IN/003-10/02

Université Abou Bekr Belkaid — جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

جامعة أبي بكر بلقايد - تلمسان
المكتبة
كلية العلوم

Mémoire de fin d'études

Pour l'obtention du diplôme d'Ingénieur d'État en Informatique

Option : *Système d'information avancé*

Thème

Etude de la qualité de service (QoS) dans les réseaux 802.11

Réalisé par :

- *M. BENDIMERAD Fayçal*
- *M. MEBAREK Farid*

Présenté le 27 Septembre 2011 devant le jury composé de MM.

- *M. Benaissa M.* — ***Président***
- *M. Benamar A.* — ***Examinateur***
- *M.Benmaamar B.* — ***Examinateur***
- *M^me^ Didi Fedoua.* — ***Encadreur***

Année universitaire : *2010-2011*

Inscrit Sous le N°: .....
Date le: 02 OCT. 2011
Code: 5670

Remerciements

Notamment nos remerciements vont en faveur de notre encadreur Madame *DIDI Fedoua* pour son aide, son assistance et son encouragement tout au long de ce travail, nous lui sont vraiment reconnaissant pour sa compréhension qu'elle a crée autour de nous afin qu'on soit autonome tout au long de ce travail.

Que Monsieur *BENAISSA M.*, veuille croire à ma profonde reconnaissance pour avoir accepté de présider ce jury et plus particulièrement d'avoir été un enseignant exemplaire tout au long de mon cursus universitaire.

Que les honorables membres du jury, Monsieur *BENAMAR A* et Monsieur *BENMAAMAR B.* veuillent croire en mes remerciements anticipés pour avoir bien voulu accepter d'enrichir et de faire évoluer ce travail.

Nous tenons à remercier également toute les enseignants de l'université Abou Bekr Belkaid qui nous ont encadrés tout au long de notre cursus universitaires.

Une dernier pensée à toute personne ayant contribué de prés ou de loin à la réalisation de ce travaille.

جامعة ابي بكر بلقايد - تلمسان
المكتبة
كلية العلوم

Bibliothèque science
BFS13670

Dédicaces

A mes très chers parents. J'espère qu'ils trouveront dans ce travail le témoignage de ma reconnaissance éternelle.

A ma sœur Amina et mes frères Moumen et Nassim qui m'ont toujours soutenue et encouragé.

A mes oncles, mes tentes, à toutes mes cousins et mes cousines qui ont tous contribué par leur encouragement de ce travail.

A mes proches ami(e)s, avec lesquelles j'ai partagé tant de bons moments,
A mon binôme Farid.

A tous mes enseignants pour le savoir acquis.

A tous ceux que j'aime et qui m'aiment,
Je dédie ce travail.

B. Fayssal

Dédicaces

Je dédie ce modeste travail en premier lieu à mes chère parents, en reconnaissance de leurs soutien dans mes études dés mon jeune âge.

A mes deux familles.

A mes chère frères : Mourad, Kamel et Oussama.

A l'ensemble de mes oncles et de mes tantes spécialement à :Hassane,Mohamed,Omar et à tous les membres de ma famille .qui ont tous contribué par leurs encouragements ce travail.

A mes proches
amis :Mohammed,Zaki,Smail,Mohamed et à tous mes autres amis .
A mon binôme Fayssal

A toute la promotion 5ème année ingénieur Informatique.

Ma dédicace est également pour tous les amis des autres promotions.

Résumé

Notre objectif est d'améliorer la performance d'un réseau sans fil infrastructurel à multi-station en essayant d'avoir une meilleure qualité de service en contrôlant le délai de bout en bout, la latence des flux et de réduire les pertes de paquet.

En outre, nous appliquerons le mode MPDU (Mac Protocol Data Unit) qui est un protocole d'accès au medium utilisé dans la norme IEEE 802.11n qui permet d'appliquer une différenciation de services sur les réseaux sans fil afin d'avoir une certaine QoS dans le réseau.

Dans ce travail, nous avons étudié à travers la simulation un mécanisme proposé par le RFC 802.11e.

Mots clés: IEEE 802.11e, QoS, Wi-Fi.

Abstract

Our objective is to improve the performance of a network infrastructure to multi-stations, trying to get a better quality of service for controlling the start time to finish time, the latency of flows and more reduce losses.

In addition, we will apply the method MPDU (MAC Protocol Data Unit) which is a medium access protocol used in IEEE 802.11n, which is used to apply a service differentiation in Wireless networks in order to have some QoS in the network.

In this work, we proposed a solution to improve QoS in networks 802.11.

Keywords: IEEE 802.11e, QoS, Wi-Fi

Table des matières

Liste des figures

Liste des tableaux

Acronymes

A	
AC:	Access Category
ACK:	ACKnowledgement
AES:	Advanced Encryption Standard
AF:	Assured Forwarding
AIFS:	Arbitration Inter-Frame Spacing
AIFSN:	Arbitration Inter-Frame Spacing Number
AP:	Access Point
ART :	Autorité de Régulation des Télécommunications
ARQ:	Automatic Repeat reQuest
B	
BA:	Behavior Aggregate
BE:	Best Effort
BK:	Background
BLR:	Boucle Locale Radio
BS:	Base Station
BSA:	Basic Service Area
BSS:	Basic Service Set
BSSID:	Basic Service Set IDentifier
C	
CBQ:	Class Based Queuing
CBR:	Constant Bit Rate
CCA:	Clear Channel Assessment
CFP:	Contention-free period
CL:	Controlled load
CP:	Contention période
CRC:	Cyclic Redundancy Check
CSMA/CA:	Carrier sense multiple access with collision voidance
CTS:	Clear to Send
CW:	Collision Windows
D	
DECT:	Digital Enhanced Cordless Telecommunication
DCF:	Distributed Coordination Function
DIFS:	DCF Interframe Space
DiffServ:	Differenciated Service (services différenciés)

DLP:	Direct Link Protocol
DS:	Distribution System
DSCP:	Differentiated Services Code Point
DSDV:	Destination Sequenced Distance Vector
DSSS:	Direct Sequence Spread Spectrum
E	
EDCA:	Enhanced Distribution Channel Access
EDCF:	Enhanced Distribution Coordination Function
EF:	Expedited Forwarding
ESS:	Extended Service System
ESSID:	Extented Service Set Identifier
ETSI:	European Telecommunications Standards Institute
F	
FCC:	Federal Communication Commission pour les Etats-Unis,
FHSS:	Frequency Hopping Spread Spectrum
FQMM:	Flexible QoS Model for MANETs
FTP:	File Transfer Protocol
G	
GSM:	Global System for Mobile Communication
GPRS:	General Packet Radio Service
GS:	Guaranteed Service
H	
HC:	Hybrid Coordinator
HCCA:	Hybrid Coordination Channel Access
HCF:	Hybrid Coordination Function
HiperLAN1:	High Performance Radio LAN 1.0
hiperLAN2:	High Performance Radio LAN 2.0
HomeRF:	Home Radio Frequency
HR:	High Rate
I	
IBSS:	Independent Basic Service Set
ID:	IDentification
IEEE:	Institute of Electrical and Electronics Engineers
IETF:	Internet Engineering Task Force
IFS:	Inter Frame Spacing
IntServ:	Integrated Service (services intégrés)
IR:	Infrarouge

irDA:	Infrared data association
ISM:	Industrial Scientific Medical
ISO:	International Standardisations Organization
ITU:	International Telecommunication Union
L	
LAN:	Local Area Network
LLC:	Logical Link Control
LOS:	Line Of Sight
LSAP:	Logical Service Access Point
M	
MAC:	Medium Access Control
MPDU:	Mac Protocol Data Unit
MPEG:	Moving Pictures Experts Group
MSDU:	Mac Service Data Unit
N	
NACK:	Negative ACKnowledgement
NAV:	Network Allocation Vector
NIC:	Network Interface Controller
NLOS:	Non Line Of Sight
NS:	Network Simulator
O	
OFDM:	Orthogonal Frequency Division Multiplexing
OSI:	Open System Interconnection
P	
PCF:	Point Coordination Function
PCS:	Physical Carrier Sense
PDA:	Personal Digital Assistant
PF:	Persistence Factor
PHB:	Per-Hop Behavior
PHY:	PHYsical layer
PIFS:	PCF Interframe Space
PLCP:	Physical Layer Convergence Protocol
PMD:	Physical Medium Dependent
Q	
QoS:	Quality of Service
QSTA:	Quality enhanced STAtion
R	

RSVP:	Resource ReSerVation Protocol
RTS:	Request To Send
S	
SFD:	Start Frame Delimiter
SIFS:	Short Inter Frame Space
SSID:	Service Set Identifier
STA:	Station
SW-ARQ:	Stop and Wait-Automatic Repeat Request
T	
TC:	Traffic Category
TDMA:	Time Division Multiple Access
TOS:	Type of Service
TXOP:	Transmission Opportunity
U	
UMTS:	Universal Mobile Telecommunications System
U-NII:	Unlicensed-National Information Infrastructure
UIT:	Union Internationale des télécoms
UP:	User Priority
V	
VCS:	Virtual Carrier Sense
VoIP:	Voice over IP
W	
WECA:	Wireless Ethernet Compatibility Alliance
WEP:	Wired Equivalent Privacy
WiFi:	Wireless Fidelity
WiMAX:	Worldwide Interoperability for Microwave Access
WLAN:	Wireless Local Area Network
WMAN:	Wireless Metropolitan Area Network
WPA:	Wifi Protected Access
WPAN:	Wireless Personal Area Network
WWAN:	Wireless Wide Area Network

Introduction Générale

L'informatique connaît une évolution cruciale qui a donné naissance à beaucoup de nouvelles applications comme son introduction dans l'enseignement pour développer les compétences nécessaires à l'utilisation des nouvelles technologies de l'information et de la communication. L'informatique s'est banalisée l'ordinateur s'accapare nos bureaux, modifie nos modes de travail, envahit nos maisons, s'intègre dans les objets les plus quotidiens et nous propose des loisirs inédits. Il est même à l'origine de nouveaux modes de sociabilité et d'une nouvelle économie l'informatique est partout !

L'explosion des réseaux et notamment de l'Internet, a favorisé l'émergence de nouveaux moyens de transport de l'information, comme la transmission hertzienne. Au vue de leurs avantages, de plus en plus populaires la disparition des câblages et la facilité d'installation dans les bâtiments, plusieurs normes ont été définies pour l'élaboration de réseaux sans fil, les plus connus du grand public sont le Wifi (IEEE 802.11), le DECT et le Bluetooth (IEEE 802.15).

La norme la plus utilisée dans le déploiement des réseaux locaux sans fil est sans conteste le 802.11. Cette norme se base sur les structures logique et physique de réseau Ethernet mais est confrontée à ses lacunes en matières de Qualité de Service (QOS), c'est pourquoi il a fallu mettre en place des mécanismes permettant de supporter des applications spécifiques telles le multimédia ou la téléphonie sur IP qui, contrairement à la DATA, nécessite des délais de transmission constant (gigue faible) et relativement court, phénomènes auxquels la transmission audio et vidéo sont très sensibles.

L'**IEEE** (Institute of Electrical and Electronic Engineers) lança le premier standard pour réseaux locaux sans-fil 802.11 depuis 1997. Le besoin de la qualité de service dans le WiFi a permis la création de la norme 802.11e qui utilise plusieurs mécanismes parmi eux **EDCA** (Enhanced Distributed Channel Access) et **HCCA** (Hybrid Controlled Channel Access).

Jusqu'en 2005, les trames WiFi avaient toutes le même niveau de priorité quelque soit la station émettrice et donc quelques soit le type de trafic, mais de nouveaux mécanismes de QoS ont été introduits depuis. Dans ce PFE, nous nous intéressons plus particulièrement au Bloc d'Acquittement (**BA**). Le Block Ack a été

initialement défini par l'IEEE 802.11e et 802.11n comme un paramètre facultatif pour améliorer l'efficacité de la couche d'accès MAC. Son fonctionnement, au lieu de transmettre un seul Ack pour chaque MPDU, plusieurs MPDU peuvent recevoir un seul Ack par l'intermédiaire d'une trame BlockAck (BA).

Ce travail est composé de trois chapitres intitulés comme suit nous avons commencé dans le premier chapitre par présenter quelques points essentiels relatifs à la norme IEEE 802.11. Ensuite, nous approfondissons les méthodes d'accès proposées par l'IEEE 802.11 pour les transmissions avec support de la qualité de service (QoS) dans le deuxième chapitre. Le dernier chapitre est consacré à l'évaluation des résultats de simulation, relative au gain en termes d'amélioration des performances globales du réseau et des paramètres de QOS des différents flux, quant on active le mécanisme du Bloc Ack. Nous avons essayé aussi d'améliorer le mécanisme en proposant une approche qui essaye de mieux exploiter le média en accordant aux trafics best effort une meilleure priorité d'accès en l'absence des trafics multimédia.

Chapitre 1 Les réseaux sans fil et les réseaux 802.11 Wifi

La mobilité des utilisateurs et leur besoin d'accès itinérant aux réseaux informatiques rendent les réseaux traditionnels (filaires) obsolètes. De plus, le besoin accru d'accéder à différents types d'applications multimédia via le support radio pousse la recherche à trouver de nouvelles solutions de plus en plus adaptées à cet environnement. Ainsi, la standardisation de nombreuses technologies sans fil allant des réseaux personnels à faible couverture jusqu'aux réseaux à couverture mondiale.

Un nouveau type de réseau local (**LAN** *Local Area Network*) est apparu depuis quelques années, les réseaux locaux sans fil **(WLAN** *Wireless LAN*). Ils proposent une alternative aux LANs traditionnels à base de paire torsadée, câble coaxial ou fibre optique. Les réseaux sans fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. WLAN est un système de transmission de donnée conçu pour assurer une liaison indépendante de l'emplacement des périphériques informatiques qui composent le réseau et utilisant les ondes radio plutôt qu'une infrastructure câblée.

Dans ce chapitre, nous décrivons les différentes catégories des réseaux sans fil allant des réseaux personnels jusqu'aux réseaux étendus en passant par les réseaux locaux et les réseaux métropolitains, nous nous intéressons ensuite à la norme IEEE 802.11, nommé également pour raison commerciale Wi-Fi pour Wireless Fidelity.

I. Les réseaux sans fil

Un réseau sans fil est un réseau dans lequel au moins deux terminaux sont capables de communiquer entre eux sur une liaison utilisant des signaux radioélectriques (radio et infrarouge). Ces réseaux dits aussi Wireless, sont de plusieurs sortes WiFi (Wireless Fidelity), Bluetooth, BLR (Boucle Locale Radio), UMTS (Universal Mobile Telecommunications System). Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions.

I.1. Catégories des réseaux sans fil

Les réseaux sans fil sont classés en quatre catégories selon leur étendue géographique et normalisés par un certain nombre d'organismes parmi lesquels nous citerons l'ISO (International Standardisations Organization), l'IEEE (Institute of Electrical and Electronics Engineers) et l'ETSI (European Telecommunications Standards Institute). Nous distinguons

- Réseaux personnels sans fil (WPAN) ex Bluetooth (IEEE 802.15.1), HomeRF.
- Réseaux locaux sans fil (WLAN) ex Wifi (IEEE 802.11), HiperLAN.
- Réseaux métropolitain sans fil (WMAN) ex BLR (IEEE 802.16), WiMax.
- Réseaux étendus sans fil (WWAN) ex GSM, GPRS, UMTS.

Ces réseaux sans fil WPAN, WLAN, WMAN et WWAN peuvent atteindre des débits de plusieurs mégabits/s, voire de plusieurs dizaines de mégabits/s.

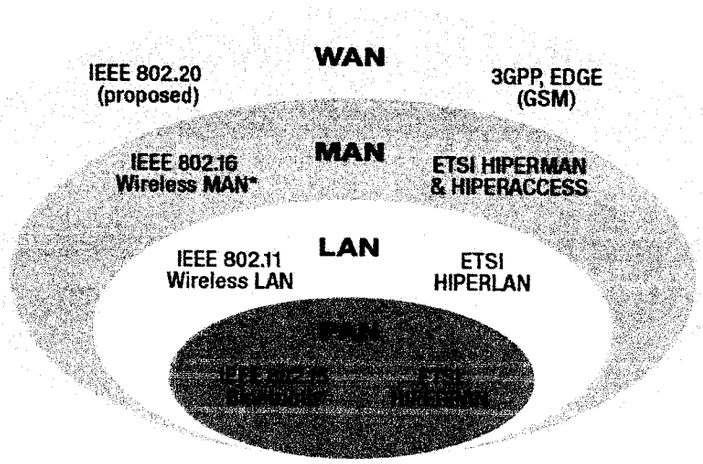


Figure 1.1. Classification des réseaux sans fil

I.1.1. Réseaux personnels sans fil (WPAN)

Le réseau personnel sans fil ou le réseau individuel sans fil **WPAN** (*Wireless Personal Area Network*) concerne les réseaux sans fil d'une faible portée, de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou

bien à permettre la liaison sans fil entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN

- **La technologie Bluetooth (IEEE 802.15.1)** lancée par Ericsson en 1994, proposant un débit théorique de 1Mbps pour une portée maximale d'une trentaine de mètres. Bluetooth possède l'avantage d'être très peu gourmand en énergie, ce qui le rend particulièrement adapté à une utilisation au sein de petits périphériques. [15]

- **HomeRF (*Home Radio Frequency*)** lancée en 1998 par le HomeRF Working Group (formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft) propose un débit théorique de 10Mbps avec une portée d'environ 50 à 100 mètres sans amplificateur. [15]

- **La technologie ZigBee (IEEE 802.15.4)** permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégré dans de petits appareils électroniques (appareils électroménagers, hifi, jouets, ...). [15]

- **Les liaisons infrarouges** permettent de créer des liaisons sans fil de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde. Cette technologie est largement utilisée pour la domotique (télécommandes) mais souffre toutefois des perturbations dues aux interférences lumineuses. L'association **irDA** (infrared data association) formée en 1995 regroupe plus de 150 membres. [15]

I.1.2. Réseaux locaux sans fil (WLAN)

Le réseau local sans fil **WLAN** (*Wireless Local Area Network*) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes

- **WiFi (IEEE 802.11)** soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres. [3]
- **HiperLAN1 (High Performance Radio LAN 1.0)** est un standard de l'ETSI (European Telecommunications Standards Institute). Elle utilise la bande de fréquence 5.15 – 5.30 GHZ et pouvant atteindre des débits de 23.5 mégabits par seconde sur une distance d'environ 50 mètres. [3]
- **HiperLAN2 (High Performance Radio LAN 2.0)** norme européenne élaborée par l'ETSI, permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 MHz. [3]
- **DECT (Digital Enhanced Cordless Telecommunication)** norme des téléphones sans fil domestiques. *ALCATEL* et *ASCOM* développent pour les environnements industriels, telles les centrales nucléaires, une solution basée sur cette norme qui limite les interférences. [3]

I.1.3. Réseaux métropolitains sans fil (WMAN)

Le réseau métropolitain sans fil (WMAN pour *Wireless Metropolitan Area Network*) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication.

La norme de réseau métropolitain sans fil la plus connue est le **WiMAX**, permettant d'obtenir des débits de l'ordre de 70 Mbit/s sur un rayon de 50 kilomètres. Le standard WiMax possède l'avantage de permettre une

connexion sans fil entre une station de base **BTS** (*Base Transceiver Station*) et des milliers d'abonnés sans nécessiter de ligne visuelle directe **LOS** (Line Of Sight) ou **NLOS** (Non Line Of Sight). Dans la réalité le **WiMAX** ne permet de franchir que de petits obstacles tels que des arbres ou une maison mais ne peut en aucun cas traverser les collines ou les immeubles. [16]

I.1.4. Réseaux étendus sans fil (WWAN)

Le réseau étendu sans fil (WWAN pour *Wireless Wide Area Network*) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connecté à un réseau étendu sans fil. Les principales technologies sont les suivantes

- GSM (*Global System for Mobile Communication* ou Groupe Spécial Mobile)
- GPRS (*General Packet Radio Service*)
- UMTS (*Universal Mobile Telecommunication System*)

I.2. Les bande de fréquences

Les bandes utilisées dans les réseaux sans fil et notamment dans l'IEEE 802.11 sont dites sans License. La bande de 2.4 GHz est la bande utilisée par le standard d'origine ainsi que pour les amendements IEEE 802.11b et 802.11g. La bande de 5GHz est réservé à l'amendement IEEE 802.11a.

Comme les Etats-Unis libère trois bandes de fréquence à destination pour l'industrie, la Science et la Médecine. Ces bandes de fréquence sont les bandes *902-928 MHz*, *2.400-2.4835 GHz*, *5.725-5.850 GHz*. En Europe la bande s'étalant de *890 à 915 MHz* est utilisée pour les communications mobiles, ainsi seules les bandes *2.400 à 2.4835 GHz* et *5.725 à 5.850 GHz* sont disponibles pour une utilisation radioamateur. Deux groupes sont représentés

- Les technologies pour les téléphones portables (de 824 à 2170 MHz).
- Les technologies utilisées pour l'informatique, pour les WPAN et WLAN, fonctionnent sur la bande **ISM** (Industrial Scientific Medical) de 2400 à 2500 MHz, la bande **U-NII** (Unlicensed-National Information Infrastructure) de 5150 à 5720 MHz. [14]

I.2.1. Bande ISM

La bande ISM est une bande de fréquence qui n'est pas soumise à des réglementations nationales et qui peuvent être utilisées librement pour des applications industrielles, scientifiques et médicales. Sa situation n'est pas uniformément réglée dans le monde. Il y a par exemple trois bandes ISM (902 - 928 MHz ; 2 400 - 2 483,5 MHz et 5 800 MHz), mais seule la bande des 2,4 GHz avec une bande passante de 83.5 MHz, est utilisé par la norme 802.11.

La largeur de bande ISM est variable suivant les pays, de même que la puissance utilisable. Par ailleurs la sous-bande 2.400-2.4835 GHz, est fortement utilisée par différents standards et perturbée par des appareils (four à micro-onde, clavier et souris sans fil…) fonctionnant dans ces fréquences. [17]

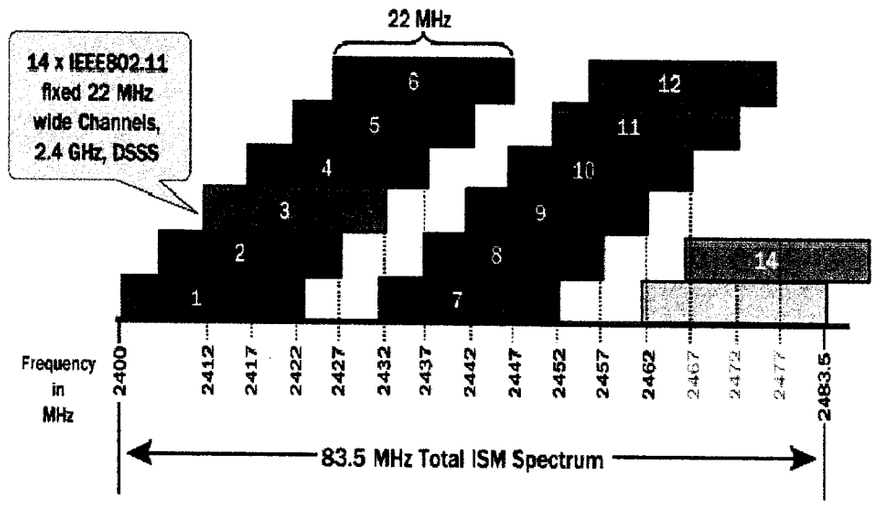


Figure 1.2. Représentation graphique des canaux de transmission dans la bande ISM (2,4GHz)

I.2.2. Bande U-NII

La bande U-NII (Unlicensed National Information Infrastructure) 5.15-5.35 GHz, 5.725-5.825 GHz offre une bande passante totale de 300MHz, chacune utilisant une puissance de signal différente. Fait partie du spectre des fréquences radio utilisées par IEEE 802.11a, appareils et par de nombreux fournisseurs de services Internet sans fil. Il fonctionne sur trois gammes

- U-NII faible (U-NII-1) 5.15-5.25 GHz. La réglementation exige l'utilisation d'une antenne intégrée. Puissance limitée à 40 mW.
- U-NII Mid (U-NII-2) 5.25-5.35 GHz. Le règlement permet à un utilisateur d'installé une antenne. Puissance limitée à 250 mW.
- U-NII dans le monde de 5.47 à 5.725 GHz. Les deux intérieurs et une utilisation en extérieur. Puissance limitée à 250 mW.
- U-NII supérieur (U-NII-3) 5,725 à 5,825 GHz. Parfois appelé *U-NII / ISM* en raison du chevauchement avec la bande ISM. Le règlement permettre une antenne installée par l'utilisateur. Puissance limitée à 1 W. [17]

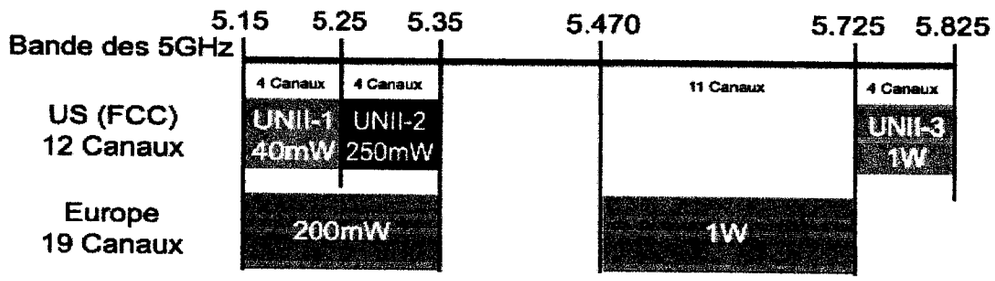


Figure 1.3. La bande U-NII

I.3. Les organismes de réglementation

Ces bandes sont reconnues par les organismes de réglementations internationaux pour une utilisation sans licence. Ces organismes sont

FCC Federal Communication Commission pour les Etats-Unis,

ETSI European Telecommunications Standards Institute pour l'Europe,

MKK Kensa-kentei Kyokai pour le Japon,

ART Autorité de Régulation des Télécommunications pour la France. [11]

I.3.1. Les organismes de normalisation

Deux organismes s'occupent de la standardisation des réseaux sans fil WLAN

ETSI En Europe, le groupe HiperLan (High Performance Radio LAN) issu de l'ETSI définit deux standards, HiperLan 1 offrant un débit de 10 et 20 Mbit/s et HiperLan 2 offrant un débit de 54 Mbit/s.

IEEE Au Etats-Unis, c'est le comité 802 (dénommé ainsi par sa date de création -Février 1980-) issu de l'IEEE qui a définit le standard IEEE 802.11 et ses extensions (802.11a, 802.11b, ...).

Ces deux standard sont incompatibles, de plus HiperLan utilise uniquement la bande U-NII tandis 802.11 utilise les bandes ISM et U-NII. Actuellement seuls des produits issus de la norme 802.11 sont commercialisés.

WECA Le terme WiFi est une norme délivrée par la WECA aux produits 802.11b. Cette dernière, composée de 140 entreprises, teste et gère l'interopérabilité entre les équipements répondant à la norme 802.11b. Dernièrement le terme Wifi 5 certifie la norme 802.11a.

I.4. Sécurité

Les réseaux sans fil rencontrent aujourd'hui un succès important car ils permettent via la norme IEEE 802.11b et n, de déployer des moyens de transmissions sans contrainte d'immobilité liée aux câblages et aux prises. Le point crucial lors d'une installation réseau sans fil, est la mise en place d'éléments de protection. La sécurité a toujours été le point faible des réseaux WiFi, à cause principalement de sa nature physique. De nouvelles parades de sécurité sont en cours de normalisation et seront utilisables, pour l'instant le meilleur moyen de sécurisation est d'utiliser les mêmes mécanismes de protection que les réseaux filaires. De nombreuses évolutions protocolaires ont rythmé la sécurité des réseaux sans fil. Cependant, une solution vient d'être apportée à cette faille de sécurité, par l'utilisation du protocole d'identification par serveur d'authentification 802.1x, une solution plus robuste est apportée par la norme IEEE 802.1X. Le standard IEEE 802.1X est utilisable en environnement sans fil comme en environnement filaire. [19]

I.5. Avantages des réseaux sans fil

- **Facilité et souplesse** les réseaux à technologie sans fil d'un point de vue esthétique résident dans le fait que l'on n'a plus besoin de relier physiquement les équipements par câble, ce qui permet aux nombreux utilisateurs de s'affranchir des longs câbles encombrants.

- **Vitesse et simplicité d'installation** installation d'un système de réseau local sans fil peut être rapide et facile et peut éliminer la nécessité de tirer le câble à travers les murs et les plafonds.
- **Coût** si leur installation est parfois un peu plus couteuse qu'un réseau filaire, les réseaux sans fil ont des coûts de maintenance très réduits.
- **Evolutivité** les réseaux sans fil peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins. [18]

I.6. Inconvénients des réseaux sans fil

Malgré leurs nombreux avantages, les réseaux sans fil posent des problèmes. Les principaux dangers sont les suivants

- **L'écoute clandestine des données transmises** elle peut conduire à la révélation d'information confidentielles ou de certificats utilisateur non protégés, est un risque d'usurpation d'identité.
- **L'interception et la modification des données transmises** si un pirate parvient à accéder au réseau, il ou elle peut y adjoindre un ordinateur malveillant pour intercepter, modifier et transmettre les communications entre deux utilisateurs autorisés.
- **L'usurpation** l'accès permanent au réseau permet à un utilisateur malveillant d'envoyer des données semblant émaner d'un utilisateur autorisé par le biais de procédés normalement depuis l'extérieur du réseau.

Le refus de service l'utilisateur malveillant dispose ici de toute une palette de possibilité. Les perturbations du signal radio peuvent être obtenues à l'aide d'un dispositif aussi simple qu'un four à micro-onde et les interférences provenant d'autres appareils sans fil, tels que les téléphones sans fil. [18]

II. Le WIFI

II.1. Introduction

Le Wi-Fi (Wireless Fidelity) représente un label défini par la WECA (Alliance permettant la Compatibilité Ethernet du matériel Wireless), mais il est utilisé comme un nom commun représentant les liaisons sans fil dans le monde informatique.

Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA), des objets communicants ou même des périphériques à une liaison haut débit de 11 Mbit/s théoriques ou 6 Mbit/s réels en 802.11b à 54 Mbit/s théoriques ou environ 25 Mbit/s réels en 802.11a ou 802.11g et 600 Mbit/s théoriques pour le 802.11n, sur un rayon entre une vingtaine et une cinquantaine de mètres en intérieur.

Le standard IEEE 802.11 est un système de transmission de données assurant la liaison entre les périphériques par les ondes radio plutôt que par un réseau filaire. L'IEEE a ratifié la spécification 802.11, norme régissant les WLANs, en 1997. Le standard 802.11 définit les deux premières couches inférieures du modèle OSI (Open System Interconnection), la couche physique et la couche de liaison de données. [20]

II.2. Définition

Le **Wi-Fi** est une technologie de réseau informatique sans fil mise en place pour fonctionner en réseau interne et, depuis, devenue un moyen d'accès à haut débit à Internet. Il est basé sur la norme IEEE 802.11 (ISO/IEC 8802-11). Cette norme IEEE 802.11 est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le nom *wifi* correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, anciennement WECA (*Wireless Ethernet Compatibility Alliance*), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau wifi est en réalité un réseau répondant à la norme 802.11. [14]

Figure 1.4. Logo de Wi-Fi

II.3. Les équipements WiFi

Il existe différents types d'équipement pour la mise en place d'un réseau sans fil

II.3.1. Les adaptateurs sans fil ou cartes d'accès

En anglais **wireless adapters** ou **network interface controller** (NIC). Il s'agit d'une carte réseau à la norme 802.11 permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs WiFi sont disponibles dans de nombreux formats (carte PCI, carte PCMCIA, adaptateur USB, carte compactflash, ...). On appelle station tout équipement possédant une telle carte. A noter que les composants Wi-Fi deviennent des standards sur les portables (label Centrino d'Intel). [4]

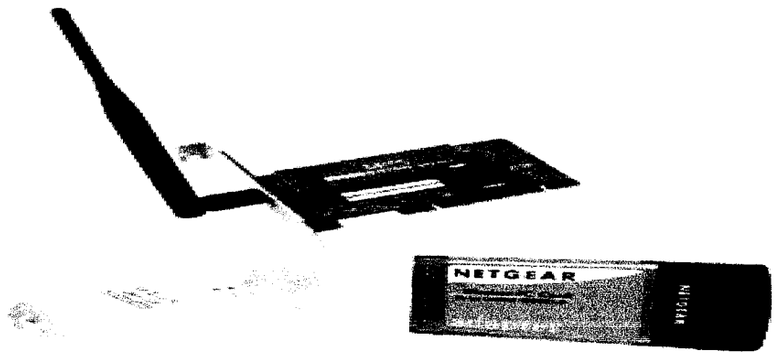


Figure 1.5. Les adaptateurs sans fil ou carte d'accès

II.3.2. Les points d'accès

Notés AP pour *Access point*, parfois appelés bornes sans fil, permettant de donner un accès au réseau filaire (auquel il est raccordé) aux différentes stations avoisinantes équipées de cartes WiFi. Cette sorte de hub est l'élément nécessaire pour déployer un réseau centralisé en mode infrastructure. Certains modèles proposent des fonctions de modem ADSL et comprennent plus ou moins de fonctions comme un pare-feu. [4]

Figure 1.6. Les points d'accès

II.3.3. Les autres

- **Smart Display** écrans mobiles, soutenus par Microsoft.
- **Rétroprojecteurs** pour des présentations avec portables mobiles.
- **Chaînes WiFi** offrant la capacité de lire les MP3 directement sur le disque dur d'un ordinateur grâce à l'interface Ethernet sans fil intégrée.
- **Assistant personnel** les PDA intégrant le WiFi est parfois plus avantageux qu'un portable pour lire ses mails, importer des documents voir surfer sur le net.
- **Caméra vidéo** transmettre des images à distance à l'ordinateur qui les enregistre.

Les composants Wi-Fi ne sont pas plus onéreux que ceux des réseaux filaires, bientôt toutes les plates-formes seront vendues avec des modules Wi-Fi intégrés. C'est déjà le cas dans le monde des PC portables, sous l'impulsion d'Intel, qui fait sa révolution sans fil grâce au Centrino. [4]

II.4. Les modes opératoires

La norme 802.11 considère deux types d'équipements, une station sans fil et un point d'accès, qui joue le rôle de pont entre le réseau filaire et le réseau sans fil. Ce point d'accès se comporte habituellement d'un émetteur/récepteur radio, d'une carte réseau filaire et d'un logiciel de pontage conforme au standard 802.1d. Le point d'accès se comporte comme la station de base du réseau sans fil, agrégeant l'accès de multiples stations sans fil sur le réseau filaire. Les stations sans fil comprennent des cartes d'accès 802.11 ou adaptateurs sans fil (Wireless adapters ou Network Interface Controller **NIC**). Ces adaptateurs sont disponibles dans de nombreux formats (Carte PCI, PCMCIA, USB, etc....).

Le standard 802.11 a définit deux modes de fonctionnement

- Le mode Ad Hoc
- Le mode Infrastructure

II.4.1. Le mode Ad Hoc

En mode Ad Hoc, les stations sans fil se connectent les unes aux autres afin de constituer un réseau point à point (en anglais peer to peer), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de serveur.

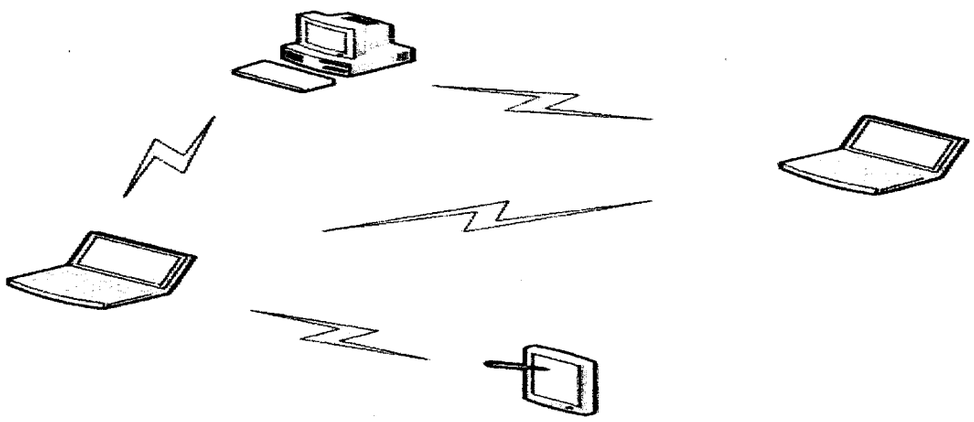


Figure 1.7. Le mode Ad Hoc

L'ensemble formé par les différentes stations est appelé IBSS (Independant Basic Service Set). Un **IBSS** est un réseau sans-fil constitué au minimum de deux stations et n'utilisant pas de point d'accès, il constitue un réseau provisoire permettant à des personnes géographiquement proches d'échanger des données. IBSS est identifié par un SSID (Service Set IDentifier).

II.4.2. Le mode Infrastructure

En mode Infrastructure, chaque station se connecte à un AP (Access Point) via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situées dans sa zone de couverture est appelé BSS (Basic Service Set) et constitue une cellule. Chaque BSS est identifié par un BSSID, un identifiant de 6 octets (48 bits). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès.

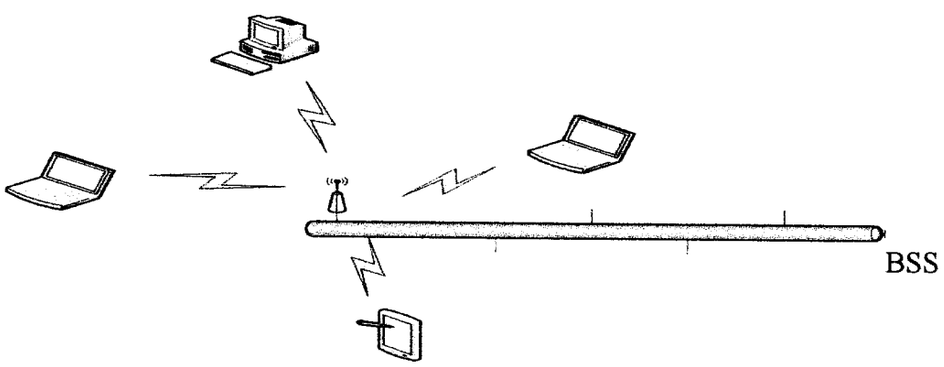


Figure 1.8. Le mode Infrastructure

Lorsque plusieurs points d'accès sont reliés entre eux (plusieurs BSS) par une liaison, ils forment un système de distribution (**DS** Distribution System). Celui-ci

constitue un **ESS** (Extended Service Set). Le système de distribution **DS** peut être aussi bien un réseau filaire qu'un réseau sans fil. Afin d'échanger des informations sur les stations et permettre le cas échéant de transmettre les données des stations mobiles. Cette caractéristique permettant aux stations de "passer de façon transparente" d'un point d'accès à un autre est appelé itinérance (en anglais ***roaming)***.

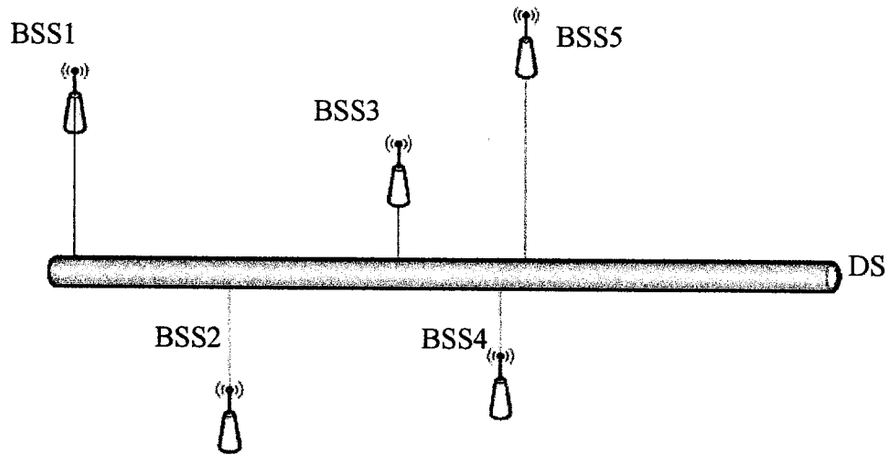


Figure 1.9. Ensemble de service étendu (ESS)

Comme ce mode est le plus utilisé pour les grands réseaux sans fil (plus de 50 utilisateurs potentiels), il est intéressant de s'attarder sur la manière dont les cellules sont placées géographiquement. En effet, les AP proches utilisant des fréquences identiques risquent de créer des interférences et de pénaliser le réseau. [6]

a. La communication avec le point d'accès

Lors de l'entrée d'une station dans une cellule, celle-ci diffuse sur chaque canal une requête de sondage contenant le SSID pour lequel elle est configurée ainsi que les débits que son adaptateur sans fil supporte. Si aucun SSID n'est configuré, la station écoute le réseau à la recherche d'un SSID.

En effet chaque point d'accès diffuse régulièrement (à raison d'un envoi toutes les 0.1 secondes environ) une trame balise nommée **beacon** donnant des informations sur son BSSID, ses caractéristiques et éventuellement son SSID. Le SSID est automatiquement diffusé par défaut, mais il est possible de désactiver cette option.

A chaque requête de sondage reçue, le point d'accès vérifie le SSID et la demande de débit présente dans la trame balise. Si le SSID correspond à celui du point d'accès, ce dernier envoie une réponse contenant des informations sur sa charge et des

données de synchronisation. La station recevant la réponse peut ainsi constater la qualité du signal émis par le point d'accès afin de juger de la distance à laquelle il se situe.

Une station se trouvant à la portée de plusieurs points d'accès (possédant bien évidemment le même SSID) pourra ainsi choisir le point d'accès offrant le meilleur compromis de débit et de charge. Lorsqu'une station se trouve dans le rayon d'action de plusieurs points d'accès, c'est elle qui choisit auquel se connecter. [6]

b. Les hotspots

Un **hotspot** est une borne d'accès Wi-Fi installée dans les lieux publics et de passage, donnant accès à un réseau métropolitain privé ou public. Les métiers des services et de la restauration ne s'y sont pas trompés et l'intérêt pour les hotspots va grandissant pour attirer une clientèle de consommateurs technophiles. Il est même question de transformer les antiques taxiphones des bars en hotspots.

Une fois ce travail accompli, l'installation du réseau peut commencer. Selon le choix de l'administrateur, le réseau peut être ouvert ou sécurisé. Dans le premier cas, l'usage d'une vieille machine ne contenant pas de données personnelles est le plus conseillé. Dans le cas où le réseau est sécurisé, les utilisateurs potentiels doivent, recevoir chacun un login, un mot de passe et éventuellement une clé. [6]

Le standard 802.11 définisse deux autres modes de fonctionnement, appartenant au mode infrastructure

- **Point-to-point** est un cas particulier du mode Infrastructure. Il permet de connecter deux points du réseau grâce à deux antennes généralement directionnelles. Cette solution est souvent utilisée pour connecter deux bâtiments éloignés sans installer de câbles transversaux, pour des raisons économiques, de sécurité ou de facilité. [6]
- **Point-to-multipoint** il désigne la liaison entre un point et plusieurs points, telle que la connexion entre un bâtiment central et plusieurs bâtiments satellites. [6]

II.5. Les principaux risques qui touchent la sécurité du Wifi

L'interception de données que peut effectuer toute personne se trouvant dans le rayon de portée d'un point d'accès en écoutant toutes les communications circulant sur le réseau, le détournement de connexion afin d'obtenir l'accès à un réseau local ou à

Internet, le brouillage des transmissions en produisant des interférences au moyen des signaux radio émis et les dénis de service (envoi d'informations afin de perturber volontairement le fonctionnement du réseau) constituent les principaux risques qui peut subir un réseau sans fil à sa mauvaise protection.

Dans le but de sécuriser Wifi, il suffit d'appliquer quelques mesures de sécurité dont on cite principalement

- Changer le mot de passe utilisateur du routeur WiFi.
- Définir le nom du réseau (SSID).
- Activer le cryptage du réseau (clef de sécurité).
- Filtrer les adresses MAC.
- Configurer les machines WiFi.
- Activer le partage de fichiers.

II.6. Les différentes versions de la norme IEEE 802.11

La norme à la base, soit IEEE 802.11, offrait des débits de 1 ou 2 Mbps, mais des révisions ont été apportées à la norme originale afin d'optimiser le débit. C'est notamment le cas des normes 802.11a, 802.11b et 802.11g (appelées normes 802.11 physiques). D'autres comme la norme 802.11i a été édictée afin de préciser des éléments permettant d'assurer une meilleure sécurité ou la 802.11e une meilleure interopérabilité. Nous allons aborder ci-après un rapide aperçu des différentes normes existantes ou en développement

- **802.11 a** est une extension du standard 802.11, mais utilise la bande de fréquences de 5 GHz et offre des débits de 54 Mbit/s qui décroissent plus vite avec la distance. Sa portée va d'une trentaine de mètres jusqu'à une centaine de mètres. Sa couche physique utilise une méthode de modulation appelée le multiplexage orthogonal par division de fréquence **OFDM** (Orthogonal Frequency Division Multiplexing).
- **802.11 b** permet des débits théoriques de 11 Mbits/s avec des débits pratiques qui peuvent chuter jusqu'à 5.5, 2 et 1 Mbits/s, dans la bande de 2.4 GHz et utilise l'encodage DSSS. Ses performances sont similaires à l'Ethernet. Il a une

portée allant de quelques dizaines à quelques centaines de mètres sur la bande ISM.

- **802.11 c** apporte les informations nécessaires pour assurer le bon fonctionnement des ponts réseaux. Ce standard est utilisé pour l'interopérabilité des points d'accès (AP).
- **802.11 d** ce groupe de travail a été mis en place pour un besoin de normalisation. En effet suite à la vulgarisation du 802.11, seuls quelques pays ont mis en place des règles pour le fonctionnement de celui-ci.
- **802.11 e** La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche liaison de données. Ainsi, cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de manière à permettre, notamment, une meilleure transmission de la voix et de la vidéo. Cette norme sera étudiée un peu plus loin dans notre projet.
- **802.11 f** est une recommandation à l'intention des vendeurs de points d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole *Inter-Access point roaming protocol* permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau.
- **802.11 g** utilise la bande de fréquence de 2.4 GHz et permet des débits théoriques de 54 Mbits/s si les distances sont relativement courtes d'une centaine de mètres. Elle utilise la modulation OFDM au niveau physique. Cette norme a une compatibilité descendante avec la norme 802.11b.
- **802.11 h** décrit des mécanismes permettant de mesurer et d'abandonner les canaux afin de respecter leurs conditions d'utilisations locales, notamment nécessaires pour l'utilisation de la bande ISM à 5 GHz en Europe.
- **802.11 i** met en place les mécanismes afin de garantir la sécurité. Cette norme définit des techniques de chiffrage telles que l'**AES** (Advanced Encryption Standard).
- **802.11 IR** a été élaborée de manière à utiliser des signaux infrarouges. Cette norme est désormais dépassée techniquement.
- **802.11 j** La norme *802.11j* est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

- **802.11k** Cette norme permet aux appareils compatibles de faire des mesures de signaux complètes pour améliorer l'efficacité des communications, son avantage est d'améliorer le roaming automatique via des **sites report**.
- **802.11m** Le groupe de travail 802.11m se charge de la maintenance, des corrections, des ajouts, clarification et interprétations des documents relatifs à la famille de spécifications 802.11.
- **802.11 n** son but est d'étendre le standard 802.11 pour atteindre un débit de 540 Mbit/s tout en assurant une rétrocompatibilité avec les trois précédents amendements (a, b et g). Sa portée est d'une centaine de mètres. Il utilise les deux bandes 2.4 et 5 GHz.
- **802.11 s** est actuellement en cours d'élaboration. Le débit théorique atteint aujourd'hui 1 à 2 Mbit/s. Elle vise à implémenter la mobilité sur les réseaux de type adhoc.
- **802.11 x** Sécurisation de divers médias y compris le lien sans fil par le biais de mécanismes d'authentification forts et de serveur RADIUS avec une distribution dynamique des clés. [14]

Les normes 802.11a, 802.11b et 802.11g, appelées « normes physique » correspondent à des révisions du standard 802.11 et proposent des modes de fonctionnement, permettant d'obtenir différents portée en fonction du débit. Dans le tableau suivant, est résumé les normes physiques du 802.11

Normes	Normalisation	Bande (GHZ)	Débit théorique (Mbits/s)	Débit réel (Mbits/s)	Portée théorique (m)	Modulation utilisée
802.11	1997	2.4	2	<1	100	FHSS-DSSS
802.11a	1999	5	54	2-24	20	OFDM
802.11b	1999	2.4	11	4-6	60	DSSS
802.11g	2003	2.4	54	20-28	20	OFDM

FHSS Frequency Hopping Spread Spectrum
DSSS Direct Sequence Spread Spectrum
OFDM Orthogonal Frequency Division Multiplexing

Tableau 1.1. Les normes physiques du 802.11

III. Présentation du standard IEEE 802.11

III.1. Introduction

La norme 802.11, comme toutes les normes définies par le comité 802, couvre les deux premières couches (basse) du modèle OSI, c'est-à-dire la couche physique (niveau 1) et la couche liaison de données (niveau 2). Cette dernière est elle-même subdivisée en deux sous-couches, la sous-couche **LLC** (Logical Link Control) et la couche **MAC** (Medium Access Control).

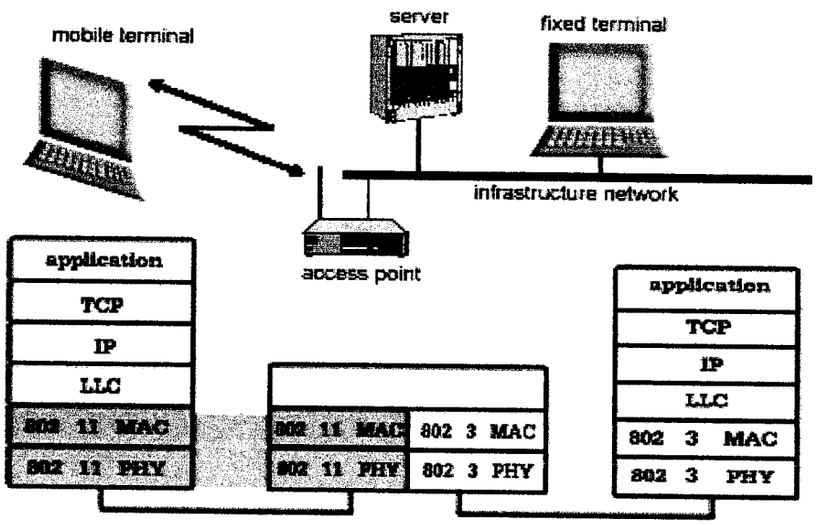


Figure 1.10. Couches du modèle OSI

La figure suivante illustre l'architecture du modèle proposé par le groupe de travail IEEE 802.11 comparée à celle du modèle OSI (Open System Interconnection). [14]

OSI Layer 2 ***Data Link Layer***	802.11 Logical Link Control (LLC)					
	802.11 Medium Access Control (MAC)					
OSI Layer 1 ***Physical Layer (PHY)***	FHSS	DSSS	IR	Wi-Fi 802.11b	Wi-Fi 802.11g	Wi-Fi5 802.11a

Figure 1.11. Modèle en couches de l'IEEE 802.11

III.2. La couche physique (802.11 PHY)

La couche physique définit la technique de transmission (modulation des ondes radioélectriques), l'encodage et la signalisation de la transmission. Le signal électrique hertzien va transporter l'information, il va être modifié suivant les informations à transporter. Tout signal électrique sinusoïdal peut varier suivant son amplitude (tension en volt), sa fréquence (en hertz) et sa phase (en degré). C'est donc sur un de ces trois paramètres que l'on peut modifier un signal électrique pour le coder. La couche physique est divisée en deux sous couches

- **PLCP** *(Physical Layer Convergence Protocol)* s'occupe de l'écoute du support et de la signalisation en fournissant un **CCA** (Clear Channel Assessment) à la couche MAC.
- **PMD** *(Physical Medium Dependent)* traite l'encodage des données et la modulation. [14]

La norme physique 802.11 propose trois couches différentes suivant trois techniques de transmission

- ✓ Le Frequency Hopping Spread Spectrum (FHSS).
- ✓ Le Direct Sequence Spread Spectrum (DSSS).
- ✓ Le support Infrarouge (IR).

III.2.1. FHSS (Frequency Hopping Spread Spectrum)

FHSS désigne une technique d'étalement de bande fondée sur le *saut de fréquence*. Elle consiste à diviser la bande passante disponible en 79 sous canaux, de 1MHz de largeur de bande offrant, chacun un débit d'au moins 1MB/s avec codage binaire. L'émetteur et le récepteur s'entendent sur une séquence de *sauts de fréquence porteuse* pour envoyer les données successivement sur des différents sous-canaux, ce qui sert à ne pas utiliser les sous-canaux fortement perturbés. La séquence de sauts est calculée pour minimiser la probabilité que deux émissions utilisent le même sous-canal. Grace à cette technique, on peut émettre des données dans une plage de fréquence même perturbée. Si l'on avait découpé la bande en une seule plage, la plage entière aurait été perturbée, ce qui aurait rendu toute émission impossible. Avec ce découpage en 79 sous plage, une perturbation n'affecte que quelque sous plage. Dans ce cas, on réussit la communication malgré des perturbations. [7]

Pays	Etats-Unis	Europe	Japon
Nombre de canaux utilisés	79	79	23

Tableau 1.2. Nombre de sous canaux utilisés pour le FHSS

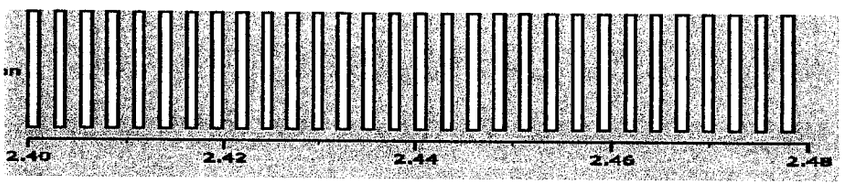


Figure 1.12. FHSS 802.11 sans perturbations

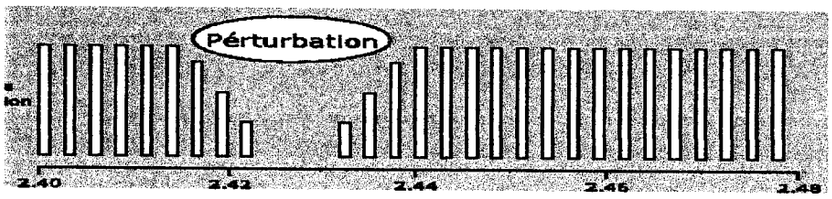


Figure 1.13. FHSS 802.11 avec perturbations

III.2.2. DSSS (Direct Sequence Spread Spectrum)

DSSS (Direct Sequence Spread Spectrum) ou étalement du spectre par séquence directe. De même que pour le FSSS, le DSSS est une technique dite à étalement de spectre fonctionnant sur la bande ISM des 2,4 GHz. Cette fois-ci la bande est divisée en 14 canaux de 20 MHz, chaque canal de 20 MHz étant constitué de quatre unités de 5 MHz. Chaque canal est espacé de 5 MHz, sauf le canal 14, espacé de 12 MHz avec le canal 13. [7]

Canal	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Fréquence (GHz)	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472	2.477

Tableau 1.3. Les fréquences du DSSS

III.2.3. Le support Infrarouge

Le standard IEEE 802.11 prévoit également une alternative à l'utilisation des ondes radio la lumière infrarouge. La technologie infrarouge a pour caractéristique principale d'utiliser une onde lumineuse pour la transmission de données. Ainsi les transmissions se font de façon unidirectionnelle, soit en "vue directe" soit par réflexion. Le caractère non dissipatif des ondes lumineuses offre un niveau de sécurité plus élevé. Il est possible grâce à la technologie infrarouge d'obtenir des débits allant de 1 à 2 Mbit/s en utilisant une modulation appelé PPM (pulse position modulation). [7]

III.3. La couche liaison de donnée (802.11 MAC)

802.11 MAC est la 2ème couche du modèle OSI. Cette couche a pour objectif de réaliser le transport des données. Elle est subdivisée en deux sous couches

- La sous couche LLC (Logical Link Control).
- La sous couche MAC (Medium Access Control).

III.3.1. La sous couche LLC

La sous couche la plus haute est celle du contrôle da la liaison logique LLC (Logical Link Control) utilise les mêmes propriétés que la sous couche LLC 802.2 et permet de relier un réseau local sans fil (WLAN) a tout autre réseau locaux appartenant a la famille IEEE. Cette couche permet d'établir un lien logique entre la couche MAC et la couche du 3ème niveau du modèle OSI (Couche réseau). Ce lien se fait par l'intermédiaire du **LSAP** (Logical Service Access Point). La couche LLC fournit deux types de fonctionnalité

- ✓ Un système de contrôle de flux.
- ✓ Un système de reprise après erreur.

III.3.2. La sous couche MAC

La sous-couche basse est celle du contrôle d'accès au support (MAC Media Access Control) est redéfinie par la norme 802.11 (Niv2). Elle caractérise l'accès au média de façon commune aux différentes normes 802.11 physiques, elle est équivalente à la norme 802.3 **Ethernet** avec des fonctionnalités nécessaires aux transmissions radio

(le taux d'erreur est supérieur au support filaire) qui sont normalement confiées aux protocoles supérieurs, comme la fragmentation, le contrôle d'erreur (CRC), les retransmissions de paquet et les accusés de réception.

De plus, la couche MAC définit deux méthodes d'accès différentes, la DCF (Distributed Coordination Function) ou CP (Contention Period), appelée aussi mode d'accès à compétition, et la PCF (Point Coordination Function) ou CFP (Contention Free Period) appelée aussi mode d'accès contrôlé. Elle est indépendante des caractéristiques du support physique, des débits et elle supporte les deux topologies infrastructure et ad-hoc. En plus de la transmission des données, d'autres services de base sont fournis tels que

- Association/désassociassions,
- Confidentialité (mécanisme **WEP** (Wired Equivalent Privacy) etc.),
- Authentification et contrôle d'accès,
- Fragmentation/réassemblage,
- Economie d'énergie.

a- Le format de la trame MAC

Le standard 802.11 définit le format des trames échangées. Chaque trame est constituée d'un en tête appelé **MAC header**, d'une longueur de 30 octets, d'un corps et d'un CRC permettant la correction d'erreur. [3]

En tête MAC

Champ de contrôle 2 octets	**Durée /ID 2 octets**	**Adresse1 6 octets**	**Adresse2 6 octets**	**Adresse3 6 octets**	**Contrôle de séquence 2 octets**	**Adresse4 6 octets**	**Corps de la trame**	**CRC 4octets**

Figure 1.14. Format de la trame MAC

b- Mécanisme de réservation

- *Ecoute du support physique*

Il s'effectue à la fois au niveau physique à l'aide du **PCS** (Physical Carrier Sense), et au niveau MAC à l'aide du **VCS** (Virtual Carrier Sense). [3]

- *Détection de la porteuse physique*

Elle est effectuée par la couche physique et dépend du medium et de la couche physique et de la modulation utilisé. [3]

- *Détection de porteuse virtuellement (NAV)*

Pour pallier les manques de la fonction physique de détection de porteuse, 802.11 intègre une fonction virtuelle de détection de porteuse basées sur un mécanisme appelée **NAV** (Network Allocation Vector). NAV est un temporisateur qui indique le temps pendant lequel le medium sera réservé. Une station qui souhaite émettre positionne le NAV à la valeur du temps pendant lequel elle souhaite utiliser le medium dans la trame. [3]

- *VCS ou RTS/CTS*

Le VSC est un mécanisme de réservation, qui vient complexifier quelque peu le fonctionnement de CSMA/CA. Lorsque deux station veulent communiquer, la station émettrice attend pendant un DIFS, puis doit d'abord envoyer une demande d'émission, appelée **RTS** (Request To Send), à la station de destination. Lorsque les autres stations détectent la trame, elles mettent à jour leur temporisateur NAV, à partir du champ de durée de vie de la trame. La station de destination, quand à elle, attend pendant un SIFS avant de renvoyer à la source une réponse, appelée **CTS** (Clear To Send), lui indiquant qu'elle peut commencer à émettre ses données. Ces deux technique RTS et CTS du mécanisme VSC sont utilisés nécessairement pour résoudre lez problème de la station caché, que nous venons de le définir par la suite. [3]

III.4. Problème de station cachée

Une station est dite cachée, si elle est dans la portée du récepteur, et en dehors de la portée de l'émetteur. La réservation RTS/CTS permet de résoudre un problème connu des réseaux hertziens, à savoir le problème de la station cachée. Exemple Un BSS composé de deux stations A, B et un AP (Access Point). Les stations peuvent communiquer avec l'AP, mais ne se voient pas entre elles. Lorsque A émet une trame vers l'AP, B ne va pas la détecté et va donc également émettre si elle en a besoin ; il se produit alors une collision. Pour éviter cette situation, A va commencer par envoyer un

RTS à l'AP, qui va répondre par un CTS. La station B détecte le CTS et va donc en déduire que le support vient d'être réservé. Elle retarde ainsi l'envoie de ses données, évitant une collision. Il se peut qu'une collision se produise tout de même si A et B envoient un RTS en même temps; ce pendant, une trame RTS n'occupant que 20 octets au maximum, ce cas de figure n'est presque pas pénalisant. [2]

Pour combler ces problèmes, 802.11 utilise le mécanisme d'esquive de collision (Collision Avoidance) appelé **CSMA/CA**.

IV. Les trames IEEE 802.11

Les paquets de données, provenant de la couche réseau, sont encapsulés au niveau 2 par un en-tête MAC, formant une **MPDU** (Mac Protocol Data Unit). Cette MPDU est ensuite encapsulée dans une seconde trame au niveau 1 (physique) pour permettre la transmission sur le média. Cette encapsulation consiste à rajouter un préambule et un en-tête à la MPDU, cet ensemble forme une PLCP-PDU. Toutes les trames IEEE 802.11 sont composées de la manière illustrée à la figure suivante

Préambule	En-tête PLCP	Données MAC	CRC

Figure 1.15. Structure de base de la trame 802.11

- **Préambule** est dépendant de la couche physique et contient deux séquences. Une séquence permettant de Synchro est utilisée par le circuit physique pour sélectionner l'antenne à laquelle se raccorder, une séquence SFD (Start Frame Delimiter) est utilisée pour définir le début de la trame.

- **L'en-tête PLCP (Physical Layer Convergence Protocol)** contient des informations logiques utilisées par la couche physique pour décoder la trame.

- **Le champ CRC (Cyclic Redundancy Check)** Champ de détection d'erreur CRC sur 16bits.

- **Données MAC (Medium Access Control)** La trame MAC comporte un champ de contrôle assez complexe, dont les zones sont détaillées précédemment. [16]

IV.1. Niveau physique

Le préambule permet la détection du début de trame, la synchronisation de la trame, il permet la prise du canal pour l'émission ou **CCA** (Clear Channel Assesment). L'en-tête contient diverses informations, variable suivant l'interface physique utilisée.

IV.1.1. La structure de la trame en FHSS (802.11 FHSS)

Une trame au niveau physique est composée de trois parties. Elle débute par un *préambule*, suivi d'un *entête* et se termine par la partie données

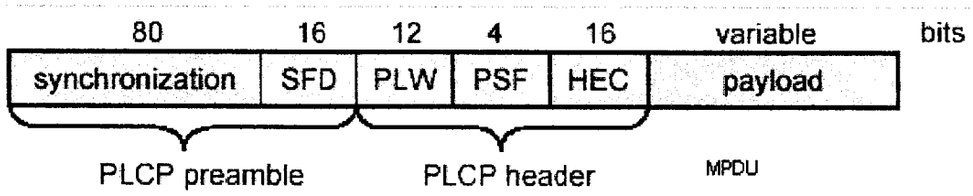


Figure 1.16. Trame 802.11 au niveau physique pour le FHSS

- **Préambule** est toujours transmis à 1 Mbits/s, composé en deux parties
    - Une suite de 80 bits de synchronisation en alternance de 0 et de 1. Elle permet de sélectionner le meilleur point d'accès et de se synchroniser avec (PA et STA).
    - Le Start Frame Delimiter (SFD) de 16 bits. Il indique le début de la trame.
- **En-tête (header)** est toujours transmis à 1 Mbits/s, composé en trois parties
    - PLW (PLCP-PDU Length Word) sur 12 bits indique la longueur (en nombre d'octets) de la trame (PLCP-PDU), cela permet à la couche physique déterminer la fin de la trame.
    - PSF (PLCP Signaling Field) sur 4 bits indique le débit utilisé sur l'interface radio. (1 ou 2 Mbits/s) pour la transmission des données (MPDU).
    - HEC (Header Error Check) est un CRC de 16 bits permettant de détecter les erreurs des champs de l'en-tête (PLW et PSF).
- **La partie donnée**
    - La trame MAC contient les données relatives à la couche MAC. [3]

IV.1.2. La structure de la trame en DSSS (802.11 DSSS)

Une trame au niveau physique est composée, comme pour la technique, de trois parties un *préambule*, puis un *entête* et enfin la partie données.

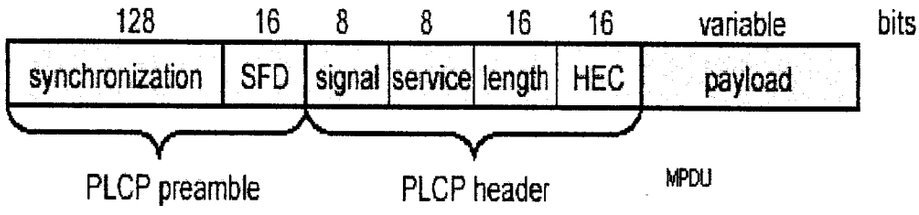


Figure 1.17. Trame 802.11 au niveau physique pour le DSSS

- **Préambule** est toujours transmis à 1 Mbits/s. Le préambule de la trame DSSS est identique à la trame FHSS, si ce n'est une longueur de synchronisation plus longue, et une valeur de 0xF3A0 (1111 0011 1010 0000) pour le SFD.
- **En-tête (header)** est toujours transmis à 1 Mbits/s, composé en quatre parties
    - **Signal** sur 8 bits, qui indique la vitesse sélectionnée pour la transmission des données (MPDU)
        - Si la valeur est à **0x0A** la transmission se déroulera à 1Mbits/s.
        - Si la valeur est à **0x14** la transmission se déroulera à 2Mbits/s.
        - Si la valeur est à **0x37** la transmission se déroulera à 5,5Mbits/s.
        - Si la valeur est à **0x6E** la transmission se déroulera à 11Mbits/s.
    - **Service** sur 8 bits réservé pour un usage futur (valeur 0x00 ? IEEE 802.11).
    - **Longueur** sur 16 bits, qui indique la longueur (en nombre d'octets) de la trame à suivre (MPDU), cela permet à la couche physique déterminer la fin de la trame.
    - **CRC** sur 16 bits permettant de détecter les erreurs des champs de l'en-tête (Signal, Service et Lenght). [3]
- **La partie donnée**
    - La trame MAC contient les données de la trame physique. Elles sont transmises selon la modulation sélectionnée dans le champ *signal.* [3]

IV.2. Niveau MAC

Il existe trois sortes de trames les trames de données utilisées pour la transmission de données utilisateur, les trames de contrôle utilisées pour l'accès au support (RTS, CTS, ACK...) et les trames de gestion utilisées pour l'association à un point d'accès ou pour la synchronisation et l'authentification. La taille maximale d'une trame est de 2347 octets.

IV.2.1. Format Général

Le standard 802.11 définit le format des trames échangées. Chaque trame est constituée d'un en-tête appelé **MAC header** (longueur de 30 octets), d'un corps et d'un CRC permettent la correction d'erreur.

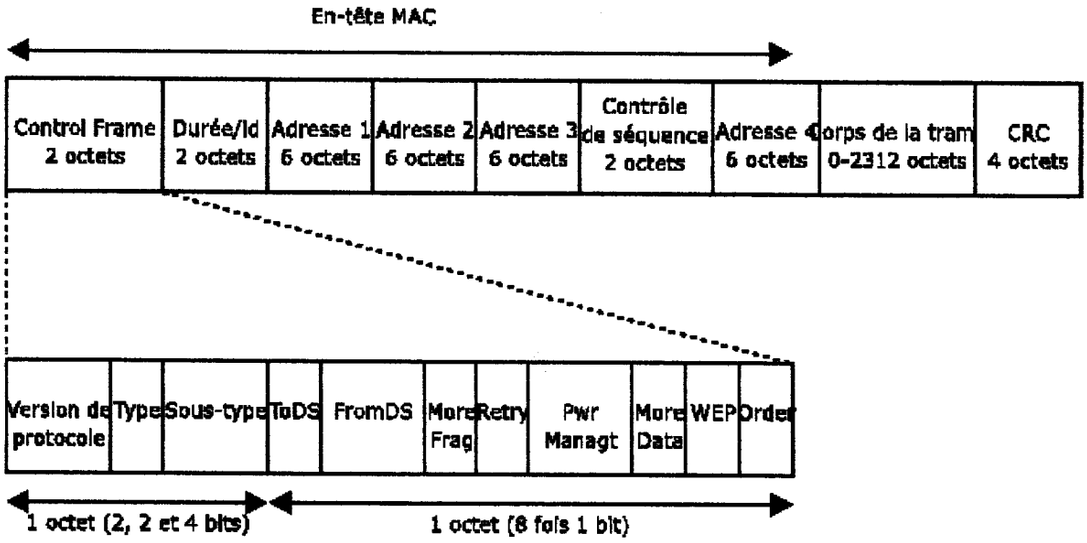


Figure 1.18. Champ de contrôle de trame

A. Les zones de contrôle de trame

A l'intérieur de la zone MAC, le premier champ permet d'émettre des informations sur le contrôle de la trame. 11 sous champs sur 2 octets

- **Le champ version de protocole** Il contient 2 bits qui peuvent être utilisé pour reconnaitre des versions futures du standard 802.11. La valeur de ce champ est fixée à 0 dans la version actuelle.

- **Le champ type** Il indique le type de la trame à transmettre sur le réseau. Il existe trois types de trames les trames de gestion, de contrôle et de données. Voire la figure suivante [3]

Type	00	01	10	11
Nature	Gestion	Contrôle	Données	Reserve

Tableau 1.4. Description du différentes trames en fonction du champ type

- **Le champ sous type** Pour chaque type de trame, le champ sous type nous donne la fonction à réaliser. Nous donnons quelques valeurs des champs sous type pour les différentes trames de gestion, de contrôle et de données.

- **Le champ To DS** Pour le système de distribution (To Distribution System). Le bit est à 1 lorsque la trame est adressée au point d'accès pour qu'il la fasse suivre au système de distribution ; sinon, ce bit est à 0.

- **Le champ From DS** Venant du système de distribution (From Distribution System). Ce bit est mis à 1 lorsque la trame vient du DS; dans le cas contraire il est à 0.

- **Le champ More Frag** Autres fragments. Ce bit est mis à 1 quand d'autres fragments suivent celui en cours de transmission, à 0 pour le dernier fragment de la trame. Rappelons qu'une trame est fragmentée en plusieurs fragments.

- **Le champ de retransmission (Retry)** Ce champ renseigne si la trame est transmise pour la première ou si elle retransmise.

- **Le champ More Data** Autres données. Le point d'accès utilise ce champ pour indiquer à la station terminale en mode économie d'énergie, s'il a ou pas des trames en attente qui lui sont destinées.

- **Le champ Pwr Mgt** Gestion d'énergie. Ce champ indique l'état de la station après la transmission. Si ce bit est à 0, la station est en mode normal, dans le cas contraire la station est en état d'économie d'énergie.

- **Le champ WEP** Sécurité. Ce champ permet de déterminer si la station utilise le cryptage ou non.

- **Le champ d'ordre (Order)** Ce champ permet de vérifier si l'ordre de réception des fragments est le bon. [3]

B. Duré / ID

Ce champ a deux sens, dépendant du type de trame Pour les trames de polling en mode d'économie d'énergie, c'est l'ID de la station. Et dans les autres trames, c'est la valeur de durée utilisée pour le calcul du vecteur d'allocation NAV. [3]

C. Les champs adresse 1, 2, 3 et 4

Ces champs correspondent à des adresses MAC de stations sources, stations destinations ou de BSSID (Basic Service Set Identifier). Dans le tableau suivant, nous résumons la signification des 4 adresses. [3]

To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	Destination	Source	BSSID	Non utilise
0	1	Destination	BSSID	Source	Non utilise
1	0	BSSID	Source	Destination	Non utilise
1	1	BSSID (destination)	BSSID (source)	Destination	Source

Tableau 1.5. Signification des adresses dans la trame des données

D. Le champ contrôle de séquence

Ce champ est utilise pour représenter l'ordre des différents fragments appartenant à la même trame et pour reconnaitre les paquets dupliqués. [3]

E. CRC (Cyclic Redundancy Check)

Il sert au contrôle d'erreur à partir d'un polynôme générateur standard qui s'étend sur 32 bits. [3]

IV.2.2. La trame de contrôle

Les trames de contrôle permettent l'accès au support et ont pour fonction d'envoyer les commandes et informations de supervision aux éléments du réseau. Dans la partie contrôle de trame, les champs de " ToDS " à " order " sont à 0. Les trames de contrôle en existent plusieurs parmi lesquels on peut citer

- **Trame RTS (Request To Send)** paquet spécial d'appel envoyé par la station source avant le paquet de données.
- **Trame CTS (Clear To Send)** envoyé par la station destination pour indiquer être prête à recevoir les trames.

- **Trame ACK(Acknowlegment)** pour l'accuse de réception.
- **Trame PS-Poll.**

Sous type	Nature du sous type
1010	PS-Poll
1011	RTS
1100	CTS
1101	ACK

Tableau 1.6. Description du sous-type pour la trames de contrôle

IV.2.3. La trame de gestion

Elle est utilisée lors des procédures d'association et de désassociassions (d'une station avec le point d'accès), de la synchronisation et de l'authentification. [3]

Sous type	Nature de sous type
0000	Requête d'association
0001	Réponse a une Requête d'association
0010	Requête de réassociation
0011	Réponse a une Requête de réassociation
0100	Interrogation (probe) requête
0101	Interrogation (probe) réponse
1010	Désassociassions
1011	Authentification
1100	Desauthentification

Tableau 1.7. Description du sous-type pour la trames de gestion

IV.2.4. La trame de données

Elles contiennent des données utilisateurs, notamment les adresses source, destination et BSSID, ce qui permet aux point d'accès d'acheminer correctement les trames. [3]

sous type	nature du sous type
0000	Données
0001	données+CF-ACK
0010	données+CF-Poll
0011	Doneness +CF-ACK+CF-Poll
0101	CF-ACK (pas de données)
0110	CF-Poll (pas de données)
0111	CF-ACK+CF-Poll (pas de données)

Tableau 1.8. Description du sous-type pour la trames de données

Conclusion

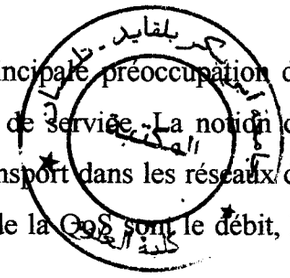
Nous pouvons conclure que les réseaux sans fil régis par la norme IEEE 802.11 ont connu un essor prodigieux ces dernières années, à la maturité de ses normes telles que 802.11a, 802.11b et n, 802.11e, ...

La technologie Wi-Fi et ses propriétés de mobilité qui sont surtout destinées à créer des réseaux locaux avec un câblage moins onéreux (ou inexistant) et une facilité d'installation importante du fait qu'elle a une mise en œuvre rapide et simple et des diminutions potentielles des coûts de déploiement. Aussi, si les débits binaires s'améliorent encore, la technologie Wi-Fi va devenir très intéressante pour la mise en œuvre de petits réseaux dans de petites structures.

Quelque soit le mode opératoire utilisé, Ad Hoc ou Infrastructure, les réseaux sans fil connaissent aujourd'hui un grand développement dans de nombreux domaines. Le chapitre suivant est dédié à clarifier les aspects liés à la qualité de service.

Chapitre 2. Généralités sur la qualité de service

Introduction



Dans le cas de la spécification IEEE 802.11e, la principale préoccupation du groupe de travail est de répondre aux exigences de qualité de service. La notion de qualité de service (QoS) est un concept important pour le transport dans les réseaux de l'information avec un maximum de fiabilité. Les métriques de la QoS sont le débit, le délai de transmission, la gigue et le taux de perte.

Dans ce chapitre nous définirons la notion de la qualité de service et les contraintes qu'elle affronte dans les réseaux. Nous présenterons aussi les modèles d'architecture de la QoS en générale qui sont le mode DiffServ et le mode IntServ. A la fin, nous aborderons les mécanismes de QoS dans 802.11e, un nouveau mécanisme de SW-ARQ (Stop and Wait-Automatic Repeat Request), nommé block d'acquittement (Block Acknoledgement) est utilisé. Ce mécanisme sera simulé par nos soins pour en démontrer l'influence qu'il a sur les performances globales du réseau et les paramètres de QOS en particulier comme on va le constater dans le chapitre qui suit.

I. Définition de la qualité de service

La qualité de service ou QoS (*quality of service*) est une expression qui n'a pas toujours été claire. Son but, est de fournir le meilleur et le plus prévisible service de réseau en fournissant une bande passante réservée, une gigue et un délai contrôlés, et en améliorant le taux de pertes de paquets. Nous pouvons donc dire que la QoS est un ensemble d'outils qui permet de mieux gérer et contrôler le réseau. En général, la qualité de service n'appartient pas à une couche particulière mais elle demande des efforts coordonnés de toutes les couches.

En résume, la qualité de service désigne la capacité à fournir un service (notamment un support de communication) conforme à des exigences en matière de temps de réponse et de bande passante. [1]

I.1. Paramètre de la qualité de service

Les principaux critères permettent d'apprécier la qualité de service sont les suivant

I.1.1. La bande passante

L'augmentation de la capacité de la bande passante résout les problèmes de congestion mais c'est une solution à court terme, très couteuse et ne garantit pas une qualité de service QoS pour le trafic exigeant comme la VoIP et la vidéoconférence. De plus, elle permet que toutes les applications reçoivent le même traitement ce qui ne protège pas le trafic critique de l'entreprise contre des nouvelles applications.

- **Les outils de QoS qui affectent la bande passante**

La compression améliore la bande passante en comprimant les entêtes ou les données significatives et en réduisant le nombre de bits total requis pour transmettre des données. Le contrôle d'admission affecte aussi la bande passante en diminuant la charge introduite dans le réseau en rejetant les nouveaux appels de la voix et de la vidéo. En outre, la mise en file d'attente affecte la bande passante en réservant une quantité minimale de bande passante pour des types particuliers de paquets. [5]

I.1.2. Le délai

Il y a deux sortes de délais qui sont les délais fixes et les délais variables

a. Les délais fixes

- Délai de sérialisation c'est le temps pris pour encoder les bits d'un paquet sur le lien physique.

La formule utilisée pour calculer ce délai est $\frac{\text{le nombre des bits envoyés}}{\text{la vitesse du lien}}$

- Délai de propagation c'est le temps pris pour qu'un bit passe de la fin d'un routeur à l'autre routeur.

La formule utilisée pour calculer ce délai est $\frac{\text{longueur de lien}}{\text{la vitesse de la lumière}}$

La lumière utilisée dans les réseaux sans fil est réduite et cette réduction est due à l'atténuation causée par le conduit transportant le signal.

- Délai de codage c'est le temps de conversion Analogique/numérique par le codeur, et vice-versa. [5]

b. Les délais variables

- Délai de traitement dans le réseau, c'est le temps d'attente dans les files d'attente des équipements.
- Délai de traitement (*processing*) c'est le temps requis dès la réception du paquet jusqu'à la mise en file d'attente pour transmettre.
- Délai de compression c'est le temps pris pour faire la compression.
- Délai du réseau c'est le délai créé par le trafic traversant les composants du réseau. [5]

- **Les outils de QoS qui affectent le délai**

L'ordonnancement de la file d'attente affecte le délai en arrangeant les paquets selon leur priorité. Ceux qui sont plus sensibles seront servis en premier. La fragmentation aussi affecte le délai en divisant les grands paquets en petits paquets pour ne pas retarder le trafic sensible au délai après la transmission des grands paquets car le routeur ne peut pas arrêter un paquet une fois commencé à transmettre. La compression et le *shaping* affectent aussi le délai. Le *shaping* retarde les paquets en les mettant dans des files d'attente même quand une bande passante réelle est disponible. [5]

I.1.3. La gigue

La gigue est la variation des délais à travers le réseau. La Figure 2.1 illustre un exemple de la gigue lors de la transmission de trois paquets d'un appel téléphonique où nous remarquons qu'à la transmission le délai entre les deux premiers paquets transmis est de 20 microsecondes alors qu'il varie à la réception. [5]

- **Les outils de QoS qui affectent la gigue**

La mise en file d'attente, la fragmentation, la compression et le *shaping* sont les outils qui affectent la gigue. [5]

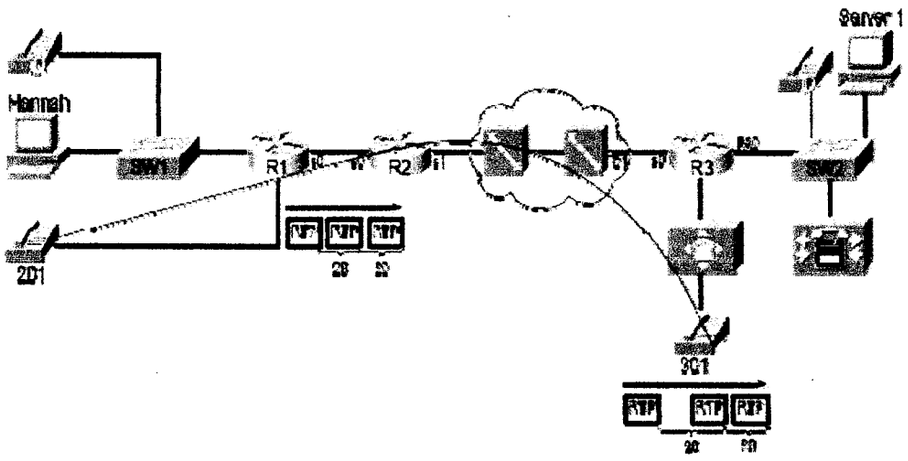


Figure 2.1. Exemple de la gigue

I.1.4. La perte

Les routeurs perdent ou jettent les paquets pour plusieurs raisons. La plupart d'entre eux ne peuvent pas être résolus par les outils de QoS. [5]

- **Les outils de QoS qui affectent la perte**

Quelques outils de QoS peuvent affecter la perte des paquets, tels que la mise en file d'attente qui a pour effet de créer de grandes files d'attente ce qui augmente le délai. Le RED (*Radom Early Detection*) permet de jeter les paquets aléatoirement quand les queues commencent à être pleines. [5]

I.2. But de QoS

Le but de la QoS est d'optimiser les ressources de réseau et de garantir de bonnes performances aux applications critiques.

La Qualité de service sur les réseaux permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par les applications suivant les protocoles mis en œuvre au niveau de la couche réseau. Elle permet ainsi aux fournisseurs de service (département réseaux des entreprises, opérateurs ...) de s'engager formellement auprès de leurs clients sur les caractéristiques de transport des données applicatives sur leurs infrastructures IP. [11]

II. Les niveaux de la qualité de service

Le réseau 802.11 est devenu un réseau à différenciation de services en distinguant deux classes de services supplémentaires par apport au service traditionnel du **Best Effort**. Ces nouveaux services sont la classe charge contrôlée, mieux connue sous le nom **CLS** (Controlled Load Service), où les performances reçues sont celles d'un réseau peut charger, et la classe de service garanti **GS** (Guaranteed Service) où l'application qui demande le service possède l'assurance que les performances du réseau vont rester celles dont elle a besoin.

II.1. Le service de charge contrôlée CL (Controlled Load)

Effectue une différentiation entre les trafics et leur attribue des codes de priorité en fonction de la sensibilité des applications bien évidement, ce service est plus adéquat que le Best Effort, il offre un service proche de celui présenté par le Best Effort lorsque celui-ci se trouve particulièrement dans des conditions de réseau non congestionnés. Sa garantie est fournie pour le débit. Mais contrairement au Best Effort, le service différencié ne détériore pas la qualité du flot lorsque le réseau est surchargé. En effet, les applications qui demandent ce type de service doivent tenir informé le réseau de trafic qui va le traverser, de manière à obtenir une meilleure exploitation du service et du réseau lui-même. Néanmoins, le réseau ne promet pas de garanties temporelles. [8]

II.2. Le service garanti GS (Guaranteed Service)

Les auteurs définissent le service garantie **GS** (Guaranteed Service) comme étant « un service qui doit assurer de fermes garanties, de telle sorte que le délai de bout en bout mesuré sur les paquets d'un flot n'excède pas une certaine limite ». La classe de service garanti livre des données (applications) en fonction des paramètres et de classe de service demandée.

La classe de service garanti permet ainsi d'apporter aux applications un contrôle considérable de point de vue délai. Le délai d'une application se subdivisant en plusieurs sous-délais, seul le délai d'attente est déterminé par le service garanti, grâce au paramètre R de TSpec (les autres délais sont plutôt liés aux propriétés physiques du réseau). De ce fait, une application peut précisément estimer à l'avance quel délai de mise en attente le service garanti peut offrir. Par conséquent, si le délai d'une

application est supérieur à celui attendu, celle-ci peut modifier le token-bucket du trafic ainsi que le taux de données pour obtenir un plus faible délai. Pour les performances qu'il offre, ce service est particulièrement adapté aux applications temps-réel non adaptatives ayant des exigences de qualité de service très strictes. [8]

III. Files d'attente pour le traitement différencié des paquets

Voici des différents exemples de file d'attente pour le traitement différencié des paquets

- *Priority Queuing (PQ)* les files d'attentes privilégiées ont la priorité la plus élevée, le taux des arrivées plus petit que le taux de départ.
- *Weighted Round Robin Queuing* (WRR) files d'attente entretenues dans la mode round robin, le temps de service proportionnels au poids.
- *Weighted Fair Queuing* (WFQ) Le taux minimum garanti par classe. Le temps de service de chaque paquet dans chaque file d'attente est une fonction de la longueur de paquet et du poids de file d'attente. Le temps de service courant est mis à jour chaque fois qu'un paquet est envoyé.
- *Class Based Queuing* (CBQ) le taux maximum par classe est configuré.

Tous les mécanismes de files d'attente ont leurs avantages et inconvénients. La file d'attente FIFO est bonne pour les grandes files d'attente et les environnements *fast_switching* avec des résultats prévisibles. Mais ils ne mettent en application aucune politique de service. Dans la file d'attente à priorité le trafic prioritaire reçoit une faible gigue et une basse perte de paquet. Ce type de file d'attente met en application des politiques de service. La différence principale entre la file d'attente basée sur classe (CBQ) et la file d'attente à priorité (PQ) est que CBQ offre au moins un certain niveau de service à la file d'attente à basse priorité. WFQ offre une répartition dynamique des ressources à toutes les files d'attente basées sur les poids configurés. [5]

IV. Le multimédia

Les systèmes multimédias sont des systèmes de traitement d'information traitant une combinaison des données de multimédia telle que le texte, les graphiques, les images, l'audio et la vidéo. Les applications des multimédias sont classées selon les critères suivants

a. Le degré d'interactivité certaines applications telles que la vidéoconférence, *(teleworking)* et les jeux ont besoin de plus d'interactivité et d'un petit délai de transmission que d'autres applications comme l'accès aux bases de données, la vidéo à la demande et le courriel. **[12]**

b. Le type de distribution les applications de diffusion comme la télévision et les services d'information sont distribués par multicast tandis que d'autres applications comme l'accès aux bases de données, *groupware*, la vidéoconférence et les jeux transmettent par des communications point-à-point ou point-à-groupe. **[12]**

c. La complexité informatique les terminaux mobiles sont limités par des ressources qui doivent être prises en considération par des applications mobiles de multimédia. **[12]**

d. Les besoins d'entrée-sortie quelques applications ont besoin de différents dispositifs d'entrée-sortie. Dans les terminaux mobiles d'aujourd'hui, on peut trouver des dispositifs d'entrée tels que le microphone, les blocs de touches, les claviers, les écrans à contact et des dispositifs de sortie tels que les haut-parleurs, les écrans et les signaux audio. **[12]**

e. Sans dispositifs d'entrée ou de sortie.

Les applications multimédias ont besoin de la transmission de différents types de trafics sous des contraintes variables (largeur de bande, délai etc.). **[12]**

IV.1. Contraintes associées aux applications

Les contraintes des applications multimédias mettent l'accent sur le délai et les erreurs de transmission qui sont supportés par une application spécifique. De telles contraintes s'appellent la qualité du service. Pendant la transmission de la vidéo, les erreurs dans les parties critiques de données, telles que l'information sur le mode de

codage ou les voies de compensation de mouvements mènent à des artefacts « Perturbation artificielle de l'image ou du son, qui se manifeste de manière inattendue, lorsque ces derniers sont reproduits par un appareil » **[21]** très inquiétants. D'où la synchronisation entre la voix et la vidéo devient importante lorsque ces deux sont transmises ensemble. Enfin, la transmission de données graphiques soutient habituellement un grand délai.

IV.2. Contraintes spécifique au multimédia

Sans qualité de service, les flots de la vidéo se dégradent; l'image devient très saccadée, la voix n'est plus synchronisée avec la vidéo et le mouvement apparaît lent. Alors, les applications ont des besoins variés en termes de la bande passante, le délai, la gigue et la perte des paquets. La qualité de service (QoS) permet au réseau de mieux (*best-effort*) de fournir les besoins appropriés des ressources de QoS pour chaque application. Le Tableau ci-dessous, montre quelques applications avec leurs besoins typiques de QoS. [12]

	Voix	**Vidéo interactive (2 voies)**	**Flot de vidéo (1 voie)**	**Données (interactive et mission critique)**	**Données (non interactive et non mission critique)**
Bande passante	Basse	Haute	Haute	Variable typiquement moyenne	Variable typiquement haute
Perte	Basse	Basse	Basse	Moyenne	Haute
Délai	Basse	Basse	Haute	Moyenne	Haute
Gigue	Basse	Basse	Haute	Moyenne	Haute

Tableau 2.1. Quelques applications avec leurs besoins de QoS

On constate d'après ce tableau que la voix n'a pas besoin d'une grande bande passante mais elle ne tolère pas le délai, ni la gigue, ni la perte (parfois elle tolère un peu de perte). La vidéo interactive telle que la vidéoconférence a les mêmes spécifiques que la voix mais elle demande une grande bande passante. Néanmoins, le flot de vidéo telle que la vidéo peut accepter le délai et la gigue mais ne tolère pas la perte. [12]

IV.2.1 Les caractéristiques du trafic vidéo

Les codeurs vidéo convertissent l'audio et la vidéo analogiques en numériques. La voix est envoyée comme un flot séparé de la vidéo. Les codeurs tels que les G.711 et G.729 sont utilisés pour la voix tandis qu'une grande variété de codeurs incluant l'**ITU** (International Telecommunication Union) H.261 et le MPEG (*Moving pictures Experts Group*) convertissent le flux de la vidéo. [12]

IV.2.2 Les contraintes de QoS de la vidéo

La vidéo demande une bande passante plus grande que celle de la voix, parce qu'elle utilise une variété de taille et de taux de paquets pour supporter un simple flot de vidéo. La moyenne de la bande passante requise pour une section de vidéo dépend de la complexité et de la quantité du mouvement de la vidéo. Le tableau suivant cite quatre codeurs de vidéo et leur bande passante requise. [12]

Codeur vidéo	Marge de la bande passante requise
MPEG-1	500 à 1500 Kbits/sec
MPEG-2	1.5 à 10 Mbits/sec
MPEG-4	28.8 à 400 Kbits/sec
H.261	100 à 400 Kbits/sec

Tableau 2.2. La bande passante requise de quatre codeurs de video

V. Les modèles d'architecture de QoS

L'**IEFT** (Internet Engineering Task Force) propose deux approches pour garantir la QoS pour les réseaux filaires qui sont les services intégrés **IntServ** et les services différenciés **DiffServ**.

V.1. Le modèle IntServ (Integrated Service)

IntServ est un modèle différent du DiffServ. Dans IntServ, chaque application est libre de demander une qualité de service spécifique à ses besoins. Pour fournir des garanties par flux, le RFC 1633 d'IntServ décrit deux mécanismes

- **La réservation des ressources** s'agit d'offrir un service de type garanti tel qu'il existe dans les réseaux à circuits en utilisant le protocole RSVP (*Resource reSerVation*

Protocol). Chaque routeur IntServ maintient les informations sur les états de tous les flux comme la bande passante requise, le délai et le coût.

- **Le contrôle d'admission** décide quand la demande de réservation doit être rejetée.

IntServ possède quelque désavantages, le RSVP ne passe pas à l'échelle (*scalability*) parce que le routeur du cœur doit maintenir les états de réservation de tous les flux qui le traversent et les messages de rafraîchissement de RSVP doivent être émis périodiquement pour chaque flux. [10]

V.2. Le modèle DiffServ (Differenciated Service)

DiffServ a été proposé pour éviter le problème de mise à l'échelle imposé par IntServ. Il consiste à différencier les flux dans des classes offrant chacune une qualité de service différente et dans lesquelles sont agrégés plusieurs flux. Le classement se fait par les routeurs de bordure grâce à un code présent dans l'entête du paquet IP. Les routeurs du cœur de réseau utilisent ce code pour déterminer la qualité de service requise par le paquet. Tous les flux appartenant à une même classe reçoivent le même traitement. Ensuite, des traitements différenciés seront appliqués aux différentes classes de trafic.

DiffServ définit chaque classe ou catégorie de paquets comme un BA (Behavior Aggregate). Le fait d'associer un outil de QoS à un BA s'appelle PHB (Per-Hop Behavior). En général, l'IP définit un octet (8 bits PPPDTRC0) qui est le type de service (ToS Type of Service)

- PPP (*IP precedence*) définissent la priorité du datagramme (111= la plus grande priorité).
- D *(Delay)* pour le délai s'il est mis à 1 c'est-à-dire que le service nécessite un faible délai.
- T (*Throughput*) pour le débit s'il est mis à 1 c'est-à-dire que le service nécessite un haut débit.
- R (*Reliability*) pour la fiabilité s'il est mis à 1 c'est-à-dire que le service nécessite une grande fiabilité.

- C (*Cost*) pour le coût s'il est mis à 1 c'est-à-dire que le service nécessite un faible coût et le dernier bit est inutilisé.

Les six premiers bits de l'octet **ToS** seront le champ DSCP (*Differentiated Services Code Point*) créé par DiffServ, ce qui permet 64 combinaisons différentes de classifications. Donc, une compatibilité avec l'IP précédence est nécessaire.

Le tableau ci-dessous, montre la compatibilité entre les valeurs DSCP et l'IP précédence. [10]

Noms des «class selector»	**Marge des valeurs DSCP**	**Valeur en binaire**	**Compatible avec *IP précédence***	**PHB**
Par défaut	0-7	000xxx	0	Best effort
CS1	8-15	001xxx	1	Classe 1 (AF)
CS2	16-23	010xxx	2	Classe 2
CS3	24-31	011xxx	3	Classe 3
CS4	32-39	100xxx	4	Classe 4
CS5	40-47	101xxx	5	Express forwarding
CS6	48-55	110xxx	6	Contrôle
CS7	56-63	111xxx	7	Contrôle

Tableau 2.3. Compatibilité entre les valeurs DSCP et l'IP precedence

DiffServ suggère deux autres ensembles de PHB et de valeurs DSCP en plus des sélecteurs de classes (CS)

- **Assured Forwarding (AF)** définit dans le RFC 2597, permet à l'utilisateur de choisir une des 4 classes AF pour chaque flux afin de garantir un acheminement de paquets IP avec une haute probabilité. Chaque classe obtient une quantité différente de ressources dans les routeurs du coeur du réseau. Dans chaque classe, un algorithme de rejet sélectif différencie entre trois niveaux de probabilités de rejets. En cas de congestion, les parquets de basse priorité seront rejetés en premier.

- **Expedited Forwarding (EF)** *ou premium service,* définit dans le RFC 2598 ; il a pour but de minimiser la perte, le délai et la gigue et de garantir une bande passante. Pour cela, le RFC de EF propose deux actions de QoS la mise en file d'attente et le *policing.* [10]

VI. Protocoles de la couche MAC pour les réseaux WLAN

Le médium de contrôle d'accès (MAC *Medium Access Control*) de IEEE 802.11 ne possède pas la différenciation de service. Tous les types du trafic tels que les paquets de données, de la voix et de la vidéo, sont traités de la même façon. Ce qui provoque une détérioration de la qualité de la voix et de la vidéo quand le réseau est congestionné. La norme IEEE 802.11 définit deux modes de fonctionnement qui sont

- La fonction de coordination distribuée **DCF** (*Distributed Coordination Function*).
- La fonction de coordination par point **PCF** (*Point Coordination Function*).

Le **DCF** est responsable des services asynchrones, alors que PCF a été développé pour les services à contraintes temporelles. Le **PCF** est utilisé pendant la Contention Free Period (CFP) période de non contention, alors que DCF utilise la Contention Période (CP). Une CFP et une CP forment une super trame. Les super trames sont séparées par des trames périodiques de gestion appelées **Beacon** ou balise. 802.11 utilise trois intervalles de temps différents, nommés Interframe Spaces (espaces inter frame) pour contrôler l'accès au medium

- Short Inter Frame Space (SIFS)
- PCF Inter Frame Space (PIFS)
- DCF Inter Frame Space (DIFS)

- **SIFS** est le plus court intervalle. Il est utilisé pour les accusés de réception ACK, les trames **CTS** (Clear to Send) et les différents fragments du paquet d'information MPDU, ainsi que pour la réponse d'une station au AP dans le mode Polling (mode vote) dans PCF. SIFS représente la plus haute priorité et assure qu'une station est capable de finir la séquence de transmission de trame avant qu'une autre station puisse accéder au medium.

- **PIFS** est plus long que SIFS. Après l'expiration de cet intervalle, n'importe quelle trame du mode PCF peut être transmise.

- **DIFS** est plus long que PIFS. Après l'expiration de cet intervalle, n'importe quelle trame du mode DCF peut être transmise, de façon asynchrone selon le mécanisme de backoff de la CSMA/CA. Donc DIFS a la plus faible priorité. [8]

VI.1. DCF (Distributed Coordination Function)

Dans **DCF** les stations utilisent le mode de contention pour accéder au canal. Pour cela elles utilisent le mécanisme CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) pour que plusieurs stations puissent accéder le medium en utilisant la méthode de détection de porteuse à accès multiples et évitement de collision. DCF ne fonctionne que durant la période CP.

Chaque station, après que le médium devient libre, attend une durée fixe DIFS suivit d'une durée aléatoire appelée **Backoff time**, avant de commencer à émettre, si le canal est toujours libre. Effectivement la durée backoff time est donnée par la formule

$$Backoff\ time = Random\ (0, CW) \times SlotTime$$

Random (0, CW) est une valeur aléatoire entière uniformément distribué sur [0, CW] avec

- CW (Contention Window).
- La fenêtre de contention vérifiant $CWmin \leq CW \leq CWmax = 1023$.
- Initialement on a CW=CWmin=15 dans 802.11. Slot Time est une durée fixe (9µs dans 802.11a).

- **Le principe du protocole CSMA/CA**

L'émetteur attend qu'aucune émission ne soit en cours. Puis, il attend de nouveau pendant une durée prédéfinie nommée DIFS (Distributed Inter Frame Space) suivie d'un délai d'attente aléatoire supplémentaire CW (Collision Windows, fenêtre de collision). L'émetteur avant d'envoyer le paquet, il envoie une demande de permission sous forme d'un paquet minuscule RTS (Request to send). Le destinataire envoie très rapidement un paquet CTS (Clear To Send) pour autoriser la station à émettre, dans un délai inférieur au DIFS nommé SIFS (Short Inter Frame Space).

La station reçoit le CTS, attend un court délai le SIFS et envoie son paquet de données. La station reçoit le message, attend le SIFS et renvoie un ACK pour assurer à l'émetteur que le paquet a bien été reçu sans collision. [11]

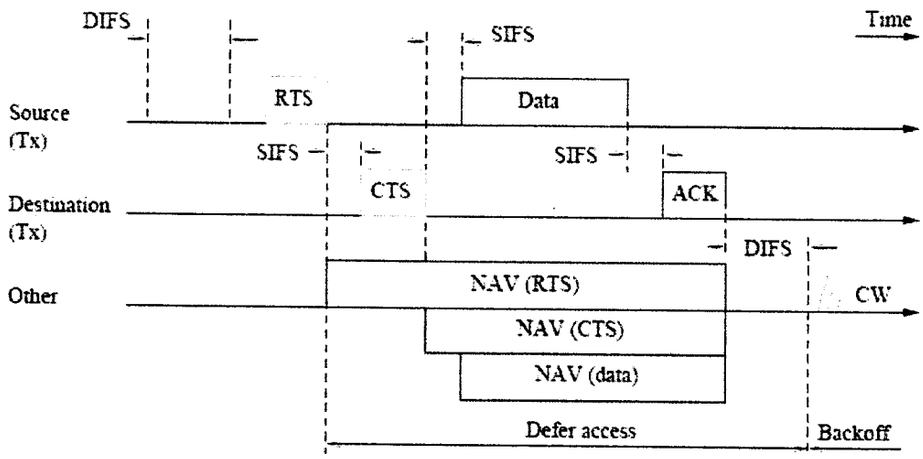


Figure 2.2. fonctionnement de mécanisme DCF

- **NAV** (Network Allocation Vector) est un temporisateur qui indique le temps pendent lequel le médium sera réservé.

VI.2. PCF (Point Coordination Function)

Ce mécanisme est utilisé uniquement dans le mode infrastructure. Il est basé sur un algorithme centralisé permettant de transmettre des données synchrones et asynchrones. Le point d'accès définit un point de coordination PC (Point Coordination) qui lui permet de communiquer avec les stations et ordonner les transmissions par distribution de droit d'utilisation de support suivant une liste de priorité (Polling List). Le PC détermine deux périodes de temps alternatives

- La **CP** (Contention Period) c'est une période de temps avec contention durant laquelle la méthode DCF est utilisée.
- La **CFP** (Contention Free Period) c'est une période de temps sans contention durant laquelle la méthode d'accès PCF est utilisée.

Au début de la période sans contention, le PC acquiert le contrôle de support et garde ce contrôle pendant toute cette période. Si le support est libre pendant la durée

PIFS, le PC commence par envoyer une trame Beacon pour informer les stations de la durée de cette période qui leur permet de mettre à jour leur NAV.

Ensuite, le PC attend un SIFS et commence à envoyer les données par l'intermédiaire de CF-Down tandis que les stations émettrices utilisent les trames CFP-Up. Les différentes trames sont espacées par ses SIFS. Ces trames peuvent comporter des données, des CFPoll pour permettre au PC de scruter les stations, des trames Ack pour signifier une transmission réussie. La période CFP se termine par l'émission d'une trame CF-End [9].

La figure suivante illustre le déroulement de la transmission pour les deux périodes CFP et CP.

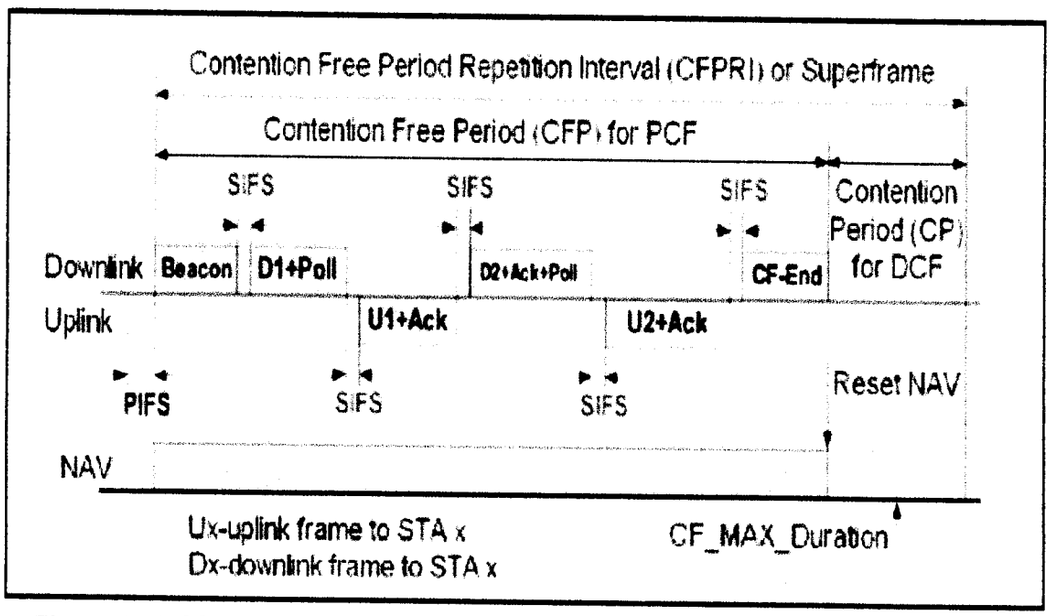


Figure 2.3. Mécanisme de transmission pour les deux périodes CFP et CP

VII. Les limitations de la QoS dans 802.11

Le mécanisme DCF ne peut supporter que le trafic best effort, sans garantie de qualité de service. Mais il ne peut pas supporter les services tels que la voix sur IP, la vidéoconférence ayant une contrainte temporelle de débit, de délai et de la gigue et tolère quelques pertes.

D'autre part, le mécanisme PCF a été conçu pour supporter les applications temps réels mais il présente quelque problème qui dégrade ses performances en qualité

de service; Comme l'alternance entre les périodes CP et CFP mène à un retard imprévisible des trames Beacon. Ce retard provoque des délais supplémentaires sur les différentes transmissions en mode PCF, et détériore la qualité de service; Pour la durée de transmission d'une station élue est difficile à contrôler. Cette durée dépend du débit canal de cette dernière qui varie selon les types de codage de la couche physique. Par la suite, la tâche est pénible pour le point d'accès.

À cause du manque de service de QoS fourni par la norme 802.11, l'IEEE a constitué le groupe de travail E (TGe) qui a un but de concevoir une nouvelle norme connue sous le nom 802.11e afin de fournir une QoS suffisante au WLAN pour supporter des services comme la voix, la vidéo et d'autres, permettant au WLAN de soutenir toutes les applications et fonctions comme un réseau filaire.

La norme 802.11e définit le HCF (*Hybrid Coordination Function*) qui introduit deux nouveaux systèmes qui sont EDCA et HCCA. L'EDCA est une extension de DCF et le HCCA est une extension de PCF [9]. L'architecture de 802.11e est illustrée dans la figure suivante.

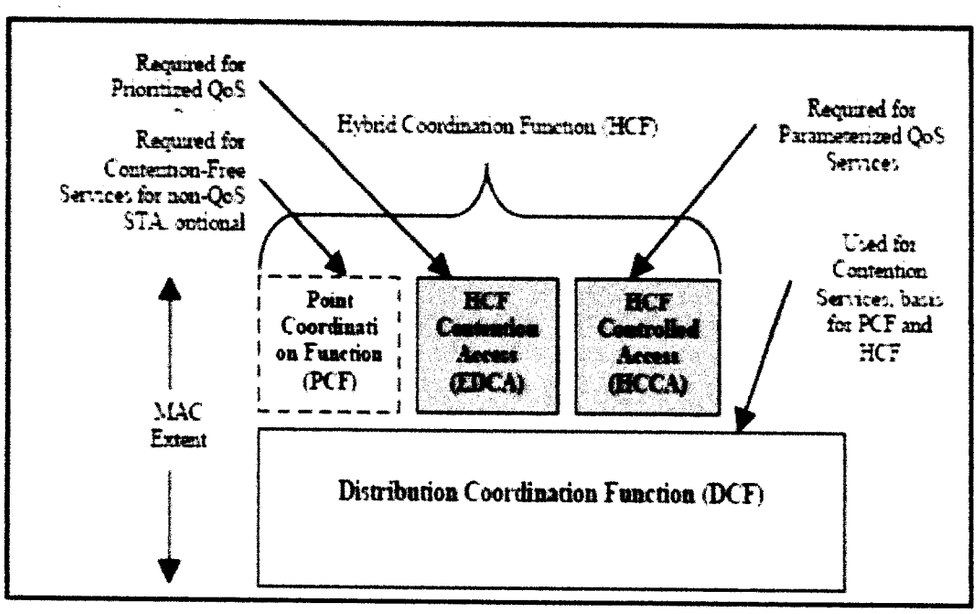


Figure 2.4. L'architecture de l'IEEE 802.11e [22]

VIII. Les mécanismes de Qos dans 802.11e

Plusieurs mécanismes permettant d'introduire la qualité de service dans les réseaux IEEE 802.11 ont été proposés. La majorité de ces études permettent de garantir le trafic réel (qu'il soit audio ou vidéo) en se basant principalement sur la méthode DCF et PCF. Donc des nouveaux mécanismes de QoS ont été créés

1- EDCA (Enhanced Distributed Channel Access).
2- HCCA (Hybrid Coordination Channel Access).
3- Autres mécanismes.

VIII.1. Le mode EDCA

L'EDCA (*Enhanced Distributed Coordination Function*) est un système d'accès basé sur la contention. C'est une extension du mécanisme DCF pour fournir un support des priorités du trafic différencié. La fenêtre de contention et les temps *backoff* sont ajustés pour augmenter ou diminuer la probabilité d'accès au medium afin de favoriser ou défavoriser la transmission de données aux flux de données de priorités faibles ou élevées. En fait, le trafic à priorité élevée a une chance plus grande d'être transmis que le trafic moins prioritaire. De plus, un TXOP (*Transmit Opportunity*) est assigné à chaque niveau de priorité. Un TXOP est un intervalle de temps durant lequel une station qui a obtenu l'accès au médium peut transmettre le plus possible de trames venant du niveau supérieur.

Le mécanisme EDCA fournit un accès différencié et distribué au milieu sans fil WM (*Wireless Medium*) pour les stations de qualités améliorées QSTAs (*Quality enhanced STAtion*) en utilisant huit niveaux différents de priorités d'utilisateur UP (*User Priority*) qui sont disponibles en basant sur la désignation de la norme d'IEEE 802.1D. EDCA définit quatre catégories d'accès **AC** avec des paramètres différents, ils sont désignés par les flux qui les utilisent

- AC_BK pour le trafic à temps non réel (Background).
- AC_BE pour le trafic à temps réel (Best-Effort).
- AC_VI pour la vidéo (vidéo).
- AC_VO pour la voix (voice). [9]

Les ACs sont dérivés d'UP (User Priority) tels que présenté dans la figure 2.5.

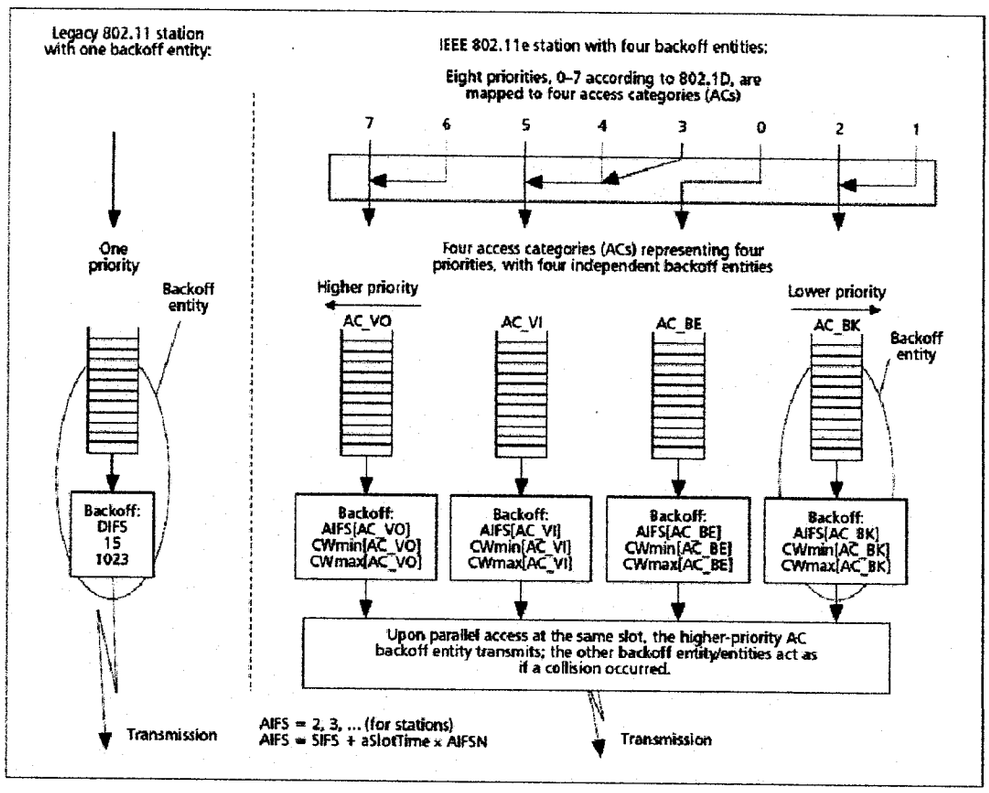


Figure 2.5. La station 802.11 et la station 802.11e avec quatre AC dans une seul station

En remarque dans la figure que DIFS est remplacer par AIFS [AC], avec

$$AIFS\,[AC] = SIFS + AIFSN\,[AC] \times SlotTime \text{ ou } AIFSN \geq 2,$$

Avec AIFS [AC] ≥ DIFS, et AIFSN [AC].

Et que CWmin [AC], CWmax [AC] varient avec les AC (audio < vidéo < données). Facteur de persistance PF différent par AC au début, puis fixé a la valeur 2 par la suite, avec $CWnew = (CWold + 1) \times PF - 1$. *[9]*

VIII.2. Le mode HCCA

Dans le mode HCCA (*HCF Controlled Channel Access*), l'intervalle entre deux trames de balise (*beacon frame*) est divisé en deux périodes CFP (*Contention Free Period*) et de CP (*Contention Period*), le HCCA permet aux CFP de transmettre à n'importe quel temps pendant CP. Ce mode ne peut être utilisé que dans un mode Infrastructure où il y a un point d'accès AP (*Access Point*).

La transmission avec HCCA peuvent se résumer de la manière suivante La station HC interroge les stations en fonction des paramètres liés à la qualité de service (QoS) ; celles-ci répondent avec ou sans les données qu'elles souhaitent envoyer. Deux scénario de transmission sont alors possible soit le HC transmet les données reçues à leurs destinataires dans un ordre qu'il définit ; soit il distribue des TXOP aux QSTA en fonction de leurs priorités, afin qu'elles puissent transmettre les données elles mêmes. La figure 2.6 présente les deux périodes et illustre le fait que toutes les stations n'ont pas le même temps de transmission. [9]

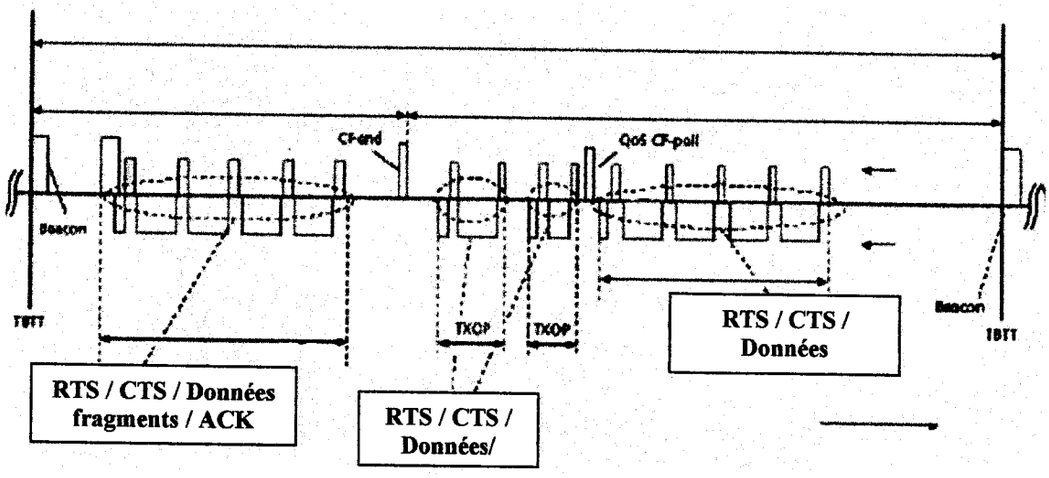


Figure 2.6. Super-trame 802.11, utilisation des TXOP.

VIII.3. Autres mécanismes

VIII.3.1. DLP (Direct Link Protocol)

Dans l'ancien standard, une station ne peut pas envoyer d'information directement à une autre station sans passer par l'AP dans le mode infrastructure. D'un autre coté, dans l'IEEE802.11e, un nouvel protocole DLP est introduit pour qu'une QSTA soit capable de manipuler des communications directes avec d'autres stations en mode infrastructure, ce qui augmente d'une façon significatif l'utilité de la bande passante.

Avec DLP, l'émetteur envoie en premier un message de demande DLP incluant les débits supportés et d'autres informations au récepteur à travers l'QAP. Lorsque le récepteur acquitte cette demande, une liaison direct est établit entres ces deux QSTAs.

S'il n'existe pas de transmission de trame entre les deux QSTAs pour une durée de DLPtimeOUT, la liaison directe est annulée. Dans ce cas, les trames entre ces deux stations reviennent à travers le QAP.

Cependant avec le DLP, le trafic entre les deux stations ne sera pas enregistré dans le QAP pour la diffusion, ce qui entraine l'activation du mode « enregistrement de puissance » dans les stations fréquemment et réduit l'efficacité du « enregistrement de puissance » en absence de DLP.

VIII.3.2. CFB (Contention Free Bursts)

La méthode **CFB** permet à une station (QoS station) ou un AP (QoS AP) d'envoyer plusieurs trames immédiatement sans chercher à accéder au canal de nouveau.

La station (ou bien l'AP) continue à transmettre après un temps SIFS dans la limite du créneau de transmission TXOP qui lui est accordé.

La méthode CFB améliore beaucoup les performances en réduisant les backoffs et les overheads associés aux DIFS.

CFB permet surtout d'améliorer le débit de la carte 802.11g dans un environnement mixte avec la 802.11b .La station 802.11g qui est donc plus rapide peut transmettre plusieurs trames dans une période où la station 802.11b ne peut transmettre qu'une seul trame.

VIII.3.3. Block d'acquittement "Block Acknowledgement"

La sous-couche MAC, est basée sur un simple schéma SW-ARQ. Ce qui implique beaucoup d'ajout dans les entêtes du à la transmission immédiate des ACKs. Un nouveau mécanisme de SW-ARQ, nommé Bloc d'acquittement (Block ACK) est utilisé pour améliorer la couche MAC à été proposé dans la norme IEEE 802.11e. Dans ce mécanisme, un groupe de trames de données peuvent être transmises une par une séparées par l'intervalle SIFS. Ensuite, une seule trame de block d'acquittement est transmise vers l'émetteur pour l'informer du nombre de trames transmises correctement. Evidemment, ce schéma peut améliorer l'efficacité du canal.

- **Le schéma DCF**

Dans le schéma DCF, l'émetteur transmet une trame après la transmission de trame de données le récepteur doit examiner une moyenne d'inactivité pour l'espace de distribution inter-trame (DIFS), plus la durée de backoff. Si ce cadre est bien reçu, le récepteur renvoie un accusé de réception (ACK) après une période SIFS, qui est l'intervalle nécessaire par la couche physique (PHY). Toutes les autres stations diffère l'affirmation du canal jusqu'à la fin de la transmission ACK. Après cela, le récepteur et toutes les autres stations diffèrent une durée DIFS avant les prochaines transmissions.

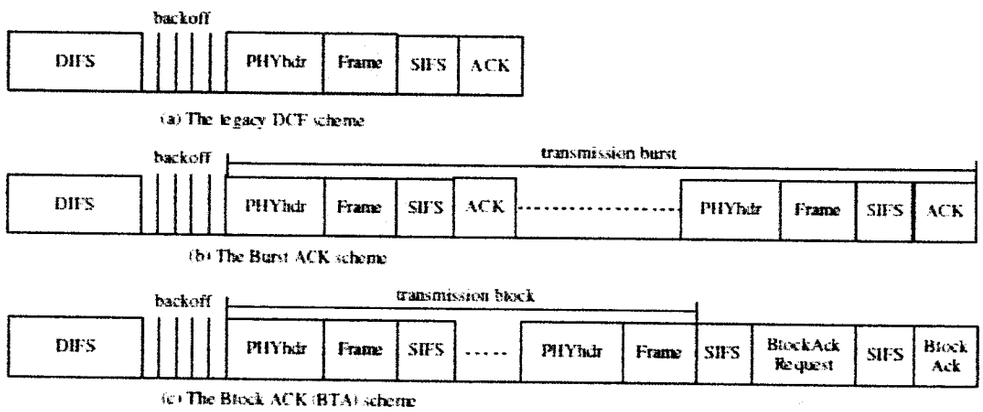


Figure 2.7. Schéma DCF et le BlockACK.

- **Il y a deux types de BlockAck utilisés dans le 802.11e immédiat et différé**

Dans le cas du BlockAck immédiat, l'émetteur transmet une trame de demande BlockAck après la transmission d'un groupe de trames de données ; le récepteur doit, par conséquent, retourner le BlockAck après un délai de SIFS. Si l'émetteur reçoit la trame BlockAck, il retransmet les trames de données non acquittées avec le BlockAck. Le mécanisme BlockAck immédiat est très utilisé par les applications qui demandent une bande passante très grande avec une latence faible. Cependant. Il est très difficile de l'implémenter pour générer un BlockAck dans l'intervalle SIFS.

D'un autre coté, le BlockAck différé ne requiert pas cette limitation stricte en timing. Avec ce type de mécanisme, le récepteur est autorisé, en premier lieu, à envoyer une trame d'acquittement normale pour acquitter la demande BlockAck. Ensuite, le récepteur peut retourner le BlockAck à n'importe quel moment à contrainte de

n'excéder jamais le BlockAckTimeOut. Le mécanisme de BlockAck différé est utilisé pour les applications qui tolèrent une latence modérée. Si l'émetteur n'a pas reçue le BlockAck ou la trame d'acquittement normale par le récepteur, il transmettra la trame de demande BlockAck. Lorsque le nombre de retransmission de demande BlockAck atteint son maximum, la totalité des trames de données déjà envoyées seront rejetées. [6]

Conclusion

Ce deuxième chapitre a abordé le principe de base de la conception des réseaux sans file qui était le service basé sur le best effort, ce dernier ne répond pas aux exigences actuelles des applications (multimédia) en terme de délai et de latence et surtout ne garantie pas la qualité de service.

L'introduction du concept de la QoS dans la 802.11 a donné naissance à la norme 802.11e et a introduit les mécanismes EDCA et HCCA et d'autres mécanismes pour l'amélioration des protocoles existants afin de supporter une différenciation des flux (DiffServ). Ceci a permis d'intégrer le wifi dans les protocoles et modèles de QoS de l'internet.

Chapitre 3. Simulation et résultats

I. Introduction

Avec l'évolution rapide et continue des systèmes informatiques dans les réseaux sans fil, ceci rend ces systèmes de plus en plus complexes. Les besoins des systèmes de communication en terme d'interopérabilité, de passage en échelle, de sécurité et de performance (délai de bout en bout, utilisation des ressources, débit...) compliquent la maintenance et la mise en œuvre de ces systèmes. En plus de la complexité des problèmes concernés et la grande diversité des architectures rencontrées, de nombreuses solutions sont envisageables pour un même problème. Chacune des solutions envisagées doit être testée, évaluée, caractérisée et critiquée avant d'envisager son implémentation concrète dans un réseau. La simulation nous permet d'effectuer ces tests à moindres coûts. La simulation permet ainsi de tester sans aucun coût ces nouvelles technologies, les nouveaux protocoles mais aussi d'anticiper les problèmes qui pourront se poser dans le futur.

Le standard 802.11e adopté, pour introduire de nouveaux mécanismes de QoS, n'a pas fait toutes ses preuves et la recherche dans ce domaine reste active. Dans notre PFE, on a simulé le mécanisme d'acquittement groupé (Block Acknowledgement) selon différentes valeurs, le but est de distinguer leur impact sur la Qualité de service et les performances du réseau en général. Les résultats de simulation seront analysés, par l'intermédiaire d'une comparaison entres les différents scénarios.

II. C'est quoi la simulation ?

La simulation consiste à représenter par un programme informatique un réseau, et un scénario d'utilisation de ce réseau afin de recueillir des statistiques permettant d'évaluer le fonctionnement d'un mécanisme donné. C'est donc une approche technique permettant d'anticiper les problèmes qui pourraient surgir au niveau pratique et d'implémenter la technologie la mieux adaptée aux besoins.

La simulation est la méthode la plus utilisée pour estimer les performances et le comportement des réseaux informatiques. Elle est préférable aux méthodes analytiques, car elle permet d'interpréter d'une façon plus simple le comportement des réseaux, sans pour cela perdre en exactitude. De nombreux logiciels de simulation à événement discrets sont utilisés pour l'évaluation des performances des réseaux informatiques. Le simulateur le plus connu dans le monde universitaire qui est le **NS** (Network Simulator), d'autres logiciels connus dans ce domaine sont :

-OPNET (Optimum Network Performance).

-QNAP/Modline.

-MATLAB, MAPPLE, MATHEMATICA : pour le calcul numérique et l'évaluation complexe.

III. NS-3 Network Simulator

Network Simulator 3 (NS-3) est un nouveau logiciel de simulation de réseaux informatiques (n'est pas une extension de NS-2) qui est écrit entièrement en C++ ou Python, Les résultats de certaines simulations sont visualisés dans des fichiers ".pcap" qui peuvent être utilisés par d'autres applications pour analyser les traces.

IV. Présentation de la plate forme de travail

Nos simulations ont été faites sous NS-3, il faut savoir que la version FEDORA-12 de Linux est la seul version qui intègre l'installation de NS sans problème, car d'autres versions nous ont posées des problèmes de variables d'environnement.

Puisque Windows est la plateforme la plus largement utilisée, NS-3 dispose d'une solution pour ceux qui veulent utiliser cet environnement, grâce à la **Virtualisation permettant** d'utiliser le système Linux sous Windows en tant que machine virtuelle. Il existe actuellement plusieurs systèmes de virtualisation, deux des plus populaires sont **VirtualBox** et **VMware**.

Pour intégrer le package NS sous fedora, il faut :

1. Télécharger le package ns-allinone-3.10.tar en exécutant la commande suivante dans un terminal :

wget http://www.nsnam.org/releases/ns-allinone-3.10.tar.bz2

2. Le décompresser dans le répertoire de travail préféré :

   tar xjf ns-allinone-3.10.tar.bz2

3. Puis l'installer en exécutant la commande : ./build.py
4. La commande ./waf permet de configurer et de construire le projet NS-3

V. Simulation

Chaque scénario écrit ; décrit un réseau se composant d'un point d'accès et six stations en mode infrastructure et se situant dans le même BSS, chacune des stations transmet des flux audio+vidéo et donnée (Best Effort). NS3 intègre le mécanisme BA (Block Acknowledgement) dans les modules dont il dispose pour simuler les réseaux Wifi, chose qui n'était pas possible sous NS2, ce module permet de changer le nombre de trames à acquitter ensemble et pour chaque catégorie de trafic indépendamment des autres. Donc, si le nombre de paquets regroupés dans la file atteint cette valeur, Block Ack va transmettre cet acquittement groupé. Le but de cette simulation c'est de mettre en évidence l'influence de ce mécanisme sur les paramètres de QOS des différents trafics. Pour cela, on s'intéresse aux valeurs des paramètres de QOS suivants pour les trois types de trafics que sont l'audio, la vidéo et les data et deux paramètres décrivant les performances globales du réseau en entier :

-Débit de transmission.
-Le nombre total de collision.
-Le taux d'utilisation du réseau.
-La latence des applications dans le réseau.

NS3 génère des résultats sous la forme d'un fichier trace. Wireshark a été conçu et mis en place pour analyser ce dit fichier et en déduire les paramètres qui nous intéressent comme le débit total de réseau ainsi que le débit de chaque station du réseau test, le taux de collisions et la gigue observée pendant la simulation. En outre, l'analyseur génère un fichier texte avec des statistiques comme on va le voir ci-dessous. Donc, après l'extraction des résultats de chaque scénario, il ne reste plus qu'à dessiner les graphiques correspondants dans MATLAB.

-Scénario 1 sans BA

Dans ce premier scénario, le mécanisme d'acquittement groupé n'est pas activé, c'est-à-dire chaque trame est acquittée individuellement, ce qui va infailliblement créer de l'overhead dans le réseau, et donc va influer sur la QOS des trafics et les pénaliser. Ces stations sont disposées, de façon à ce qu'il n'y ait pas de stations cachées afin d'optimiser le débit. Il n'y a pas non plus de mobilité des stations et les trafics générés possèdent les caractéristiques suivantes :

Parametres	**Audio PCM**	**Vidéo CBR**	**Data**
CWmin	7	16	32
CWmax	15	31	1023
AIFSN	1	1	2
Packet Size (Bytes)	160	1280	1600
Packet Interval (ms)	20	16	12.5
Sending Rate (KB/s)	8	80	128

SIFS	16 µs	**PHY hdr**	20 µs
DIFS	34 µs	**Propagation Delay**	1 µs
PHY rate	54 Kb/s	**CWmin**	16 µs
Slot Time	9 µs	**CWmax**	1023 µs

Tableau 3.1. Les paramètres de simulation

-Scénario 2 avec BA

La simulation consiste à modifier la valeur du block ack de la valeur 1, à la valeur de 6 blocs pour le deuxième scénario et à 10 blocs pour le troisième scénario. La figure ci-dessous donne la topologie du réseau simulé

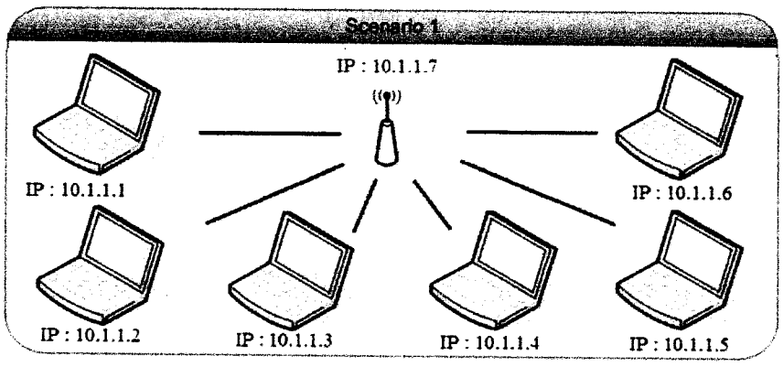


Figure 3.1. Topologie du réseau simulé

VI. Résultats de Simulation

Le débit de transmission et latence des données de type data, audio et vidéo

A. Simulation 1 avec une valeur de BA de 1

Lors de cette simulation, le trafic UDP est généré à partir des stations avec un débit moyen de 0.477 Mbps. Les statistiques obtenues en résultats sont présentés dans le tableau suivant:

Variable	Résultat
Débit moyen de chaque station	488.6 Kb/s
Nombre de Collisions	118
Transmissions sans Collisions	1546
% de Collisions	7.09%

Tableau 3.2. Résultat de la 1ère simulation

B. Simulation 2 avec activation du BA à une valeur de 6

Lors de cette simulation, le trafic UDP est généré à partir des stations avec un taux moyen de transmission de 0.545 Mbps. Les résultats sont présentés dans le Tableau suivant:

المكتبة

Variable	Résultat
Débit moyen de chaque station	558.1 Kb/s
Nombre de Collisions	89
Transmissions sans Collisions	1565
% de Collisions	5.38%

Tableau 3.3. Résultat de la 2ème simulation

C. Simulation 3 avec activation du BA à une valeur de 10

Lors de cette simulation, le trafic UDP est généré à partir de la station avec un taux de 0.542 Mbps. Sa sortie a obtenue des statistiques sur le débit et le délai. Les résultats sont présentés dans le Tableau suivant:

Variable	Résultat
Débit moyen de chaque station	555 Kb/s
Nombre de Collisions	92
Transmissions sans Collisions	1560
% de Collisions	5.56%

Tableau 3.4. Résultat de la 3ème simulation

VII. Discussion des résultats

a- Le débit de transmission des données

Une première conclusion s'impose à la lecture des trois tableaux précédents, ou on remarque une diminution significative du taux de collisions qui passe de 7% à 5% en augmentant la valeur des ack de 1 à 10. Et une amélioration du débit du trafic moyen.
Les graphes présentés ci-dessous représentent les résultats de simulation des trois scénarios pour les trois types de trafics énoncés ultérieurement qu'on va comparer.

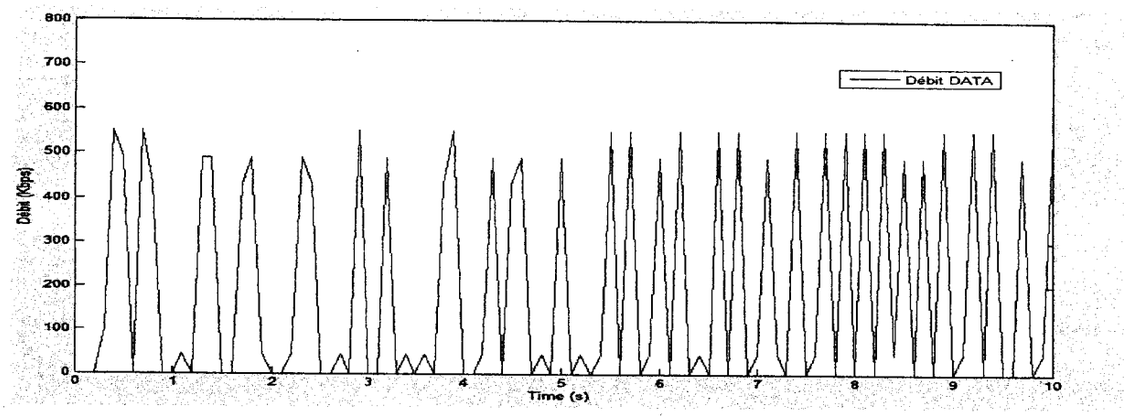


Figure 3.2. Débit de transmission des données sans BA

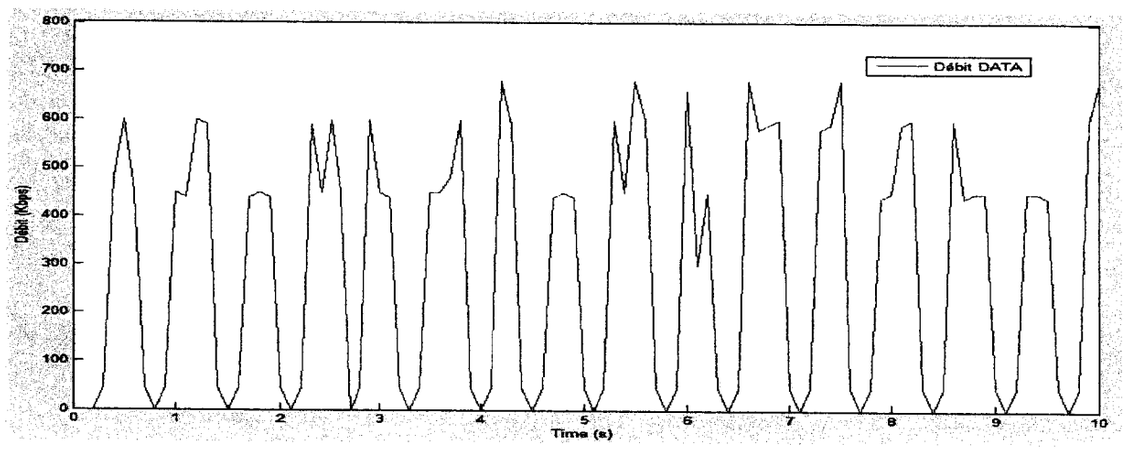


Figure 3.3. Débit de transmission des données avec BA de 6

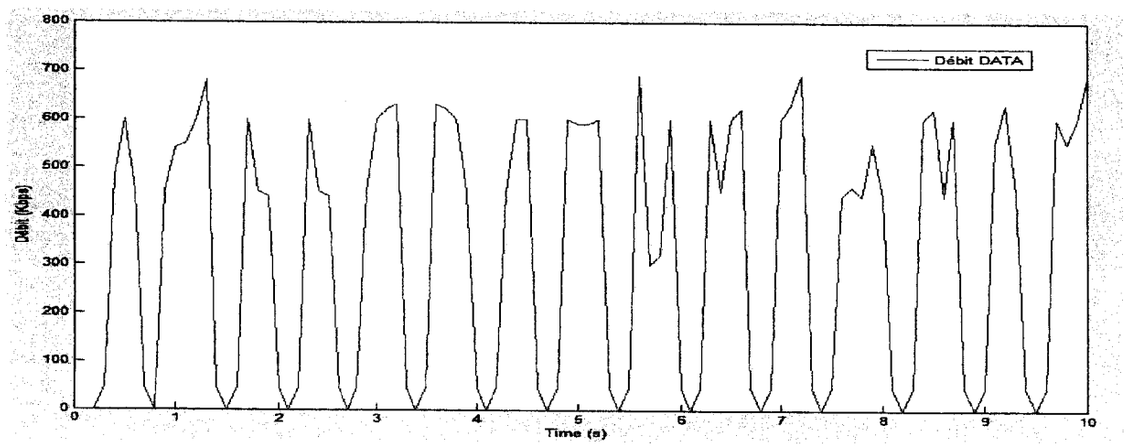


Figure 3.4. Débit de transmission des données avec BA de 10

On remarque une nette amélioration du débit global du réseau pour le trafic data, surtout pour les grandes valeurs du bloc ack. On remarque que le débit atteint jusqu'à 700Kbps pour une valeur de BA de 10, pour 550Kbps quant la valeur du BA est de 1 seulement.

b- Le débit et latence audio

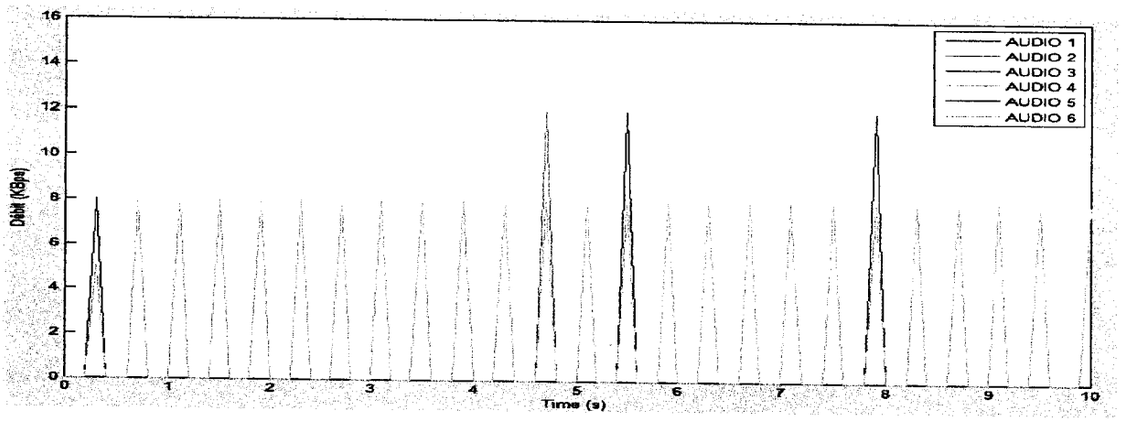


Figure 3.5. Débit audio sans BA

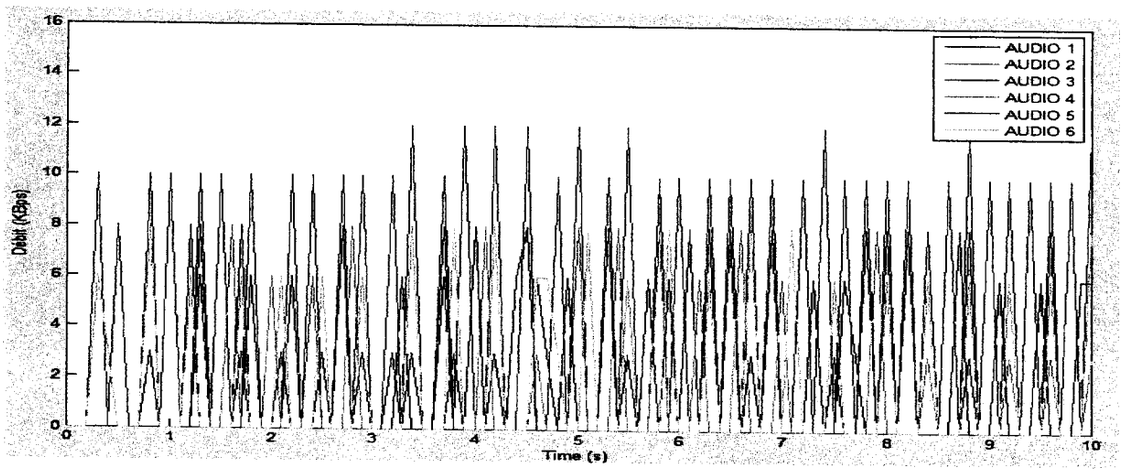


Figure 3.6. Débit audio avec BA d'une valeur de 6

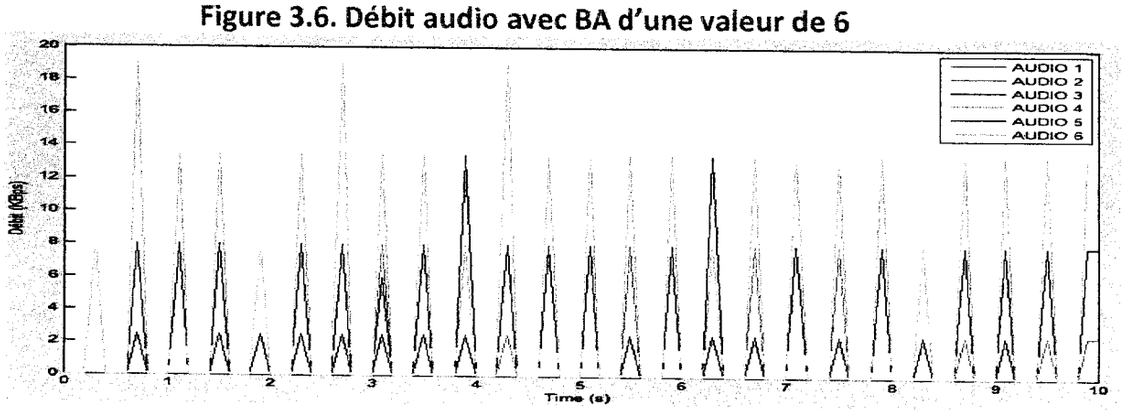


Figure 3.7. Débit audio avec BA d'une valeur de 10

La même remarque s'applique au débit du trafic audio qui augmente quant on augmente la valeur des ack, de 8 à 18 KBps, donc l'influence des acquittements groupés se voient nettement ici.

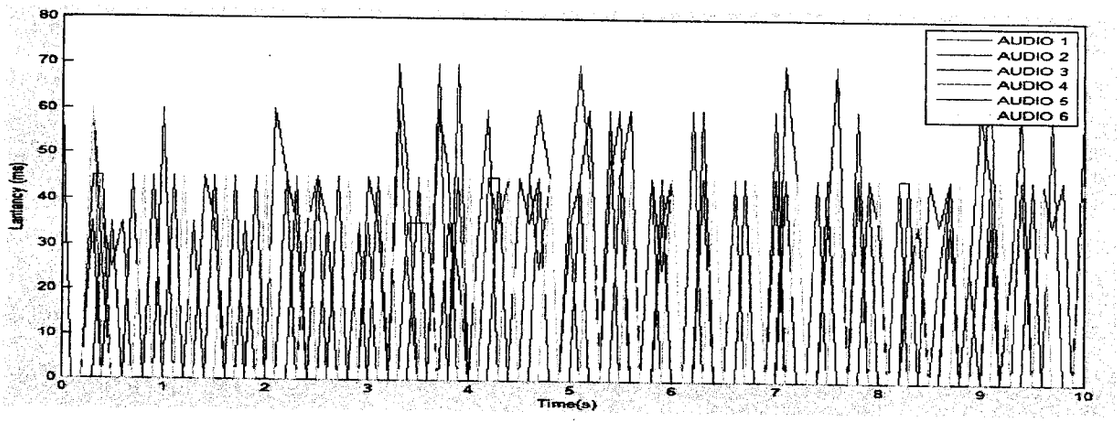


Figure 3.8. Latence audio sans BA

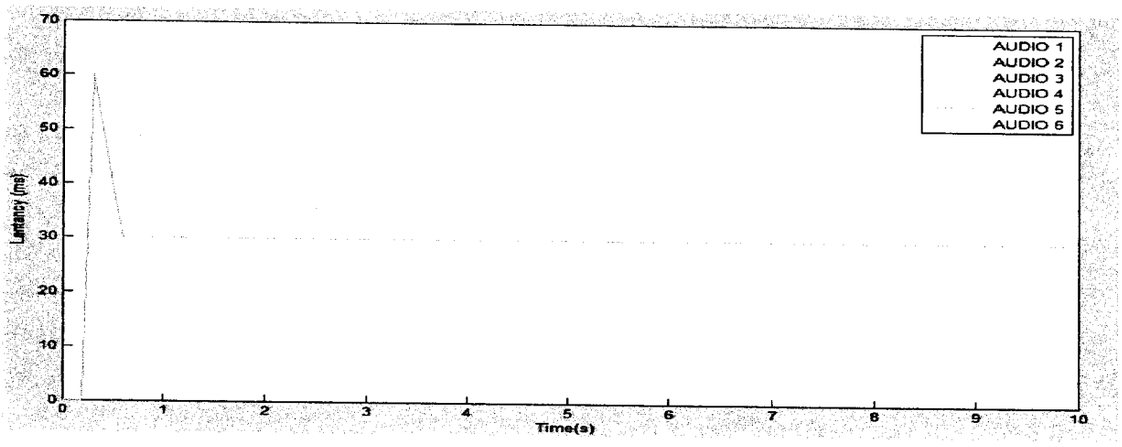


Figure 3.9. Latence audio avec BA d'une valeur de 6

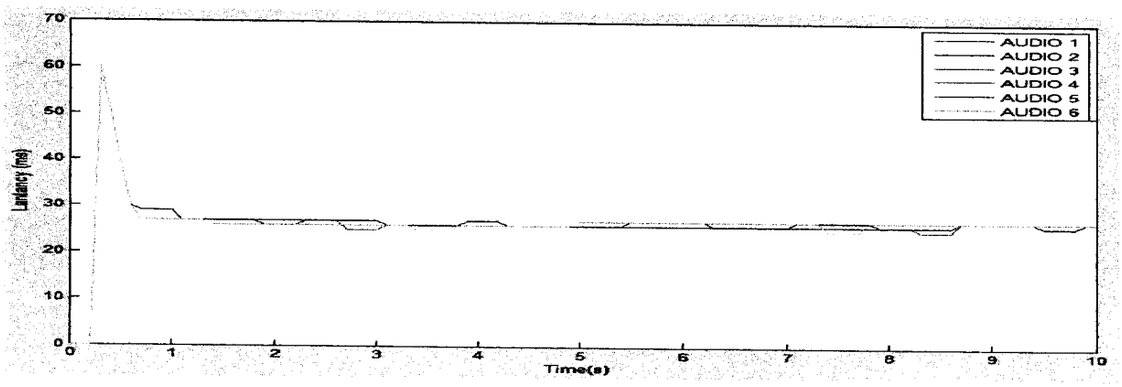


Figure 3.10. Latence audio avec BA d'une valeur de 10

Dans les graphes ci-dessus, on remarque que la latence se stabilise à une valeur de 30ms quant on active le BA, alors qu'elle fluctue très vite et tout le temps pendant la désactivation du BA et atteint parfois jusqu'à 70ms. Chose qui va dégrader grandement la qualité des transmissions audio, qui est une application très sensible quant à la latence.

c- Le débit et latence vidéo :

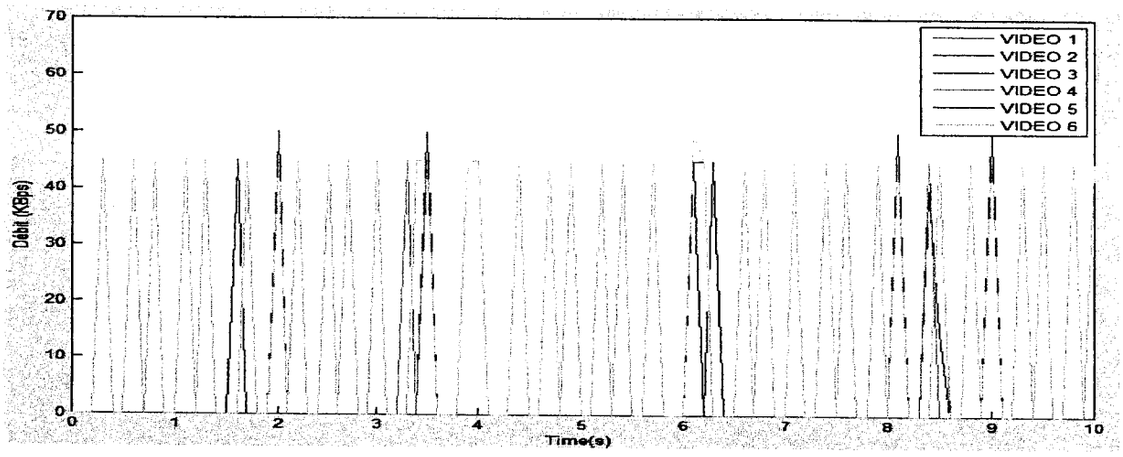


Figure 3.11. Débit vidéo sans BA

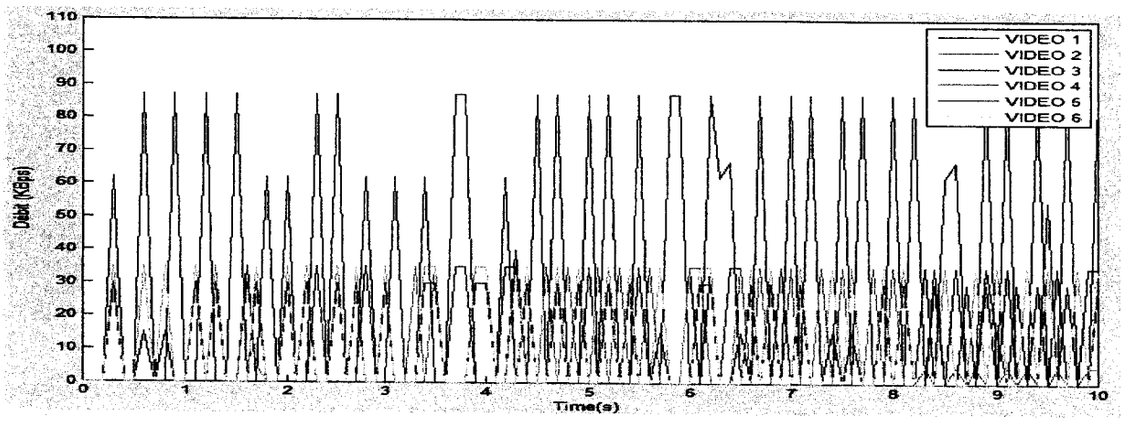


Figure 3.12. Débit vidéo avec BA d'une valeur de 6

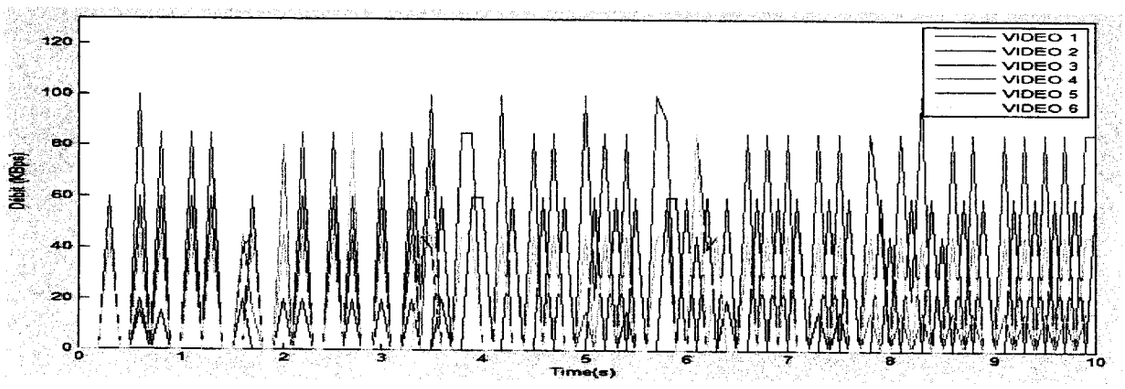


Figure 3.13. Débit vidéo avec BA d'une valeur de 10

Le débit du trafic vidéo qui est une caractéristique importante pour juger de la QOS de ce type de trafic s'améliore avec l'activation du BA, comme on peut le constater sur les figures ci-dessus.

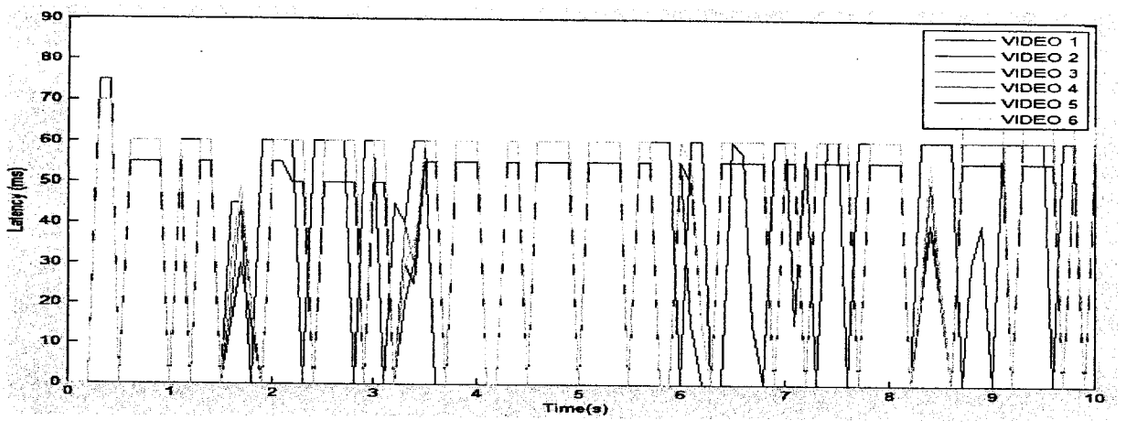


Figure 3.14. Latence vidéo sans BA

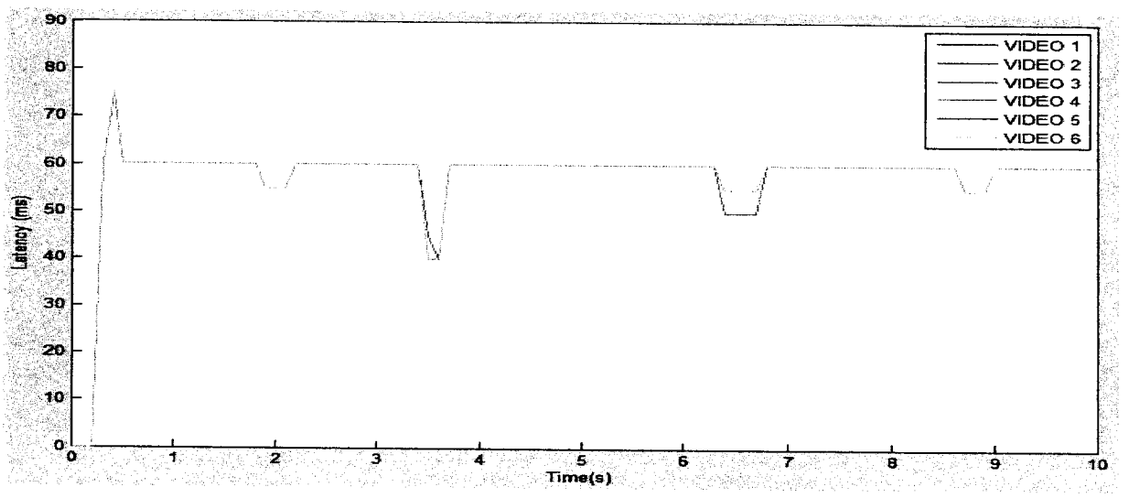


Figure 3.15. Latence vidéo avec BA d'une valeur de 6

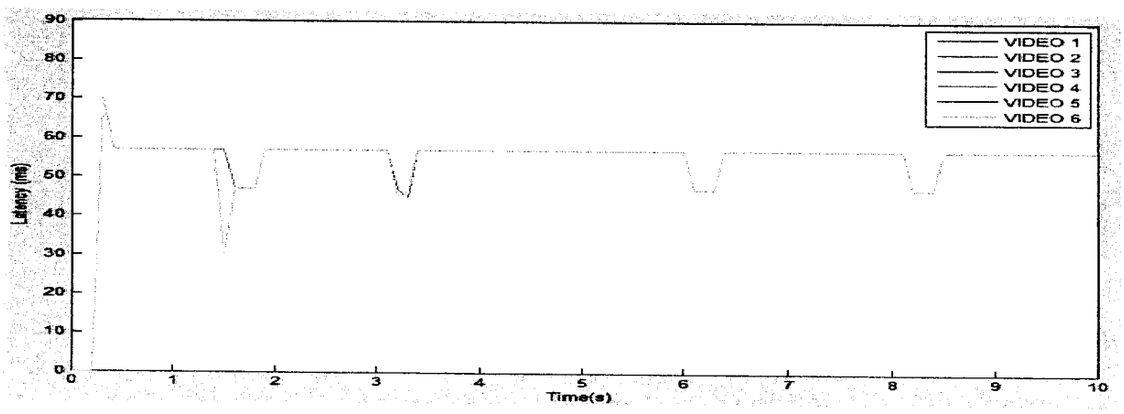


Figure 3.16. Latence vidéo avec BA d'une valeur de 10

Comme pour la latence audio, la latence vidéo se stabilise dans le cas de l'activation du BA, tout en restant majoré par une valeur de 70ms, alors que dans le premier scénario, la latence fluctue trop souvent.

Conclusions

Dans ce chapitre, on a simulé l'influence et l'impact qu'a le mécanisme de l'acquittement groupé sur les performances globales du réseau, en termes de diminution du nombre de collisions et augmentation du débit. On a réussi à démontrer l'avantage certain qu'apporte ce mécanisme dans le gain de ressources du réseau et l'amélioration de la QOS des différents trafics. Donc la gestion de la QOS s'en trouve facilitée et plus facilement garantie. Nous conseillons donc fortement les constructeurs informatiques de matériel WIFI d'intégrer ce mécanisme dans leur politique d'amélioration de la qualité de service.

Conclusion générale

L'objectif de ce mémoire, était d'étudier les problèmes liés à la gestion de la qualité de service dans des environnements sans fil.

IEEE 802.11 est la norme des réseaux locaux sans fil la plus déployée mais elle ne garantit pas une qualité de service suffisante pour les différents types de service. De ce fait, le groupe de travail 802.11 a mis en œuvre une nouvelle version de la norme 802.11 à savoir la norme 802.11e qui a pour but de garantir la qualité de service pour les utilisateurs et pour les applications multimédias.

Dans ce contexte, l'introduction du protocole BA (Bloc Acknoledgment) au niveau MAC afin d'améliorer la qualité de service s'avère importante. Notre but s'articule autour de cette analyse des problèmes de garantie de qualité de service dans les réseaux 802.11 et de l'apport de la norme 802.11e.

Une solution est de jumeler le protocole de contrôle d'accès au médium avec un mécanisme de contrôle des flots émis par les différentes stations. Il serait alors possible de s'assurer que les services à forte contrainte de latence sont bien utilisés par des applications multimédias. Ce type de vérification, complète certaines études récentes visant à détecter de mauvais comportements des utilisateurs dans les réseaux wifi ou à estimer les ressources des WLAN consommées par chaque utilisateur. Les protocoles de qualité de services devront donc s'efforcer d'évaluer au mieux l'état du réseau afin de ne pas sur ou sous-évaluer sa capacité mais devrons aussi être adaptatif afin de réagir rapidement et efficacement à la mobilité de ces réseaux. Dans notre travail, on a étudié un nouveau mécanisme de qualité de service le BA qui consiste à acquitter un certain nombre de trames par un seul ACK, qu'on appelle le ACK groupé et qui peut varier d'un réseau à l'autre. Cette possibilité peut potentiellement augmenter la largeur de bande disponible pour la communication des stations. Puis on a comparé en utilisant la simulation le comportement d'un réseau infrastructure sans BA et un réseau avec le BA activé et on a remarqué l'efficacité de ce protocole, puisque les performances du réseau s'améliorent nettement. Donc on aurait tendance à conseiller aux constructeurs d'implémenter ce mécanisme dans les AP, car il a une nette influence sur les performances globales du réseau et des paramètres de qos des trafics temps réel en particulier.

Annexe A. Le simulateur NS-3

Le simulateur NS et sa structure :

1. Cadre général :

Le logiciel NS est un simulateur de réseau à événement discrets. Il est utilisé principalement pour la recherche Internet. Le projet NS3 est créé en 2006, il est un projet qui s'efforce de maintenir un environnement ouvert pour les développeurs « open-source », de partager leurs logiciel. Sa documentation est disponible sous quatre formes :

- NS-3 Doxygen/Manual : Documentation de publique APIs du simulateur.
- Tutorial.
- Reference Manual : Manuel de référence.
- NS-3 wiki.

Le NS-3 n'est pas une extension de NS-2, c'est un nouveau simulateur. Ces deux derniers sont écrits en C++, mais NS-3 est nouveau simulateur qui ne supporte pas les API de NS-2. Par contre quelques modèles de NS-2 sont introduits sur le NS-3.

2. Structure du simulateur :

Le simulateur NS est développé suivant un modèle orienté objet, avec une architecture modulaire, ce qui rend la modification et l'extension du simulateur relativement facile.

Le Simulateur de réseau NS-3 est écrit comme une bibliothèque qui peut être statique ou dynamique par le langage C++, qui définit la topologie du simulateur. Il est constitué d'un système de gestion de code source Mercurial **SCM** (Software Configuration Management) avec des librairies qui exporte la totalité de ses API par Python, ce qui permet au Python script d'importer une grande partie de module NS-3 dans une même manière que les bibliothèques de NS-3, qu'elles sont liée par les programme en C++. Donc, les programmes de simulation sont le code C++ ou le Python script, l'utilisation du système de construction Waf pour la configuration du simulateur NS-3.

3. L'organisation du NS-3 :

Le code source de NS-3 est organisé dans un sous répertoire 'src' et peut être décrite par le schéma suivant. Nous décrivons d'abord le cœur du simulateur, les composants qui sont communes à tous les protocoles, le matériel et les modèles de l'environnement. Le noyau de simulation est mis en œuvre dans 'src/core'. Les paquets sont des objets fondamentaux dans un simulateur de réseau et sont mises en œuvre dans 'src/réseau'. Ces deux modules de simulation sont destinés à comprendre un noyau de simulation générique qui peut être utilisé par différents types de réseaux. En plus de ce qui précède les bases de NS-3, nous introduisons, également deux autres modules qui complètent le noyau C + + basé sur l'API. Le NS-3 peut accéder à toutes les API directement afin que *l'API* fournisse une interface commode ou encapsulation des API de bas niveau.

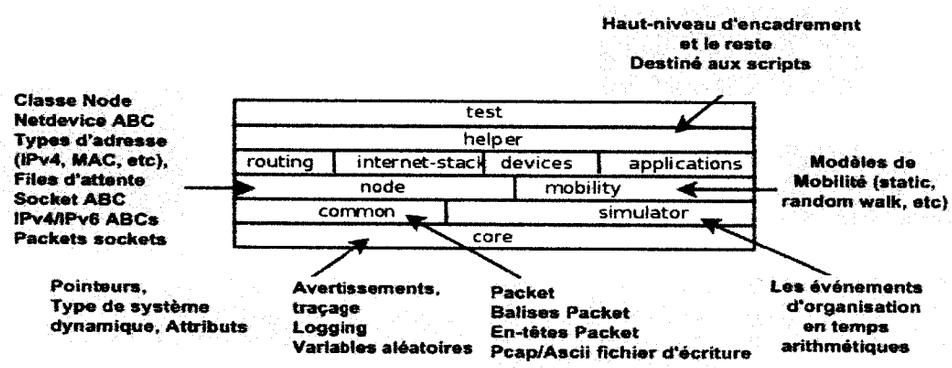


Figure 1. L'organisation du logiciel NS-3.

4. Environnement de développement :

Les scripts dans le NS-3 on réaliser en C + + ou Python. Au NS-3.2, la plupart des *API* NS-3 sont disponible en Python, mais les modèles dans les deux cas sont écrits en C + +. Il y a certain temps pour examiner les concepts les plus avancés ou peut-être les caractéristiques du langage familier, des idiomes et des design patterns tels qu'ils apparaissent.

Le NS-3 utilise plusieurs composantes de la GNU "toolchain" pour le développement. Le logiciel ToolChain est un ensemble des outils de programmation disponibles dans un environnement donné. Le NS-3 utilise aussi **gcc**, **binutils** GNU, et **gdb**. Cependant, nous n'utilisons pas la GNU construire des outils système, nous

utilisons Waf pour ces fonctions. Typiquement, le NS-3 se réalise sous Linux ou sous un environnement semblablement à se système. Pour ceux fonctionnant sous Windows, il existe des environnements qui simulent l'environnement Linux à des degrés divers. Le NS-3 appuie le développement dans l'environnement Cygwin pour ces utilisateurs.

5. Concept de base :

En premier nous devons faire avant de commencer à regarder ou écrire le code NS-3 et d'expliquer ces concepts de base et quelques abstractions dans le système.

- **Clé d'abstractions:**

Dans cette section, nous passerons en revue de quelques termes qui sont couramment utilisés dans les réseaux, mais elles ont une signification particulière dans NS-3.

- **Node:**

En NS-3, le dispositif d'abstraction de base est appelé le nœud. Cette abstraction est représenté en C + + par la classe 'Node'. Cette classe fournit des méthodes pour gérer les représentations des dispositifs de calcul dans les simulations. L'utilisation d'un nœud comme un ordinateur sur lequel nous pouvons ajouter des fonctionnalités.

- **Application:**

Dans le concept de base, un programme peut génère une certaine activité à les simuler. Ce concept est représenté en C + + par une classe 'Application'. La classe Application fournit des méthodes pour gérer les applications représenté de notre version au niveau d'utilisateur pour les simulations. En utilise des spécialisations de classe d'application appelé **UdpEchoClientApplication** et **UdpEchoServerApplication**. Ces applications forment une configuration client/serveur et utilisé pour générer des paquets d'écho sur le réseau simulé.

- **Channel:**

La classe Canal fournit des méthodes pour la gestion des nœuds qui se communique. Les canaux peuvent également être spécialisés par les développeurs dans la programmation. Le canal spécialisé peut modéliser des choses aussi compliqué qu'un commutateur Ethernet de grande taille ou d'un espace en trois dimensions sur les

réseaux sans fil. Nous allons utiliser des versions spécialisées appelée **CsmaChannel**, **PointToPointChannel** et **WifiChannel**. Le CsmaChannel, est un modèle d'un sous-réseau de communication qui met en œuvre une détection de porteuse d'accès moyen. Cela nous donne la fonctionnalité Ethernet-like.

- **Net device:**

En NS-3, le dispositif de net couvre à la fois le pilote et le matériel de simulation. Un dispositif de net est installé dans un nœud afin de permettre ce nœud de communiquer avec d'autres nœuds pour une simulation. Le Net Devices est représenté en C + + par la classe 'netdevice'. Cette classe fournit des méthodes pour gérer les connexions entre le nœud et le Canal, et peuvent être spécialisés par les développeurs. Nous allons utiliser le netdevice de plusieurs versions appelé **CsmaNetDevice**, **PointToPointNetDevice** et **WifiNetDevice**.

- **Topology Helpers:**

Dans un véritable réseau, vous trouverez des ordinateurs (hôtes) intégré. En NS-3, on dirait que vous trouverez des nœuds avec le NetDevices. Pour la simulation d'un vaste réseau vous aurez besoin d'organiser de nombreuses connexions entre les nœuds, NetDevices et canaux. Depuis la connexion NetDevices à un nœud, aux canaux et à l'attribution des adresses IP, sont des tâches communes dans NS-3, nous fournissons ce que nous appelons *Topology Helpers* pour le rend aussi facile. On prend de nombreuses opérations comme *distinctes NS-3* pour créer un netdevice, ajouter une adresse MAC, installer le périphérique sur un nœud, nœud configurer la pile de protocole, puis connectez le netdevice à un canal.

Conclusion

Le simulateur de réseaux NS est un système complexe. Il est impossible de couvrir toutes les scripts et astuce pour bien savoir à le manipuler. Toutefois, le NS est le meilleur simulateur de réseaux et téléchargeable gratuitement, se présente beaucoup d'avantages par son utilisation du langage C++ et Python qui donne un avantage au développeur du langage C++ par rapport aux autres simulateurs.

BIBLIOGRAPHIE

[1] : AL AGHA Pujolle Vivier, «Réseaux de mobile et réseaus sans fil» , Dunor,2001.

[2] : J.L Mélin, « Qualité de service sur IP » Edition Eyrolles 2001.

[3] : Paul Muhlethaler, « 802.11 et les réseaux sans fil », Edition Eyrolles, 2002.

[4] : KRIM Mourad, « Branchez-vous WiFi », magazine PCMAX juin 2003, page 16 à 19.

[5]: Odom, Wendell, et Michael J. Cavanaugh. 2004. *IP Telephony Self-Study Cisco DQOS Exam Certification Guide*. USA: Cisco Press.

[6] : HOUDA Labiod, Hossam Afifi, « De Bluetooth à WiFi : sécurité, qualité de service et aspect pratiques », Lavoisier, Paris, 2004.

[7] : Rabih Moawad, « QoS dans les WPAN, WLAN et WMAN », Mémoire DEA réseaux et télécommunication, Université Libanaise Saint Joseph Décembre 2004

[8] : LEILA Toumi, « Algorithmes et mécanismes pour la qualité de service dans des réseaux hétérogènes », thèse de doctorat informatique, Systèmes et réseaux , Institut National Polytechnique de GRENOBLE, Décembre 2002.

[9] : Mangold, S., S. Choi, G. R. Hiertz, O. Klein, B. Walke, P. Res et G. Aachen « Analysis of IEEE 802.11e for QoS support in wireless LANs ». *IEEE Wireless Communications,* vol. 10, no 6, p. 40-50, 2003.

[10] : Younes Nadine, « la qualité de services multimédia sur les réseaux AD HOC sans fil à multi-sauts », MONTREAL ,2009.

[11] : BOUAMAMA Nadjib. SAILE Yassine. HAFERSAS Nabil. « Qualité de Service suivant la norme 802.11e » Université de Reims Champagne - Ardenne 2007-2008.

[12]: Mahbubur Rahman, Syed *"Chapter 19 - Mobile Multimedia over Wireless Network"*. Multimedia Networking: Technology, Management and Applications, 2002.

[13]: *Hannan, Xiao* , *Chua Kee Chaing* et *Seah Khoon Guan Winston*. 2003. « Quality of Service Models for Ad Hoc Wireless Networks ». In *The handbook of ad hoc wireless networks Ilyas, M.* CRC press.

SITOGRAPHIE

[14]: http://www.commentcamarche.net

[15]: http://www.wi-fi.org

[16]: http://www.cisco.com

[17]: http://www.isi.edu/nsnam

[18]: http://rubb.free.fr

[19]: http://technet.microsoft.com

[20]: http://www.techno-science.net

[21]: http://www.granddictionnaire.com

[22]: https://enterprise1.opnet.com/tsts/4dcgi/Biblio_FullAbstract?BiblioID=1159