

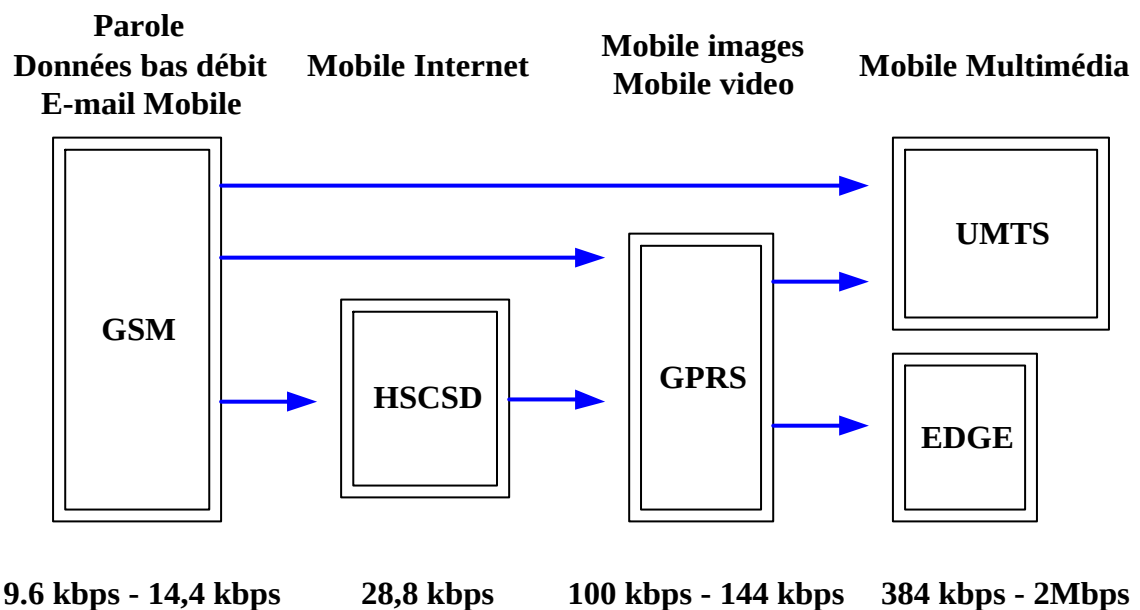


Figure 1.1.8.b. Migration des systèmes de deuxième génération vers UMTS

❑ **Le GSM** (*Global System for Mobile Communication*)

❑ **Le HSCSD** (*High Speed Circuit-Switched Data*) est une technologie à débit légèrement supérieur au GSM qui permet une couverture radio étendue grâce au nouveau schéma de codage des canaux de trafic (TCH). Mais la commutation de circuit est conservée.

❑ **Le GPRS** (*General Packet Radio Service*) permet un débit correct et une transmission de données par paquets (optimisation des ressources radio) grâce au nouveau schéma de codage des canaux de trafic et à la modification du BSS.

❑ **L'EDGE** (*Enhanced Data rates for GSM Evolution*) permet un débit élevé grâce à la modulation PSK des canaux radio GPRS. Cette technologie nécessite une bonne qualité radio et des investissements de densification des BTS.

❑ **L'UMTS** (*Universal Mobile Telecommunication System*) : cette technologie nouvelle offre un débit autour de 2 Mbit/s et une qualité de service équivalente à celle des réseaux filaires.

Technologies	Débits	Technique de commutation
GSM (<i>Global System for Mobil communication</i>)	9.6kb/s	Circuit
GSM (<i>Global System for Mobil communication</i>)	14.4kb/s	Circuit haut débit
HSCSD (<i>High Speed Circuit Switched Data</i>)	56 kb/s	Paquets haut débit
GPRS (<i>General Packet Radio Service</i>)	112 kb/s	Paquets
EDGE (<i>Enhanced Data rates for global Evolution</i>)	300 kb/s	Paquets haut débit
UMTS (<i>Universal Mobile Telecommunication System</i>)	2 Mb/s	Paquets très haut débit

Tableau 1.1.3. Tableau récapitulatif de l'évolution du système GSM vers l'UMTS

CHAPITRE II. INTERNET et INTRANET

II.1. L’Intranet [2] [3]

II.1.1. *Intranet en quelques mots*

Face aux soucis de compétitivité et de performance auxquels les entreprises modernes éprouvent le besoin de fédérer les systèmes d’informations d’un côté, et de standardiser les systèmes de communications, de l’autre côté. Elles ont recours à un nouveau système appelé « Intranet », qui n’est qu’une application à l’intérieure de l’entreprise.

Le réseau Intranet est un réseau qui permet l’interconnexion de plusieurs machines et surtout permettant l’échange des données dans une entreprise. En effet, l’Intranet favorise la facilité d’accès aux bases de données tant interne qu’externe de l’entreprise et permet également de mettre en commun les documents, les informations et les connaissances qui constituent la mémoire collective de l’entreprise.

I.1.2. *L’architecture Intranet*

L’architecture Intranet permet de router tout type de documents texte, son ou/et image d’une personne à une autre, d’une personne à une application ou entre deux applications. Le réseau Intranet est une forme simplifiée d’un réseau Internet, lors de l’échange des données dans ce premier, Intranet utilise également les standards HTML (*HyperText Markup Language*), HTTP (*HyperText Transfer Protocol*) et le protocole de communication TCI/IP (*Transmission Control Protocol/Internet Protocol*).

La figure suivante représente la structure générale d’un réseau Intranet.

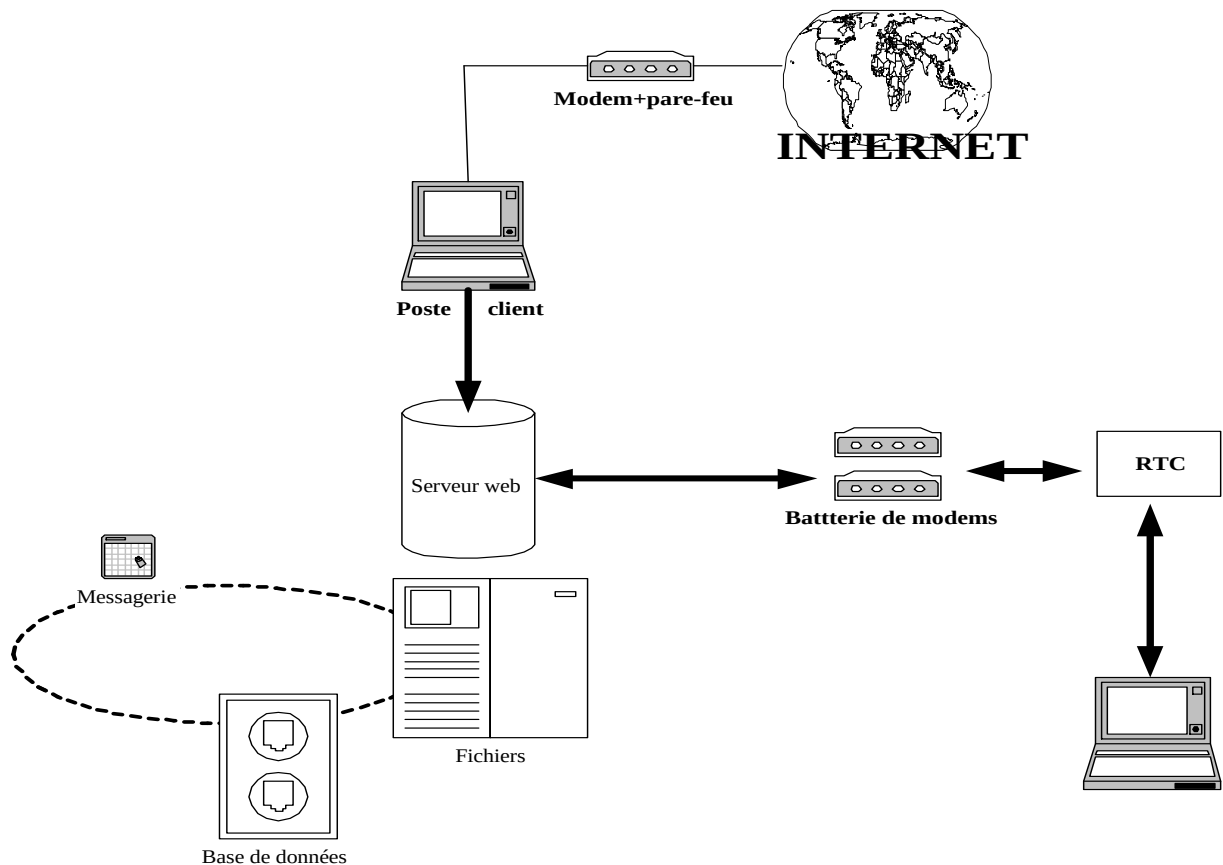


Figure 1.2.1. Structure d'un Intranet

1.1.3. Les principales fonctions de l'Intranet

Les principales fonctions de l'Intranet sont

- les messageries électroniques : Les clients sont en mesure d'accéder à un bureau de poste électronique soit à travers un annuaire stocké sur le réseau, soit directement. Le système d'adressage à l'Intranet est toujours le même que celui de l'Internet et il est aujourd'hui devenu standard.
- la conférence électronique : Une conférence électronique se constitue à l'instigation d'un utilisateur et sur le sujet de son choix. Tous les utilisateurs de l'Internet sont invités à s'exprimer soit plus précisément en répondant à une question, soit librement pour faire part de leur expérience.

- le travail de groupe : le travail de groupe est organisé dans les forums qui sont des espaces de discussions électroniques.
- le transfert de fichiers et la possibilité d'interroger ou d'alimenter les bases de données connectées au réseau de l'entreprise.
- la fonction la plus importante est que l'architecture Intranet prolonge la démarche client/serveur. L'application cliente peut se dialoguer avec le serveur central sur lequel sont disponibles les applications et les données communes de l'entreprise.

II.2. Internet [2] [3] [6]

II.2.1. Présentation

L'Internet est la mise en réseau des machines localisées sur toute la planète qui a rendu possible l'accès à des données situées sur des machines distantes, et permettant ainsi à deux utilisateurs ou plus d'échanger rapidement des informations, des messages et de se communiquer directement. Un ensemble de protocoles a été fourni pour accomplir ces tâches et qui permet le routage des informations (paquets de données). La structure logique d'Internet est donc basée sur la famille du protocole TCP/IP.

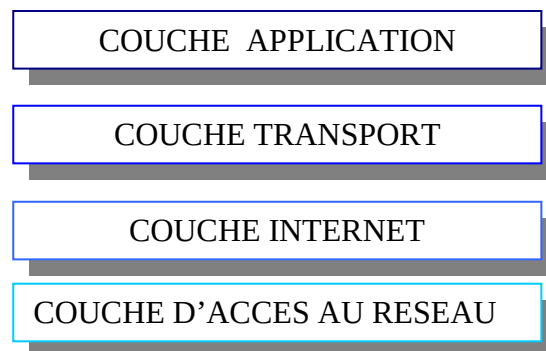
Plusieurs chemins sont possibles pour l'acheminement des données vers l'Internet :

- A l'aide du Réseau Téléphonique Commuté (RTC) : c'est le moyen le plus couramment utilisé pour se connecter à l'Internet, mais il est plus lent car le transfert de données se fait en utilisant un modem analogique avec un débit maximal de 56 kbits/s.
- A l'aide du réseau Numéris : cette méthode nous permet de se connecter au service du fournisseur d'accès à l'aide d'un adaptateur (carte insérée dans le pronostic ou boîtier externe) dont le débit atteint de 128 kbits/s.
- A l'aide d'une liaison ADSL : cette liaison permet un débit de plusieurs millions de bits par seconde. Mais aujourd'hui, les fournisseurs n'utilisent qu'un débit de 512 kbits/s ou 1Mbits/s de l'Internet au P.C. (*Personnal Computer*) de l'utilisateur, et de 128 kbits/s ou 256 kbits/s dans l'autre sens.

- A l'aide d'un câble : cette méthode permet d'offrir un débit de 512 kbit/s.
- A l'aide d'un satellite : la liaison par satellite met en œuvre beaucoup d'entités comme l'utilisation d'une carte dans le PC, d'une parabole et d'un modem (pour envoyer les requêtes vers les fournisseurs, par voie téléphonique ordinaire).

II.2.2. Modèle d'architectures TCI/IP

Au lieu de représenter un processus de communication de l'Internet par un modèle en 7 couches (modèle OSI), il est plus commode de le présenter par un modèle en 4 couches entre deux ordinateurs ou plus.



- **La couche d'accès au réseau** : la couche d'accès au réseau se contente de définir que l'hôte doit se connecter au réseau à l'aide d'un protocole, afin de transmettre des paquets IP par ce canal. Les protocoles utilisables sont notamment Ethernet FDDI, ISDN, etc.
- **La couche Internet** : qui est destinée à permettre aux ordinateurs hôtes d'envoyer des paquets sur un réseau quelconque, de piloter le mécanisme d'adressage et de choisir un itinéraire.
- **La couche transport** : Elle est chargée d'établir une liaison de transport entre deux processus s'exécutant sur différentes machines. Deux protocoles correspondants à cette couche ont fait l'objet d'une normalisation : le Transmission Control Protocol (TCP) et l'User Datagram Protocol (UDP).
- **La couche application** : Elle constitue l'interface avec l'utilisateur et regroupe toute une série de protocoles de haut niveau.

Chaque couche met ses services à la disposition de la couche supérieure et fait appel aux services de la couche inférieure. Le flux de données est donc vertical. La communication logique qui intervient entre les couches de même niveau des ordinateurs se communique entre eux. Elle fait appel à des règles destinées à coordonner la communication.

Le modèle d'architecture de communication à 4 couches n'est qu'une présentation allégée du modèle 7 couches OSI (*Open Systems Interconnection*). Le tableau suivant fournit la correspondance entre ces 2 modèles.

MODELES TCP/IP	MODELE OSI 7 COUCHES
COUCHE APPLICATION	COUCHE APPLICATION
	COUCHE PRESENTATION
	COUCHE SESSION
COUCHE TRANSPORT	COUCHE TRANSPORT
COUCHE INTERNET	COUCHE RESEAU
	COUCHE LIAISON
COUCHE D'ACCES AU RESEAU	COUCHE PHYSIQUE

Tableau 1.2.1. Correspondance entre les modèles OSI à 7 couches et TCP/IP

II.2.3. Infrastructures

(voir Figure 1.2.2.)

- **L'utilisateur** : il est équipé d'un ordinateur et selon le type de connexion avec le fournisseur d'accès, il est équipé d'un modem, d'un adaptateur Numéris, d'un modem-câble, d'un boîtier ADSL ou d'une carte pour la réception satellite.
- **La supervision** : c'est la tour de contrôle du fournisseur ; elle surveille en permanence tous les équipements du fournisseur d'accès (modem, routeur, serveur, etc....)

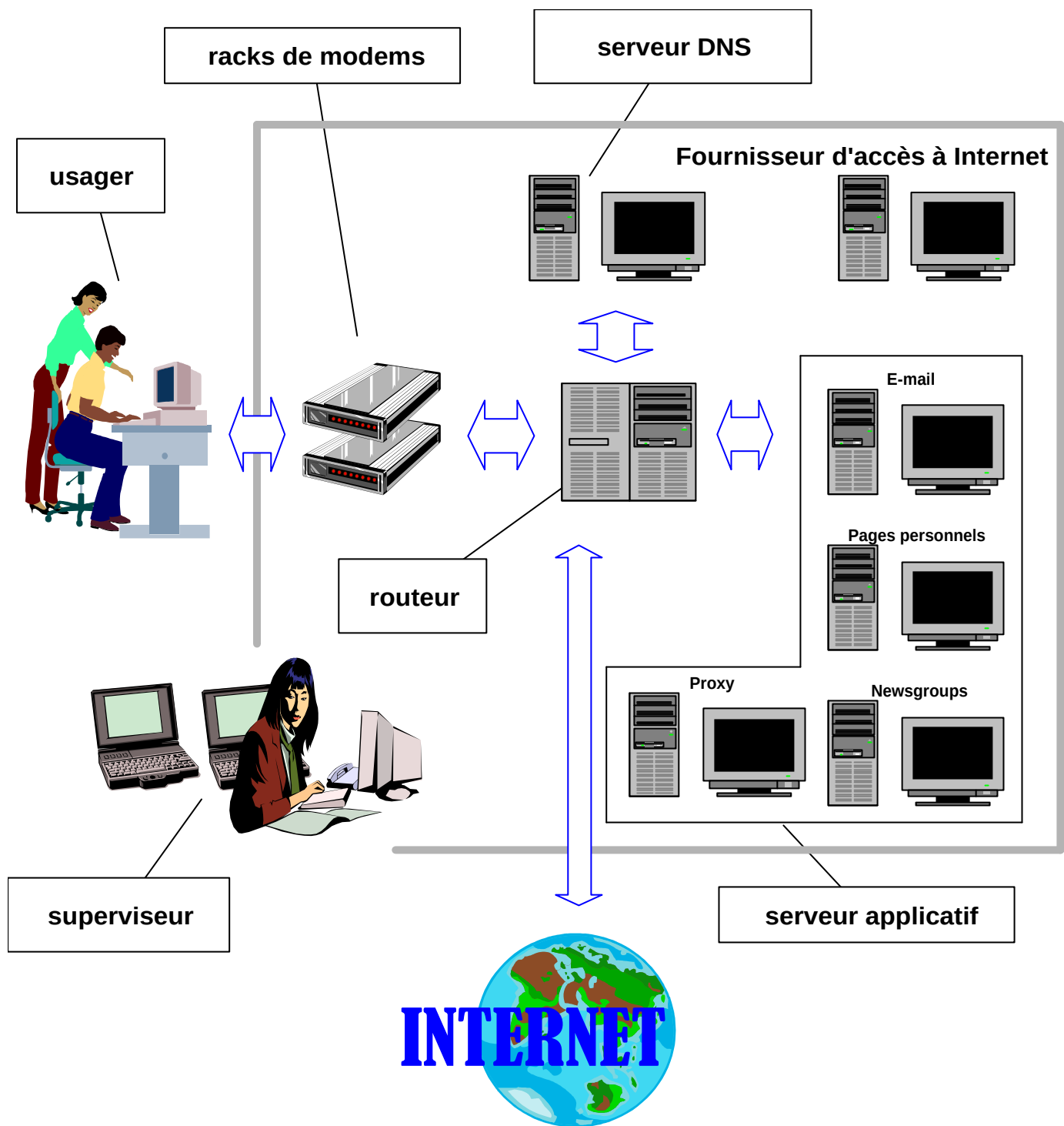


Figure 1.2.2. Structure d'Internet

- **Les racks de modem** : qui permettent la communication avec les abonnés
- **Le routeur** : c'est la gare de triage de données, cet équipement électronique dirige les données soit vers un autre routeur soit vers un serveur d'application selon l'adresse IP du destinataire. Les routeurs s'échangent en permanence des informations pour mettre à jour leur table de routage.
- **Le serveur DNS** : qui transforme toute adresse logique en adresse IP, et permet au routeur de localiser dans le monde la machine abritant le site recherché.
- **Les serveurs d'applications** : il reçoit les requêtes et réclame un traitement local

II.2.4. Les protocoles Internet

II.2.4.1. Le protocole IP

Le protocole IP met à la disposition de la couche supérieure les services suivants : l'adressage des nœuds du réseau, service du datagramme, fragmentation des paquets de données, sélection des paramètres de transmission.

Le protocole IP est situé dans la couche Internet et assure le transport des paquets de données d'un hôte à un autre

II.2.4.2. Le protocole de contrôle de transmission (TCP)

Le protocole **TCP** est un protocole appartenant à la couche transport intéressant les connexions. Il constitue un service de transmission de données en duplex. En outre, il a pour fonction :

- connexion et déconnexion de bout à bout entre des applications adressées
- détection et répartition d'erreur
- contrôle de flux
- défragmentation
- transfert de flux de données

- contrôle de flux de données

II.2.4.3. Protocole de Transfert HyperTexte (HTTP)

C'est le protocole de la couche application, le protocole HTTP est basé sur le protocole TCP/IP. Il règle la communication entre le serveur Web et le client Web, c'est-à-dire le protocole HTTP (*HyperText Transfer Protocol*) qui définit le format, le contenu, et l'ordre des messages échangés entre le client et le serveur. Le protocole HTTP est un protocole sans connexion, c'est-à-dire que le serveur et le client terminent le processus à l'issue de chaque commande

II.2.4.4. Le protocole de transfert de fichier FTP

Le protocole FTP (*File Transfer Protocol*) permet l'échange de fichier entre deux machines indépendamment du système d'exploitation et il est basé sur le protocole TCP. Il appartient à la couche Application.

II.2.4.5. Le protocole de transfert simple de courrier SMTP

Le protocole SMTP (*Simple Mail Transfer Protocol*) est un protocole simple basé sur FTP et il est destiné à l'échange des courriers électroniques entre différentes machines. Il fait aussi partie de la couche Application.

II.2.4.6. Le protocole de bureau de poste POP

C'est un protocole standard utilisé par les clients de messagerie pour lire des informations provenant du serveur. La dernière version est nommée **POP3**. En particulier, POP3 permet de déterminer si les messages lus doivent être conservés sur le serveur ou s'ils doivent être supprimés après avoir été transmis.

II.2.4.7. Le protocole d'accès au message électronique IMAP

c'est un protocole de messagerie étendue dont les fonctionnalités sont supérieures au protocole POP3. Il a pour but de transmettre des messages selon les besoins et de sélectionner les données à transmettre.

En outre, le protocole IMAP (*Internet Mail Application Protocol*) permet la mise en place des boîtes aux lettres hiérarchiques directement sur le serveur. Il permet aussi d'accéder aux

différentes boîtes aux lettres lors d'une connexion, ainsi que de modifier le statut d'un message et d'enregistrer ou de supprimer des messages sur le serveur.

II.2.5. Services disponibles sur l'Internet

Les services disponibles sur Internet peuvent être classés en 2 catégories : les services de base et les services d'information :

II.2.5.1. Les services de base

ils sont nécessaires à tout organisme connecté au réseau et comprennent :

- **la messagerie**

Elle permet aux utilisateurs d'échanger entre eux des messages composés d'un texte et éventuellement de pièces jointes. Ce message ne comporte que quelques lignes. L'envoi d'un message de ce type nécessite un logiciel adéquat sur le poste de travail, auquel on doit fournir l'adresse du destinataire. L'adresse électronique du destinataire est unique, et est souvent du type [Prenom.Nom@domaine.mg](#)

- **le DNS (*Domain Name Server*)**

C'est un service réparti dans lequel participe de nombreuses machines sur l'Internet, il permet d'associer des noms de machines à des adresses IP et réciproquement. Ce service peut aussi fournir de nombreux autres services notamment l'acheminement du courrier électronique.

- **les forums**

Ils regroupent, au sein d'un même service, des lieux d'échange où les utilisateurs peuvent dialoguer.

- **L'accès distant**

L'accès aux ordinateurs par le service Telnet permet le contrôle d'un matériel éloigné

II.2.5.2. Les services d'information

Leur apparition sur le réseau est relativement tard, et ils comprennent :

- **Le transfert de fichier**

Il est connu sous le nom de **FTP**, et il permet de rapatrier des fichiers quelconques depuis des serveurs d'archives

- **Les bases de données WAIS**

Les serveurs WAIS permettent de rechercher des informations sur d'immenses bases de données.

- **Le dialogue interactif : IRC**

Le service IRC (*Internet Relay Chat*) permet de dialoguer dans des forums mais de manière différente de celle des News, les dialogues se font ici en direct.

- **Les services IP multicast**

Ils permettent l'audio et la vidéo-conférence, ainsi que de nombreux autres services coopératifs

- **Le WWW (*World Wide Web*)**

C'est le service le plus utilisé en terme de nombre de paquet qui transite sur le réseau. Il permet l'accès à des documents multimédia sur des serveurs WWW.

- **Le WAP (*Wireless Application Protocol*)**

Ce service est un nouveau service qui est introduit dans le domaine Internet. Il permet la communication des mobiles avec les réseaux Internet et Intranet. Il permet aux clients mobiles de consulter des données et des applications circulant sur les réseaux Internet et de pouvoir se connecter rapidement avec des ordinateurs existant dans un réseau Intranet partout où ils se trouvent. Ceux-ci sont possibles avec la présence de la couche WAE (*Wireless Application Environment*), qui fournit l'interaction entre les applications WAP/Web et les appareils mobiles qui contiennent un micro-navigateur WAP.

Chapitre III. LA TECHNOLOGIE WAP

III.1. Définition et présentation [1] [30] [31] [32] [33] [35] [37]

La technologie WAP (*Wireless Application Protocol*) permet à des terminaux mobiles (téléphone portable, PDA etc...) d'accéder à des documents circulants par des réseaux sans fil et de pouvoir formater ces documents. Un protocole universel appelé Wireless Application Protocol (WAP) a été donc créé. Il fournit à des clients mobiles, à des clients WAP, l'accès à des services Internet. WAP est un protocole de communications et d'environnement d'application; en d'autres termes, le standard WAP spécifie donc les deux éléments essentiels de la communication sans fil: un protocole d'application couvrant toute la chaîne de connexion et un environnement d'application basé sur un navigateur similaire à un navigateur Web. Le modèle WAP est donc très semblable à celui de l'Internet de bureau traditionnel. L'appareil mobile comporte un logiciel navigateur qui connecte à une passerelle WAP (infrastructure logiciel qui réside dans le Réseau de l'Opérateur et qui optimise la transmission de données dans le réseau sans fil) et fait des demandes pour les informations du serveur Web dans la forme normale d'un URL (*Universal Resource Locator*). Les données venant des appareils mobiles peuvent être mémorisées sur tout serveur Web sur l'Internet. Le contenu doit être formaté pour le petit écran du téléphone mobile et la faible bande passante du réseau sans fil. Il est écrit dans un langage appelé WML (*Wireless Markup Language*).

Depuis la mise en œuvre de cette technologie, certains terminaux mobiles (GSM, GPRS, UMPS,...) dans lesquels sont incorporés des navigateurs WAP ne sont plus de simples téléphones, mais des appareils sophistiqués capables d'exécuter des applications et de communiquer avec des ordinateurs et des applications sur un réseau sans fil. Ces navigateurs WAP peuvent être construits sur tout système d'exploitation y compris PalmOS, EPOC, Windows CE, FLEXOS, OS/9, et JavaOS, etc. et peuvent traiter le contenu décrit en WML (*Wireless Markup Language*) et d'exécuter des applications écrites dans le langage de script appelé WMLScript.

WAP définit un groupe de composants standards qui permet la communication entre les terminaux mobiles et le serveur du réseau:

- Modèle standard de nom : le standard URL WWW est utilisé pour identifier le contenu du WAP dans le serveur d'origine. Il permet aussi d'identifier les ressources locaux dans ce dispositif .

- Contenu typique : tout le contenu du WAP offre un type spécifique compatible avec le WWW typique. Ceci permet aux utilisateurs-agents du WAP de traiter correctement le contenu basé sur ce type.

- Formats standards de contenu : basés sur la technologie WWW.

- Protocoles standards de communication

III.2. Architecture [1] [30] [32] [35] [37]

La technologie WAP doit permettre d'accéder à des services Web ; un serveur WAP est donc semblable à un serveur WEB, mais la façon d'y accéder est un peu particulière. WAP utilise la technologie « proxy » pour assurer la communication entre le domaine sans fil et le WWW.

En général, les architectures WAP reposent sur quatre briques technologiques, chacune étant nécessaire pour garantir l'acheminement d'un message par le protocole WAP (*Figure 1.3.1.*):

- La mise en place d'un serveur Web et/ou d'un serveur d'application disposant de contenu au format WAP (ou plus précisément WML)

- L'intégration d'une passerelle ou d'un serveur proxy WAP

- Le réseau de l'opérateur

- L'utilisation par le client d'un terminal WAP (qui héberge un navigateur WAP)

Les similitudes avec les architectures Web s'expliquent facilement. En effet, ces deux architectures remplissent la même mission, celle de générer des documents à partir de différentes sources de données et de les transmettre à un navigateur dédié.

On sait que le protocole WAP est indépendant des architectures matérielles utilisées par l'opérateur, ce qui lui permet de circuler sur des réseaux aux formats aussi divers que GSM, CDMA, GPRS, UMTS, ...

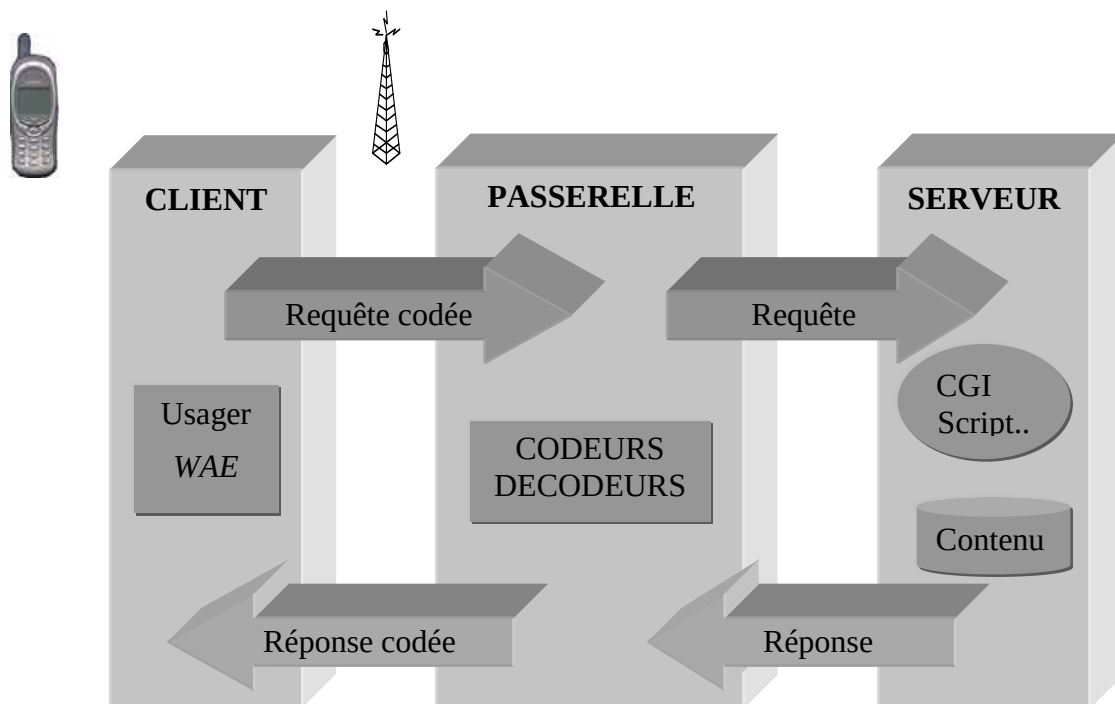


Figure 1.3.1. Structure d'un réseau WAP dans le cas général

Le schéma de la Figure 1.3.1. ci-dessus est en quelque sorte une vulgarisation de l'architecture WAP. Celui-ci peut être variée, la passerelle peut donc être située à différents endroits sur le réseau.

III.2.1. Le terminal WAP

Le terminal WAP est un terminal mobile bibande doté d'un écran tactile, permettant d'accéder à l'Internet et qui peut synchroniser par d'autres terminaux de communications. Il possède une pile IP réduite, ce qui lui confère des capacités IP réduites elles aussi. Lorsqu'une connexion est ouverte, le terminal WAP établit une liaison PPP jusqu'au Fournisseur d'Accès à Internet, de la même façon que pour une connexion Internet standard. Grâce à cette connexion PPP, après avoir été identifié avec un login et un mot de passe, le terminal WAP obtient une adresse IP temporaire et devient capable d'accéder à n'importe quels services Internet ou Intranet grâce au portail WAP de son choix.

Les téléphones compatibles WAP incorporent un modem à même de se connecter à la demande à une passerelle spéciale appelée « Gateway » pour lui indiquer la page Internet que l'utilisateur souhaite visualiser.

Les navigateurs WAP :

Caractéristiques de quelques mobiles :

	Nokia 7110	Ericsson R320	Ericsson R380	UP Browser
Taille de la carte	1 397 o	3 000 o	3 800 o	1 492 o
Taille d'image	1 397 o	3 000 o	3 800 o	1 492 o
Nombre de colonnes	19	14		
Nombre de lignes	5	5	7	
Largeur de l'écran	95 pixels	101 pixels	304 pixels	
Hauteur de l'écran	45 pixels	52 pixels	98 pixels	
Formatage	Aucun	Condensé, gras	Condensé, étendu, gras, italique	Variable selon les modèles
Alignement	gauche	Gauche, centré, droit	Gauche, centré, droit, justifié	Variables selon les modèles

Tableau 1.3.1. Caractéristiques de quelques outils de navigation WAP

Les limitations techniques des portables constituent l'un des plus grands problèmes de l'utilisation du WAP. Les portables sont essentiellement caractérisés par :

- l'absence d'un véritable clavier
- la limitation des caractéristiques de l'écran par :
 - o sa taille
 - o sa résolution
 - o sa profondeur de couleur
- la mémoire relativement réduite

Il faut savoir donc que la taille maximale d'une carte dépend de la capacité mémoire disponible (qui varie d'un modèle à l'autre). Cette taille de la mémoire ne fait pas partie des spécifications du forum WAP et diffère d'un utilisateur à l'autre. Par ailleurs, tous les modèles ne prennent pas en charge l'ensemble des attributs de formatage des textes.

III.2.2. La passerelle WAP ou serveur proxy WAP

III.2.2.1. Définition et rôles

Pour permettre aux mobiles d'accéder effectivement à des sites WAP, il faut que l'opérateur du réseau téléphonie mobile dispose d'une nouvelle technologie. Si on consulte un site WAP par l'intermédiaire d'une connexion Internet classique (à l'aide d'un poste téléphonique fixe) et non à travers un réseau de téléphonie mobile, on n'a naturellement pas besoin de passerelle . Cependant, on ne peut pas accéder à certaines pages spécifiques aux fournisseurs d'accès.

Le serveur proxy WAP interconnecte le réseau sans fil à un réseau IP sur lequel se trouvent le serveur Web et le serveur de données et d'applications, c'est-à-dire, il joue le rôle d'interface entre le terminal mobile fonctionnant sur un réseau sans fil et le réseau IP. Le proxy WAP comprend les fonctionnalités suivantes :

- Protocole passerelle : le protocole passerelle traduit les requêtes en provenance de la pile de protocole WAP (WSP,, WTP, WTLS,et WDP) vers la pile de protocole WWW (http et TCI/TP) et vice versa. C'est-à-dire, il se charge de la transformation des protocoles WAP et http.
- Encodeur/décodeur : il permet de transformer le contenu du WAP en provenance du serveur (donnée au format ASCII, *American Standard Code for Information Interchange*) en données binaire compactée (encodage des documents WML et des scripts WMLScript avant leur envoi vers le mobile) afin de réduire la taille de donnée quittant le réseau du serveur. Ce qui est plus adaptée à transiter sur le réseau sans fil de bande passante plus étroite. Dans l'autre sens, l'Encodeur/décodeur crée une requête http normale à partir de la requête WAP.

III.2.2.2. Les différents emplacements de passerelle WAP

III.2.2.2.1. Passerelle WAP chez l'opérateur

Cette solution technologique est celle qui est mise en œuvre pour une connexion WAP dans la plupart des cas. Autrement dit, elle présente le matériel mis en oeuvre par les opérateurs téléphoniques pour que les usagers puissent accéder aux contenus WAP. Dans ce cas précis, l'opérateur héberge aussi bien la passerelle WAP que le RAS (*Remote Access Service*) qui permet d'accéder à Internet. C'est cette solution, facile à mettre en œuvre qui est utilisée dans le cas de la diffusion de contenus WAP sur les sites des opérateurs.

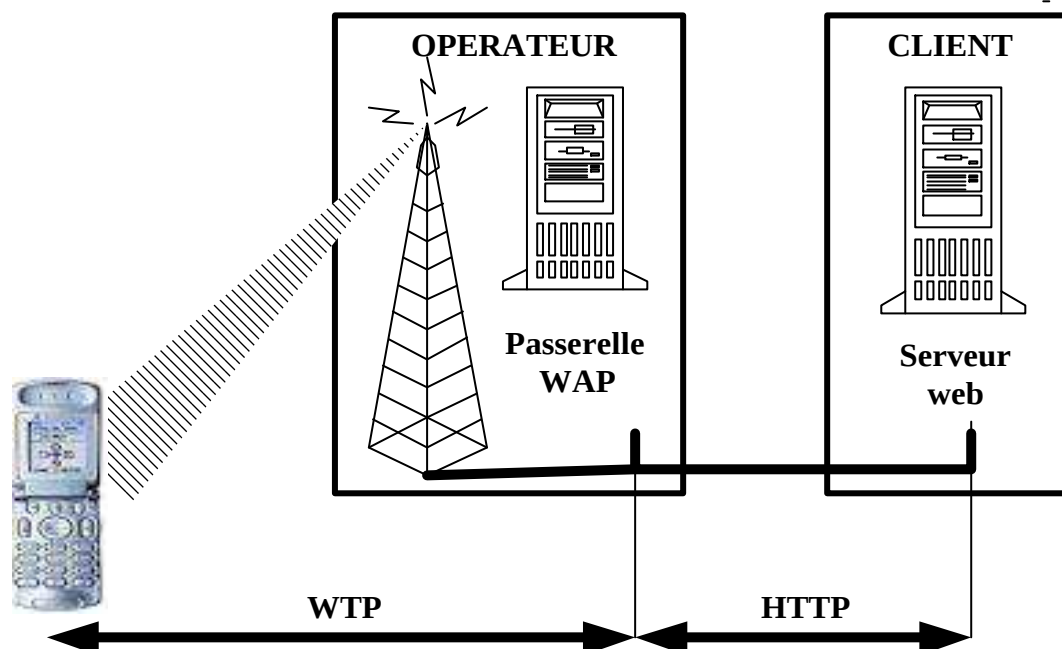


Figure 1.3.2. Passerelle WAP chez l'opérateur

III.2.2.2.2. Passerelle chez un fournisseur

Cet aspect présente l'avantage, pour les fournisseur d'accès, de ne pas être dépendants des opérateurs téléphoniques et de pouvoir ainsi administrer leur propre passerelle WAP. Dans ce cas, seule la connectivité GSM/RTC des opérateurs est utilisée. L'utilisateur compose ainsi directement le numéro du fournisseur qui devient donc un opérateur téléphonique alternatif spécialisé dans la connexion Internet via le WAP.

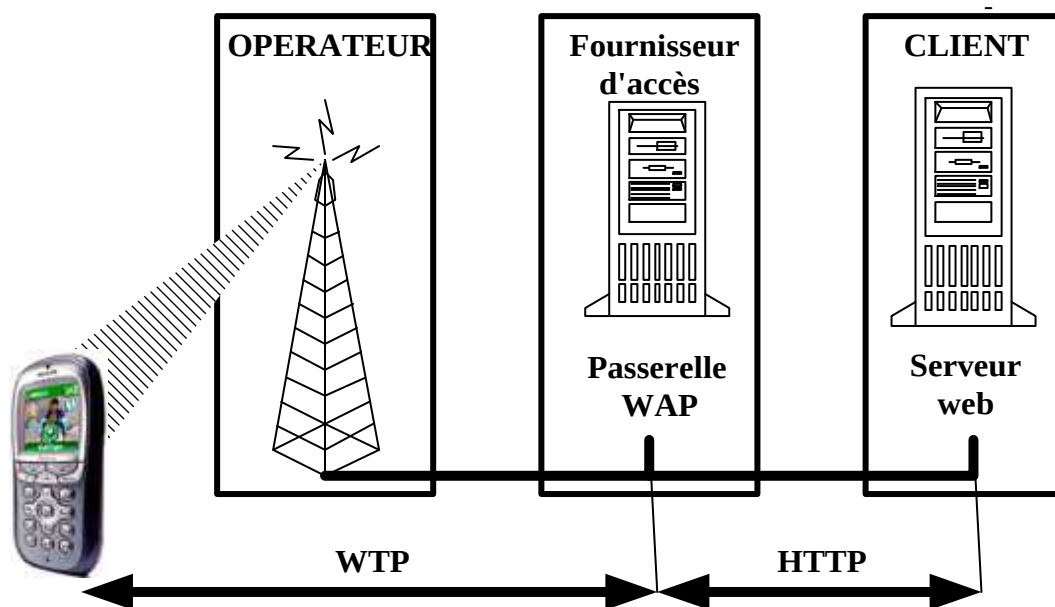


Figure 1.3.3. Passerelle WAP chez un fournisseur sans hébergement d'un site Web

Si le fournisseur a également la vocation d'héberger des sites Web, on se retrouve dans la configuration ci-dessous :

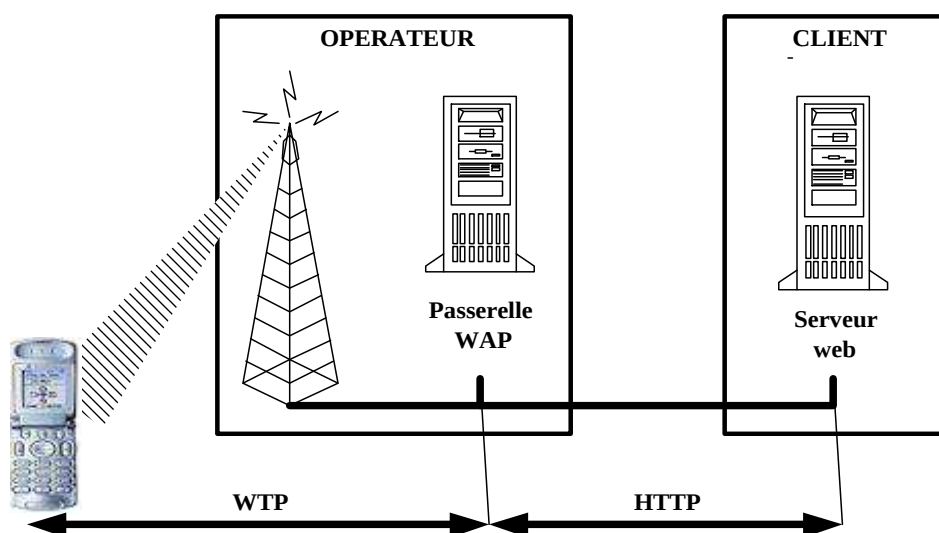


Figure 1.3.4. Passerelle WAP chez un fournisseur avec hébergement d'un site Web

Dans ce cas, on ne parle plus de passerelle WAP mais bien de serveur WAP, puisque la machine qui l'héberge intègre à la fois la passerelle WAP mais aussi un serveur d'application WAP. Le fournisseur devient donc un opérateur téléphonique alternatif spécialisé dans la connexion Internet via le WAP mais aussi dans la diffusion du contenu.

III.2.2.2.3. Passerelle WAP en interne

Cette solution peut être envisageable dans le cas d'applications WAP dédiées à une entreprise et exploitant des données sur l'Intranet. Et si le client veut également garder la maîtrise complète des connexion WAP, il peut décider d'avoir sa propre passerelle WAP.

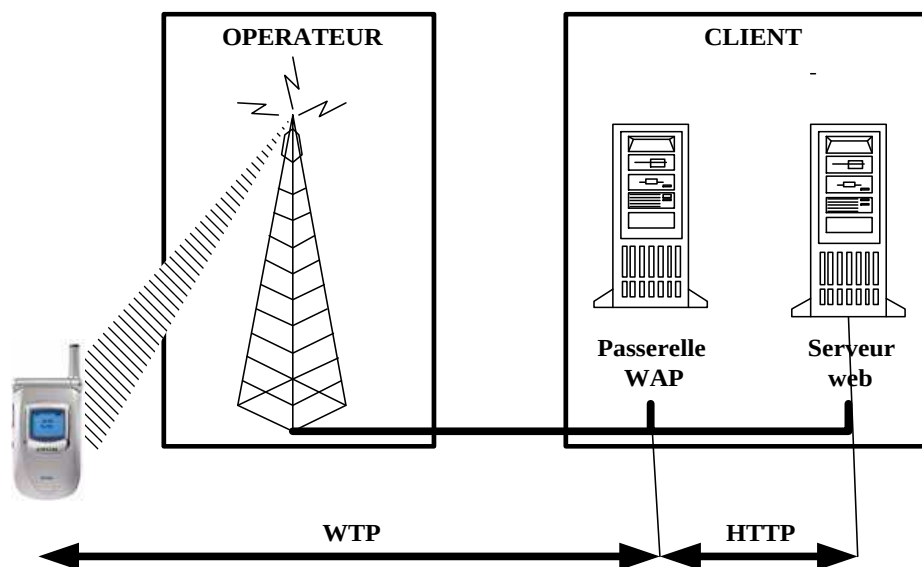


Figure 1.3.5. Passerelle WAP chez le client

III.2.2.3. Impératives techniques des passerelles WAP

Pour accéder au monde WAP, il faut d'abord accéder à une passerelle à l'aide du numéro de téléphone, de l'adresse IP de la passerelle qui sert également de serveur proxy, ainsi que d'un nom d'utilisateur, d'un mot de passe et des informations techniques concernant le processus de transmission. L'accès à la passerelle est comparable à un accès « by-call » à Internet au cours duquel une connexion à un numéro déterminé alloue une adresse IP temporaire à l'équipement local et établit une connexion réseau.

Dans le cas d'Internet, les demandes et le contenu des pages WML sont transmis par le protocole http 1.1 (*HyperText Transfert Protocol*) entre des serveurs Web normaux. La passerelle WAP à laquelle le téléphone portable est connecté favorise seulement la conversion des fichiers WML et des fichiers WMLScript au format ASCII en un format binaire spécial utilisé par les mobiles WAP. Ce format binaire est appelé WBXML (*WAP Binary XML*). Ce code binaire n'occupe environ qu'un quart de la taille du fichier d'origine. L'opération de compilation en binaire est réalisée par des compilateurs qui prennent en charge les éléments de structure du langage XML (*Extensible Meta Language*) et peuvent ainsi éliminer automatiquement les éléments inconnus de ce langage. C'est ainsi que les balises META-informations et les éléments redondants (ou les commentaires) ne sont pas transmis, ce qui réduit beaucoup les temps de transmission. L'en-tête DTD est omis alors de la compilation, ce qui n'autorise pas pour autant de la supprimer du code source des fichiers WML. En effet, le compilateur y trouve des informations concernant la version et les extensions phone.com éventuellement utilisées.

Lors de la conversion au format binaire WBXML, le contenu de page n'est pas modifié ; ce qui signifie que les données d'origine peuvent être restaurées, à l'exécution des données redondantes, que l'utilisateur ne voit en aucun cas. Il y a cependant une exception. Normalement, vous appelez à partir de votre mobile des pages WAP spéciales, c'est-à-dire les documents programmés en WML. Il existe également la possibilité d'appeler des pages Web normales. Les téléphones mobiles n'étant pas capables d'afficher des fichiers programmés en HTML (*HyperText Markup Language*), ces pages sont également converties au format WML par la passerelle.

Remarques : il ne faut cependant pas se faire d'illusion. Bien qu'il soit théoriquement possible de convertir n'importe quel fichier HTML au format WML pour pouvoir l'afficher sur n'importe quel mobile, on risque de rencontrer des difficultés incontournables lors de ce cas :

- ❑ Le langage HTML n'est pas prévu pour des afficheurs aux performances réduites, ce qui élimine un grand nombre de fonctions lors de la conversion. Si un paragraphe particulièrement important d'une page Web est identifié par une couleur spéciale, cette mise en évidence sera perdue lors de la conversion en WML, ce qui impose de trouver une alternative. En effet, la passerelle élimine cette mise en évidence.

- ❑ Les pages Web sont programmées pour des navigateurs Web. En général, elles contiennent beaucoup plus de textes que ce qui est raisonnablement affichable sur un mobile. Par

ailleurs, les images sont très largement utilisées sur le WWW et sont trop nombreux et surtout trop volumineuses pour le WAP. L'élimination des images implique généralement la perte d'une partie importante des fonctionnalités de la page concernée.

III.2.2.4. Fonctionnement de la passerelle WAP

Dans l'architecture d'une passerelle, on va retrouver un certain nombre de couches du protocole WAP (à l'exception de la couche application WAE). La passerelle est chargée de convertir les données, reçues dans les datagrammes WDP, en paquets conformes au protocole HTTP pour pouvoir dialoguer avec des serveurs Web et vice-versa.

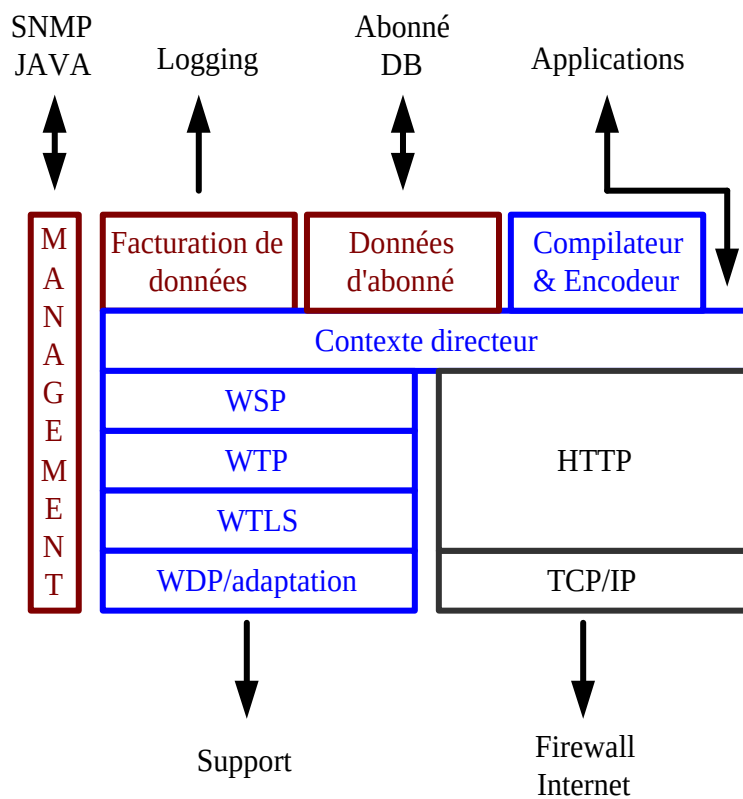


Figure 1.3.6. Détail du fonctionnement de la passerelle

III.2.3. Le serveur d'application WAP

III.2.3.1. Structure

Le serveur d'application WAP n'est autre qu'un serveur http, c'est-à-dire un serveur Web standard, qui délivre des documents WML, des scripts WML et des images au format Wbmp.

Cependant, Il faut prendre un peu d'écart par rapport aux serveurs Web classiques qui existent sur Internet et qui n'hébergent que des pages HTML. En effet, dans l'architecture WAP, le serveur Web a le rôle de fournir des documents qui seront affichés sur le navigateur via la passerelle WAP. Ainsi, son but n'est plus seulement de fournir des documents au format HTML mais également au format WML (Wireless Markup Language), langage en vigueur sur les terminaux WAP. Pour cela, il pourra être couplé à des bases de données pour générer le contenu ou à des serveurs d'applications (destinés à la traduction des pages HTML en WML par exemple). Parfois, certains constructeurs ont mis sur le marché un produit appelé « serveur WAP » qui est en réalité une passerelle WAP associée à un serveur http . La partie passerelle s'occupe de la connexion, le serveur s'occupe de fournir le contenu .

III.2.3.2. Qu'est - ce qu'un serveur Web standard ?

Un serveur Web est une application qui stocke des pages électroniques composées de données multimédias. Lorsqu'un client envoie une requête qui demande une page spécifique, le serveur la traite et renvoie au client la réponse qui lui convient.

Exemples de serveur Web : Apache, CERN, Plexus, NCSA...

III.2.3.3. Concept d'URL

L'URL (*Universal Resource Locator*) décrit le protocole utilisé pour aboutir au serveur cible. Il constitue le nom du système (nom du serveur) où réside le document, le chemin d'accès et le nom du fichier. Un URL prend alors la forme suivante :

Méthode_ d'accès://<net_loc>[:n°de_port]/chemin/fichier

Où :

- **'méthode_d'accès'** représente le protocole par le terminal pour communiquer avec le serveur. Le « deux point » suivit de « deux slash » («:// ») sépare le protocole de l'identité du serveur .

- **'<net_loc>'** indique l'adresse IP ou le nom de domaine de la machine hébergeant le serveur Web. Le [:n°de_port] comme il indique : c'est le port utilisé par la machine hôte ; c'est une option facultative car s'il n'est pas identifié, c'est le numéro de port par défaut qui sera utilisé.

- La **'barre oblique'** (ou « slash ») identifie que l'on est dans le répertoire de la machine
- **'chemin'** indique le répertoire sur lequel se situe le fichier à consulter.

Principes d'un serveur Web

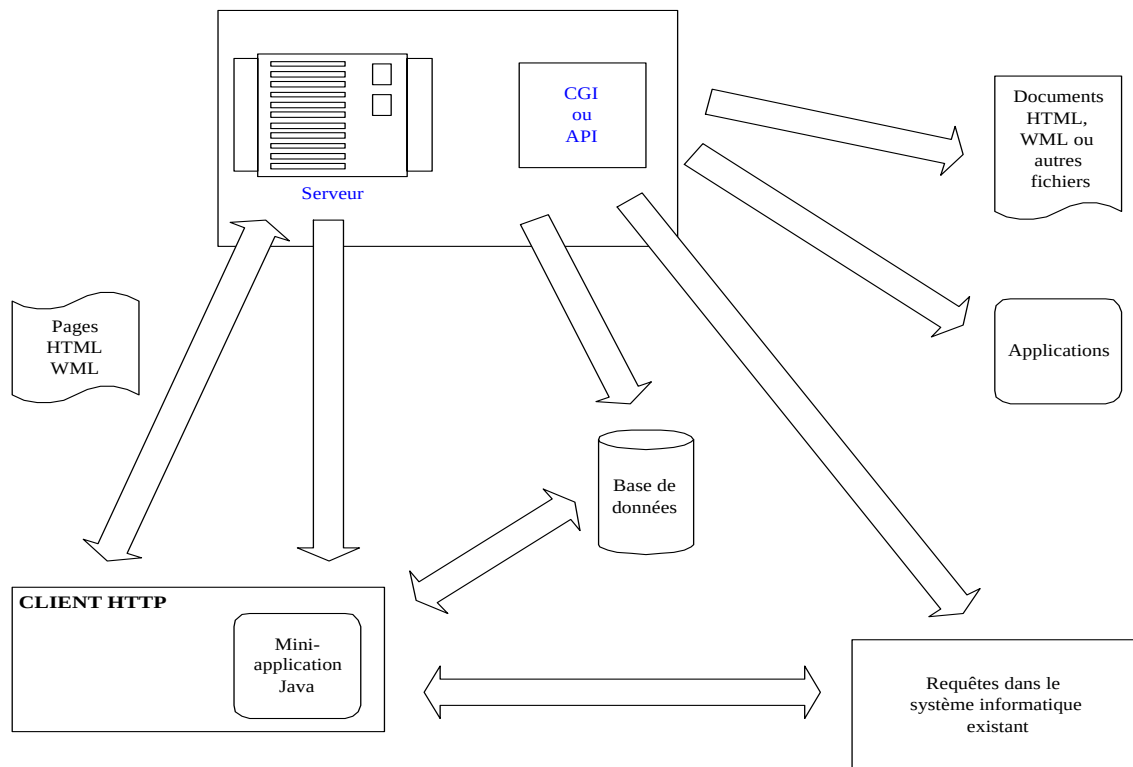


Figure 1.3.7. Schéma de principe d'un serveur Web

III.2.4. Le réseau opérateur

WAP est un protocole qui n'a pas été défini comme exclusif par un opérateur, bien au contraire, c'est tout un consortium qui a bâti cette norme. Ainsi, quasiment tous les types de supports physiques sont exploitables. Parmi les plus connus, on trouvera

- Le GSM (*Global System Communication for Mobile* - 9,6 kb/s - 14,4 kb/s)
- TDMA (*Time Division Multiple Access*)
- CDMA (*Code Division Multiple Access*)
- PDC (*norme japonaise*)

- SMS (*Short Message Service*)

De la même façon, WAP a été développé dans un souci d'évolutivité. Les normes émergentes sont également gérées :

- GPRS (*General Packet Radio Service* - 112 kb/s)
- EDGE (*Enhanced Data rates for Global Evolution* - 300 kb/s)
- UMTS (*Universal Mobil Telecommunication System* – 2Mb/s)

III.2.5. Fonctionnement de la transaction

L'appareil mobile supportant les fonctionnalités du WAP ou tout autre appareil capable de supporter cette technologie désirant recevoir des données, en provenance d'un serveur WAP, doit se connecter à une passerelle à l'aide d'un numéro de téléphone ou un assistant de connexion qui le composera pour l'utilisateur. La figure ci-après (*Figure 1.3.8.*) présente le détail de la transaction qui se fait lors d'une requête.

1. L'utilisateur appuie sur une touche de son téléphone mobile à laquelle correspond une URL
2. Une requête est envoyée à la passerelle configurée par défaut, en utilisant le protocole WAP
3. La passerelle WAP crée une requête HTTP conventionnelle pour l'URL demandée et la transmet au serveur Web par une transmission de type IP.
4. Cette requête HTTP est analysée par le serveur Web. Si l'URL correspond à un fichier statique (wml ou html), le serveur Web va chercher ce fichier et lui ajoute une en-tête HTTP. Si l'URL correspond à un script CGI (*Common Gateway Interface*) ou un script PHP (*Preprocessor Hyper Protocol*) ou autre, dans ce cas, le serveur lance l'application correspondante.
5. Le serveur Web retourne le jeu de cartes WML avec l'en-tête HTTP ajouté, ou directement les données WML issues du script.
6. La passerelle WAP vérifie l'en-tête HTTP et le contenu WML, et code le tout dans une forme binaire. La passerelle crée alors une réponse au format WAP qui est transmise au navigateur par l'intermédiaire du réseau sans fil.

7. Le navigateur reçoit une réponse. Il interprète le contenu WML et affiche la première carte du jeu de carte (voir description du langage WML).

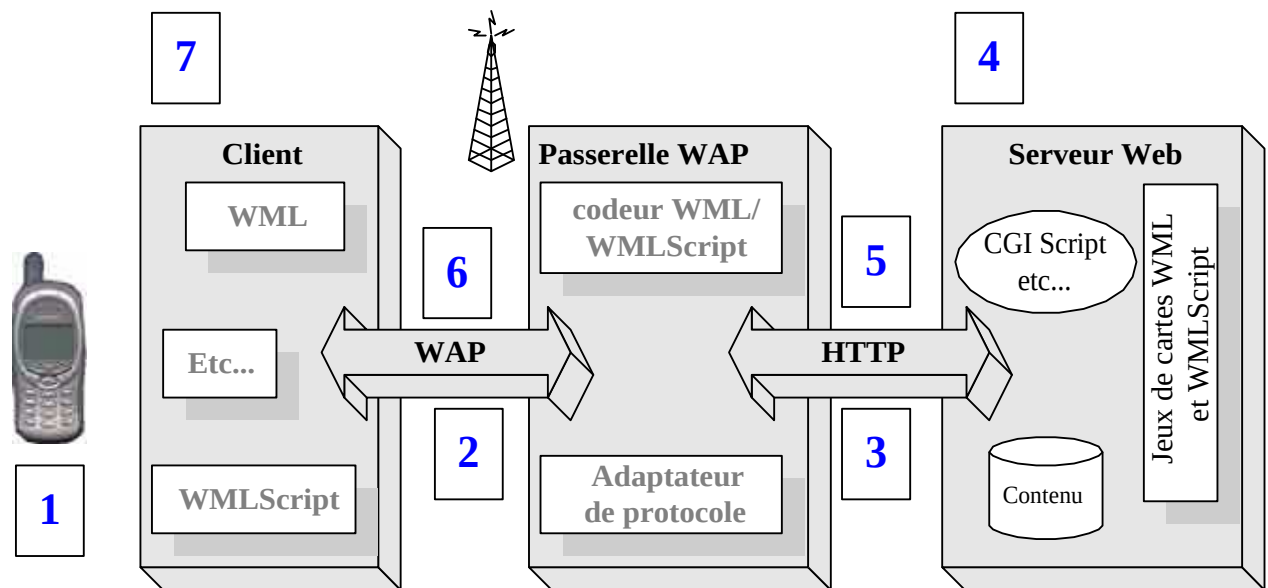


Figure 1.3.8. Echange d'informations à travers une passerelle lors d'une requête

III.3. La structure du protocole WAP [1] [30] [32] [35] [36]

Pour séparer les différents traitements de données nécessaires pour effectuer la transaction, le protocole WAP est défini selon des couches : c'est-à-dire des niveaux d'abstraction des données (dans l'esprit du *model OSI*). Cela donne la possibilité d'implémenter (en quelque sorte de programmer avec un langage spécifique) différemment chacune de ses couches. Chacune de ses couches définit alors une interface vis-à-vis de la couche suivante, ce qui permet une grande modularité des services ; une évolutivité de chacune des implémentations est donc possible.

Le protocole WAP est décrit par cinq couches utilisant chacune des applications et des protocoles :

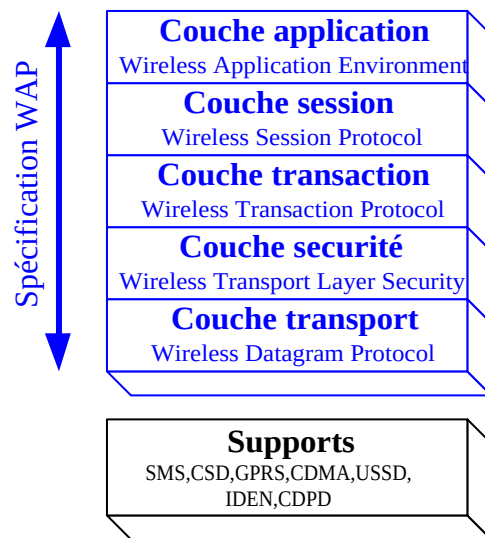


Figure 1.3.9. Modèle de couches du protocole WAP

III.3.1. La couche application : Wireless Application Environment (WAE) [17] [18]

III.3.1.2. Structure et présentation

La couche application comprend le Wireless Application Environment, et se situe au niveau le plus haut de la pile WAP. elle a pour but d'offrir une connectivité grâce à laquelle les contraintes entre opérateurs téléphoniques, fournisseurs et constructeurs de terminaux disparaissent. Cette couche est un mélange de différentes techniques issues du Web et de la téléphonie. C'est par la couche application qu'est définie l'interface utilisateur sur son mobile et que des applications peuvent être développées. Cette couche fournit ainsi des fonctionnalités applicatives telles que :

- Le WML (*Wireless Markup Language*, que l'on peut traduire par *Langage à balises pour le monde sans fil*) : il s'agit d'un langage qui formalise l'écriture d'un document avec des balises de formatage indiquant la façon dont doit être présenté le document sur un terminal mobile et définit les liens établis avec d'autres documents. Il s'agit d'un langage définit beaucoup plus strictement que le HTML, par une DTD (*Document Type Definition*, un document qui indique la syntaxe à respecter pour établir un document).

- Le WMLScript : un langage de script interprété par le terminal mobile, dérivé de l'ECMAScript à l'image du [Javascript](#) (il n'est toutefois pas compatible). il permet d'exécuter de petits scripts contenant des instructions simples telles que les boucles, les structures conditionnelles, les fonctions, ...

- le WTA (*Wireless Telephony Application*) : ensemble d'interfaces prédéfinies servant à créer des applications en téléphonie, c'est-à-dire permettant d'accéder à différentes fonctions de la téléphonie d'un terminal comme par exemple la composition d'un numéro.

III.3.1.2. Fonctions de la couche WAE

Les fonctions de la couche application peuvent être décomposées en deux :

- Définir une architecture pour les applications qui correspondent à l'architecture WAP, qui s'adaptent aux faibles capacités des terminaux WAP et la faible bande passante qui leur est permise. Elle doit également être sécurisée, simple et supportant les règles de normalisation internationales.

- Définir un modèle de programmation idéal : permettant de créer des applications interactives qui est basée sur les standards du Web

III.3.2. La couche session : Wireless Session Protocol (WSP) [19] [20] [21] [22]

III.3.2.1. Structure et présentation

La couche session permet d'établir une session entre un client et un serveur c'est-à-dire de définir les paramètres de connexion pour effectuer des transactions. La couche WSP permet ainsi à la couche application de bénéficier deux types de sessions différentes :

- Session orientée connexion : dans laquelle la couche session va interagir avec la couche transaction.

- Session orientée non-connexion : dans laquelle la couche session va directement agir au niveau de la couche transport pour l'envoi de datagrammes bruts.

III.3.2.2. Caractéristiques de la couche WSP

WSP est actuellement dans son ensemble l'équivalent du protocole HTTP (dans sa version 1.1), c'est-à-dire que le WSP consiste en un ensemble de services pour des applications de navigation (Browsing Applications, WSP/B). On retrouve d'ailleurs un bon nombre d'implémentations identiques au HTTP dans WSP. Les principales caractéristiques de la couche WSP sont :

- L'établissement d'une connexion avec acquittement entre un client, un serveur et la libération de cette connexion.
- Négociation des différentes fonctionnalités mises en œuvre dans la couche session.
- Echange de données entre le client et le serveur avec compression de données.
- Arrêt et reprise de la connexion en cours.

III.3.3. La couche transaction : Wireless Transaction Protocol (WTP) [23]

III.3.3.1. Présentation de la couche transaction

La couche WTP ou transaction gère le déroulement de la transaction, elle définit donc la fiabilité du service, c'est-à-dire assure l'exécution des transactions déclarées comme étant garanties et non garanties. Elle permet de gérer trois types de connexion qui ont été définies pour s'adapter au fonctionnement du WAP à travers les téléphones mobiles :

- **Classe 0** : connexion à sens unique sans acquittement (non fiable). Elle a été principalement conçue pour l'application du protocole PUSH (cf ultérieurement) permettant à un serveur d'envoyer des informations vers un mobile donné sans aucune vérification, le but étant ici d'optimiser le temps de la connexion et la bande passante du réseau.

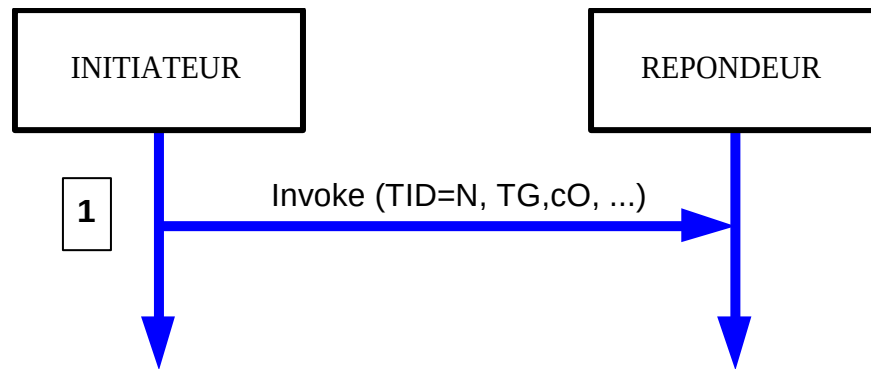


Figure 1.3.10. Connexion à sens unique sans acquittement

- **Classe 1** : connexion à sens unique avec acquittement (fiable). Elle permet d'effectuer un PUSH (on peut imaginer ce genre de transaction pour des informations distribuées de grande importance comme des avis de cotation en bourse). Dans ce mode de connexion, le client acquitte les données envoyées et la connexion se termine quand le serveur reçoit cet acquittement.

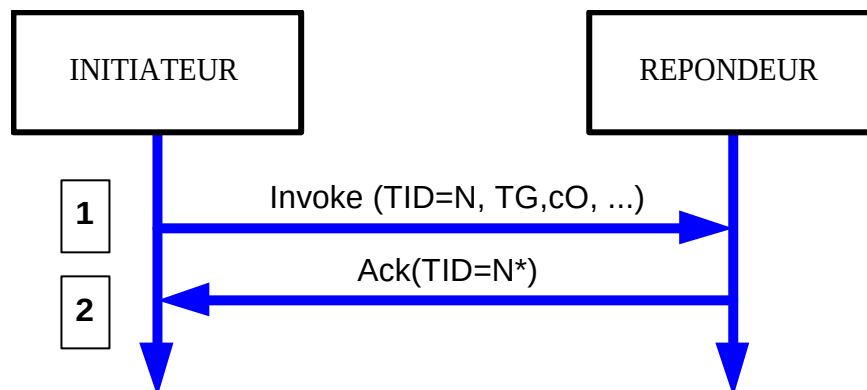


Figure 1.3.11. Connexion à sens unique avec acquittement

- **Classe 2** : connexion à double sens (avec accusé de réception) avec acquittement (fiable) . Elle permet d'effectuer toutes les autres connexions qui nécessitent un échange fiable entre le client et le serveur. Cette transmission est dite à double sens car chaque message envoyé donne lieu à un message de réponse de la part de la machine destination et cette réponse donne lieu à un acquittement de la part de la machine source.

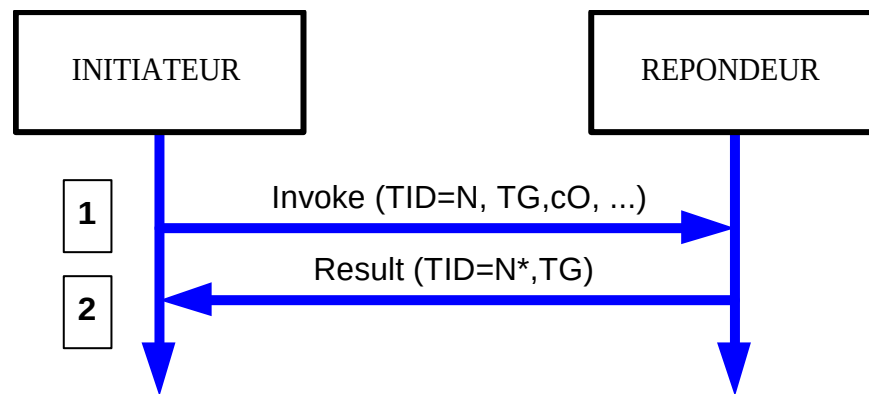


Figure 1.3.12. Connexion à double sens avec acquittement

Ces trois types de connexion peuvent être asynchrones. Les acquittements peuvent être mis en attente et regroupés afin de réduire le nombre de messages échangés.

Il est facile à ce niveau de faire un parallèle avec le protocole TCP/IP, et il ne faut pas cependant se laisser surprendre par le nom attribué aux couches car dans le respect du modèle OSI, la couche transaction WAP est au niveau de la couche application et non plus de la couche transport. C'est en quelque sorte une pile browser allégée.

Cette couche sert ainsi d'interface avec le monde IP pour intégrer les données dans des paquets UDP/IP si le réseau supporte ce protocole.

III.3.3.2. Les avantages de la couche WTP

Ils permettent :

Une plus grande fiabilité que simplement en mode datagramme : WTP évite aux niveau des couches supérieures d'avoir à retransmettre des données ou de les acquitter.

Une plus grande efficacité dans les services orientés connexion. En effet, WTP ne se soucie en aucune manière de l'état de la connexion.

WTP, étant orienté connexion, a été conçu pour l'usage des services utilisant des échanges entre client et serveur comme l'affichage de pages html.

III.3.4. La couche sécurité : Wireless Transport Layer Security (WTLS) [25] [26] [27] [28] [29]

III.3.4.1. Structure et présentation

La couche sécurité vient s'intégrer juste au-dessus de la couche transport de telle sorte qu'elle se situe au niveau le plus bas possible, ce qui permet d'assurer grâce à des normes établies une meilleure sécurité. Le protocole WTLS permet de respecter trois des quatre contraintes principales lorsqu'on parle de la sécurité liée aux réseaux :

- **la confidentialité** : elle assure aux deux parties (mécanisme client serveur) un accès aux informations échangées. Ceci est assuré par un mécanisme d'encryption des données.
- **l'intégrité des données** : cela permet de s'assurer que les données n'ont pas été altérées par l'une des deux parties. On utilise pour cela des algorithmes de hachage pour s'assurer de la validité des données. Il y a une rémission si un changement d'empreinte est détecté d'un côté ou de l'autre.
- **l'authentification** (coté serveur) : l'authentification a pour but de prouver qu'un tiers est bien celui qu'il prétend être. Des certificats permettent d'authentifier les serveurs.

Seul le principe de non-répudiation n'est pas géré par la couche sécurité : celle-ci a pour but de faire preuve juridique qu'une transaction a bien eu lieu. Ce mécanisme est souvent associé à une signature numérique.

On peut penser que les mécanismes de sécurité mis en œuvre nécessitent de grosse puissance de calcul, mais il n'en est rien. WTLS a été pensé de manière à s'adapter aux capacités des réseaux et terminaux mobiles, c'est-à-dire faibles taux de transfert, interactions lentes, capacités de calcul et de mémoire limitées et restriction gouvernementale en matière de chiffre.

III.3.4.2. Fonctions de la couche WTLS

La couche sécurité est construite de façon modulaire, c'est-à-dire qu'elle dépend du niveau de sécurité demandé pour une application donnée. La couche WTLS permet d'avoir une interface pour l'administration des connexions sécurisées. Ce modèle respecte les spécificités définies par TLS 1.0.

La couche WTLS permet à un client d'établir une connexion sécurisée avec un serveur et de fixer les options de sécurités prises en compte. L'établissement de la connexion sécurisée s'effectue en plusieurs étapes et le client aussi bien que le serveur peut annuler la communication à tout moment. La négociation inclut les paramètres de sécurité, l'échange de clés et l'authentification.

Pour réaliser toutes ces opérations, la couche WTLS est en fait subdivisée en deux autres couches. L'une est appelée la couche enregistrement, chargée de transmettre les données, éventuellement les compresser, d'appliquer un code d'authentification, de chiffrer et de faire les opérations inverses pour le déchiffrement. L'autre couche est en fait le protocole d'accord permettant aux deux éléments de se mettre d'accord sur la sécurité mise en jeu.

Par ailleurs, la couche sécurité assure une protection contre les attaques de type « Denial-of-Service ». Le noyau de cette fonction est le protocole WTLS, qui est basé techniquement sur le TLS, le successeur du protocole SSL.

III.3.5. La couche transport : Wireless Datagram Protocol (WDP) [24]

III.3.5.1. Structure et présentation

La couche WDP est à la base de la pile du protocole WAP. Elle assure l'indépendance vis-à-vis du type de réseau utilisé par l'opérateur. Pour cela, elle permet d'interagir avec les protocoles de transfert de données proposés par les opérateurs, en s'adaptant au mode de support utilisé. En tant que mécanisme de transport général, le protocole WDP assure donc la communication entre le « Bearer » (interface entre WAP et les réseaux physiques, comme les réseaux GSM ou TCI/IP) et les couches situées au-dessus. C'est par cette couche que sont transmis et reçus tous les datagrammes WAP. Le protocole WDP s'intègre dans la couche transport du modèle OSI.

III.3.5.2. Fonctions de la couche WDP

La couche WDP assure les fonctions suivantes :

- L'adressage des ports correspondants aux applications
- Une fonction optionnelle de segmentation et réassemblage

- Une autre fonction optionnelle de détection d'erreur

Le protocole WDP fournit à la couche supérieure un service fiable. Cependant, comme le protocole WDP peut accepter différents supports physiques, l'implémentation est différente suivant le type de support utilisé et les performances ne sont pas égales pour tous les supports.

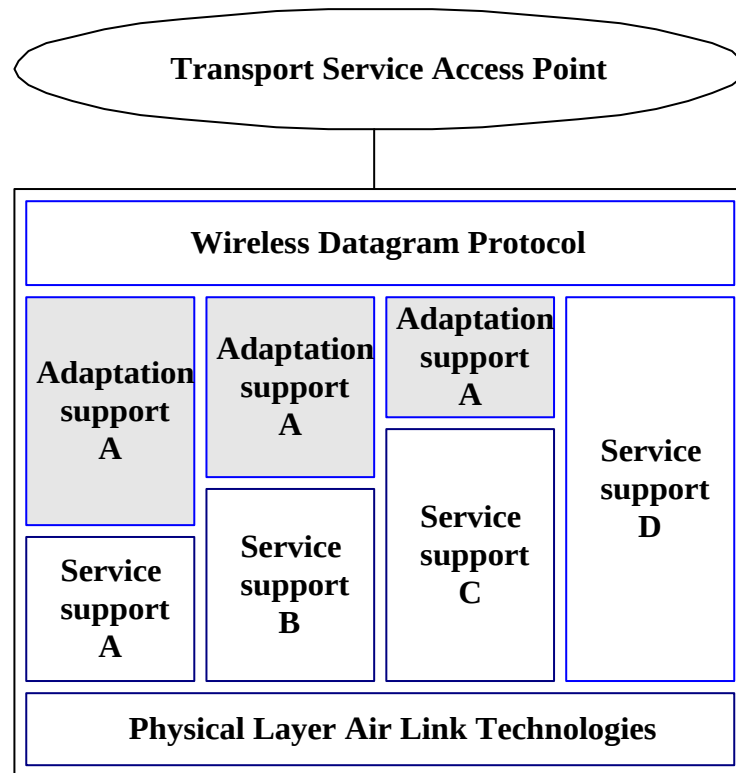


Figure 1.3.13. Implémentation et performances de quelques supports

III.4. Les supports [1] [34] [36] [37]

Les protocoles WAP sont désignés pour traiter une variété de différents services supports, tel qu'un message court, et est donnée ensuite en un paquet. Les supports offrent les différences de niveaux de qualité de service en respectant l'erreur de retard, et le délai. Les protocoles WAP sont désignés pour compenser ou de tolérer cette variation de niveau de service.

Bien que la couche WPD produit la convergence entre le support service et le reste de la pile WAP, la spécification WDP liste les supports qui sont supportés et les techniques utilisées pour permettre aux protocoles WAP de passer sur chaque support. La liste de supports prise en charge

changera tout le temps si l'on ajoute un nouveau support suivant l'évolution dans le domaine sans fil sur le marché.

III.5. Comparaison entre la pile WAP et la pile TCP/IP

De même qu'il est possible de faire un parallélisme entre le modèle OSI et la pile TCP/IP, on peut également le faire pour la pile WAP. En effet, celle-ci est conforme au modèle multicouche défini par le modèle OSI. WAP a été créé sur la base de la pile IP, intégrant la sécurité définie par la norme TLS.

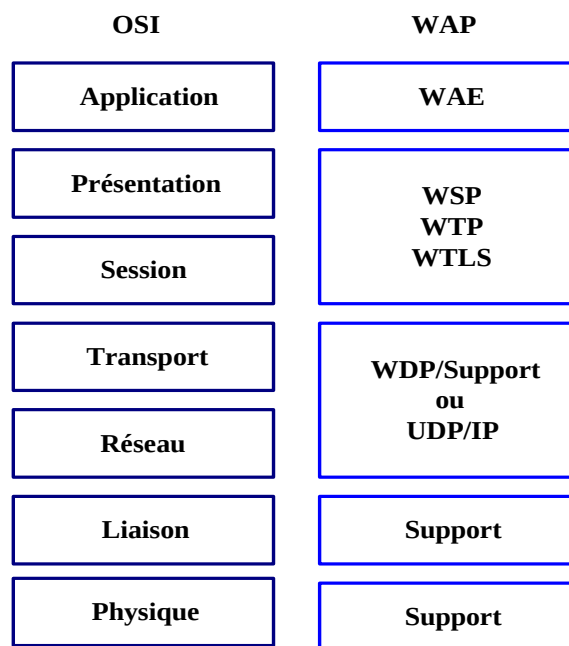


Figure 1.3.14. Comparaison entre les modèles de couches OSI et WAP

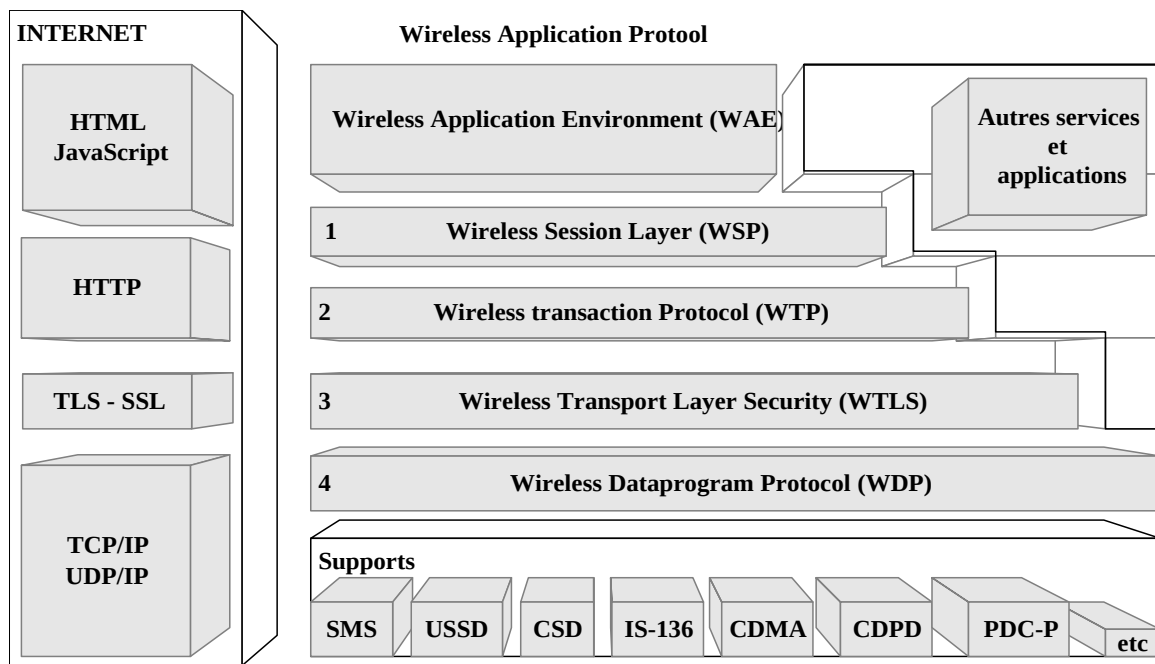


Figure 1.3.15. Comparaison entre la pile TCP/IP et la pile WAP

III.6. Sécurité [25] [27] [28] [29]

III.6.1. Sécurité de « bout à bout »

WAP permet une sécurité flexible de l'infrastructure qui converge dans la sécurité d'une connexion établie entre un client WAP et le serveur. WAP peut fournir un type de sécurité « bout à bout » (end-to-end) entre les extrémités du protocole WAP. Si un navigateur ou le serveur possède une sécurité de type « bout à bout », il doit se communiquer directement en utilisant les protocoles WAP. Le type de sécurité « bout à bout » peut aussi être achevé quand le « proxy WAP » est approuvé ou, par exemple, localisé dans la même place physiquement en sécurité que le serveur d'origine (Figure 1.3.16.).

Actuellement, la sécurité de bout à bout pour une transaction électronique n'est pas garantie, en effet ni SSL ni WTLS ne gèrent l'authentification du client. Ce problème est résolu à partir de la version 1.2 du protocole WAP. L'idée de cette version est de pouvoir récupérer à partir du terminal des informations relatives à son propriétaire.

La solution retenue est l'utilisation d'un module embarqué sur le terminal, le WIM (WAP Identity Module). Le module WIM permet au protocole WTLS (ou à d'autres fonctions de la

couche application) de sauvegarder et de récupérer à partir du portable des informations relatives au client, comme l'intégration de clés publiques et privées au sein de WIM. En effet le langage WMLScript, enrichi de la bibliothèque " crypto " permet d'interagir avec le module WIM. Le terminal peut alors être utilisé par exemple comme étant périphérique de signature numérique. Ce module prend tout son intérêt par son indépendance avec le type de terminal mobile. Il permet aux développeurs de mettre en place des solutions pleinement sécurisées.

Pour le cas du téléphone portable, on imagine très bien de pouvoir intégrer ce module à l'intérieur même de la carte SIM (*Subscriber Identity Module*). Des solutions proposant cette méthode existent déjà. Elles peuvent être basées sur Java Card mais d'autres supports peuvent également être mis en œuvre pour supporter ce module WIM, parmi lesquels on retrouve les smart cards (dotées de microprocesseurs), les cartes SIM, ou bien encore les cartes EMV (*Europay Mastercard Visa*) et SET (*Secure Electronic Transaction*)

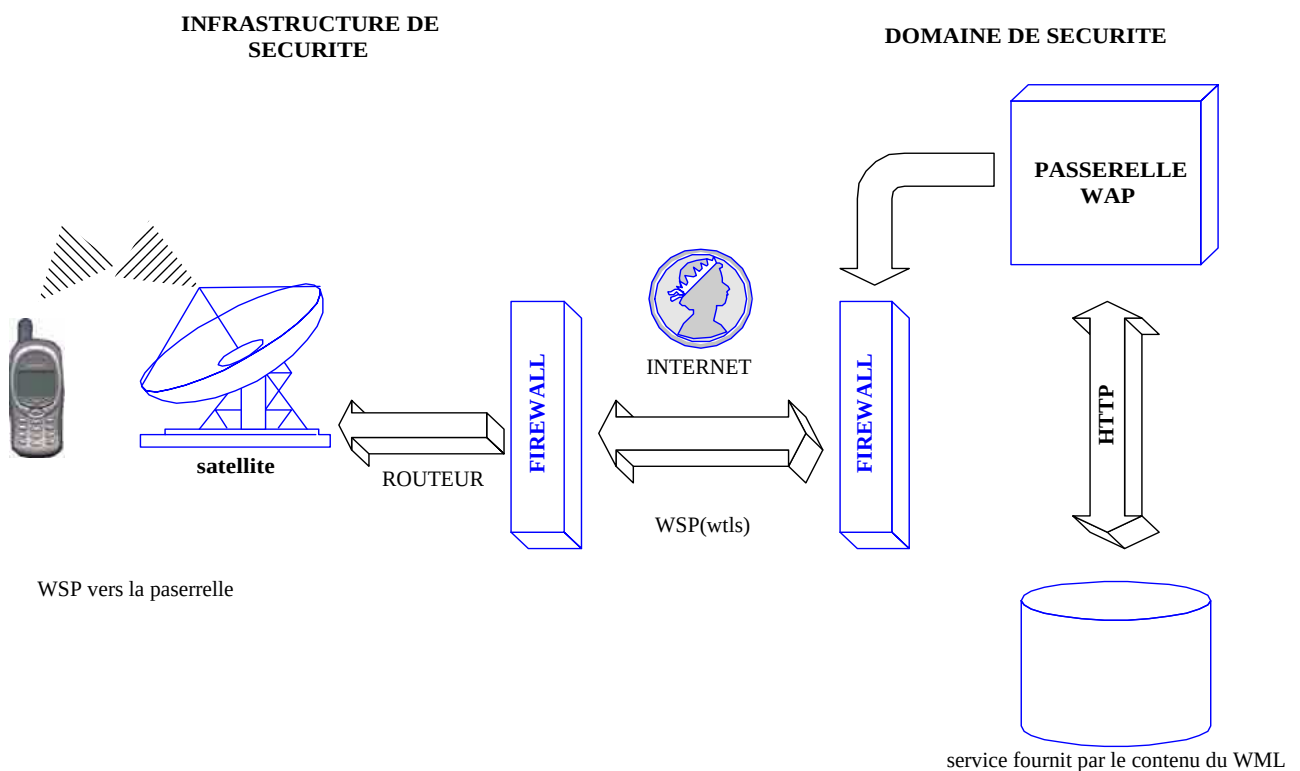


Figure 1.3.16. Représentation de type de sécurité « bout à bout »

III.6.2. le cryptage des données

Dans les transactions électroniques qui peuvent s'effectuer, deux techniques de cryptage sont utilisées pour garantir la sécurité :

- **La cryptographie à clé secrète** : cette technique dite également symétrique ou à clé partagée. Elle permet d'assurer les fonctions de confidentialité et d'intégrité
- **La cryptographie à clé publique dans la phase de négociation** : qui permet d'assurer (couplée avec des certificats) les quatre points clés : confidentialité, intégrité, authentification et non répudiation.

Pendant la transaction, la clé secrète est utilisée. Elle est connue uniquement des deux parties de la connexion et est générée de façon aléatoire. Cette clé sert à la fois à chiffrer et à déchiffrer les données. Seule la connaissance de cette clé permet de retrouver les messages en clair. La longueur de cette clé est comprise entre 40 et 128 bits. Pour que cette clé soit échangée sans risque entre les deux parties, il est important que l'échange ait lieu de manière extrêmement sécurisé.

Pour assurer cette confidentialité et intégrité, la cryptographie à clé publique intervient dans la phase d'initialisation. Le mécanisme est le suivant :

Chaque partie possède une paire de clés : publique et privée. La clé privée n'est connue que par son propriétaire alors que la clé publique peut être connue de n'importe qui sans précautions particulières. Celle-ci peut être demandée directement à son propriétaire ou bien à un organisme de certification possédant cette clé.

On appelle ce mécanisme :asymétrique car un message codé avec la clé privée ne peut être récupéré qu'avec la clé publique et inversement. Ainsi, si on code avec une clé privée, dans ce cas, tous ceux qui possèdent cette clé publique pourront décoder le message. A l'inverse, si on code avec une clé publique, dans ce cas, seul le propriétaire de cette clé privée sera capable de décoder le message. C'est ce mécanisme qui est utilisé pour l'échange de la clé secrète.

Cette méthode très efficace est de plus en plus utilisée. Cependant, dans le cas du WAP, elle ne peut être exploitée que dans la phase d'initialisation car elle nécessite l'emploi de clés de taille relativement importantes (512 ou 1024 bits) ce qui n'est pas compatible avec l'utilisation des

réseaux sans fil. En effet, la bande passante étant surchargée, il est important de ne pas l'alourdir encore plus.

Dans cette phase, on peut aussi utiliser les certificats d'authentification pour authentifier les parties en présence et vérifier les signatures numériques.

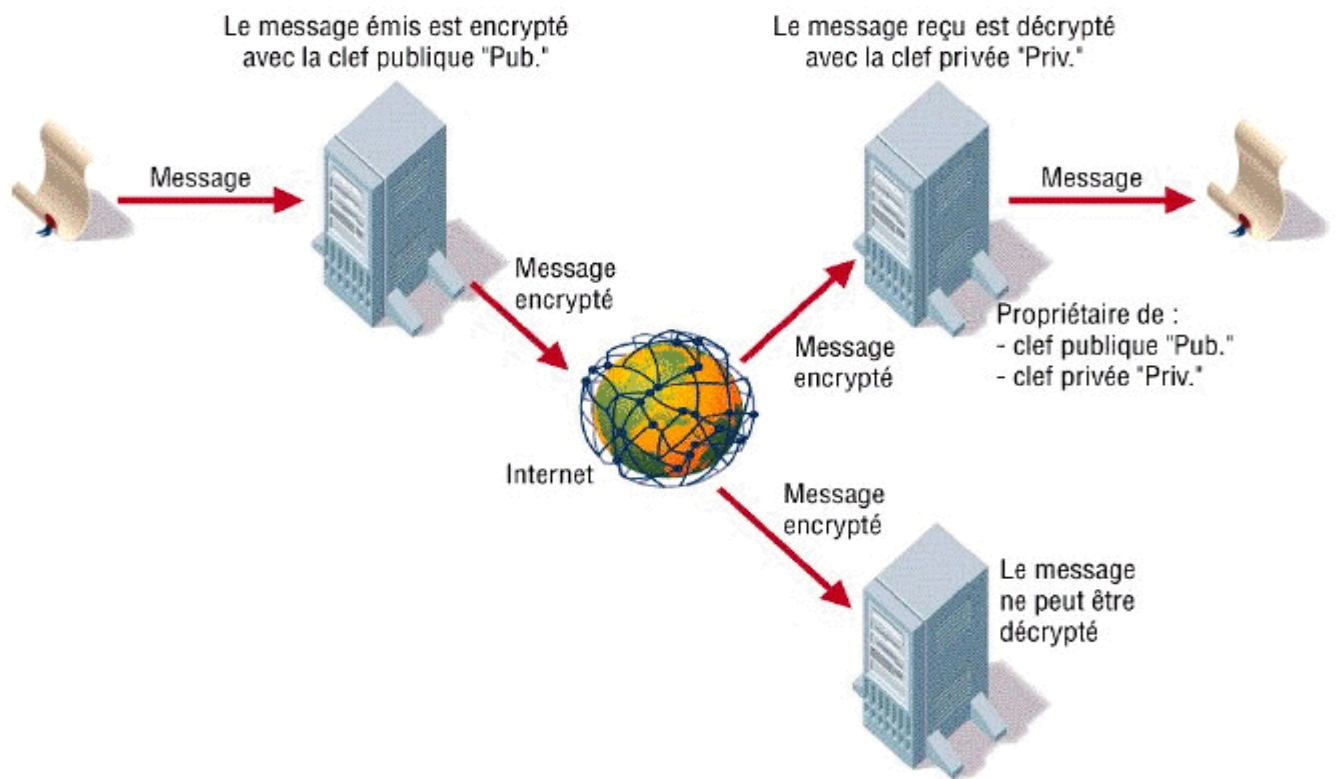


Figure 1.3.17. Mécanisme de cryptage et de décryptage de données

III.7. Les compléments sur le WAP

III.7.1 Le protocole « PUSH » [47] [48] [49] [50]

Il est facile de comprendre la différence entre le push et le pull, ne serait-ce que par leur signification anglaise. Dans le pull, le client retire vers lui l'information qui l'intéresse, alors que dans le push c'est le serveur qui est l'initiateur du message

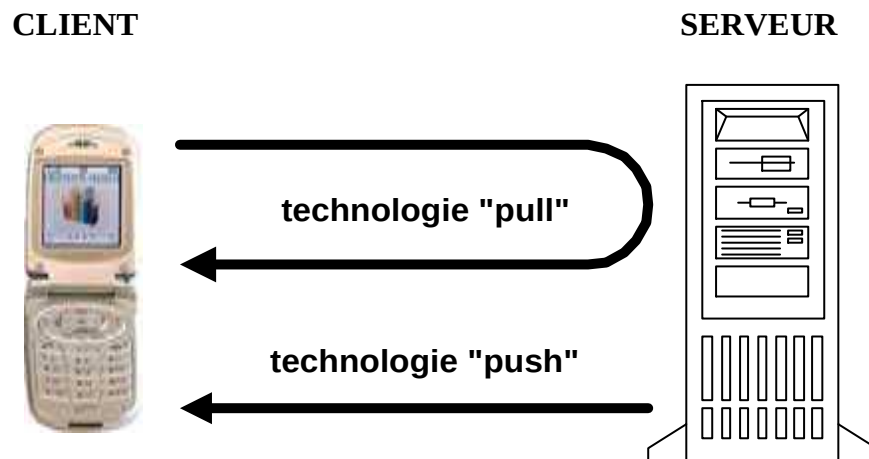


Figure 1.3.18. Schéma simplifié des transactions « push » et « pull »

En fait, ce schéma est un peu simplifié car, comme le serveur initiateur et le mobile ne sont absolument pas sur le même réseau, il est nécessaire d'employer une passerelle :

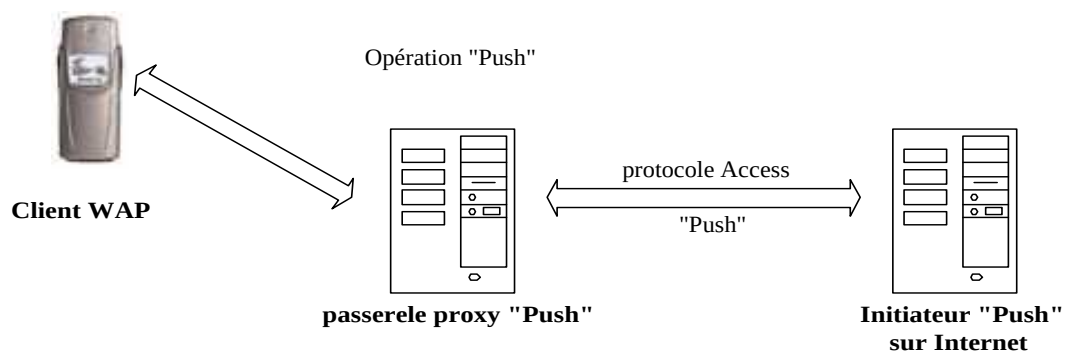


Figure 1.3.19. Représentation avec une passerelle « push »

Comme la passerelle push est le lien entre le réseau Internet et le réseau sans fil, elle doit être capable de contrôler les fonctions suivantes :

- Identification et authentification de l'initiateur du push
- L'analyse et la détection d'erreur dans le contenu

- Résolution d'adresse
- Encodage conforme aux contraintes du réseau sans fil
- Conversion de protocole

Bien entendu toutes les communications se font par l'intermédiaire du protocole HTTP (même on prévoit d'autres supports). Au contraire, pour tout ce qui touche les transmissions sans fil de la passerelle push jusqu'au mobile, les communications se font par le support de la couche WSP qui définit tous les mécanismes de fonctionnement nécessaires au push.

III.7.2. Le protocole « WCMP » ou Wireless Control Message Protocol [45] [46]

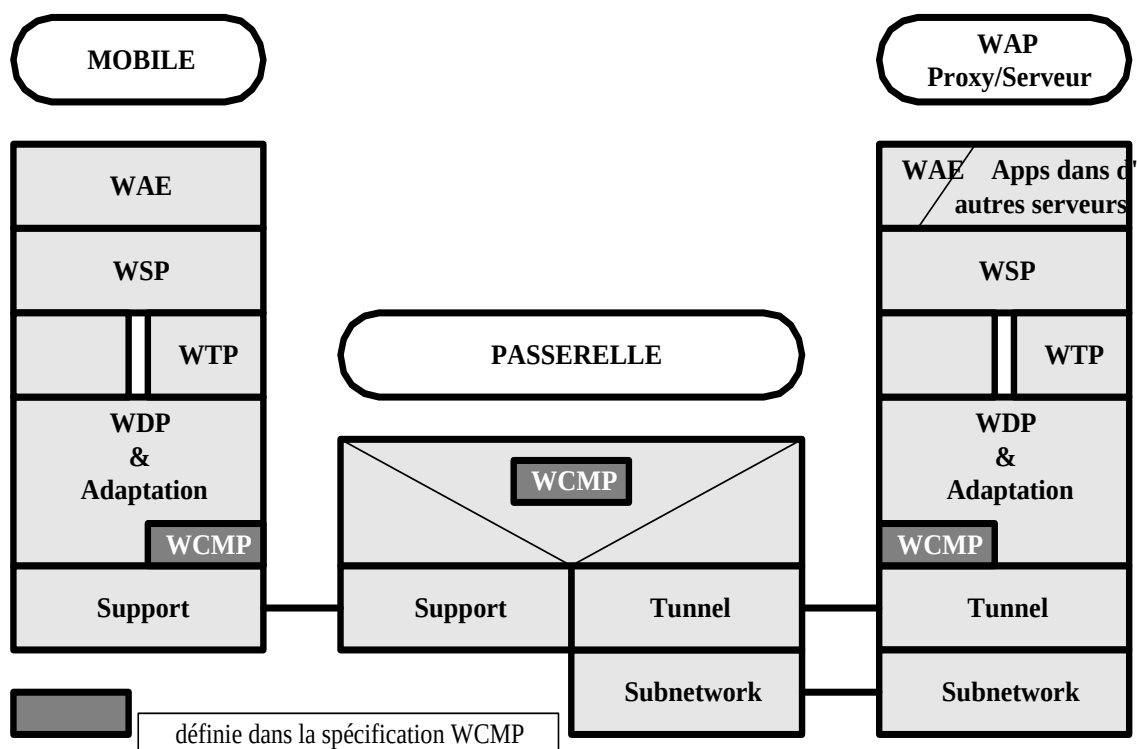


Figure 1.3.20. Interaction du protocole WCMP dans la pile WAP

WCMP est l'équivalent d'ICMP sous le protocole IP, il sert à rendre compte des erreurs qui peuvent avoir lieu au cours d'une connexion. Ce mode est utilisé par WDP au niveau des nœuds d'interconnexion ou des passerelles pour signaler les erreurs survenues (Figure 1.3.20.). Tout comme WDP, WCMP n'est utilisé que dans les environnements qui ne supportent pas IP (car dans ce cas, ICMP est utilisé)

L'en-tête WCMP est simple puisqu'elle ne comprend que 3 champs :

- Type : indique le type de message
- Code : définit le format du champ données
- Données : peuvent être des reports d'erreurs ou d'informations

Bit/Octet T	0	1	2	3	4	5	6	7
1	Type de message de contrôle							
2	Code de contrôle de message							
3 – N	Zone de données pour WCMP (0 .. N octets)							

Tableau 1.3.2. Structure d'information WCMP

Les types compris entre 0 et 127 correspondent à des types d'erreurs, alors que ceux qui sont compris entre 128 et 191 correspondent à des messages d'informations. Globalement, on retrouve, pour le type d'erreurs qu'ICMP un ajout de 50 sur le champ type.

III.8. Applications [1] [30] [31] [36] [37]

WAP est utilisé pour développer les formes évoluées des applications existantes et les nouvelles versions. Le WAP a donné un élan considérable pour les nouveaux opérateurs pour faire du mobile un canal de distribution pour leur produit et service existant. Le protocole d'application du mobile (WAP) permettra alors aux clients de répondre facilement aux informations parvenues au téléphone en utilisant de nouveau menu pour accéder aux services mobiles. Cela fait parti de l'attribution des opérateurs de réseau en fournissant des services à valeur ajoutée auxquels les clients font leurs requêtes et peuvent répondre facilement (en utilisant le menu au lieu de la saisie d'un mot clé, par exemple).

Le WAP, généralement un trafic supplémentaire sur le réseau, est donc une source de revenu additionnelle pour les opérateurs.

Auparavant, les développeurs d'applications avaient écrit des logiciels d'applications propriétaires et étaient obligés de porter ces applications sur différent type et support de réseaux avec la même plate-forme.

En séparant les supports d'application, le WAP a facilité la migration des applications entre le réseau et le support. Comme tel, Le WAP est similaire au Java dans le fait qu'il simplifie le développement d'applications. Ceci réduit le coût des applications pour les mobiles et encourage donc l'entrée des développeurs de logiciels au sein de l'industrie du mobile.

Les applications d'entreprise qui ont été améliorées par l'utilisation de l'interface WAP incluent :

- Point Eloigné de Vente
- Service après vente
- Positionnement de véhicules .
- E-mail d'entreprise
- Accès aux réseaux distants
- Transfert de fichiers
- Navigation sur Web
- Partage de documents
- Audio
- Images fixes
- Images animées
- Domotique

Pour les clients, les applications qui ont été améliorées par l'utilisation de l'interface WAP incluent :

- Internet e-mail
- Chat
- Services d'information
- Le paiement d'avance
- Affinité de programmes
- Commerce mobile
- Messagerie

Chapitre IV. LE LANGAGE WML : Wireless Markup Language

[1] [38] [39] [41]

IV.1. Définition et structure du langage WML

Le langage WML est un langage à balise basé sur XML, ce qui est en fait l'équivalent du HTML (HyperText Markup Language) pour les navigateurs. Il est utilisé pour décrire une page de manière simple et efficace dont les contextes et les contraintes d'utilisation mobile étaient très différents de ceux du Web. Le WML permet à des terminaux mobiles (téléphones mobiles, pagers ou des assistants digitaux personnels, etc.) d'afficher des documents reliés par des liens hypertextes. Le WML est donc très proche du HTML, mais il est toutefois beaucoup moins souple que ce dernier car il doit être conforme à des documents appelés DTD (Document Type Definition), indiquant la syntaxe à suivre pour créer un document WML.

Le WML se doit d'être compact, il a été élaboré pour tenir compte des contraintes propres aux mobiles :

- petite taille de l'écran (de 4 à 5 lignes de texte),
- faible capacité de saisie (limitée à quelques touches)
- limitation en mémoire et en puissance de calcul
- faible bande passante et temps de latence importante des réseaux existants.

Le langage WML permet ainsi l'affichage des textes, d'images, de tableaux sur l'écran du terminal mobile. Chaque document WML doit spécifier la version de XML utilisée ainsi que la référence à une DTD définissant l'ensemble des balises utilisées. Le début d'un document WML se présente toujours de la façon suivante :

```
< ? xml version = " " ?>
```

```
< ! DOCTYPE wml PUBLIC "-//WAPFORUM/DTD WML 1.1//EN"
```

```
"http://www.wapforum.org/DTD/wml_1.2.xml ">
```

La première ligne indique la version de XML. La deuxième ligne référence un document externe appelé DTD, qui contient la définition de toutes les balises utilisées dans la suite du document.

IV.2. Les principales fonctionnalités du WML

➤ Présentation:

WML peut supporter un texte ou une image avec un grand nombre de possibilités de mises en forme

➤ Organisation sous forme de paquet et de fichier :

En WML, toutes les informations sont regroupées dans un paquet qui contient un fichier et chaque paquet spécifie une ou plusieurs unités d'interaction avec l'utilisateur

➤ Navigation:

Avec WML, on peut avoir des liens entre les fichiers. Cela revient à la navigation dans HTML.

WML peut aussi supporter les ancres permettant de se déplacer dans un paquet ou de se positionner dans une carte particulière d'un paquet.

➤ Substitution de texte :

Cela permet une variable par son contenu lors de l'affichage de la carte. Les variables sont substituées par le micro-navigateur du mobile et elles sont définies dans les cartes.

IV.3. La syntaxe du langage WML

La constitution d'une page WML ou d'un document WML (DECK) est très métaphorique, elle s'apparente à un jeu de cartes constitués d'une série de cartes représentant des entités documentaires tel qu'un écran de texte, un champ,... Chaque jeu de carte ou paquet WML commence par la balise `<wml>` et finit par `</wml>`, et une carte est en réalité un ensemble de balises WML entouré par les balises `<card>` et `</card>`. Le paquet WML minimal est donc un fichier texte comportant une seule carte.

IV.4. Eléments du langage

Le WML est un langage composé de balises. Toute balise exprime une action destinée à être interprétée par le navigateur.

Chaque balise est décrite avec son utilisation et sa syntaxe, c'est-à-dire la liste de ses attributs et leur signification. La syntaxe d'une balise est donc indiquée en utilisant le formalisme des documents de description (DTD) de XML.

➤ Les entités :

Ils permettent de définir une seule fois un élément (équivalent aux directives *#define* dans C). Chaque référence a une entité et remplacée par la chaîne de caractères lors de l'analyse de documents.

Exemple : `<!ENTITY : boolean «(true /false)»` > définit l'entité *boolean*

➤ Les éléments

Un document WML est formé d'une suite de balises ou éléments imbriqués. Une balise est constituée d'un marqueur de début, d'un contenu et d'un marqueur de fin. Il existe deux formes de balises :

- Balise avec un contenu : `<balise> .....</balise>`
- Balise sans contenu : `<balise/>`

Les balises se déclarent ainsi :

`<!ELEMENT nom_balise sous_élément>`, *nom_balise* est l'élément proprement dit, *sous-élément* désigne soit un groupe d'un ou plusieurs sous-groupes, soit une chaîne de caractère, soit EMPTY, soit ANY. Les deux derniers permettent de spécifier si l'élément doit être vide.

Une balise peut contenir une chaîne de caractères exprimée par PCDATA ou d'autres balises.

ainsi :

`<!ELEMENT A (#PCDATA)>` définit un élément A qui ne contient qu'une chaîne de caractères.

`<!ELEMENT A (#PCDATA | B | C)*>` spécifie A contenant un mélange de chaîne de caractères et d'éléments B et C.

➤ Les attributs :

Une balise ne pourrait avoir aucun attribut ou en avoir plusieurs. Les attributs sont définis grâce à un mot clé `ATTLIST`. Il existe plusieurs types d'attributs :

- ✓ Attribut optionnel sans valeur par défaut
- ✓ Attribut optionnel avec une valeur par défaut
- ✓ Attribut obligatoire
- ✓ Attribut à valeur fixe

Les attributs sont typés en chaîne de caractères (CDATA), liste énumérée, ID ou IDREF, ENTITY ou ENTITIES, NMTOKEN ou NMTOKENS .

Les plus courants sont :

- CDATA qui correspond à une chaîne de caractères
- Une liste énumérée : c'est une liste de valeurs séparées par le caractère " | "
- NMTOKEN : il définit un attribut qui a comme valeur un mot
- ID indique que cet attribut spécifie une valeur unique dans le document. l'attribut est alors l'identifiant unique de la balise.

IV.5. Spécification du langage WML

Le WML impose une syntaxe plus stricte que le HTML. Alors que la plupart des navigateurs Web sont assez indulgents avec les petites erreurs qui peuvent se trouver dans les fichiers HTML,

il est impératif de respecter de manière très stricte les règles du langage WML. Du point de vue programmation, le WML présente cinq différences majeures par rapport à HTML.

IV.5.1. Les endtags

Toutes les balises ou commandes doivent impérativement être terminées par une balise de fin. Un paragraphe débute dans les deux langages par la balise <p> et se termine normalement par une balise </p>. Le HTML ne comprend pas de fin pour
, autrement dit pour un saut de ligne : il n'existe donc pas de balise </br>. (cette absence peut paraître logique, car un saut de ligne n'a en principe aucun besoin d'être « terminé »).

La syntaxe plus stricte du WML impose que toutes les balises doivent impérativement être terminées. Pour éviter des constructions de type
</br>, ce langage prévoit des « *balises vides* » (empty tags). Au lieu d'ajouter une balise de fin explicite, il suffit d'inclure un « *slash* » (« / ») comme dernier caractère à l'intérieur des crochets :
.

IV.5.2. Sensibilité à la casse

Le langage HTML laisse au programmeur le choix d'écrire les commandes en minuscules ou en majuscules.

Le langage WML est sensible à la casse, c'est-à-dire qu'il fait la différence entre les majuscules et les minuscules. Il est alors impérativement nécessaire que les commandes et les attributs associés soient tous écrits en minuscules.

Remarque : il existe bien quelques navigateurs qui acceptent les commandes écrites en majuscules, mais ils ne présentent qu'une minorité. Il est donc conseillé de n'utiliser que des minuscules pour les commandes.

IV.5.3. Coder tous les caractères spéciaux

Les caractères spéciaux comme les accentués doivent être codés lorsqu'ils sont écrits dans les pages HTML par exemple ´ pour « é ». La plupart des navigateurs sont assez indulgents et autorisent également la présence des caractères accentués non codés. Le protocole WAP est nettement moins tolérant, les navigateurs WAP ne savent pas correctement interpréter les caractères spéciaux non codés.

IV.5.4. Les différences du point de vue de l'utilisateur

Les utilisateurs ne sont naturellement pas concernés par la manière dont le programmeur a obtenu un certain résultat. Les performances du langage de programmation sont cependant très importantes pour l'utilisateur.

A l'instar du langage HTML, le WML est un langage permettant de décrire le contenu des documents transmis par internet. Le HTML a été développé pour permettre la présentation de documents compliqués sur des écrans modernes, il prend en charge l'ensemble des fonctions d'un traitement de texte moderne ainsi que des fonctions complémentaires de gestion de liens permettant de structurer les documents ; tandis que le WML poursuit l'objectif d'utiliser de manière aussi efficace que possible des écrans dont la taille, la profondeur de couleur et la résolution sont fortement limitées.

Remarques : les avantages du langage HTML sont très évidents, en ce qui concerne son utilisation sur le Web : le HTML est indépendant de la plate-forme (il peut être utilisé pratiquement sur tous les types d'ordinateurs. En outre, il permet de lier entre eux différents documents grâce à des liens hypertextes.

IV.5.5. WML est parfaitement adapté au WAP

Le WML n'a été conçu que pour supporter un type d'affichages limité . D'abord , la grande majorité des téléphones mobiles WAP ne disposent que d'un affichage en noir et blanc. La profondeur de couleur que l'on peut utiliser est donc limitée à 1 bit. En outre, l'affichage des textes est également différent. Sur la plupart des pages Web, on a l'habitude de voir des caractères de différentes tailles. Les pages WML sont en revanche assez spéciales. Le nombre des caractères que l'écran d'un téléphone mobile peut afficher varie d'un modèle à l'autre. Les seuls moyens de formatage utilisés sont le passage en « gras », en « italique » et parfois quelques autres formats complémentaires. Enfin, on peut aligner un texte à gauche ou à droite ou au centre.

Pour le programmeur, la différence essentielle entre WML et HTML est que les pages WAP disposent d'un nombre de commandes inférieur aux pages HTML

IV.5.6. La structure Card

Toutes les pages Web appartenant à un même projet sont regroupées à l'intérieur d'un site, sur le Word Wide Web. Chaque page est enregistrée dans un fichier séparé. Il y a une quasi-identité entre les pages et les fichiers correspondants.

La structure WAP est quelque peu différente. Elle définit en particulier de nouveaux concepts : *Deck* (qui signifie en français pile), et *Card* (en français, carte). Plusieurs pages sont enregistrées ensemble dans un fichier pour réduire autant que faire se peut le temps de chargement de différentes pages dans un site. En WML, ce fichier est appelé « Deck » : il contient un site complet, vu sous l'angle du programmeur HTML. Le navigateur WAP peut alors déterminer dans quelle partie de la pile il doit afficher. La pile est ainsi divisée en une ou plusieurs cartes, chacune d'entre elles représente une page. Un nom est attribué à chaque carte, de manière à ce que le navigateur sache laquelle il doit afficher. En l'absence de désignation d'une carte, le navigateur affiche automatiquement la première carte de la pile.

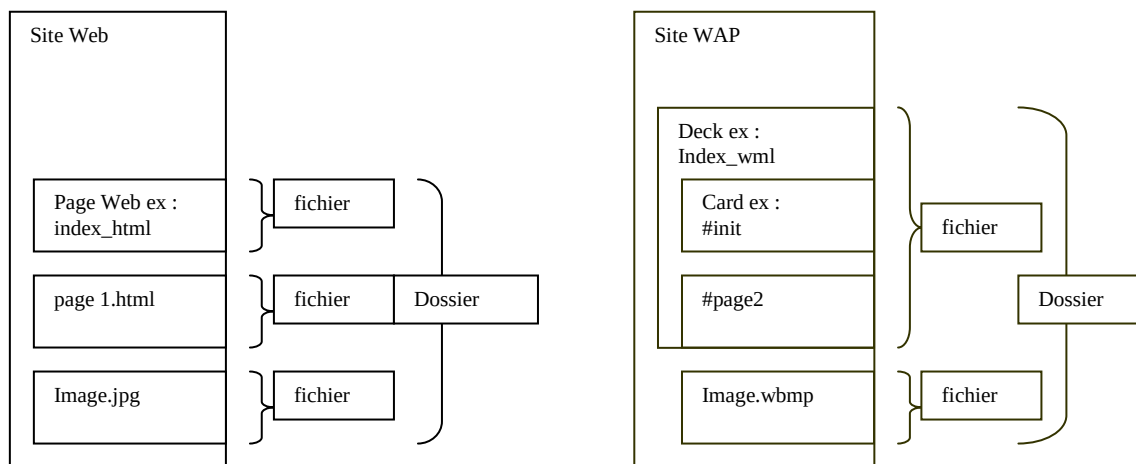


Figure 1.4.1. Différence entre les structures des documents Web et WAP

Chapitre V. LE LANGAGE DE SCRIPT : WMLScript

[40] [42] [43] [44]

V.1. Présentation

Le WMLScript est un langage de script basé sur ECMAScript. Ce n'est pas un nouveau langage puisqu'il ressemble en fait à JScript de Microsoft, et à JavaScript de Netscape. Il a été simplifié pour supporter des réseaux à faible bande passante et à s'adapter spécialement aux besoins des mobiles. La saisie et l'affichage des données sont réalisés par des formulaires WML classiques. WMLScript s'utilise depuis WML pour l'enrichir. WMLScript est donc un langage de programmation très simple qui permet d'inclure une certaine dose d'intelligence dans les pages WML.

V.2. Intérêt du script et conseils d'utilisation

WMLScript est le langage de script de l'environnement de développement WAP. WMLScript permet un large éventail d'actions, parmi lesquelles :

- Effectuer des contrôles de surface concernant les saisies réalisées par l'utilisateur. Vous pouvez ainsi tester la cohérence d'une saisie de plusieurs champs ou de la conformité à un format de données (date numéro d'identification normé, etc.)
- Réaliser des calculs et des traitements simples sur la mobilité.
- Afficher rapidement pour l'utilisateur des messages d'alerte, d'information ou de confirmation sans emprunter le réseau.
- Accéder à certaines fonctionnalités du navigateur et de téléphone (par exemple enregistrement des données sur la carte SIM, envoi de messages ou appel de numéros de téléphone).

V.3. Conventions

En comparaison avec des langages de programmation de haut niveau (Delphi , C++, etc.), un nombre très limité de conventions sont nécessaires pour WMLScript. Cependant il faut impérativement les respecter pour obtenir des scripts fonctionnels :

- WMLScript est sensible à la casse (on fait la distinction entre les majuscules et les minuscules).
- On utilise comme séparateur décimal un point (.) , et non une virgule (,)
- Les noms des variables peuvent contenir des chiffres , mais le premier caractère doit être une lettre.
- Chaque expression WMLScript se termine par un point-virgule (;) , placé généralement à la fin de la ligne. Les espaces et les sauts de lignes sont ignorés dans WMLScript. Les ruptures de lignes et les identifications rendent les WMLScript plus lisibles, mais n'ont aucune signification syntaxique.

Remarque : les script WML sont enregistrés sous forme de fichiers ASCII sur le serveur WAP, puis transmis sur le mobile après compression en binaire.

Chapitre VI. LA TECHNOLOGIE WAP ENVERS LE MONDE

VI.1. Intégration du WAP dans le contexte économique actuel

Dans le domaine de l'informatique, on constate une évolution rapide de la technologie moderne. Le WAP arrive donc à point nommé puisqu'il permet, à n'importe quel moment et de n'importe quel endroit (pourvu qu'il soit sous une zone de couverture d'un opérateur) d'accéder à des services disponibles sur Internet ou dédiés aux utilisateurs WAP itinérants. Il devient ainsi possible de profiter des services spécialisés comme la météo, les e-mails, la bourse, l'actualité et bien d'autres sans même avoir besoin de télévision ou d'ordinateur, simplement à partir d'un téléphone WAP. Les années à venir vont probablement voir apparaître de nouveaux grands noms sur Internet qui auront réussi à attirer les clients, mais surtout à les garder par des bouquets de services WAP attractifs.

Pour ce qui est des facturations, rien n'est pour l'instant réellement figé. En effet, France Télécom a été le premier à proposer un pack WAP pour lequel l'accès au WAP était gratuit (facturé sur le temps de consommation, soit le forfait téléphonique) dans un but certain d'une évangélisation, mais à l'heure où ces quelques lignes sont écrites, tout reste encore à définir. Pour l'instant, les opérateurs téléphoniques restent principalement maîtres des passerelles WAP (liaison GSM -Internet), utilisant des partenariats avec les fournisseurs de contenu WAP. Il est certain que tous les opérateurs vont migrer vers le WAP d'ici peu, car cela leur permettra d'accroître la valeur ajoutée des services existants avec un minimum d'investissement et de risque.

Le WAP, qui offre dès à présent des services à temps réel, de personnalisation et de localisation, est l'éclaireur d'un marché en phase d'éducation. Ces fonctions basées sur une nouvelle ergonomie des terminaux et associées à des modes de facturation simples, suffisent au démarrage du WAP.

VI.2. Perspectives de développement et évolutions envisageables

Les spécialistes du marché des télécommunications prévoient un développement exponentiel des accès Internet par le WAP. "Le milliard d'abonnés au téléphone mobile devrait être atteint en 2004, et à cette date, un tiers des abonnés à Internet privilégieront l'écran de leur téléphone mobile ou de leur assistant personnel pour accéder au Web" annonce le PDG d'Ericsson France.

"Datamonitor estime que 69 % des 270 millions de possesseurs de téléphones mobiles européens auront un accès à des services WAP en 2005. A cette date, plus de 144 millions de terminaux compatibles WAP seront vendus chaque année en Europe". Néanmoins, avant l'immersion dans le monde WAP, certaines contraintes, aujourd'hui d'actualité, doivent tout d'abord être dépassées : en premier lieu la taille d'affichage des portatifs est amenée à changer. En effet, à l'heure actuelle, les portables WAP ne disposent que d'un écran 94*65 pixels, ce qui fait défaut au confort d'affichage. De même, l'arrivée de la couleur sur les portatifs est également à attendre pour rendre la consultation plus agréable. Cela se répercutera bien évidemment sur les actuelles spécifications du langage WML qui seront amenées à évoluer.

Néanmoins, la plus grande évolution à venir est sans conteste la future transition des réseaux actuels vers les normes GPRS, EDGE et surtout UMTS. En effet, le GSM ne propose actuellement qu'un débit pauvre limité à 9.6 kbit /s ce qui ne correspond même pas à la vitesse d'un modem d'il y a 5 ans. A l'opposé, les nouveaux réseaux permettront d'atteindre des capacités nettement supérieures, ainsi le GPRS permettra d'atteindre 144 kbit/s, mais c'est surtout l'arrivée tant attendue de la norme UMTS qui fera réellement basculer la donne au profit du WAP. On pourra dans ce cas atteindre des taux de transfert de l'ordre de 2 Mbits/s, ce qui devrait permettre, par le biais de terminaux appropriés, de véhiculer de la voix, des données, mais aussi de la vidéo.

VI.3. Evolution de la technologie WAP à Madagascar

Malheureusement, Madagascar est l'un des pays les moins avancés technologiquement surtout dans les domaines de la Télécommunication et de l'informatique. Face à cette technologie WAP, seuls deux parmi les opérateurs déjà existants dans notre pays ont essayé d'abriter cette nouvelle technologie dans leurs réseaux. Mais, malgré la situation économique de notre pays, ces opérateurs n'ont pu rien faire pour le développement de leurs projets. C'est ainsi que l'introduction de la technologie WAP à Madagascar demeure un essai tout simplement. WAP présente beaucoup de difficultés face aux utilisateurs : la complexité de la manipulation de l'appareil mobile compatible WAP, les contraintes qui se posent sur la caractéristique de ce dernier exigent une limitation des applications qu'on peut faire à partir de WAP, le temps de consultation de pages WAP (faute de débit de transfert d'information dans le réseau des mobiles), le coût d'utilisation, etc.

VI.4 L'avenir de la technologie WAP

Les services WAP ne rencontrent pas les succès attendus. Plusieurs facteurs peuvent être associés à cette situation :

- Un message marketing décalé : "l'Internet mobile" par rapport aux services proposés, l'environnement graphique très rudimentaire comparé à celui du Web, des standards du forum industriel "WAP forum" instables et encore peu aboutis, un réseau GSM peu adapté à ce type de trafic.

Au cours de l'année 2001, l'introduction du GPRS, effaçant les principaux défauts associés aux réseaux mobiles actuels, devrait relancer ce marché.

- Actuellement, tous les détenteurs de terminaux WAP n'utilisent pas la fonction en raison de temps d'accès assez long, d'une qualité de service médiocre, d'une navigation de site en site très délicate. Cela explique, d'une part, le décalage entre le nombre de terminaux commercialisés et, d'autre part, les variations sur le nombre d'utilisateurs actifs.

- Dans tous les cas, les services WAP génèrent des revenus supplémentaires pour l'opérateur mobile, indépendamment du portail utilisé. Les utilisateurs de services WAP "consomment" plus de minutes que les abonnés classiques même s'ils restent connectés en moyenne seulement de 3 minutes.

Malgré ce très lent démarrage, le WAP ne paraît pas remis en cause. Dans la phase de transition vers la troisième génération, les trois opérateurs mobiles s'appuient sur cette technologie qui sera associée prochainement au GPRS. L'intégration de la fonction WAP dans tous les terminaux GSM ou GPRS commercialisés à la fin d'année 2000 confirme cette tendance.

2^{ème} PARTIE : APPLICATION SOUS LINUX

GENERALITE

Comme certains systèmes d'information sont basés sur différents outils tels que le système d'exploitation qui est nécessaire pour le développement et l'exploitation des logiciels, le programme et logiciel de traitement ou d'analyse des données. Cette seconde et dernière partie englobe les différents outils de base utilisés qu'on doit connaître afin d'élaborer une simple application par le biais du WAP et un exemple d'application qui met en œuvre une simple messagerie en utilisant le protocole WAP.

Avant d'atteindre l'objectif de ce livre qui est constitué d'une élaboration d'application permettant l'envoi et la réception d'un simple message par la simulation du protocole WAP, on va d'abord parler de l'environnement du système d'exploitation Linux afin de connaître ses points forts et ses avantages par rapport aux autres. Ensuite, la mise en œuvre du serveur Web Apache : son installation, sa configuration pour le rendre compatible WAP et sa mise en relation avec le langage de script PHP et un serveur de base de données MySQL.

De tels programmes sont indispensables à la constitution d'un serveur WAP dans lequel, d'une part, les ressources d'une telle messagerie résident et d'autre part, l'application se lance lorsque l'utilisateur réclame une demande convenable.

Chapitre I. ENVIRONNEMENT LINUX

I.1. Présentation

Linux est propriété du Finlandais Linux THORVALDS. C'est un système d'exploitation de la famille d'Unix : il ressemble à Unix mais ne provient pas du tout des mêmes sources. Il a été élaboré à l'origine pour des PC et compatibles. De nos jours, il se décline sur plusieurs plates-formes dont Sun, HP, Mac. Il y a également plusieurs distributions qui sont disponibles sur le marché : Red Hat, Suse, Caldera, Debian, Slackware, Mandrake, ... Notons toutefois que ces distributions fonctionnent toutes avec un même noyau (ou Kernel) Linux.

De plus, Linux est indépendant vis-à-vis des éditeurs de logiciels et ne se classe ni dans le domaine public, ni dans le « partagiciel » : il fait partie du « logiciel libre », appelé couramment « graticiel ».

I.2. Pourquoi utilise-t-on Linux ?

Linux , en tant que système d'exploitation de toutes sortes d'applications techniques, scientifiques, éducatives, présente beaucoup d'avantages :

- Multitâches : on peut exécuter plusieurs programmes en même temps avec le système d'exploitation Linux,
- Multi-utilisateurs : Linux supporte plusieurs utilisateurs actifs sur la même machine en même temps,
- Multi-plates formes : il fonctionne sur différents processeurs, et pas seulement Intel,
- Toutes les sources sont disponibles : le noyau, les pilotes, les outils de développement et tous programmes utilisateurs .De plus ils sont diffusables,
- Possibilité illimitée d'émulation de terminaux,
- Possibilité de gestion de plusieurs serveurs,

- Consoles virtuelles multiples : plusieurs sessions indépendantes accessibles par une combinaisons de touches. Elles sont allouées dynamiquement et l'on peut en utiliser jusqu'à 64 simultanément,
- Linux utilise le système de fichiers ISO 9660 qui peut lire tous les formats standard de CD-ROM.
- Linux utilise un système de fichiers spécial nommé UMSDOS qui autorise l'installation de Linux directement sur une partition MS-DOS,
- X Windows System (X11R6) supportant l'essentiel des cartes vidéo et des souris disponibles sur PC,
- Support des principales cartes sonores,
- Linux est un système très stables : il ne plante pratiquement jamais,
- Système Unix plus rapide par rapport aux Unix commerciaux,
- Tout ce qu'il faut pour le développement. Plusieurs langages de programmation sont disponibles : C, C++, Java, Pascal , Perl, Python, Newton, Objective C...

I.3. Quels sont ses inconvénients par rapport aux autres systèmes d 'exploitation ?

- Difficulté lors de la configuration (serveurs, noyau),
- Difficulté d'accès pour les débutants,
- Pas suffisamment de logiciels commerciaux (sauf pour la distribution Caldera par exemple).

Chapitre II. SERVEUR APACHE

« Configuration pour le rendre compatible WAP et mise en relation avec PHP, MySQL »

II.1. Présentation du serveur Apache

En général, le programme serveur Apache est livré avec toutes les versions de Linux, mais sa version varie selon la distribution et la version de Linux . Apache est un serveur http qui est configuré par modification de fichiers textes. Face aux autres serveurs http, elle demeure le plus configurable, c'est pourquoi, on peut dire que le programme Apache est le plus connu et vraisemblablement l'un des meilleurs serveurs http .

Le serveur Apache utilise normalement des fichiers HTML et les différents formats d'images habituels sur le serveur Web, par exemple JPEG, PNG, GIF, etc. En jargon technique, ces désignations sont appelées des types MIME. Un serveur Web normal ne peut rien faire avec des fichiers WML ni avec le format d'images associées WBMP (Wireless Bitmap). Pour autoriser cette opération, il faut ajouter quelques lignes dans le fichier de configuration pour que le serveur puisse identifier grâce à l'extension des fichiers (.wml ou .wbmp) de quel type de fichier il s'agit.

II.2. Qu'est-ce qu'on entend par type MIME ? [1]

Pour spécifier le type de document que le serveur Web envoie vers le micro-navigateur , on utilise ce qu'on appelle le type MIME. Il s'agit de l'acronyme de « Multipurpose Internet Mail Extensions », qui assure l'échange de données entre deux ordinateurs lorsque des fichiers qui ne sont pas du simple texte sont transmis à travers Internet. Pour la configuration du serveur WAP, ils sont différents de ceux qui sont utilisés pour configurer un serveur http normal.

Le type MIME (*Multipurpose Internet Mail Extensions*) d'un document WML est text/vnd.wap.wml. Cette information doit être indiquée dans l'en-tête http. Le concept WAP introduit aussi des nouveaux types MIME (voir *Tableau 2.3.1.*):

Parmi les types MIME spécifiés dans le *Tableau 2.3.1.* , seulement trois de ces nouveaux types MIME sont directement employés. Il est nécessaire de les déclarer dans le serveur Web utilisé pour fournir les contenus WML.

TYPE DE FICHIER	TYPE MIME ASSOCIE	DESCRIPTION
Wml	Text/vnd.wap.wml	Fichier XML
Wmlc	Application/vnd.wap.wmlc	Flux WML compilé
Wmls	Text/vnd.wap.wmlscript	Fichier WMLScript
Wmlsc	Application/vnd.wap.wmlscriptc	Flux WMLScript compilé
Wbmp	Image/vnd.wap.wbmp	Fichier graphique WBMP

Tableau 2.2.1. Types MIME utilisés par WAP

II.3. Installation de paquetage du serveur Web Apache et mise en relation avec PHP/MySQL

Définition 2.2.1

PHP est un langage orienté Web . PHP (officiellement "PHP: Hypertext Preprocessor") est un langage de script HTML, qui fonctionne coté serveur.

Définition 2.2.2

MySQL est un langage rapide, flexible, facile à utiliser. c'est aussi un véritable serveur de base de données SQL Multi-Utilisateur et multi-threaded. SQL est le plus populaire langage de base de données dans le monde, c'est un langage standard qui rend le stockage des données facile, la mise à jour et l'accès à l'information.

L'installation décrite ici prend exemple sur les paquetages et les particularités de la distribution "Mandrake 7.2", mais elle est sans doute aisément transposable à toutes les distributions Linux.

L'objectif est d'installer le serveur WEB Apache, pourvu du module PHP, lui-même possédant les extensions nécessaires pour l'accès au gestionnaire de base de données relationnelle MySQL.

II.3.1. Méthode

II.3.1.1. Choix initiaux

- Boot sur disquette d'installation ou sur le CD positionné au départ.
- Si besoin, lire le document `/doc/install/fr/install.htm` qui détaille les différents modes d'installation
- Choix de type d'installation conseillé : **expert**, puis **serveur**
- Suite de l'installation, comme d'habitude (partitionnement, niveau de sécurité moyenne, montage automatique des périphériques (supermount) ...

II.3.1.2. Sélection des groupes de paquetages

- Si on coche *sélection individuelle*, on pourra affiner le choix à l'étape suivante
- Si on choisit les paquetages individuellement, cocher **Gestion automatique des dépendances**
- Si on connaît les serveurs et les applications à installer, passer plutôt en choix alphabétique.

II.3.2. Liste des paquetages à sélectionner

- MySQL
- MySQL-bench
- MySQL-client
- MySQL-shared
- Apache
- Apache-commun

- Apache-suexec : ce paquetage est utilisé pour qu'un script CGI agit avec les droits de son propriétaire et non pas ceux de Apache.
- mod_php : il est utilisé pour l'intégration de php comme module d'Apache. En effet, lorsque le PHP est compilé en tant que module Apache, ce module hérite des permissions accordées à l'utilisateur faisant tourner Apache (par défaut, l'utilisateur "nobody").
- mod_ssl
- PHP
- PHP-MySQL (fonctions PHP pour MySQL)

Remarques :

- Pour l'installation d'un paquetage au format rpm (c'est-à-dire installation ultérieure d'un paquetage, on peut utiliser la commande :

```
# rpm -ihv paquetage.rpm
```

- Dans le cas d'installation des fichiers archives voir **ANNEXE E**.

II.4. Les fichiers de configuration du serveur Apache

Comme la plupart des distributions de Linux (par exemple MANDRAKE), les fichiers de configuration d'Apache sont placés dans le répertoire `/etc/httpd/conf` dès qu'on installe ce programme de serveur : emplacement par défaut.

Dans le cas général, on voit trois fichiers majeurs de configuration :

- `httpd.conf` ou/et `commonhttpd.conf` : fichiers de configuration principal du serveur
- `srm.conf` : fichier de configuration des ressources du serveur
- `access.conf` : fichier de contrôle d'accès global (ou ACF : Access Control File)

II.5. Lancement en mode autonome

Comme tous les langages de programmation, ce programme serveur accepte le commentaire. Ce dernier est marqué par une dièse « # » au début d'une ligne, il en est de même pour les commandes. Et si on veut rendre ces commandes active, on enlève la dièse devant chaque ligne de commandes.

Comme nous avons mentionné auparavant, il y a trois fichiers majeurs de configuration. En principe, cela dépend de la distribution de Linux et sa version utilisée. Dans ce qui suit, nous avons utilisé la distribution MANDRAKE 7.2 ; pour cette dernière, la configuration se fait presque au niveau du fichier `httpd.conf` qui est placé dans `/etc/httpd/conf`.

II.5.1. Configuration du `httpd.conf` pour rendre Apache compatible WAP

Outre la configuration de base du programme serveur Apache (voir **ANNEXE D**), une configuration supplémentaire est nécessaire pour rendre ce serveur Apache compatible WAP, il suffit tout simplement de configurer le type MIME. Pour cela, éditer le fichier de configuration `httpd.conf` par un éditeur de textes, par exemple l'éditeur `vi` ou `gedit`, puis on y ajoute quelques lignes.

- Dans la version ancienne d'Apache, le type MIME est configuré directement au niveau du fichier de configuration `httpd.conf`. Dans ce cas, on cherche le terme « `AddType` » et on y ajoute les lignes suivantes :

```
# MIME type for WAP

AddType text/vnd.wap.wml      wml

AddType text/vnd.wap.wmlscript wmls

AddType text/vnd.wap.wmlscript wmlscript

AddType application/vnd.wap.wmlc      wmlc

AddType application/vnd.wap.wmlscriptc wmlsc

AddType image/vnd.wap.wbmp      wbmp
```


- Dans la version évoluée, cette configuration est un peu plus complexe car le type MIME ne se configure pas directement dans le fichier httpd.conf, Il occupe un fichier tout entier outre que ce dernier. Il faut donc chercher ce fichier et faire la même opération que précédemment.

Remarque : Pour les autres fichiers de configuration, il faut se reporter à la configuration de base du serveur. (voir **ANNEXE D**)

II.5.2. Configuration pour httpd.conf avec la mise en relation Apache + PHP + MySQL

Dès que le programme Apache est installé, il est déjà pleinement fonctionnel, configuré et ne nécessite pas de modification pour une utilisation de base.

II.5.2.1. Utilisation du script PHP avec Apache

PHP a normalement été intégré au serveur Apache sous forme d'un module chargeable, le fichier libphp4.so, situé comme tous les autres modules d'Apache dans /usr/lib/Apache.

Pour vérifier le chargement du module, consulter la fin du fichier de configuration d'Apache, /etc/httpd/conf/httpd.conf, on doit y trouver la directive d'inclusion du fichier de configuration de PHP : « Include conf/addon-modules/php.conf » ; le chemin étant noté relativement à /etc/httpd .

Le fichier php.conf contient notamment la directive d'inclusion du module PHP, et la description des extensions de fichiers qui devront être interprétés par ce module :

```
LoadModule php4_module /usr/lib/Apache/libphp4.so
```

```
AddModule mod_php4.c
```

```
AddType application/x-httpd-php .php .php4 .php3 .phtml
```

```
AddType application/x-httpd-php-source .phps
```

PHP possède lui aussi son fichier de configuration, **/etc/php.ini**. Observer que PHP prend bien en compte le module d'extension MySQL, par la présence de l'extension=MySQL.so (en ligne 243)

En cas de modification, par exemple PHP fonctionne comme un module d'Apache, il faut redémarrer Apache pour qu'il réinitialise PHP par la lecture de php.ini (rappel de la commande : /etc/rc.d/init.d/httpd stop|start)

II.5.2.2. Utilisation de la base de données MySQL avec Apache

On peut changer le format historique d'Apache pour qu'il soit facilement lisible par MySQL en ajoutant les lignes suivantes dans le fichier de configuration d'Apache :

LogFormat \

```
"\"%h\",%{Y%m%d%H%M%S}t,%>s,\"%b\", \"%{Content-Type}o\", \
```

```
\"%U\", \"%{Referer}i\", \"%{User-Agent}i\""
```

II.4.3. Lancement et relancement du serveur en mode autonome

Pour lancer le serveur httpd en mode autonome, il suffit de se placer sous root dans un consol et de taper la commande :

httpd & : si on ne modifie pas la directive ServerRoot

où

httpd -d /server/root : où **server/root** le chemin que nous avons affecté à la directive **ServerRoot**.

Pour relancer le serveur httpd après une modification des fichiers de configuration, nous avons recours aux commandes suivantes :

- **1^{ère} Méthode**

ps ax | grep httpd

kill -HUP pid

La première ligne est utilisée pour obtenir l'identifiant - **pid** - du processus correspondant au serveur httpd.

- **2nd Méthode**

L'utilisation de la commande :

/etc/rc.d/init.d/httpd [**option**]

L'option [**option**] peut prendre :

- o stop
- o start
- o restart

Chapitre III. APPLICATIONS

« Simulation sur ordinateur »

But :

Cette simulation est faite pour illustrer un exemple de mise en oeuvre d'une application WAP, plus précisément d'une simple messagerie . Il s'agira :

- en premier lieux, de montrer comment concevoir un site WAP ?

à savoir :

- mise en place d'un serveur WAP
 - élaboration des pages WAP
 - mise en relation du WML , PHP et MySQL
- en second lieu, d'expliquer la transaction qui se fait lors de l'envoi ou de la réception d'un simple message à partir du WAP.

III.1 Présentation

Cet exemple d'application est un programme permettant l'envoi et la réception d'un simple message texte à partir de la technologie WAP. En effet, grâce à lui, l'envoi d'un message à partir d'un terminal mobile d'un réseau sans fil ou d'un émulateur de portable compatible WAP ou d'un navigateur WAP connecté à l'Internet via le protocole WAP vers un terminal d'un réseau Intranet devient possible et vice-versa.

Tous les programmes dans cet application sont écrits de façon à ce qu'on peut les visualiser sur n'importe quel navigateur WAP car ils sont tous élaborés à partir du langage WML. Certains fichiers WML sont générés par le langage de script PHP afin de les rendre dynamiques.

La figure ci-dessous donne l'organigramme représentant les fichiers pris en compte

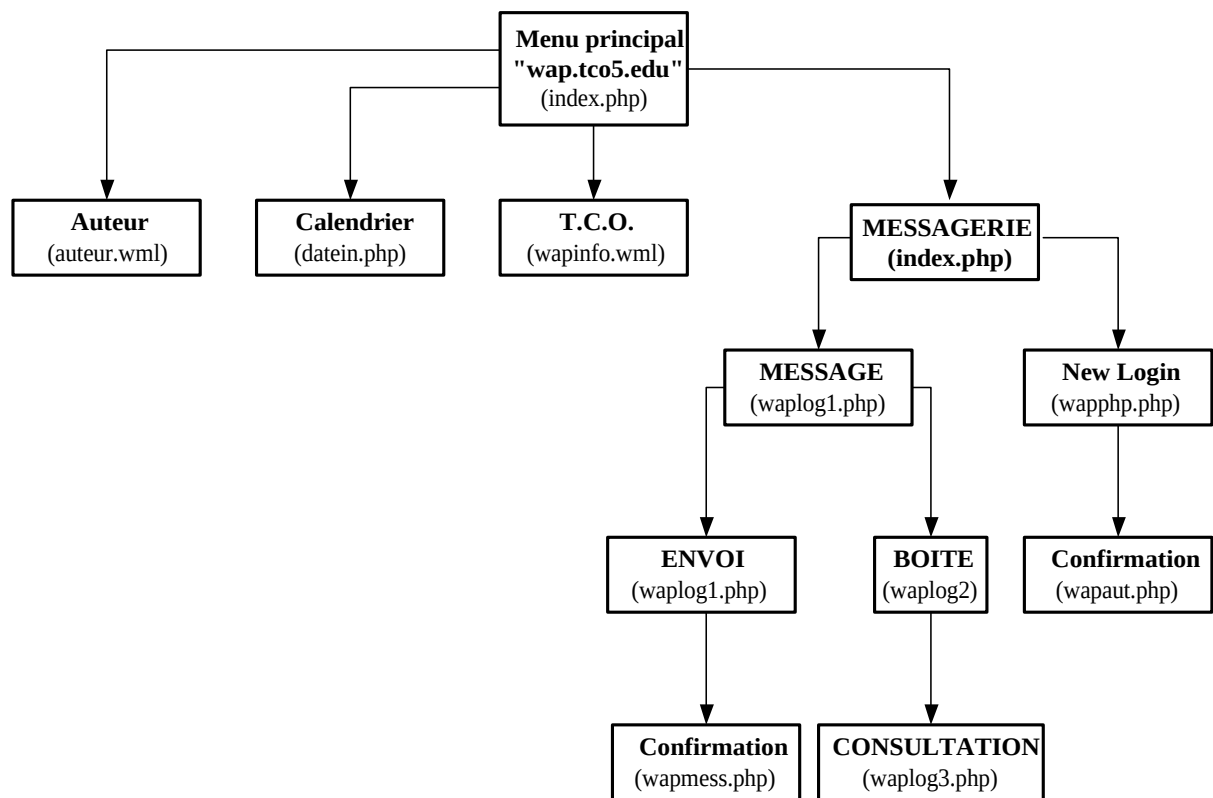


Figure 2.3.1. Arborescence des fichiers résidant dans « wap.tco5.edu »

Pourquoi utiliser PHP ?

- Le langage PHP possède les mêmes fonctions que les autres langages permettant d'écrire des scripts CGI, comme collecter des données, générer dynamiquement des pages Web ou bien envoyer et recevoir des cookies.

- La plus grande qualité et le plus important avantage du langage PHP est le support d'un grand nombre de bases de données. Réaliser une page Web dynamique interférant une base de données est extrêmement simple. Les bases de données suivantes sont supportées par PHP: Adabas D, dBase, Empress, FilePro, Informix, MySQL, Oracle, etc.

Pourquoi utiliser MySQL ?

Le serveur de base de données MySQL est utilisé pour stocker les informations des utilisateurs afin de pouvoir les authentifier et pour stocker des données comme les messages, dates, etc. Ainsi, l'utilisateur a la possibilité :

- D'insérer des données dans la table qu'il crée lors de l'inscription dans ce service de messagerie,
- De mettre à jour les données déjà stockées dans la table,
- De supprimer ces données.

III.2. Les formulaires

III.2.1 Principaux techniques d'élaboration d'un page WAP généré à partir du script PHP

Chaque fichier ou document doit se conformer à certaines règles de syntaxe :

- Chaque document WML doit contenir dans son en-tête la déclaration XML de la DTD du langage WML.

```
< ? xml version = " " ?>
```

```
< ! DOCTYPE wml PUBLIC "-//WAPFORUM/DTD WML 1.1//EN"
```

```
"http://www.wapforum.org/DTD/wml_1.2.xml " >
```

- Certaines pages sont générées à partir du script PHP afin de les rendre dynamiques. Dans ce cas, il faut indiquer un Content-Type correct pour que le terminal puisse reconnaître le code WML. Le Content-Type correspondant est :

Content-type : text/vnd.wap.wml

En outre, l'utilisation d'une page WML généré à partir du script PHP change l'historique de l'en-tête de cette page. Ainsi, l'en-tête devient :

```
<?php
```

```
Header( "Content-type: text/vnd.wap.wml");
```

```
echo "<?xml version=\"1.0\"?>";
```

```
echo "<!DOCTYPE wml PUBLIC \" -//WAPFORUM//DTD WML 1.1//EN\" ";
```

```
echo " \"http://www.wapforum.org/DTD/wml_1.1.xml\">"
```

```
?>
```

- Wml dispose d'un ensemble de caractères spéciaux :

L'interprétation du code source WML ne prend pas en charge les caractères spéciaux qui sont écrits directement ou explicitement dans le programme source. Dans le langage WML, les caractères spéciaux doivent être codés. Le tableau ci-dessous présente les codes de quelques caractères spéciaux les plus utilisés.

Caractère	Code
<	<
>	>
'	&apos
«	"
&	&
\$	\$\$
Espace	

Tableau 2.3.1. Codes de quelques caractères spéciaux

Comment élaborer le contenu d'une telle page ?

- Le code PHP est inclus entre **<?php** et **?>** qui permettent au navigateur de passer en "mode PHP". Ce qui distingue le PHP des langages de script comme le Javascript est que le code est exécuté sur le serveur. Si vous avez un script similaire sur votre serveur, le client ne reçoit que le résultat du script, sans aucun moyen d'avoir accès au code qui a produit ce résultat.

Exemple :

```
<?php
    mysql_connect ("wap.tco5.edu", "tco5", "rado");
?>
```

- On écrit une page WML avec un code inclus à l'intérieur afin de réaliser une action précise (dans ce cas là, afficher du texte). Ce qui différencie le script PHP des autres scripts CGI écrits dans d'autres langages tels que le Perl ou le C (Au lieu d'écrire un programme avec de nombreuses lignes de commandes afin d'afficher une page WML).

Exemple :

```
<?php
Header( "Content-type: text/vnd.wap.wml");
echo "<?xml version=\"1.0\"?>";
echo "<!DOCTYPE wml PUBLIC \" -//WAPFORUM//DTD WML 1.1//EN\" ";
echo " \"http://www.wapforum.org/DTD/wml_1.1.xml\">";
?>
<wml>
  <card id="start3" title="MESSAGE">
    <p align="center">
      <?php
        $date = date("d/m/Y");
        echo"<strong>$date</strong>";
      ?>
    <br/>
  </p>
</card>
</wml>
```

III.2.2. Conception d'un site de simple messagerie

Les codes sources ci-après ne représentent que les principaux formulaires de cet exemple d'application. Ils sont tous générés à partir du script PHP, ainsi ils ont le même en-tête que celui qu'on a décrit précédemment.

III.2.2.1. Formulaire de page d'accueil

```
<wml>
  <card id="card1" title="wap.tcom.edu">
    <p align="center">
      <a href="#card2">Messagerie</a><br/>
      <a href="wapinfo.wml">T.C.O.</a><br/>
      <a href="datein.php">Calendrier</a><br/>
    </p>
  </card>
</wml>
```



```

        <a href="auteur.wml">Auteur</a>
    </p>
</card>
<card id="card2" title="MESSAGERIE">
    <p>
        <?php
            mysql_connect ("wap.tco5.edu","tco5","rado");
        ?>
    </p>
    <p align="center">
        <a href="wapphp.php">New Login</a><br/>
        <a href="waplog.php">Login Now</a><br/>
        <a href="#card1">Menu</a><br/>
    </p>
</card>
</wml>

```

III.2.2.2. Formulaire de page d'inscription

Le corps du programme suivant permet la saisie et l'envoi des informations de l'utilisateur par une méthode POST.

```

<wml>
    <card title="New login" newcontext="true">
        <p>
            <strong>Login :</strong> <input name="nom" type="text" maxlength="30" />
            <strong>Password :</strong> <input name="pass" type="password"
maxlength="32" />
            <strong>Sexe :</strong> <input name="sexe" type="text" maxlength="4" />
            <strong>Ville :</strong> <input name="ville" type="text" maxlength="32" />
            <do type="accept" label="Login">
                <go href="wapaut.php" method="post">
                    <postfield name="nom" value="$(nom)" />

```

```

        <postfield name="pass" value="$(pass)" />
        <postfield name="sexe" value="$(sexe)" />
        <postfield name="ville" value="$(ville)" />
    </go>
</do>
</p>
<p>
    <do type="accept" label="Menu">
        <go href="index.php"/>
    </do>
</p>
</card>
</wml>

```

III.2.2.3. Formulaire de page d'authentification

Ce programme permet la saisie du nom de login et du mot de passe de l'utilisateur afin de l'authentifier.

```

<wml>
    <card newcontext="true">
        <p>
            <strong>Login :</strong> <input name="nom" type="text" maxlength="30" />
            <strong>Password :</strong> <input name="passe" type="password"
maxlength="32" />
        </p>
        <p>
            <a href="wlog.php?nom=$(nom)&pass=$(passe)"></a>
        </p>
        <p>
            <do type="accept" label="Menu">
                <go href="index.php"></go>
            </do>
        </p>
    </card>
</wml>

```

```

</card>
</wml>

```

III.2.2.4. Formulaire de page d'écriture d'un message

Le programme suivant permet l'affichage de la date courante, la saisie du message et l'envoi de ces données vers le serveur de base de données.

```

<wml>
  <card id="start3" title="MESSAGE">
    <p align="center">
      <?php
        $date = date("d/m/Y");
        echo "<strong>$date</strong>";
      ?>
      <br/>
    </p>
    <p align="center">
      <a href="#ecrit">Ecrire</a><br/>
      <a href="waplog2.php?nom=$(nom)">Consulter</a><br/>
      <do type="accept" label="Menu">
        <go href="index.php"/>
      </do>
    </p>
  </card>
<!-- ecriture d'un message-->
  <card id="ecrit" title="ENVOI">
    <p>
      <strong>A : </strong>
      <input name="des"/>
    </p>
    <p>
      <strong>Message :</strong>
      <input name="message"/>
    </p>
  </card>

```

```

<p align="right">
  <do type="prev" label="Back"><prev/></do>
  <anchor title="Connexion">Envoyer
    <go href="wapmess.php" method="post">
      <postfield name="nom" value="$(nom)"/>
      <postfield name="des" value="$(des)"/>
      <postfield name="message" value="$(message)"/>
    </go>
  </anchor>
</p>
</card>
</wml>

```

III.2.2.5. Formulaire de page de Consultation d'un message

```

<wml>
  <card id="lire" title="CONSULTATION">
    <p>
      <?php
        mysql_select_db ("messengerie");
        $query = " SELECT * FROM $nom WHERE id = $ni";
        $result = mysql_query ($query);
        $ro = mysql_num_rows ($result);
        if ($ro < '1'){
          echo "impossible";
          echo "<do type='prev' label='Back'><prev/></do>";
        } else {
          $row = mysql_fetch_object ($result);
          $from = $row->expediteur;
          $mess = $row->message;
          echo "<do type='prev' label='Back'><prev/></do>";
          echo "<b>De : </b>$from<br/>";
          echo "<b>Message : </b>$mess<br/><br/>";
          echo "<a href='#code'>Done</a>";
        }
      </?php>
    </p>
  </card>
</wml>

```

```

    }
    mysql_free_result ($result);
?>
<do type="accept" label="Supprimer">
    <go href="waplog4.php?nom=$(nom)&ni=$(ni)">
    </go>
</do>
</p>
</card>
<card id="code">
    <p align="center">
        <?php
            echo "<br/>";
            echo "<br/>";
            mysql_select_db ("messagerie");
            $que = " UPDATE $nom SET code ='1' WHERE id = '$ni'";
            $res = mysql_query ($que);
            if ($res){
                echo "<a href='waplog2.php?nom=$(nom)&ni=$(ni)'>Done</a>";
            } else {
                echo "<a href='waplog2.php?nom=$(nom)&ni=$(ni)'>Erreur</a>";
            }
            //mysql_free_result ($res);
        ?>
    </p>
</card>
</wml>

```

III.3. Manipulation et résultats

III.3.1 Comment s'inscrire dans le site de simple messagerie « wap.tco5.edu »?

La première chose à faire est de s'inscrire, c'est-à-dire, créer un compte utilisateur. Pour cela :

- consulter d'abord le site de cette messagerie à l'aide de l'adresse « <http://wap.tco5.edu> » : *Figure 2.3.2.a*
- sélectionner '**messagerie**' : *Figure 2.3.2.a*
- Cliquer sur '**New login**' : *Figure 2.3.2.b*
- cliquer sur 'Option' et sélectionner '**Login**' : *Figure 2.3.2.c*



Figure 2.3.2. Formulaire d'inscription

III.3.2 Authentication

Pour cela, on se place dans le menu **MESSAGERIE** puis :

- Sélectionner **Login Now** : (*Figure 2.3.3.a*)
- Entrer le login et le mot de passe puis valider : (*Figure 2.3.3.b*)

- Si les paramètres introduits sont valides, on obtient sur l'afficheur comme le montre la **Figure 2.3.3.c** ; Sinon on obtient comme le montre la **Figure 2.3.3.d**



a)

b)

c)



d)

Figure 2.3.3. Formulaire d'authentification

III.3.3 Ecrire un message

Si on est dans la menu **MESSAGE** :

- Sélectionner **Ecrire** : *Figure 2.3.4.a*
- Entrer les données à envoyer puis sélectionner **Envoyer** : *Figure 2.3.4.b*
- Puis on attend le message de confirmation : *Figure 2.3.4.c*



a)

b)

c)

Figure 2.3.4. Formulaire pour l'écriture d'un message

III.3.4.Consulter un message

Supposons qu'on est dans le menu **MESSAGE** :

- Sélectionner **Consulter** : *Figure 2.3.5.a.*
- Et on a sur l'écran le menu **INFO**, on peut lire, à partir de ce menu, les informations concernant l'état du message dans la boîte, c'est-à-dire le nombre total de messages, nombre de messages déjà lus, etc. Et puis on introduit le numéro de message à consulter dans la zone de saisie **Consulter**, puis sélectionner **Lire** : *Figure 2.3.5.b.*

- On obtient sur l'écran le message qu'on veut lire : **Figure 2.3.5.c.**
- On a la possibilité d'effacer le message courant en sélectionnant **Option**, puis **Supprimer** : **Figure 2.3.5.c.**



a)

b)

c)

Figure 2.3.5. Formulaire pour la consultation d'un message

CONCLUSION

Bien avant l'introduction des services WAP, des briques de base sont disponibles pour faire évoluer l'environnement des services et des réseaux mobiles vers la société de l'information. La multiplication des systèmes de communications : GSM, GPRS et UMTS associés à la diversification des services proposés par l'Internet.

Le service WAP fait son premier pas avec le système GSM de la seconde génération des systèmes mobiles. Cette introduction de nouveau service dans la société n'aboutit guère au but attendu à cause de l'utilisation d'un débit de transmission de données inférieur dans les réseaux mobiles existants et d'un mode de commutation par circuit.

L'arrivée des nouveaux systèmes de télécommunications sans fil a changé l'opportunité de la société d'information. Cet événement est marqué par l'apparition du nouveau standard GPRS suivi de la troisième génération de télécommunications mobiles, qui ne sont que des évolutions des systèmes de la 2G. Ces normes offrent des services à débit élevé, une transmission de données en mode paquet et proposent des architectures souples afin de minimiser l'impact d'un changement technologique à venir ; ce qui est parfaitement plus efficace pour la technologie WAP.

En réalité, ce dernier n'est qu'un protocole de communication de données circulant sur le réseau sans fil et dans un environnement d'application basé sur la technologie sans fil. La technologie WAP utilise, dans son infrastructure, la technologie proxy qui favorise l'interconnexion des réseaux sans fil et des réseaux IP. En outre, le service WAP est conçu de façon qu'il puisse supporter plusieurs types de supports comme le réseau GSM, le réseau GPRS, etc.

Ainsi, l'accès aux données stockées dans un serveur de base de données, comme MySQL situé quelque part dans le monde, à partir d'un terminal mobile ou fixe incorporant des navigateurs qui sont capables d'afficher les contenus écrits en WML par le biais du protocole WAP devient possible.

ANNEXES

ANNEXE A : Le protocole et transaction HTTP

Présentation et structure du protocole http

Le protocole http (Hypertext Transfert Protocol) est basé sur le système d'adressage universel URL, c'est un protocole utilisé par le serveur World Wide Web depuis les années 90. http est un protocole client/serveur qui permet la communication rapide des données entre le client et le serveur. Autrement dit, il rend l'échange de données plus vite aux systèmes de réseaux d'information intégrant des ressources distribuées de type multimédia.

Ce protocole est désigné pour identifier des ressources bien référencées et les méthodes de traitement associées. Les actions sont achevées par le biais de messages échangés entre le serveur et le client ; comme ce qu'on a vu dans la plupart des protocoles utilisés par Internet. Ces messages sont codés dans un format de type appelé « type MIME » (Multipurpose Internet Mail Extension) et permettant de ce fait une communication rapide de données très variées : texte, son, vidéo, image, ...

Chaque message envoyé à l'aide de protocole http contient également des informations relatives au client, au serveur et à la transaction.

Transaction http

En général, quand un client se communique avec le serveur http, deux étapes vont se produire :

- **1^{ère} étape** : le client envoie une requête à laquelle il demande ce qu'il veut pour naviguer.

Cette requête contient plusieurs champs décrivant la ressource et les informations relatives au client :

Méthode Method URL HTTP_version

En-tête From:

 If-Modified-since

 Referer:

 User-Agent

Descriptif Accept:

Content-Encoding

Content-Length:

Content-Type:

Corps de la requête

• **2nde étape** : le serveur, après avoir reçu et traité une requête, renvoie à son tour une réponse dans le format http composé d'un en-tête http décrivant le statut de la transaction, la description des données transmises aux clients et des données requises. Le type de données est spécifié par le serveur à l'aide du type MIME qui est précisé par le champs Content-Type. Le client utilise exclusivement ce type pour identifier le contenu de la réponse.

Format http d'une réponse

Statut HTTP-Version Status-Code Reason-Phrase

En-tête Location :

Server :

Descriptif Content-Encoding

Content-Length:

Content-Type:

Date :

Expires :

Last-Modified :

Document Document HTML

ANNEXE B : Comparaison WTLS et SSL

Comme on l'a dit dans le détail de la couche WTLS, la sécurité du WAP a été copiée sur SSL

▪ SSL : Secure Socket Layer

Le protocole SSL, bien connu des internautes, est actuellement la référence pour sécuriser une transmission sur Internet.

Fonctionnement :

Le navigateur fait une demande de transaction sécurisée au serveur . le serveur lui envoie son certificat d'authentification délivré par un organisme officiel. Ce certificat comporte une clé publique. Le navigateur s'assure tout d'abord que le certificat délivré est valide puis il envoie au serveur une clé secrète codée issue de la clé publique (de 56 ou 128 bits). Seul le serveur sera donc capable de décoder cette clé secrète car il détient la clé privée. Cette clé secrète ainsi créée sera utilisée par l'algorithme de Bulk (cryptographie symétrique) pour encoder les messages.

Le serveur et le client possèdent maintenant une clé secrète partagée et les échanges sont faits par l'intermédiaire de cette clé. Pour assurer l'intégrité des données, on utilise un algorithme de hash.

On voit bien que ce mécanisme permet d'assurer la confidentialité (mécanisme de chiffrement), l'intégrité (algorithme de hash) et l'authentification (certificats). Cependant seule l'authentification du serveur est implémentée et la non-répudiation n'est pas prise en compte.

▪ WTLS : Wireless Transport Layer Security

Quand on pense à la sécurité, on imagine des transmissions fiables qui ne sont pas garanties dans le cas du WAP ; en effet, la bande passante est étroite et la qualité des transmissions n'est pas garantie. Pour s'adapter au mieux à ces contraintes, WTLS définit un nombre d'en-têtes moins importants que SSL et la compression y est plus élevée. Dans le but d'augmenter encore plus la sécurité, WTLS définit en outre la possibilité de réactualiser la clé secrète sans passer par la phase de négociation pénalisante en terme de bande passante. Des solutions utilisant le protocole WTLS existent et permettent aux entreprises de profiter de WTLS dans leurs applications et d'intégrer des systèmes PKI (Public Key Infrastructure) pour la gestion des certificats d'authentification. Dans sa version 1.1, WAP permet les options de sécurité suivante :

- Confidentialité
- Intégrité
- Authentification du serveur

L'échange sécurisé nécessite un terminal mobile supportant WTLS, un serveur Web supportant SSL et une passerelle WAP (ou un serveur) supportant WTLS et SSL. Lors de l'échange sécurisé entre la passerelle WAP et un serveur Web, les données sont codées en utilisant le protocole SSL. Le serveur WAP a pour but de faire la conversion entre les formats WTLS et SSL. Ce point de liaison est critique car les données au format SSL doivent être décodées avant d'être encodées de nouveau au format WTLS. Il est donc important que ce serveur soit astreint à des règles de sécurité particulières, tant au niveau logiciel que matériel.

Les données échangées entre le terminal et la passerelle sont alors codées au format WTLS.

ANNEXE C : Relation entre WML, XML et SGML

Il y a plus de dix ans déjà, un standard a été développé pour permettre d'échanger des documents entre différentes plates-formes. Il s'agit du langage SGML (Standard Generalized Meta Language). Le SGML est une sorte de langage générique de description d'un nombre pratiquement illimité de documents de tout type, englobant aussi bien la traduction de textes sumériens que les plans de construction de la navette spatiale.

Ce langage est malheureusement beaucoup trop compliqué pour pouvoir être imposé aux développeurs du Web. C'est pourquoi le consortium WWW a développé le langage HTML, qui s'appuie très fortement sur le SGML. C'est ainsi qu'un type de document unique a été développé, en englobant une collection de feuilles de style permettant la représentation de textes, d'images et de tableaux, ainsi que de cadres (frames) et doté de possibilités multimédias limités. Le HTML n'est hélas pas très souple, car il n'existe par exemple qu'un seul jeu de commandes. En outre, il est totalement inadapté à l'utilisation par le protocole WAP.

Un nouveau langage a donc été développé il y a peu de temps par le consortium WWW. Il s'agit du XML (Extensible Meta Language), qui est une forme simplifiée de SGML permettant de définir plus simplement des documents spécifiques et offrant aux programmeurs la possibilité d'écrire des programmes de traitement de tout type de documents. Ce langage abandonne les éléments trop compliqués et parfois peu judicieux du SGML et atteint l'objectif d'être plus simple à écrire, plus facile à comprendre et plus souple, afin d'être mieux adapté aux impératifs du World Wide Web. Le XML est cependant une partie du SGML et peut donc être lu par les programmes adaptés comme un fichier SGML habituel. Du point de vue du programmeur, le XML représente donc la solution optimale en comparaison du SGML et du HTML.

Le langage XML permet ainsi de créer de nouvelles balises. Toutes les commandes sont définies dans un fichier XML de description. Ce mécanisme a été utilisé pour la définition du WML. Il s'agit donc en fait d'une application stricte du XML. Chaque page WML contient l'adresse Internet du forum WAP, dans lequel se trouve un fichier XML définissant toutes les balises du WML. Les chercheurs peuvent donc se contenter d'indiquer dans une simple ligne que leur document est un fichier WML pour pouvoir immédiatement utiliser l'ensemble des commandes de ce langage.

En conclusion, le WML est un sous-groupe du XML. Les chercheurs de WML n'ont donc aucune obligation d'apprendre le langage XML, car il suffit d'inclure deux lignes XML au début de chaque fichier WML sans y modifier quoi que soit.

ANNEXE D : Configuration de base du serveur Apache

Configuration de base de httpd.conf

httpd.conf contrôle la façon dont le serveur s'exécute, mais ne fournit pas de détails sur les fichiers qu'il compose (qui sont décrits dans srm.conf). pour lancer un serveur autonome nous devons :

- ❑ Affecter à User et à Group les noms que nous souhaitons. Ils définissent respectivement le nom d'utilisateur et de groupe, qui seront utilisés par le serveur autonome à l'exécution.
- ❑ Nous assurer que ces noms existent dans etc/passwd et etc/group
- ❑ Affecter standalone à **ServerType**
- ❑ Affecter Webmaster à nom_du_serveur à **ServeurAdmin** et ne pas oublier de créer un alias de mail dans etc/aliases
- ❑ Ne pas oublier de taper la commande newaliases pour valider nouvel alias
- ❑ Affecter à **ServerRoot** le chemin d'accès absolu du catalogue où nous prévoyons de placer le binaire httpd
- ❑ Affecter nom du serveur à **ServerName**

Configuration de base de srm.conf

Le fichier de configuration srm.conf nous indique l'endroit où le serveur httpd trouve nos documents et nos scripts. Pour lancer initialement notre serveur Web, nous devons :

- ❑ Modifier la directive **DocumentRoot**, et la faire pointer vers le catalogue correspondant de notre arbre de document. Il s'agit de cataloguer à partir duquel nous proposons des fichiers
- ❑ Affecter à la directive **UserDir** la valeur DISABLED pendant la configuration du serveur. Ceci interdit aux utilisateurs de proposer des fichiers à partir de leurs catalogues

personnels (ce qui représente un risque de sécurité potentiel), `public_html` pour le cas contraire

- ❑ Affecter à la directive **LanguagePriority** les langages par ordre de priorité `.(fr en it)`
- ❑ Modifier les directives **Alias** et **ScriptAlias** si nous prévoyons de placer nos catalogues `icon` et `cgi-bin` ailleurs que dans les chemins par défaut `(/home/httpd/icons` et `)`. L'utilisation des directives `Alias` et `ScriptAlias` supplémentaires nous permet de présenter certains documents à l'utilisateur comme s'ils étaient en réalité dans des catalogues différents, appelés parfois :catalogues virtuels .
- ❑ Ajouter les commandes ci-après pour rendre Perl actif ou enlever le dièses « # » devant toutes les lignes si elles sont déjà écrites par défaut (toujours dans `srn.conf`) :

```
Alias/perl/ .home/httpd/perl/
```

```
<Location /perl>
```

```
SetHandler perl-script
```

```
PerlHandler Apache::Registry
```

```
Option +ExecCGI
```

```
</Location>
```

Configuration de base de `access.conf`

Le Fichier de contrôle d'accès global (Access Control File) est appelé **`access.conf`** . Il contrôle le type d'accès que les clients Web effectuent sur nos catalogues.

`Access.conf` contient par défaut :

```
<Directory /home/httpd/html>
```

```
Options Indexes Includes FollowSymLinks
```

```
AllowOverride All
```

```
Order allow, deny
```

```
</Directory>
```

```
<Directory /home/httpd/cgi-bin>
```

```
AllowOverride All
```

```
</Directory>
```

Ces valeurs par défaut autorisent l'ensemble des fonctions à tous les clients Web, sans précautions de sécurité particulière.

ANNEXE E. Installation d'Apache, de Php et de MySQL à partir des fichiers archives

❑ Premières choses à faire :

Comme d'habitude dans un premier temps vous devez récupérer les archives d'Apache, php et MySQL :

- **Apache_1.3.x.tar.gz**
- **php-4_x.tar.gz**
- **MySQL-3_x.tar.gz**

Dans la plupart des distributions Apache MySQL et php sont souvent installés par défaut. Nous allons donc les désinstaller puis les réinstaller avec nos sources.

Pour vérifier s'ils sont déjà installés tapez :

```
$ rpm -qa | grep -i Apache
```

```
$ rpm -qa | grep -i php
```

```
$ rpm -qa | grep -i MySQL
```

Si ça vous retourne quelque chose dans une de ces trois commandes c'est que quelque chose est installé.

Par exemple si ça vous retourne quelque chose après **rpm -qa | grep -i Apache** il faudra taper :

```
$ rpm -e le_nom_retourne
```

Une fois le ménage fait, il ne vous reste plus qu'à installer.

❑ Installation d'Apache + php

décompresser les archives

```
$ tar -zxvf Apache_1.3.x.tar.gz
```

```
$ tar -zxvf php-4_x.tar.gz
```

configurer Apache

```
$ cd Apache_1.3.x
```

```
$ ./configure
```

configurer PHP

```
$ cd ../php-4_x
```

```
$ ./configure --enable-calendar --with-MySQL --with-Apache=../Apache_1.3.x
```

compiler PHP

```
$ make
```

```
$ make install
```

compiler Apache

```
$ cd ../Apache_1.3.x
```

```
$ ./configure --activate-module=src/modules/php4/libphp4.a
```

```
$ make
```

```
$ make install
```

Ensuite nous allons lui donner un fichier de configuration (php.ini):

```
$ cp ../php-4_x/php.ini-dist /usr/local/lib/php.ini
```

C'est dans le fichier php.ini qu'on va configurer le php (type de balise php, serveur smtp ...)

Installation de MySQL

Décompression de l'archive

```
$ tar -zxvf MySQL-x.tar.gz
```

Configuration

```
$ cd MySQL-x
```

```
$ ./configure
```

Compilation

```
$ make
```

```
$ make install
```

Par défaut MySQL s'installe dans **/usr/local/bin** et le démon sous **/usr/local/libexec**.

Une fois MySQL installé, il faut d'abord créer les bases de défaut :

```
$ ./scripts/MySQL_install_db
```

Normalement on devra voir cette notion:

Creating db table

...

Puis définir **le mot de passe d'admin** pour MySQL :

```
$ MySQLadmin -u root password 'password'
```

Maintenant lançons le serveur:

```
$ ./scripts/safe_MySQLd &
```

Maintenant que tout est installé et configuré, il ne reste plus qu'à faire les bases de données et à programmer en php.

Pour gérer les bases de données MySQL, on devrait utiliser **phpMyAdmin** C'est une interface graphique (écrite en php) qui permet de créer, modifier, supprimer des bases, des tables, ...

BIBLIOGRAPHIE

- [1] : C. IMMLER, M. KREINACKER, A. SPALLEK, « *Internet WAP* », Micro Application, 2000
- [2] : S. TABBANE, « *Réseaux mobiles* », Hermes, 1997
- [3] : A. RATSIMBAZAFY, « *Cours de Télématique et Téléinformatique, 4ème année TCO* », A.U. 1999-2000.
- [4] : BDT, « *manuel sur le développement des communications mobiles* », ITU, 1997
- [5] : P. CLERC, P. XAVIER, « *Principes fondamentaux des télécommunications* », 1998, Ellipses

DOCUMENTS CONSULTÉS SUR INTERNET

- [6] : <http://www.w3.org/Protocols/>
- [7] : <http://www.gsmworld.com>
- [8] : <http://www.etsi.org>
- [9] : <http://www.art-telecom.fr/>
- [10] : <http://www.europe.alcatel.fr/telecom/ssd/keytech/nss/gprs.htm>
- [11] : <http://www.cellular-news.com/gprs/>
- [12] : <http://membres.lycos.fr/pensarguet/WAP/GPRS.htm>
- [13] : <http://www.gsmworld.com/technology/gprs>
- [14] : <http://www.chez.com/csysteme/concept.htm>
- [15] : <http://memoireonline.free.fr/thierrydanseUMTS.htm>
- [16] : http://www.umts-forum.org/what_is_umts.html

- [17] : Wireless Application Environment Overview, Version 1999-11-04
[http://www.wapforum.org/what/technical.htm/ SPEC-WAEOverview-19991104.pdf](http://www.wapforum.org/what/technical.htm/SPEC-WAEOverview-19991104.pdf)
- [18] : Wireless Application Environment Specification, Version 1999-11-04
[http://www.wapforum.org/what/technical.htm/ SPEC-WAESpec-19991104.pdf](http://www.wapforum.org/what/technical.htm/SPEC-WAESpec-19991104.pdf)
- [19] : <http://www.wapforum.org/new/wap2.0.pdf>
- [20] : <http://www.iab.org/IAB-wireless-workshop/talks/iab-wap-1.pdf>
- [21] : <http://www.knowledgeisland.com/inet/wap/wap1.php>
- [22] : Wireless Session Protocol Specification, Version 1999-11-08
[http://www.wapforum.org/what/technical.htm/ SPEC-WSP-19991105.pdf](http://www.wapforum.org/what/technical.htm/SPEC-WSP-19991105.pdf)
- [23] : Wireless Transaction Protocol Specification, Version 1999-06-11
[http://www.wapforum.org/what/technical.htm/ SPEC-WTP-19990611.pdf](http://www.wapforum.org/what/technical.htm/SPEC-WTP-19990611.pdf)
- [24] : Wireless Datagram Protocol Specification, Version 1999-11-05
[http://www.wapforum.org/what/technical.htm/ SPEC-WDP-19991105.pdf](http://www.wapforum.org/what/technical.htm/SPEC-WDP-19991105.pdf)
- [25] : http://www.entrust.com/resources/pdf/understanding_wtls.pdf
- [26] : WTLS, Version 2001-04-06, [http://www.wmlclub.com/docs/especwap2.0/ WAP-261-WTLS-20010406-a.pdf](http://www.wmlclub.com/docs/especwap2.0/WAP-261-WTLS-20010406-a.pdf)
- [27] : http://www.wapforum.org/what/technical_1_2_1.htm
- [28] : <http://www.wapforum.org/tech/documents/WAP-199-WTLS-20000218-a.pdf>, Février 2000
- [29] : <http://www.wapforum.org/tech/documents/WAP-187-TransportE2ESec-20000711-a.pdf>,
Juillet 2000
- [30] : <http://www.sowap.com/wap-faq.html>

- [31] : <http://www.itpolicy.gov.il/topics/docs/wap.pdf>
- [32] : <http://www.nokia.com/corporate/wap/pdf/NMB3.0DSFinal.pdf>
- [33] : http://www.sorabol.ac.kr/~hspark/wap_1.htm
- [34] : http://www.medialabeurope.org/people/k-wrona/pub/mskw_iwttec99.pdf
- [35] : Wireless Application Protocol Architecture Specification,
<http://www.wapforum.org/what/technical.htm/SPEC-WAPArch-19980430.pdf>, Avril 1998
- [36] : WAP Forum, <http://www.wapforum.org/what/technical.htm>, November 2000.
- [37] : <http://www.wapgateway.org>
- [38] : WML Specification
<http://www.wapforum.org/what/technical.htm/SPEC-WML-19991104.pdf>, Novembre 1999
- [39] : <http://www.multimania.com/pensarguet/WAP-WML.htm>
- [40] : WMLScript Language Specification
<http://www.wapforum.org/what/technical.htm/SPEC-WMLScript-19991104.pdf>, Novembre 1999
- [41] : WAP Forum, Wireless Markup Language Specification,
<http://www.wapforum.org/tech/documents/WAP-191-WML-20000219-a.pdf>, Février 2000
- [42] : WMLScript Crypto API Library,
<http://www.wapforum.org/what/technical.htm/SPEC-WMLScriptCrypto-19991105.pdf>,
November 1999
- [43] : WMLScript Standard Libraries Specification,
<http://www.wapforum.org/what/technical.htm/SPEC-WMLScriptLibs-19991104.pdf>, Novembre
1999

[44] : WMLScript Statement if Intent,

<http://www.wapforum.org/what/technical.htm/SPEC-WMLScriptIntent-19980430.pdf>, Avril 1998

[45] : Wireless Control Message Protocol Specification,

<http://www.wapforum.org/what/technical.htm/SPEC-WCMP-19990804.pdf>, Août 1999

[46] : WDP/WCMP Wireless Data Gateway Adaption ,

<http://www.wapforum.org/what/technical.htm/SPEC-WDPWCMPAdapt-19991105.pdf>,
Novembre 1999

[47] : Push Access Protocol Specification,

<http://www.wapforum.org/what/technical.htm/SPEC-PAP-19991108.pdf>, Novembre 1999

[48] : Push Message Specification,

<http://www.wapforum.org/what/technical.htm/SPEC-PushMessage-19990816.pdf>, Août 1999

[49] : Push OTA Protocol Specification,

<http://www.wapforum.org/what/technical.htm/SPEC-PushOTA-19991108.pdf>, Novembre 1999

[50] : Push Architectural Overview,

<http://www.wapforum.org/what/technical.htm/SPEC-PushArchOverview-19991108.pdf>,
Novembre 1999

Nom : RASATAMANANA

Prénoms : Rado Nomeny

Adresse de l’auteur : Lot IVI 17 A Andravoahangy Tana 101

Titre : **WIRELESS APPLICATION PROTOCOL ET
SON APPLICATION AVEC SIMPLE MESSAGERIE**

Nombre de pages : 122

Nombre de tableaux : 08

Nombre de figures : 38

Mots clés : WAP, Internet, Intranet, Systèmes de téléphonie mobile

Directeur de mémoire : Monsieur RANDRIARIJONA Lucien Elineo

Résumé

Ce mémoire présente différents supports du service WAP et des techniques d'architecture pour l'acheminement des données multimédias entre le monde des réseaux téléphoniques sans fil et le monde des réseaux IP allant de l'Intranet vers l'Internet. En outre, il donne un exemple d'application illustrant l'intérêt de la technologie WAP qui permet, non seulement d'accéder aux sites Web ou aux services statiques de consultation, mais surtout aux applications et aux données.

En fait, cet ouvrage est fait pour faciliter la création rapide et sans investissement important des services WAP au niveau de l'entreprise sur la base du système informatique existant. Ainsi, les utilisateurs pourront, sans aucune contrainte géographique ou temporelle, passer des commandes, consulter les e-mail, connaître des résultats sportifs , ...

Summary

This memoir presents different supports of WAP services and some architecture techniques to dispatch multimedia data between wireless phone Network area and IP one from Intranet to Internet. Besides, there is an example illustrating the advantage of WAP technology which permits, not only access to Web sites or to consulting static services, but above all applications and data.

This work then facilitates the rapid creation of WAP services without important investment, concerning existing computered system basis in a company. Thus, users can order, read e-mails, know sports results, etc ... without any place and time constraints.