N° d'ordre : 23 / STI / TCO Année Universitaire : 2015/2016

UNIVERSITE D'ANTANANARIVO

ECOLE SUPERIEURE POLYTECHNIQUE

MENTION TELECOMMUNICATION

MEMOIRE DE FIN D'ETUDES

en vue de l'obtention

du DIPLOME LICENCE PROFESSIONNELLE

Mention : Télécommunication
Parcours : Système et traitement de l'information (STI)

Par : **RATSIMBAZAFIMANANA Manoela**

ETUDE DES PERFORMANCES DU RESEAU WIFI AVEC SIMULATION SUR OPNET

Soutenu le Lundi 03 avril 2017 devant la Commission d'Examen composée de :

Président : M. RAKOTOMALALA Mamy Alain

Examinateurs :
M. ANDRIAMANALINA Ando
M. RAVONIMANANTSOA Ndaohialy Dana
Mme ANDRIANTSILAVO Haja

Directeur de mémoire :
M. ANDRIAMIASY Zidora

REMERCIEMENTS

Tout d'abord, j'aimerais remercier le Seigneur de m'avoir toujours donné la force de bien mener la réalisation de ce travail de mémoire.

Ensuite, je tiens à remercier les personnes suivantes sans qui je n'aurais pas pu accomplir ce mémoire parmi lesquelles :

- Monsieur ANDRIANAHARISON Yvon, Professeur titulaire, Responsable du Domaine Science de l'Ingénieur de l'ESPA et à la fois Directeur de l'ESPA ;
- Monsieur RAKOTOMALALA Mamy Alain, Maitre de Conférences, Responsable de la mention Télécommunication
- Je tiens à remercier ma profonde et très sincère reconnaissance à Monsieur ANDRIAMIASY Zidora, Maitre de Conférences, pour m'avoir encadré et qui n'a cessé de me prodiguer de précieux conseils.
- Mes vifs remerciements s'adressent aussi à Monsieur RAKOTOMALALA Mamy Alain, Maitre de Conférences, qui nous a fait l'honneur de présider les membres de jury de ce mémoire.

Je témoigne toute ma reconnaissance aux autres membres du jury qui ont voulu examiner ce travail :

- Monsieur ANDRIAMANALINA Ando, Maitre de Conférences
- Monsieur RAVONIMANANTSOA Ndaohialy Danà, Assistant d'Enseignement et de Recherche
- Madame ANDRIANTSILAVO Haja, Assistant d'Enseignement et de Recherche

Ce travail de mémoire n'aurait pas pu être mené de façon efficace et rigoureuse sans l'aide des différents enseignants et personnels administratifs de l'Ecole surtout au sein de la mention Télécommunication, j'adresse toute ma gratitude.

J'exprime ma très profonde gratitude à ma famille, pour m'avoir soutenu tout au long de la réalisation de ce mémoire. Je reconnais les sacrifices que ces années ont représentés.

Enfin, je ne saurai oublier toutes les personnes qui m'ont aidée de près ou de loin dans l'élaboration du présent mémoire.

Je vous remercie tous et que le ciel vous comblera de bonheur.

TABLE DES MATIERES

ABREVIATIONS

3G	Troisième Génération
4G	Quatrième Génération
ADSL	Asymetric Digital Subscriber Line
AES	Advanced Encryption Standard
ATM	Asynchronous Transfert Mode
AP	Access Point
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CSMA/CA	Carrier Sens Multiple Acces/Collision Avoidance
DCF	Distributed Coordination Function
DFS	Sélection de Fréquence Dynamique
DIFS	Distributed Inter-Frame Space
DS	Distribution System
DSSS	Direct-Sequence Spread-Spectrum
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
FTP	File Transfer Protocol
FDDI	Fiber Distributed Data Interface
FHSS	Frequency Hopping Spread-Spectrum
GSM	Global System for Mobile Communication ou Groupe Spécial Mobile)
GPRS	Global Packet Radio Service
HTTP	Hyper Text Transfert Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industriel, Scientifique et Médical.
LLC	Logical Link Control
MAC	Medium Access Control.
MSDU	Medium Access Control Service Data Unit,
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open system interconnection.
PCF	Point Coordination Function

QoS	Qualité de Service
QAM	Quadrature Amplitude Modulation
RTS/CTS	Request to send /Clear To Send
SIFS	Short Inter-Frame Space
SMTP	Simple Mail Transfert Protocol.
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
WEP	Wired Equivalent Privacy
WIMAX	Worldwide Interoperability for Microwave Access
WIFI	Wireless Fidelity.
WPAN	Wireless Personal Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WWAN	Wireless Wide Area Network

INTRODUCTION GENERALE

Le développement des technologies sans fil offre une alternative, mais surtout une complémentarité intéressante pour le câblage. Le sans-fil présente de multiples facettes tant sur le plan des technologies (Wi-Fi, Bluetooth, WiMax,, satellites, UMTS, laser et etc.) que de ses applications (LAN, WAN, hotspots, etc.).

Mais dans le monde des réseaux, les systèmes sans fil ne sont pas isolés des autres infrastructures. S'appuyant elles-mêmes sur des câblages, les technologies sans fil s'intègrent dans le système de communication des entreprises et des particuliers.

Le marché des réseaux sans fil informatiques est en pleine croissance. De plus en plus d'entreprises investissent dans le sans fil et des opérateurs de télécommunication préparent le terrain pour accueillir de nouvelles technologies. Dans ce monde où même les particuliers disposent d'équipement sans fil, l'entreprise ne peut rester en marge et elle doit transformer son réseau pour satisfaire les nouveaux besoins.

Dans la première partie, plusieurs technologies sans fil sont étudiées afin d'avoir des connaissances sur les réseaux.

Dans la deuxième partie, nous allons voir les généralités sur la technologie wifi et ses différentes normes ainsi que l'architecture du réseau.

La troisième partie concerne la qualité de service dans le wifi et l'introduction à la norme 802.11ac.

Enfin, la dernière partie se concentre sur la simulation et l'interprétation des résultats .Ce travail se concentre sur l'étude de scénario réaliste au moyen de simulation mettant en œuvre une topologie particulière. Les descriptions des outils ainsi que des résultats de simulations sont donnés afin de faciliter la reproduction et la réutilisation des résultats. Les interprétations et les conclusions à propos des simulations permettent de justifier certaines décisions à prendre lors du déploiement du réseau sans fil.

CHAPITRE 1

GENERALITES SUR LES RESEAUX

1.1 Introduction

Malgré sa jeunesse par rapport à d'autre industrie (automobile, transport, aérien,…), l'industrie informatique a fait en peu de temps des progrès spectaculaires. Pendant ces vingt premières années, les systèmes informatiques étaient très centralisés, situés physiquement en général dans une salle. Le concept de salle d'ordinateur comme lieu où les utilisateurs apportaient leurs travaux à traiter est aujourd'hui complètement obsolète. Le modèle ancien d'un unique ordinateur est remplacé par celui d'un ensemble d'ordinateurs séparés mais interconnectés qui exécutent des taches différentes. De tels systèmes sont appelés Réseaux d'ordinateurs**.** [1]

1.2 Définition

C'est un ensemble d'ordinateurs (ou de périphériques) autonomes connectés entre eux et qui sont situés dans un certain domaine géographique. Deux stations sont considérées comme interconnectées si elles sont capables d'échanger de l'information.

Les réseaux sont bien évidemment nés d'un besoin d'échanger de l'information entre les machines. Ainsi une entreprise possédant plusieurs lieux de productions peut avoir un ordinateur sur chaque site, par exemple gérer le stock, paye, production…mais le besoin de communication va inciter le management à connecter ces ordinateurs pour pouvoir extraire et échanger des informations concernant toute l'entreprise. [2]
Dans ce cas beaucoup d'objectifs vont apparaître :

1.2.1 Partage de ressources

Rendre accessible à chaque membre de réseaux les programmes, données, équipements indépendamment de leur localisation physique :

- De partager les fichiers.
- Le transfert de fichier.
- Le partage d'application : compilateur, système de gestion de base de donnée
- Partage d'imprimante.

1.2.2 Grande fiabilité

Duplication des données sur plusieurs sites, ainsi si l'une est inutilisable (panne matérielle de la machine..), on peut utiliser une des copies.
Aussi la présence de plusieurs unités centrales fait que si l'une est en panne les autres peuvent prendre en charge son travail.

1.2.3 Réduction de coûts

Les gros ordinateurs bien qu'ils soient plus performants que les petits ordinateurs sont beaucoup plus cher, l'idée est de construire des systèmes à base de ces derniers afin de réduire le coût même si cela au détriment de la performance.

1.3 Classification des réseaux

On peut classifier les réseaux selon deux aspects : leurs tailles et leurs topologies.
Selon leurs tailles :

1.3.1 Réseaux personnels sans fils (WPAN)

Le réseau personnel sans fil (appelé également réseau individuel sans fils ou réseau domotique sans fil et noté WPAN pour 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 (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fils entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN : Bluetooth, infrarouges,…

1.3.2 Réseaux locaux sans fils (WLAN)

Le réseau local sans fil (WLAN pour 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 , hiperLAN2, …..

1.3.3 Réseaux métropolitains sans fils (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.

1.3.4 Réseaux étendus sans fils (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 fils les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fils. 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)
- Wimax (standard de réseau sans fils poussé par Intel avec Nokia, Fujitsu et Prowim). Basé sur une bande de fréquence de 2 à 11 GHz, offrant un débit maximum de 70 Mbits/s sur 50km de portée, certains le placent en concurrent de l'UMTS, même si ce dernier est davantage destiné aux utilisateurs itinérants.[2]

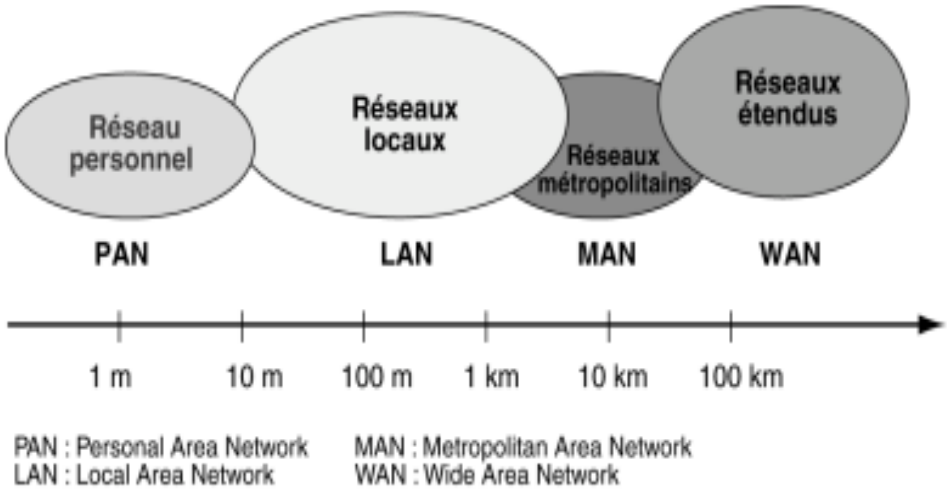


Figure 1.01 : *Les catégories de réseaux sans fil*

Selon leurs topologies :

On peut également différencier les réseaux selon leurs structures et plus précisément leurs topologies : La topologie est l'organisation physique et logique d'un réseau. L'organisation physique concerne la façon dont les machines sont connectées (Bus, Anneau, Étoile, Maillé, ...)

L'organisation logique montre comment les informations circulent sur le réseau (diffusion, point à point).[3]

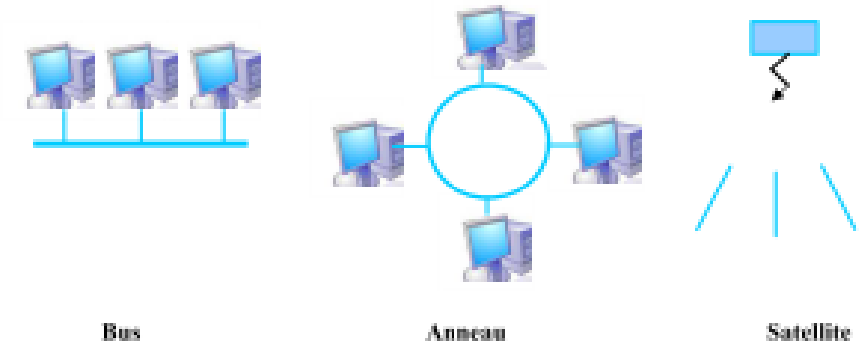


Figure 1.02 : *Réseau en mode diffusion*

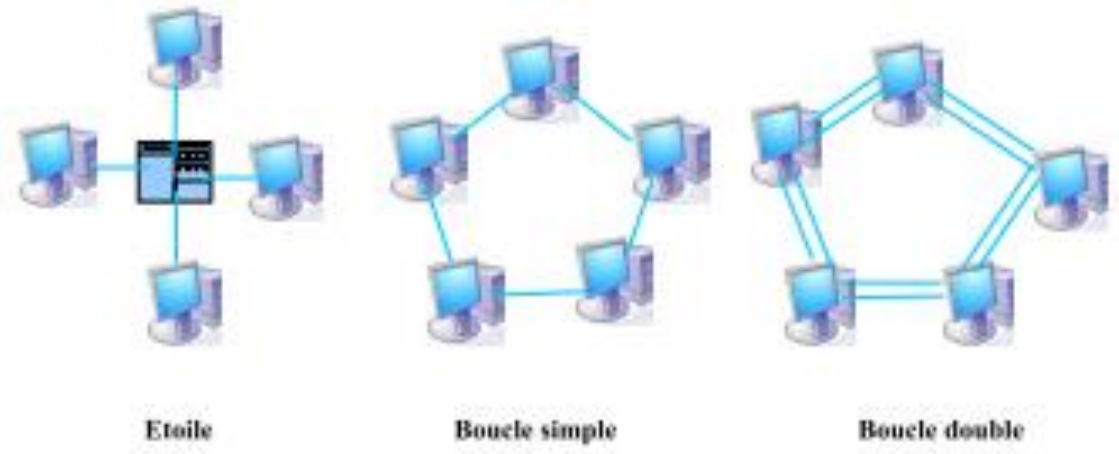


Figure 1.03 : *Réseau en mode point à point*

Comme illustré dans les figures. On distingue ainsi deux classes de réseaux :

- Ceux en mode de diffusion
- Ceux en mode point à point

Le premier mode de fonctionnement consiste à partager un seul support de transmission. Chaque message envoyé par un équipement sur le réseau est reçu par tous les autres. C'est l'adresse spécifique placée dans le message qui permettra à chaque équipement de déterminer si le message lui est adressé ou non. À tout moment un seul équipement a le droit d'envoyer un message sur le support, il faut donc qu'il vérifie au préalable si la voie est libre, sinon il attend.

Les réseaux locaux adoptent pour la plupart le mode diffusion, sur une architecture en bus ou en anneau. Dans une telle configuration la rupture du support provoque l'arrêt du réseau, par contre la panne d'un des éléments ne provoque pas (en général) la panne globale du réseau.

Dans le mode point à point le support physique (le câble) relie seulement une paire d'équipements. Quand deux éléments non directement connectés entre eux veulent communiquer ils le font par l'intermédiaire des autres nœuds du réseau.

Dans le cas de l'étoile le site central reçoit et envoie tous les messages, le fonctionnement est simple, mais la panne du nœud central paralyse tout le réseau

Dans une boucle simple, chaque nœud recevant un message de son voisin en amont le réexpédie à son voisin en aval. Pour que les messages ne tournent pas infiniment le nœud émetteur retire le message lorsqu'il lui revient. Si l'un des éléments du réseau tombe en panne, alors tout s'arrête.

Ce problème est partiellement résolu par la double boucle dont chacune des boucles fait tourner les messages dans un sens opposé.

1.4 Architecture des réseaux

• Les réseaux poste à poste (peer to peer / égal à égal),
• Réseaux organisés autour de serveurs (Client/Serveur),
• Trois tiers.

1.4.1 Les réseaux poste à poste

Dans une architecture d'égal à égal (où dans sa dénomination anglaise peer to peer), tous les ordinateurs sont égaux, il n y a pas de machine spécifique. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources. Un ordinateur relié à une imprimante pourra donc éventuellement les partager afin que tous les autres ordinateurs puissent y accéder via le réseau.

1.4.2 Architecture client/serveur

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes contactent un serveur, une machine généralement très puissante en terme de capacités d'entrée-sortie, qui leur fournit des services.
Dans un environnement purement Client/serveur, les ordinateurs du réseau (les clients) ne peuvent voir que le serveur, c'est un des principaux atouts de ce modèle.

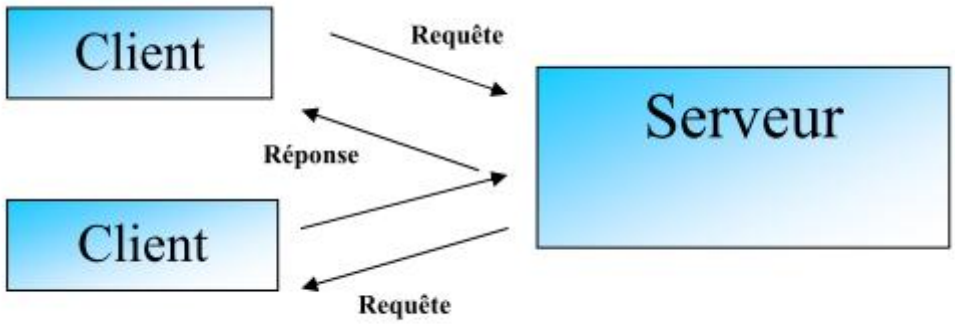


Figure 1.03 : *Architecture client/serveur*

- Le client émet une requête vers le serveur grâce à son adresse, demandant un service.
- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine.

Dans cette architecture le seul inconvénient est que le serveur peut être épuisé notamment s'il traite plusieurs clients.

1.4.3 Architecture Trois tiers

Dans l'architecture à 3 niveaux (appelées architecture 3-tier), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre :
Le client et le demandeur de ressources.

Le serveur d'application, le serveur chargé de fournir la ressource mais faisant appel à un autre serveur.

Le serveur secondaire, fournissant un service au premier serveur.

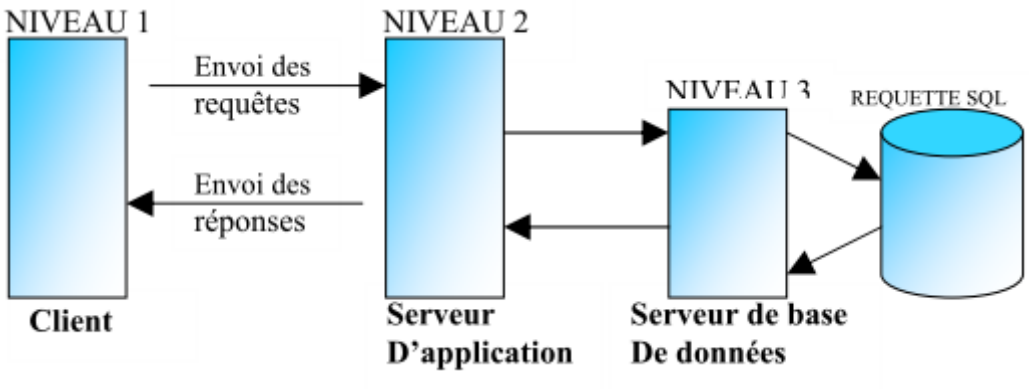


Figure 1.04 : *Architecture Trois tiers*

1.5 Notion de protocole

Pour communiquer entre deux postes de travail, les deux machines doivent être relié d'une certaine manière, et doivent utiliser un langage de communication commun. [4]

• Certaine manière revient à dire topologie.

• Langage de communication revient à dire protocole.

Un protocole est une méthode standard qui permet la communication entre deux machines, c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

Ethernet, IP, TCP, HTTP, SMTP sont des protocoles. Un groupe de protocoles complémentaires forme une pile de protocoles. [4][5]

Mais, aujourd'hui, tout le monde utilise la pile TCP-IP, aussi appelée protocoles Internet parce qu'elle a été mise au point pour le réseau Arpanet, l'ancêtre de l'internet. IP (Internet Protocol) gère l'adressage des paquets de données et TCP (Transmission Control Protocol) s'assure que les messages parviennent bien à leur destinataire.

Le fait que les LAN, les MAN et les WAN reposent tous sur le même système de transport des messages qui est très pratique : on n'a aucun système de passerelle à mettre en place pour permettre

les communications entre systèmes informatiques. On est sûr que le message parviendra bien à son destinataire quel qu'il soit et où qu'il soit.

1.6 Conclusion

Dans ce chapitre, nous avons donc vu les généralités sur les réseaux informatiques ainsi que l'architecture et la topologie des différents réseaux. La connaissance de ces différents aspects facilite la compréhension et le paramétrage de la simulation.

CHAPITRE 2

PRESENTATION DE LA TECHNOLOGIE Wi-Fi

2.1 Introduction

Les réseaux locaux sans fil connaissent actuellement un succès important, ils sont adoptés au sein des entreprises et du grand public. Ils offrent en effet une flexibilité largement supérieure aux réseaux filaires, en s'affranchissant notamment des problèmes de câblage et de mobilité des équipements. [5]

2.2 Réseaux sans fil

Un réseau sans fils (en anglais wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fils, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de « mobilité ».

On peut classer les réseaux sans fil selon quatre catégories qui se distinguent par la fréquence d'émission utilisée, par le débit et la portée de transmission : [6]

2.3 Les Technologies Wi-Fi

2.3.1 Définition de wLan

Le Wi-Fi, pour Wireless Fidelity, est une technologie standard d'accès sans fil à des réseaux locaux (WLAN). Le principe consiste à établir des liaisons radio rapides entre des terminaux et des bornes reliées aux réseaux Haut Débit. Grâce à ces bornes Wi-Fi, l'utilisateur se connecte à Internet ou au système d'informations de son entreprise et accède à de nombreuses applications reposant sur le transfert de données. Cette technologie a donc une réelle complémentarité avec les réseaux ADSL (Asymetric Digital Subscriber Line), les réseaux d'entreprise ou encore les réseaux mobiles comme GPRS/UMTS (Global Packet Radio Service / Universal Mobile Telecommunications System).

Ce standard a été développé pour favoriser l'interopérabilité du matériel entre les différents fabricants ainsi que pour permettre des évolutions futures compatibles. Ainsi, les consommateurs peuvent mélanger des équipements de différents fabricants afin de satisfaire leurs besoins. [7]

2.3.2 Présentation de la norme 802.11

2.3.2.1 Norme 802.11

Le nom Wi-Fi ou Wireless Fidelity correspond initialement au nom donné à la certification délivrée par WECA qui est l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11.

2.3.2.2 Les spécifications 802.11

La technologie 802.11 a grandement évolué depuis ses débuts, et les améliorations au standard initial utilisent une lettre, comme 802.11a, 802.11b, etc… [8]

L'IEEE a constitué de nombreux groupes de travail pour améliorer le 802.11. Les noms donnés à ces standards sont de type 802.11x, x étant une lettre comprise entre « a » et « r »

On remarque que certaines lettres n'ont pas été utilisées car les groupes de travail ont réalisés des travaux confus, obsolètes et totalement abandonnés :

- 802.11 (1997) : Elle offre un débit jusqu'à 2 Mbps.
- 802.11a (1999) : Elle permet d'obtenir un débit théorique de 54 Mbps, elle spécifie huit canaux radio dans la bande de fréquence des 5 GHz.
- 802.11b (1999) : Elle est la norme la plus rependue actuellement, elle propose un débit théorique de 11 Mbps avec une portée pouvant aller jusqu'à 300 m dans un environnement bien dégagé, la plage de fréquence utilisée est la bande de 2,4 GHz, avec 3 canaux disponibles.
- 802.11e (2005) : Elle 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 termes de bande passante et de délais de transmission de telle manière à permettre notamment une meilleure transmission de la voix et vidéo.
- 802.11f (2003) : Elle est une recommandation à l'intervention des vendeurs des points d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole IAPRP permettant à un utilisateur de changer de point d'accès de façon transparent lors d'un déplacement.
- 802.11g (2003) : Elle offre un débit théorique de 54 Mbps dans la bande des 2,4 GHz, elle a une compatibilité ascendante avec 802.11b.
- 802.11h (2003) : Elle vise à rapprocher de l'Hiperlan, d'où la lettre 'h'.

- 802.11i (2004) : Elle a pour but d'améliorer la sécurité des transmissions, elle s'appuie sur la technique de chiffrement AES et l'authentification forte 802.1x.
- 802.11j (2003) : Elle est à la réglementation japonaise tandis que 802.11h est une réglementation européenne.
- 802.11n : Ce standard en est encore à ses prémices et est très attendu. Il devrait autoriser des débits de 108 Mbps, voire 320 Mbps pour la prochaine évolution du standard.
- 802.11r (2004) : Le groupe de travail n'a pas encore établi de draft. Il prépare un standard qui devrait améliorer les temps de réassociation lors du roaming. Une conséquence directe serait le maintien de la connexion téléphonique Wi-Fi lorsqu'un utilisateur se déplace d'une zone de couverture à une autre.
- 802.11s (2011) : Le principe du mesh networking est de supprimer cette infrastructure en laissant les Access Points communiquer directement entre eux. Ils se comportent alors comme des routeurs et transmettent les paquets de proche en proche jusqu'à leurs destinataires.
- 802.11u : La norme 802.11u a été adoptée le 25 février 2011. Elle vise à faciliter la reconnaissance et la sélection de réseaux, le transfert d'informations en provenance de réseaux externes, en vue de permettre l'interopérabilité entre différents fournisseurs de services payants ou avec des hot-spots 2.0. Elle définit aussi des normes en termes d'accès à des services d'urgence. À terme, elle doit faciliter le délestage des réseaux 3G ou 4G de téléphonie mobile.
- 802.11v : La norme 802.11v a été adoptée le 2 février 2011. Elle décrit des normes de gestion des terminaux en réseau : reportings, gestion des canaux, gestion des conflits et interférence, service de filtrage du trafic...
- 802.11ac : EEE 802.11ac est la dernière évolution du standard de transmission sans fil 802.11, qui permet une connexion sans fil haut débit dans la bande de fréquences inférieure à 6 GHz (communément appelée bande des 5 GHz). Le 802.11ac offre jusqu'à 1 300 Mbit/s de débit théorique, en utilisant des canaux de 80 MHz, soit jusqu'à 7 Gbit/s de débit global pour l'ensemble de la bande des 5 GHz (de 5170 MHz à 5835 MHz). La norme a été ratifiée en janvier 2014.

2.4 Architecture du réseau

La norme 802.11, comme toutes les autres normes, une normalisation doit respecter le modèle OSI qui est différent d'une norme à une autre mais tout en conservant son aspect de couches et les différents fonctionnements et relations de ceux-ci. [9][10]

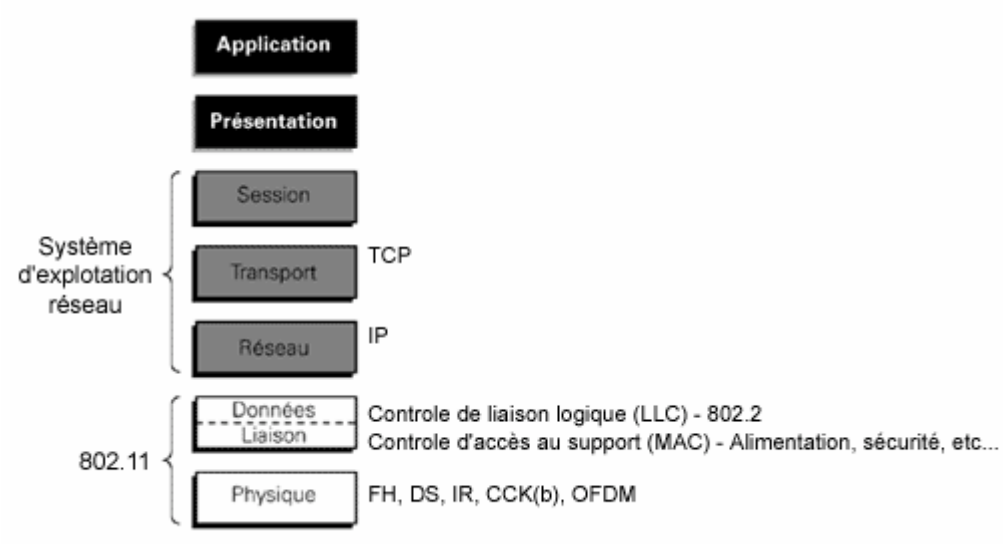


Figure 2.01 : *Représentation du modèle OSI*

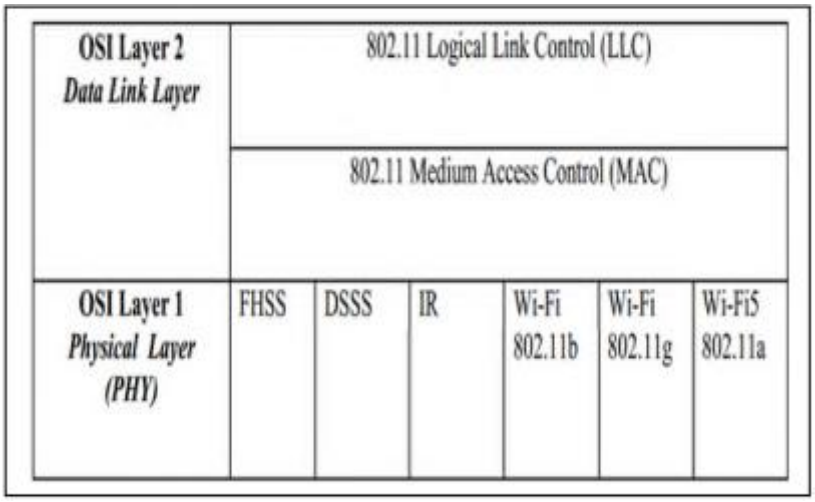


Figure 2.02 : *Modèle en couches de l'IEEE 802.11*

2.4.1 Couche physique

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

Comme nous l'avons vu ci-dessus, la norme 802.11 propose plusieurs couches physiques, définissant des modes de transmission alternatifs :

• Wi-Fi 802.11a
• Wi-Fi 802.11b
• Frequency Hopping Spread-Spectrum
• Direct-Sequence Spread-Spectrum
• Infrarouge
• …

2.4.1.1 FHSS (Frequency Hopping Spread Spectrum)

Cette technique consiste à découper la large bande de fréquence en un minimum de 75canaux (hops ou saut d'une largeur de 1 MHz), puis de transmette en utilisant une combinaison de canaux connue de toutes les stations de la cellule. Dans la norme Wi –Fi, la bande de fréquence de 2.4 GHz permet de créer 79 canaux de 1 MHz. La transmission se fait ainsi en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (d'environ 400 ms), l'émetteur et le récepteur s'accordent sur une séquence de Sauts de fréquence porteuse pour envoyer les données successivement sur les différents sous-canaux. Le principal inconvénient du FHSS vient de son débit qui est limité à 2 Mbit/s. Cette limitation est due au fait que la bande passante des canaux soit égale à 1 MHz.

2.4.1.2 DSSS (Direct Sequence Spread Spectrum)

Dans le but de lutter contre les interférences importantes mais n'affectant que des plages de fréquences assez étroites, il existe la technique de l'étalement de spectre. Comme le FHSS, le DSSS divise la bande ISM en sous bandes. Cependant la division se fait ici en 14 canaux de 22 MHz chacun. La transmission ne se fait que sur un canal donné. La largeur de la bande ISM étant égale à 83.5 MHz, il est impossible d'y placer 14 canaux adjacents de 22 MHz. Les canaux se recouvrent donc, comme illustré à la figure suivante :

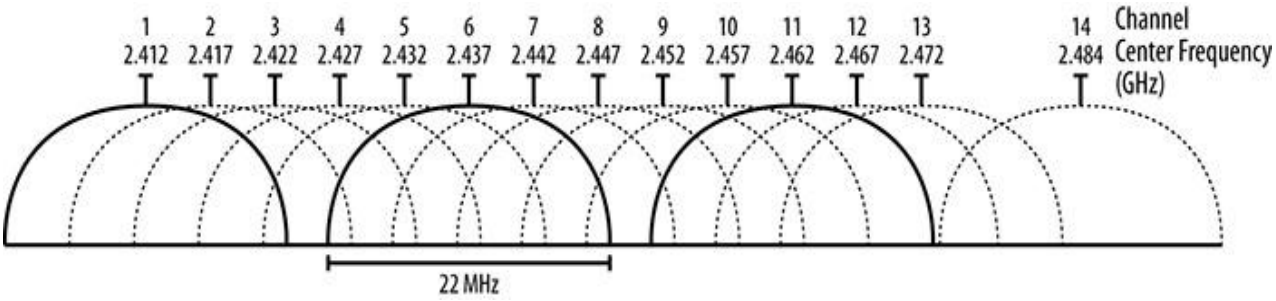


Figure 2.03 : *Décomposition de la bande ISM en sous canaux*

2.4.1.3 OFDM (Orthogonal Frequency Division Multiplexing)

Le principe de cette technique consiste à diviser le signal que l'on veut transmettre sur différentes bandes porteuses, comme si l'on combinait ce signal sur un grand nombre d'émetteurs indépendants, fonctionnant sur des fréquences différentes. Un canal est constitué de 52 porteuses de 300 KHz de largeur, 48 porteuses sont dédiées au transport de l'information utile et 4 pour la correction d'erreurs appelées porteuses pilote, Huit canaux de 20 MHz sont définis dans la bande de 5 GHz, Plus le nombre de canaux est élevé, plus les données transmises en parallèle sont nombreuses, plus la bande passante est élevée .[10]

2.4.1.4 MIMO

Le MIMO est un protocole de la couche physique et permet d'envoyer plusieurs signaux différents sur des antennes différentes à des fréquences proches pour augmenter le débit ou la portée du réseau comme montrée à l'aide de la figure suivante :

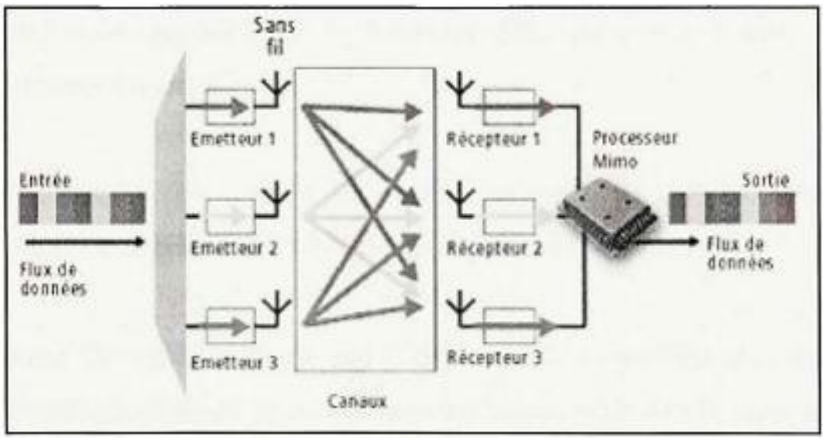


Figure 2.04 : *La technologie MIMO*

Sa particularité passe par l'utilisation simultanée de plusieurs antennes, émettrices et réceptrices. Ainsi il permet d'améliorer les performances des appareils, qui aujourd'hui connaissent des problèmes liés à la nature des ondes et à leur comportement suivant l'environnement, ce qui diminue la qualité de transmission et donc le débit ainsi que la portée.
C'est donc en remédiant à ces problèmes que le MIMO se place en tête des technologies d'avenir pour les communications mobiles.

2.4.2 Couche liaison de données

Les fonctionnalités mises en œuvre par la couche liaison de données sont les suivantes :
Procédures d'accès au support, Adressage des paquets, Formatage des trames, Contrôle d'erreur CRC, Fragmentation et réassemblage des trames.
Tout comme les autres normes de réseaux locaux de l'IEEE, la couche liaison de données des réseaux Wi-Fi se décompose en deux sous-couches :

- LLC : La couche LLC 802.11 est totalement identique à la couche LLC 802.2. Cette couche adapte les données venant des couches supérieures à la couche physique. Il est ainsi tout à fait possible de connecter un réseau wLan à tout autre réseau IEEE 802, filaire ou non.
- MAC : La couche MAC est similaire à celui de la couche MAC 802.3, elle écoute le canal, attend s'il est occupé, puis transmettre lorsqu'il sera libre. La couche MAC 802.11 se distingue cependant de la couche MAC 802.3 dans le sens où elle intègre un grand nombre de fonctionnalités supplémentaires, comme la retransmission, l'acquittement ou la fragmentation de trames. La norme 802.11 introduit, de plus, deux méthodes d'accès au support physique fondamentalement différentes, le DCF et le PCF.

2.4.2.1 Accès au canal dans la couche MAC 802.11

Le standard 802.11 se base principalement sur deux méthodes pour partager l'accès au canal :

- Un accès distribué DCF :

Dite avec contention. C'est une méthode d'accès utilisée pour les transferts asynchrones c'est à dire tout type de données et sans gestions de priorité. Elle est conçue pour permettre aux utilisateurs d'avoir chance égale d'accéder au support. Elle permet de réduire les collisions sans pouvoir les éliminer totalement. Cette méthode s'appuie sur le protocole CSMA/CA combiné à l'algorithme de back-off.

Lorsqu'une station souhaite émettre une trame de données, elle écoute le canal durant un intervalle de temps appelé DIFS. Si celui-ci est inactif durant cette période, la station transmet immédiatement sa trame. Dans le cas contraire, le canal est occupé, la station doit attendre jusqu'à ce que le canal soit inactif durant une période SIFS.À la fin de cette période, la station entre dans la procédure du Backoff qui l'oblige à calculer un Backoff Time durant lequel elle s'abstient de transmettre.

La station réceptrice vérifie le CRC de la trame reçue et envoie une trame d'acquittement à l'émetteur après un SIFS. Ce dernier est utilisé pour séparer les trames d'un dialogue. La réception de l'acquittement informe l'émetteur du succès de la transmission.

Lorsque le PCF est utilisé, le coordinateur central a la priorité d'accéder au canal. Pour cela, il utilise l'intervalle PIFS qui est plus court que le DIFS. Une fois que le canal saisit, le coordinateur central instaure le PCF. On montre dans la figure 2.05 suivante la relation entre ces temps.

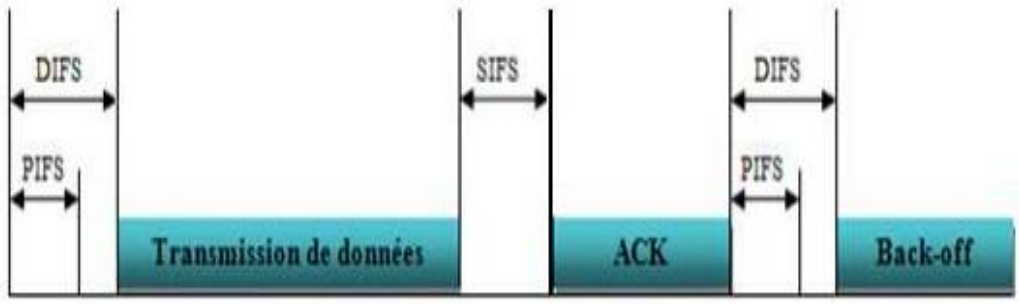


Figure 2.05 : *Relations entre les différents IFS*

2.4.2.2 Un accès centralisé PCF

Cette méthode sans contention ne permet pas de gérer les collisions. Au début de la période sans contention, le point coordinateur PC transmet des balises Beacons qui contiennent la durée maximale CFPMaxDuration de la période d'accès sans contention. Ensuite, il commence à interroger les stations associées en envoyant des trames CF-Poll afin de savoir si elles possèdent des données à transmettre. Le CF-Poll peut être accompagné d'une trame de données si le PC a des données à transmettre pour une station. La station qui est destinataire du CF-Poll envoie sa trame en intégrant un acquittement CF-ACK qui acquitte le CF-Poll après un temps d'attente SIFS.[11]

Enfin, le PC acquitte la trame envoyée par la station après un intervalle SIFS. Cet acquittement est généralement accompagné par un CF-Poll pour interroger une autre station. Dans le cas où une station interrogée ne répond pas au bout d'un temps PIFS (elle n'a pas de données à transmettre), le PC reprend l'interrogation des stations qui restent. La Figure 2.06 illustre un exemple d'une période sans contention durant laquelle le PC interroge trois stations sta1, sta2 et sta3.

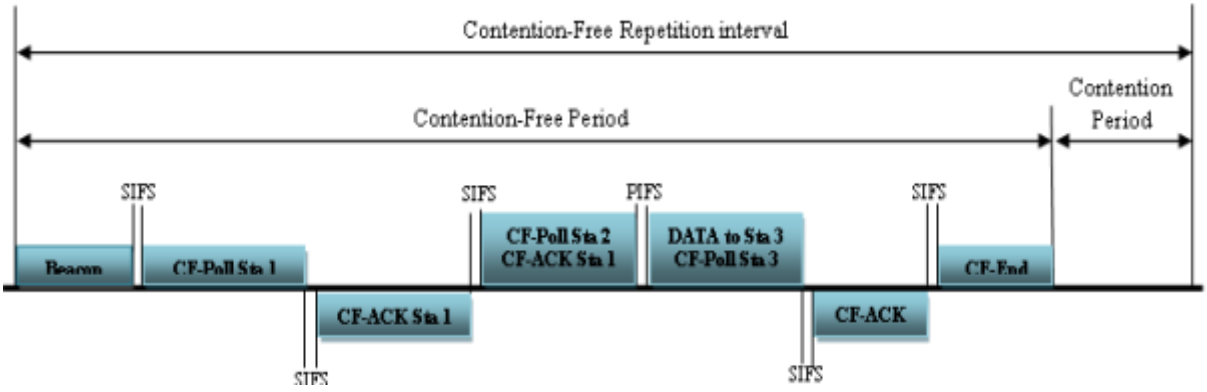


Figure 2.06 : *L'accès centralisé au canal PCF*

2.4.2.3 Livraison fiable dans la couche MAC 802.11

Le standard IEEE 802.11 a proposé plusieurs mécanismes pour pallier le manque de fiabilité de la couche physique. Un bref descriptif de ces mécanismes est donné ci-dessous :

- La retransmission : La couche MAC 802.11 se base sur le système de correction d'erreurs ARQ. Ce dernier emploie les codes de détection d'erreurs, les acquittements et les retransmissions pour assurer la fiabilité des données. En effet, la trame MAC intègre une valeur de contrôle CRC qui permet de vérifier l'intégrité des données au niveau du récepteur. Dans le cas où les données sont correctes, le récepteur envoie un acquittement à l'émetteur.
Dans le cas contraire, l'émetteur attend l'acquittement durant un certain temps timeout et retransmet la trame en considérant que la précédente est perdue.
L'émetteur répète cette opération un nombre de fois limité jusqu'à la réception d'un acquittement. La procédure d'envoi d'une trame de données et d'attente de son acquittement constitue une unité atomique de dialogue durant laquelle aucune autre station ne peut accéder au canal.

L'utilisation de RTS/CTS : Il est utilisé pour éviter les collisions des trames transmises, en même temps, par deux ou plusieurs stations, principalement, dans une configuration où deux stations éloignées communiquent avec une station se trouvant au milieu. Cette configuration
engendre le problème de « la station cachée » puisque les deux stations éloignées ne perçoivent pas leurs signaux et peuvent transmettre en même temps des trames à la station intermédiaire, ce qui provoque des collisions. Pour éviter ce problème, la requête RTS et la réponse CTS ont été intégrées au mécanisme CSMA/CA avant un envoi d'une trame de données. Ainsi, lorsqu'une station émettrice détient le canal pour une transmission, elle commence par envoyer une requête RTS à la station réceptrice qui répond par une réponse CTS. Les messages RTS/CTS sont aussi reçus par toutes les autres stations qui doivent différer leurs transmissions en conséquence.

- La fragmentation : Afin de faire face à l'évanouissement rapide du signal responsable de la corruption des trames durant leur transmission, la norme 802.11 définit la fragmentation au niveau MAC. La fragmentation permet la décomposition des paquets provenant de la couche LLC en plusieurs trames MAC. Ceci permet de réduire la taille des trames transmises sur le canal sans fil et d'augmenter le nombre de trames livrées sans erreur. Le mécanisme de fragmentation proposé par la norme 802.11 est augmenté du mécanisme burst qui permet d'envoyer tous les fragments d'un même paquet en rafale une fois le canal détenu.[12]

2.5 Architecture cellulaire

On peut citer le mode infrastructure et le mode ad-hoc.

2.5.1 Le mode ad-hoc

En mode ad hoc les machines sans fils clientes se connectent les unes aux autres afin de constituer un réseau point à point (peer to peer en anglais), c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès [12][13]

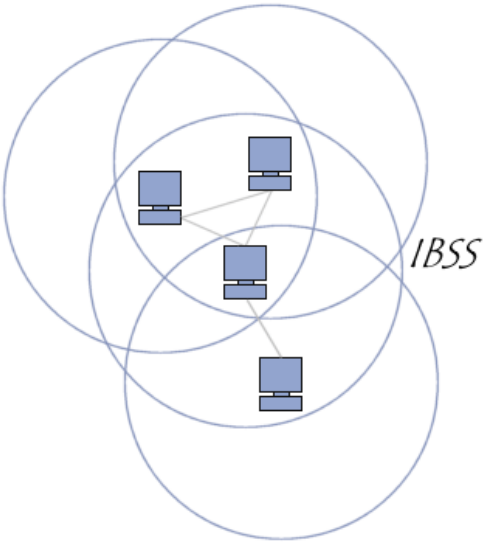


Figure 2.07 : *Mode adhoc*

L'ensemble formé par les différentes stations est appelé ensemble de services de base indépendants Un IBSS est ainsi un réseau sans fil constitué au minimum de deux stations et n'utilisant pas de point d'accès. L'IBSS constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un SSID, comme l'est un ESS en mode infrastructure.

Dans un réseau ad hoc, la portée du BSS indépendant est déterminée par la portée de chaque station. Cela signifie que si deux des stations du réseau sont hors de portée l'une de l'autre, elles ne pourront pas communiquer, même si elles « voient » d'autres stations. En effet, contrairement au mode infrastructure, le mode ad hoc ne propose pas de système de distribution capable de transmettre les trames d'une station à une autre. Ainsi un IBSS est par définition un réseau sans fil restreint.

2.5.2 Le mode infrastructure

En mode infrastructure chaque station se connecte à un point d'accès via une liaison sans fil. L'ensemble formé par le point d'accès et les stations situés dans sa zone de couverture est appelé ensemble de services de base (en anglais basic service set, noté BSS) 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.

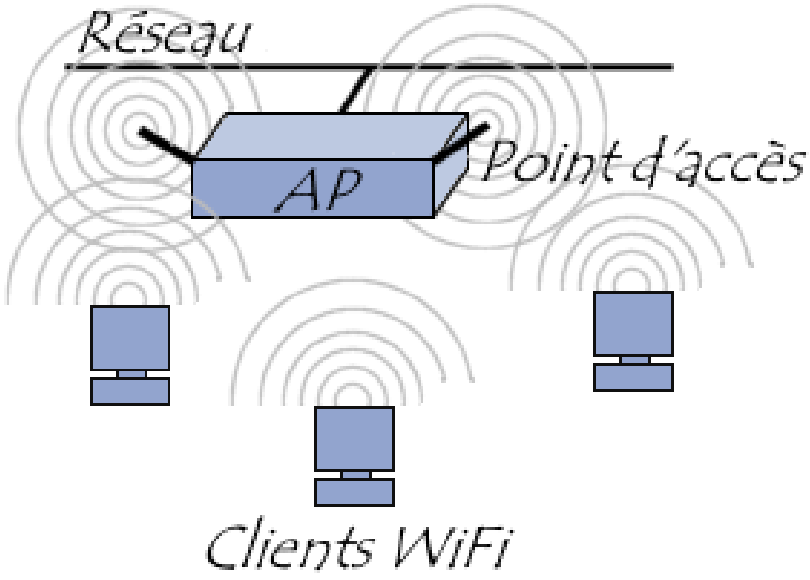


Figure 2.08 : *Mode infrastructure*

Il est possible de relier plusieurs points d'accès entre eux (ou plus exactement plusieurs BSS) par une liaison appelée système de distribution (notée DS pour Distribution System) afin de constituer un ensemble de services étendu (extended service set ou ESS). Le système de distribution (DS) peut être aussi bien un réseau filaire, qu'un câble entre deux points d'accès ou bien même un réseau sans fil.

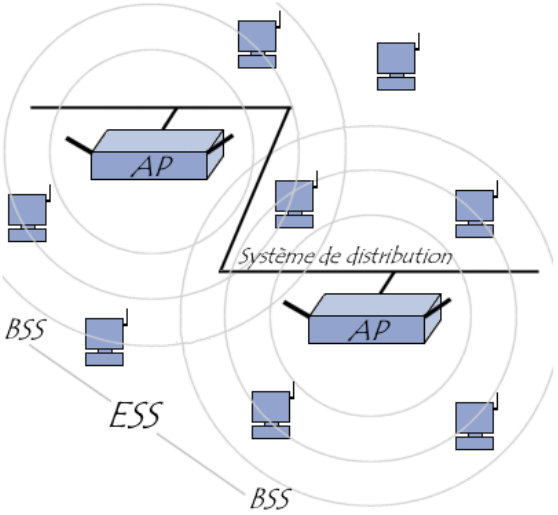


Figure 2.09 : *ESS*

Un ESS est repéré par un ESSID (Service Set Identifier), c'est-à-dire un identifiant de 32 caractères de long (au format ASCII) servant de nom pour le réseau. L'ESSID, souvent abrégé en SSID, représente le nom du réseau et représente en quelque sort un premier niveau de sécurité dans la mesure où la connaissance du SSID est nécessaire pour qu'une station se connecte au réseau étendu.

Lorsqu'un utilisateur nomade passe d'un BSS à un autre lors de son déplacement au sein de l'ESS, l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès. Les points d'accès communiquent entre eux grâce au système de distribution 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).

2.6 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 (probe request) contenant l'ESSID pour lequel elle est configurée ainsi que les débits que son adaptateur sans fil supporte. Si aucun ESSID 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 en anglais) donnant des informations sur son BSSID, ses caractéristiques et éventuellement son ESSID. L'ESSID est automatiquement diffusé par défaut, mais il est possible (et recommandé) de désactiver cette option.
A chaque requête de sondage reçue, le point d'accès vérifie l'ESSID et la demande de débit présent dans la trame balise. Si l'ESSID 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. En effet d'une manière générale, plus un point d'accès est proche, meilleur est le débit
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. [5]

2.7 Conclusion

Dans ce chapitre, nous avons présenté en particulier le WLAN ou le standard 802.11, ainsi que les améliorations de ce dernier et la topologie déployée, et nous avons décrit les couches introduites par cette norme, la couche physique qui est responsable de la modulation et la couche MAC de l'accès au support. Dans le chapitre suivant, nous présenterons une description de la qualité de service dans le wifi et de la norme 802.11 ac.

CHAPITRE 3

LA QUALITE DE SERVICE DANS LE WIFI

3.1 Introduction

Les réseaux locaux basés sur la technologie IEEE 802.11 ont pris une ampleur telle qu'ils sont déployés un peu partout dans notre entourage quotidien (aéroports, hôtels, gares, campus, etc.).Ce déploiement est favorisé par la maturité atteinte par le standard grâce aux travaux des groupes 802.11 chargés de rendre le standard plus compétitif (QoS, sécurité, haut débit).[12]

3.2 Généralités sur la qualité de service

3.2.1 Définition de la QoS

Plusieurs définitions ont été proposées pour le terme de la qualité de service dont les plus importantes sont : [13]

- La Qualité de Service (QoS) est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, taux de perte de paquets…
- La Qualité de Service est une notion subjective. Selon le type d'un service envisagé, elle pourra résider dans le débit (Un débit permet de mesurer le flux d'une quantité relative à une unité de temps au travers d'une surface quelconque.), le délai (pour les applications interactives ou la téléphonie), la disponibilité (accès à un service partagé) ou encore le taux de pertes de paquets (pertes sans influence de la voix ou de la vidéo (La vidéo regroupe l'ensemble des techniques, technologie, permettant l'enregistrement ainsi que la restitution d'images animées…).
- La Qualité de Service regroupe un ensemble de technologies mises en œuvre pour assurer des débits suffisants et constants sur les réseaux, y compris Internet.

3.2.2 But de la QoS

Le but de la QoS est donc d'optimiser les ressources du réseau (Un réseau informatique est un ensemble d'équipements reliés entre eux pour échanger des informations. Par analogie avec un filet (un réseau est un « petit rets », c'est-à-dire un petit filet), on appelle nœud (node) l'extrémité d'une connexion, qui peut être une intersection de plusieurs connexions (un ordinateur, un routeur, un concentrateur, un commutateur) 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 (Le temps est un concept développé pour représenter la variation du monde : l'Univers n'est jamais figé, les éléments qui le composent bougent, se transforment et évoluent pour l'observateur qu'est l'homme. Si on considère l'Univers...) de réponse différenciés par application suivant les protocoles mis en œuvre au niveau de la couche réseau.

Elle permet ainsi aux fournisseurs de services (départements réseaux des entreprises, opérateurs…) de s'engager formellement auprès de leurs clients sur les caractéristiques de transport (Le transport, du latin trans, au-delà, et portare, porter, est le fait de porter quelque chose, ou quelqu'un, d'un lieu à un autre.) des données (Dans les technologies de l'information (TI), une donnée est une description élémentaire, souvent codée, d'une chose, d'une transaction d'affaire, d'un événement, etc.) applicatives sur leurs infrastructures IP.

Selon le type d'un service envisagé, la qualité pourra résider :

- Le débit (téléchargement ou diffusion vidéo).
- Le délai (pour les applications ou la téléphonie).
- La disponibilité (accès à un service partagé).
- Le taux de pertes de paquets.

3.2.3 Services de la QoS

- La mise en place de la qualité de service nécessite en premier lieu la reconnaissance des différents services.
- La source et la destination du paquet.
- Le protocole utilisé (UDP/TCP/etc.).
- Les ports de source et de destination dans le cas TCP et UDP.
- La congestion des réseaux.

- La validité du routage (gestion des pannes dans un routage en cas de routes multiples par ex.)
- La bande passante consommée.
- Les temps de latence.

3.2.4 Critères de la QoS

Les principaux critères permettant d'apprécier la qualité de service sont les suivants :

- Débit (en anglais bandwidth) : parfois appelé bande passante, il définit le volume maximal d'information (bits) par unité de temps (b/s).
- Perte de paquet (en anglais packet loss) : elle correspond à la non-délivrance d'un paquet de données, la plupart du temps due à un encombrement du réseau.
- Gigue (en anglais jitter) : C'est un paramètre important pour les applications communicantes de type voix ou vidéo où la gigue doit être la plus faible possible. La gigue est due principalement aux délais de transferts variables dans les nœuds du réseau (swicthes et routeurs).
- Latence (en anglais delay) : elle caractérise le retard entre l'émission et la réception d'un paquet.

3.3 Qualité de service suivant le standard IEEE 802.11

Pour assurer une qualité de service adéquate dans les réseaux sans fil le standards IEEE 802.11 à définit deux méthodes d'accès au canal :

- Distributed Coordination Function (DCF)
- Point Coordination Function (PCF)

3.4 Problématique de la QoS dans les réseaux IEEE 802.11

Le développement du réseau Internet et le grand nombre d'utilisateurs connectes a ce réseau imposent le recours à des supports de qualité de service. Dans cette perspective, plusieurs groupes de travail ont vu le jour pour les réseaux filaires. Les nouveaux besoins en termes de mobilité des utilisateurs et la croissance des réseaux permettant le nomadisme des utilisateurs ont fait migrer le problème vers la boucle locale sans fils, entre autres les réseaux IEEE 802.11. Actuellement, le marché des télécommunications des réseaux Hots-pot est relativement faible mais on s'attend à ce qu'il subisse une croissance accrue les prochaines

années. Les fournisseurs d'accès à Internet commencent à mettre en place un large nombre de hots-pots 802.11 ou Wifi dans les divers lieux publics. Des applications multimédia telles que la voix sur IP ou la vidéo sur demande en plus des applications classiques seront de plus en plus utilisées dans ce type de réseaux. Ces applications multimédia nécessitent un niveau minimal de qualité de service en termes de bande passante, de délai, de gigue ou de taux de perte.

D'autres types d'applications avec des contraintes plus aigües en termes de QoS commencent à émerger. Des applications du standard 802.11 en milieu industriel pour la commande et la supervision des systèmes ou en milieu médical pour la télémédecine imposent des exigences strictes en termes de QoS (délais + taux d'erreurs). La réponse à ces besoins accrus en QoS dans les hots-pots 802.11 est d'autant plus difficile à cause des caractéristiques spécifiques du medium sans fils. En effet, pour la couche physique DSSS permettant un débit au-delà de 11 Mbps, parmi 11 canaux possibles, seulement 3 ne se chevauchent pas. Ce medium présente alors un taux de perte assez élève à cause des interférences. En plus, les caractéristiques du support physique ne sont pas constantes et varient dans le temps et dans l'espace. Quand les utilisateurs bougent, les chemins de bout en bout changent et les utilisateurs se réassocient chaque fois à des nouveaux Aps.

Ces utilisateurs doivent avoir la même QoS indépendamment de leurs associations et du chemin de bout en bout du trafic. Plusieurs travaux de recherche ont essayé d'évaluer les performances du standard IEEE802.11 quant à sa capacité de répondre aux besoins en termes de QoS des utilisateurs. Ces travaux ont investigue essentiellement les possibilités offertes par la sous couche MAC du standard pour garantir un niveau minimal de QoS pour les utilisateurs. Dans le même objectif, d'autres travaux ont adopté des modèles analytiques ou des approches par simulation. Plusieurs solutions ou approches pour l'amélioration du support de QoS par la couche MAC 802.11 ont été proposées.

Toutes ces insuffisances dans les modes de fonctionnement DCF et PCF du standard ont conduit à plusieurs activités de recherche pour améliorer les performances de la sous couche MAC 802.11.

3.5 Limites en termes de QoS du standard IEEE 802.11

Le contrôle d'accès au medium, le maintien de la QoS et la sécurité sont les fonctions les plus importantes de la sous couche MAC 802.11. Cependant plusieurs limitations se présentent quant au support de la qualité de service.

3.5.1 Limitations de la méthode d'accès de base DCF

Le protocole CSMA/CA utilisé avec cette méthode permet un accès Best Effort au canal. Les utilisateurs ne peuvent avoir aucune garantie de qualité de service minimale.

Toutes les stations d'un même BSS concourent pour l'accès au canal et aux ressources du réseau avec les mêmes priorités. Aucun mécanisme de différenciation entre plusieurs types de flux n'est mis en place pour garantir la bande passante, le délai de bout en bout ou la gigue pour des trafics a hautes priorités tels que la voix sur IP ou la vidéo/visioconférence. Le taux des erreurs dues à la couche physique 802.11 est à peu près trois fois plus grand que celui observe dans les réseaux locaux filaires. Le nombre important de collisions et de retransmissions implique des délais de transmission imprévisibles et une dégradation de la qualité de transmission des flux temps réel tels que pour la voix ou la vidéo.

3.5.2 Limitations de la méthode d'accès PCF

Spécialement conçue pour apporter un support de qualité de service en priorisant les applications temps réel par rapport aux autres, cette procédure d'accès avec scrutation souffre de plusieurs défaillances. Tout d'abord ce mode ne peut être utilisé qu'en alternance avec le mode d'accès DCF et ne peut jamais fonctionner à part entière.

PCF présente tous les inconvénients d'une approche centralisée tel que l'effet d'une défaillance du point central. En plus, à faible charge, les stations voulant émettre en mode PCF subiront des délais très élevés.

Elles seront obligées d'attendre d'être scrutées avant d'émettre. De plus, le coordinateur (généralement confondu avec le point d'accès) doit systématiquement accéder au canal sans fil lors de la période DCF afin de débuter la période PCF suivante.

Dans le mode PCF, il sera très difficile de répondre aux besoins d'un nombre important de trafics temps réel sans pénaliser les applications qui se dérouleront par la suite dans la période avec contention. Un autre problème de ce mode est l'impossibilité de prévoir la durée de transmission

des stations sollicitées. Une station sollicitée par le point coordinateur peut transmettre un MSDU de taille maximale 2304 octets. Cependant, le standard n'empêche pas sa fragmentation en plusieurs MPDU. Ceci, en plus des débits de transmission dépendant de l'état du canal physique, conduit à une durée de transmission d'un MSDU non contrôlée par le point coordinateur ce qui induira des délais supplémentaires pour le reste des stations en mode PCF. Enfin le mode PCF est géré par un algorithme de scrutation Round-Robin à une seule classe. Il ne lui est donc pas possible de répondre aux besoins de QoS de plusieurs types de flux (voix, vidéo,…).

3.6 Les différentes solutions de QoS dans les réseaux IEEE 802.11

Depuis l'écriture du standard IEEE 802.11 a la fin des années 90, plusieurs propositions, issues de travaux de recherches et/ou d'initiatives de la part de constructeurs, ont vu le jour pour l'amélioration du support de qualité de service dans ces réseaux. Un groupe de travail spécifique a été forme au sein de l'IEEE dans l'objectif de normaliser des amendements de la qualité de service pour le protocole 802.11. Elle reprend entre autres des techniques introduites dans divers travaux de recherche. Dans la suite de ce chapitre nous présentons tout d'abord la norme IEEE 802.11ac puis nous présenterons plusieurs approches visant à améliorer la QoS dans les réseaux 802.11.

3.7 Le nouveau standard IEEE 802.11 ac

En vue de résoudre des problèmes de congestion et pour atteindre une plus grande vitesse de transfert, l'IEEE a élaboré la nouvelle norme 802.11ac pour la technologie des réseaux sans fil. Ratifié en février 2014 et rétrocompatible avec la norme 802.11n. [14]

Fondamentalement, cela signifie fournir des débits plus importants via une connexion au réseau sans fil, améliorer l'efficacité spectrale et de la construction basées sur les techniques introduites dans la norme 802.11n en fournissant :

• des canaux plus larges,
• une modulation et un codage de niveau plus élevé,
• la formation de faisceaux,
• le MIMO (entrées multiples, sorties multiples) multiutilisateurs,
• plusieurs flux spatiaux.

Le protocole sans fil 802.11n actuel introduit les canaux de 40 MHz, une amélioration importante par rapport aux canaux de 20 MHz des normes antérieures. En théorie, avec la norme 802.11n vous pouvez utiliser jusqu'à 14 canaux. En pratique, pour éviter les interférences, vous ne pouvez en utiliser que trois ou quatre. Si vous avez des conflits entre canaux, les performances du réseau seront considérablement diminuées.

Pour augmenter la vitesse, la norme 802.11ac utilise des canaux de 80 MHz, et dans une seconde phase la largeur des canaux sera portée à 160 MHz. Par contre, atteindre des débits de données plus élevés a un coût : moins de canaux disponibles dans la bande 5 GHz.
Comme il existe de nombreuses règles régissant l'utilisation de la bande 5 GHz, le mode de fonctionnement exact pourra varier selon votre pays. Aux États-Unis, il y aura au plus cinq sélections de canaux de 80 MHZ pour la norme 802.11ac ; il y en a actuellement trois disponibles.

Pour la seconde phase du 802.11ac, il y aura au maximum deux sélections de canaux de 160 MHz, et probablement seule une des deux sera disponible. En revanche, il y a 13 canaux de 20 MHz qui ne se chevauchent pas disponibles. En Europe, il y a quatre canaux de 80 MHz disponibles pour la norme 802.11ac. Il y aura deux canaux de 160 MHz disponibles pour la deuxième phase. En comparaison, il y a 19 canaux de 20 MHz qui ne se chevauchent pas disponibles.
Il faut garder à l'esprit que les canaux de 160 MHz seront facultatifs, même lorsque la norme sera ratifiée, et généralement le multiplexage des canaux le plus important s'effectuera avec des canaux de 80 MHz. Toutefois, cela réduira significativement le nombre de canaux qui ne se chevauchent pas disponibles dans les bandes UNII 5 GHz.

	DFS COMPRISE		*DFS EXCLUE*	
Taille du canal	*EU*	*EUROPE*	*EU*	*EUROPE*
40 MHz	*6*	*9*	*4*	*2*
80 MHz	*3*	*4*	*2*	*1*
160 MHz	*1*	*2*	-	-

Tableau 3.01 : *Canaux 802.11ac disponibles*

DFS = sélection de fréquence dynamique, pour éviter toute interférence avec un radar météo

Si la DFS n'est pas utilisée, en Europe, il n'y a qu'un seul canal de 80 MHz disponible et seulement deux aux États-Unis donc les points d'accès et les clients devront prendre en charge la DFS pour déployer le 802.11ac efficacement.

3.7.1 Modulation et schéma de codage de niveau plus élevé

802.11Ac introduit une modulation d'ordre supérieur qui utilise le codage 256QAM. Le nombre de bits pouvant être encodés dans un seul symbole est augmenté et le débit peut être amélioré jusqu'à 33 %. Cependant, la conception de l'émetteur et du récepteur doit être modifiée, la conception RF du système devient plus difficile.

3.7.2 Formation de faisceaux

La formation de faisceaux est ce qui permet aux routeurs 802.11ac de délivrer un signal sans fil directement à un périphérique plutôt que de diffuser sur l'ensemble de la zone environnante le signal destiné à ce périphérique. Bien qu'il soit déjà pris en charge dans la génération précédente 802.11n, la nouvelle norme est plus efficace, en partie parce qu'elle ne comprend qu'une seule méthode de formation de faisceaux plutôt que d'offrir plusieurs options possible.

3.7.3 Le MIMO

La technologie MIMO, ou entrée multiple sortie multiple, signifie qu'il est possible d'envoyer et de recevoir simultanément plus d'un signal. La technologie 802.11ac utilisera le MIMO multiutilisateur pour prendre en charge les transmissions simultanées vers plusieurs clients, à condition qu'ils soient séparés physiquement, ce qui maximise l'utilisation de la bande RF.

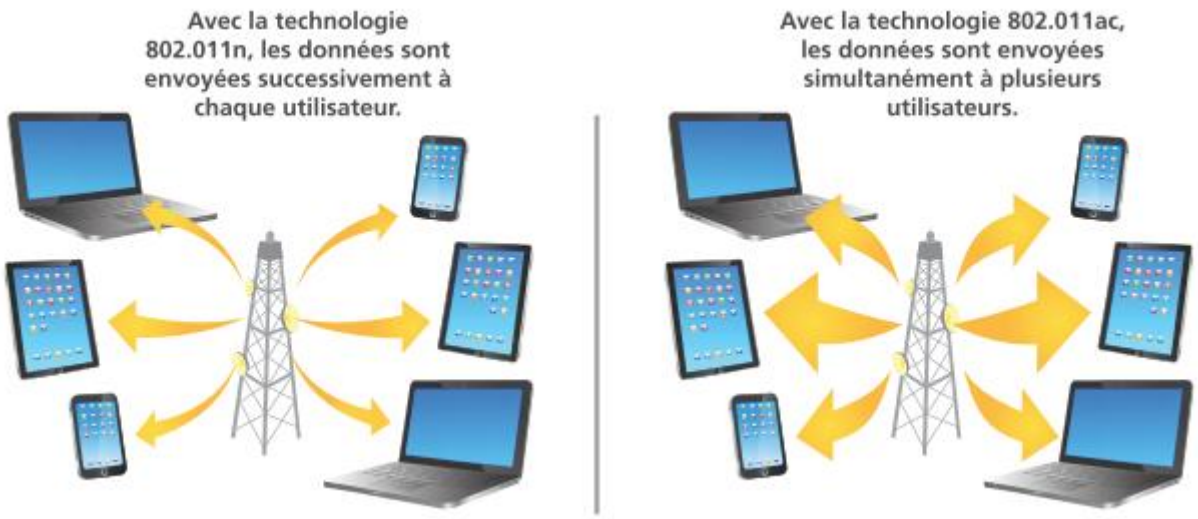


Figure 3.01 : *MIMO ET MU-MIMO*

En théorie, le 802.11ac permet de gérer jusqu'à quatre flux de données spatiales par client, et chaque appareil reçoit en permanence la totalité de la bande passante sur offre. En comparaison, un point d'accès (AP) 802.11n ne peut envoyer et recevoir des données que depuis un seul terminal à la fois. Cela signifie que, plus le nombre de périphériques utilisant un point d'accès augmente, plus le transfert de données ralentit puisque le routeur transmet tour à tour une à chaque périphérique avant de retourner au premier périphérique.

	802.11n	802.11ac
Bande de fréquence	2.4GHz et 5GHz	5GHz
Largeur de canal	20 et 40MHz	20, 40, 60, 80MHz (en option 160MHz)
Flux spatiaux	1 à 4	1 à 8 (jusqu' à 4 par client)
MIMO multiutilisateur	NON	OUI
Flux unique max. débit maximal du client	150Mb/s	433MB/s (si canal de MHz)

Tableau 3.02 : *comparaison des protocoles 802.11n et 802.11ac*

3.7.4 Protocole de sécurité

Les protocoles de sécurité utilisés avec la norme 802.11ac seront, à bien des égards, les mêmes que ceux utilisés avec la norme 802.11n. Les débits de données 802.11ac sont incompatibles avec le WEP et le TKIP, et donc les périphériques fonctionnant à très haut débit utiliseront majoritairement le AES-CCMP, le protocole de sécurité nécessaire pour la certification WPA2. [15]

Toutefois, le 802.11ac aussi permet l'utilisation du GCMP, le protocole mode compteur Galois. Comme le CCMP, il fournit des données d'authentification et de cryptage. Alors que le CCMP crypte les données divisées en blocs, puis authentifie les blocs chaînés dans la séquence, le GGMP utilise une technique appelée multiplication de champ de Galois pour authentifier chaque bloc individuellement. Cela signifie que le GRCMP peut crypter des blocs de données en parallèle plutôt qu'en série.

Lors du traitement des données transmises à des taux très élevés, la capacité à crypter et à authentifier en parallèle devient de plus en plus importante afin de réduire le temps de latence. Chaque authentification GRCMP est donc réalisée plus rapidement qu'une authentification CCMP.

La première vague de produits 802.11ac continuera à utiliser le CCMP, au moins pour la sécurité de la couche de liaison, mais la seconde vague de produits pourrait ainsi utiliser le GRCMP pour s'adapter au réseau sans fil et aux clients MU-MIMO haute densité et des canaux plus larges permettant d'atteindre des débits approchant les 7 Gbit/s. Les administrateurs doivent donc commencer à chercher le moyen de prendre en charge le GCMP dans la planification, la surveillance d'un réseau sans fil et des outils de diagnostic qui devront être prêts pour la deuxième vague de produits 802.11ac et également pour les produits 802.11ad. Ces derniers seront les plus adaptés aux communications haut débit entre appareils proches (de préférence dans la même pièce), tels que la transmission vidéo HD vers des écrans muraux sans fil.

3.8 Introduction progressive

Les périphériques et les points d'accès 802.11ac prennent en charge le MIMO à utilisateur unique, en utilisant la formation de faisceaux pour envoyer le signal efficacement à un seul périphérique à

la fois. Dans la phase suivante, des puces capables d'envoyer des signaux à plusieurs périphériques simultanément seront introduites. Plusieurs avantages en découlent : [16]

• Les périphériques les plus rapides consommeront moins d'énergie puisqu'ils pourront désactiver la radio plus rapidement

• Un signal plus efficace envoyé uniquement en direction des périphériques qui transfèrent les données, réduisant ainsi les interférences

• Les appels vocaux seront prioritaires, mais si une autre connexion, n'interférant pas avec un appel vocal existe, les données étant envoyées dans une autre direction, elle peut être transmise en même temps

• La technologie 802.11ac peut envoyer des signaux ciblés à chaque périphérique. Un périphérique avec une bande passante plus réduite (par ex. un téléphone) se verra attribuer un signal de bande passante plus faible, mais contrairement à la technologie 802.11n, les périphériques ayant besoin d'une plus grande bande passante, tels que les tablettes ou les ordinateurs portables, ne seront pas contraints d'utiliser cette même bande passante.

En théorie, la plupart des mises en œuvre initiales du 802.11ac devraient permettre d'atteindre des vitesses allant jusqu'à 1,3 Gbit/s, ainsi qu'une meilleure couverture que la norme 802.11n. Dans la pratique, bien que sensiblement plus rapide que la technologie 802.11n, la technologie 802.11ac ne permet pas d'atteindre des vitesses de l'ordre du gigabit par seconde, sauf dans des conditions de laboratoire. Dans le monde réel, sa portée est également susceptible d'être plus limitée que celle des anciennes technologies 802.11n et 802.11g à 2,4 GHz, et sa largeur de bande sera limitée à celle de la liaison la plus lente dans le réseau.

Toutefois, avec la technologie 802.11ac, le débit de l'utilisateur (en bits par seconde) va augmenter. Ce débit plus élevé augmentera la capacité des points d'accès 802.11ac. Parce qu'un utilisateur peut télécharger des fichiers et par exemple des pièces jointes à un email à des débits de transmission plus rapides, les canaux RF partagés seront plus rapidement libérés, donc un plus grand nombre d'utilisateurs transmettant à des débits plus élevés pourront se connecter au point d'accès.

Un certain nombre de produits prenant en charge la spécification préliminaire 802.11ac sont déjà disponibles. La Wi-Fi Alliance a par ailleurs démarré des programmes de certification pour la nouvelle norme et la certification et l'équipement devraient être déployés en deux phases, au

minimum : la première dès maintenant et la seconde dans un an ou plus pour inclure toutes les améliorations de la spécification.

Les ingénieurs réseau disposent d'un certain nombre d'options de mise en œuvre. Ils peuvent décider de déployer un site avec exclusivement un réseau sans fil 802.11ac à un endroit, alors que dans un autre, ils peuvent avoir besoin d'assurer la rétrocompatibilité des dispositifs existants avec la norme 802.11n et éventuellement d'autres protocoles antérieurs, même s'il est question d'un tout nouveau site.

3.9 Planifier la mise en œuvre de la technologie 802 .11ac

Cinq facteurs clés sont à considérer pour planifier le déploiement de la technologie 802.11ac :

- le débit
- la capacité
- l'attribution des canaux
- l'impact de l'utilisation de canaux DFS
- l'impact des normes plus anciennes

3.9.1 Mesurer le débit

Le facteur le plus important lors de la planification d'un réseau hybride est la précision, en particulier lors de la réalisation de l'étude du site. La technologie 802.11ac permet d'offrir de meilleures performances et requiert moins de points d'accès. Néanmoins, elle est plus complexe à déployer que les normes précédentes à cause de canaux moins nombreux et plus larges. De plus, la formation de faisceaux doit être prise en considération tout comme les modifications réglementaires, rendant indispensables la gestion et le contrôle RF. La force du signal n'est donc pas un véritable indicateur de performances du réseau sans fil, le seul vrai indicateur de performance étant le débit.

La solution optimale pour déployer correctement la technologie 802.11ac et profiter des améliorations qu'elle offre est donc de mener des études de site actives. Cela permet aux ingénieurs de mesurer et cartographier les performances exactes pour l'utilisateur final en utilisant un adaptateur 802.11ac et ainsi concevoir et déployer très précisément les réseaux 802.11ac.

3.9.2 Evaluation de la capacité

Utiliser un outil de planification de la performance du réseau qui prend en charge à la fois les protocoles existants et les nouveaux protocoles permet également aux ingénieurs d'évaluer si la capacité dans le réseau sans fil est suffisante. Les utilisateurs accèdent de plus en plus à des applications à large bande passante telles que Skype et les organisations doivent évaluer le niveau de préparation pour la VoIP, il est donc important de disposer d'un moyen pour déterminer si le réseau est en passe d'atteindre sa capacité maximale.

A l'aide d'un outil de planification qui fournit une visualisation des principaux facteurs de performance, tels que la largeur de canal, le chevauchement des canaux et la couverture MCS, les ingénieurs réseau peuvent rapidement déterminer les zones susceptibles de disposer du haut débit et donc dans lesquelles une forte densité de clients peut être prise en charge.

3.9.3 Planifier l'attribution des canaux

Il est important de développer un plan d'application des canaux lors de la planification du passage à la norme 802.11ac. Les canaux plus larges, introduits avec la norme 802.11ac, augmentent la probabilité d'interférences entre canaux adjacents, avec des conséquences néfastes sur les performances.

La norme 802.11ac définit un sous-canal « primaire » dans un canal couplé. Il s'agit du canal qui est utilisé pour la transmission à une bande passante spécifique. Un outil de planification doit indiquer où les canaux principaux et secondaires interfèrent les uns avec les autres pour permettre aux ingénieurs de revoir les allocations de canaux et la localisation des points d'accès afin de maximiser les performances.

3.9.4 Evaluer l'impact des canaux DFS

La bande 5 GHz utilisée par la norme 802.11ac contient des canaux capables de sélectionner la fréquence de manière dynamique (Dynamic Frequency Selection ou DFS) pour utiliser une plage de fréquence différente de celle du radar. Le point d'accès doit libérer le canal qu'il utilise s'il détecte un radar, ce dernier dégradant les performances. Un outil de planification intégrant un analyseur de spectre permettra à l'ingénieur réseau de détecter et de mesurer n'importe quel signal RF sur chaque canal pour savoir si les canaux DFS sont disponibles ou occupés. Il permet également aux ingénieurs d'identifier toute interférence indépendante du Wi-Fi. Ils

s'affranchissent ainsi de coûteuses modifications de topologie du réseau et disposent d'un environnement propre pour le déploiement de la technologie 802.11ac.

3.9.5 Impact des débits de transmission plus lents

Les ingénieurs ont besoin de s'assurer que la performance du 802.11ac n'est pas affectée par les débits de transmission plus lents des clients 802.11a et n. En utilisant une carte de couverture, ils peuvent visualiser les régions où les anciens clients peuvent être pris en charge, tandis qu'une étude de débit utilisant un client 802.11ac validera que le réseau sans fil puisse fournir les performances nécessaires pour l'utilisateur.Par décodage des trames de gestion 802.11ac en temps réel, les ingénieurs peuvent détecter les capacités VHT des points d'accès et ainsi résoudre les problèmes de performance des réseaux 802.11ac résultants de la présence d'anciens clients.

3.9.6 Les avantages de la technologie 802.011ac

- Un débit de données plus élevé : fournir des données à un débit de 1,3 Gbit/s soit plus du double de celle d'un réseau n certifié Wi-Fi.
- Une capacité élevée : possibilité de connecter plus de périphériques simultanément à un réseau ac certifié Wi-Fi sans diminuer les performances pour résoudre des problèmes de congestion.
- Un faible temps de latence : les produits certifiés Wi-Fi peuvent offrir une expérience utilisateur de qualité supérieure avec des applications telles que les jeux ou la diffusion de musique pour lesquelles le moindre retard peut être préjudiciable.
- Une utilisation efficace de l'alimentation : avec les améliorations du Wi-Fi certifié ac, la consommation d'énergie liée à la transmission des données est réduite.

3.10 Conclusion

Nous avons vu les généralités sur la qualité de service particulièrement dans les réseaux 802.11 et introduit les aspects de la nouvelle norme 802.11 ac. Nous allons maintenant voir dans le dernier chapitre la présentation du logiciel OPNET el la simulation.

CHAPITRE 4

SIMULATION SUR OPNET

4.1 Introduction

La quantité d'information qui circule dans nos réseaux est devenue très importante, les routeurs, qui sont les points névralgiques du réseau Internet, sont ceux qui priorisent, filtrent, et dirigent les flux Internet qui évolue rapidement en termes de taille mais également en termes d'architecture et de topologie.

Modéliser un système virtuel de façon interactive, observer les principaux concepts associés à fin d'évaluer ses performances et prévoir le comportement le déploiement physique, permet de disposer d'un réseau robuste, performant et aussi faire un gain de temps et d'argent important.

4.2 Les besoins

Le besoin de l'utilisateur est l'interactivité du simulateur. Celle-ci lui permettra de voir, en temps réel, l'évolution du trafic sur le réseau par rapport à différents critères (débit, ...).

Grâce à la constante évolution des moyens de calculs, les simulations numériques deviennent de plus en plus complexes. Il n'est pas rare de trouver différents modèles et codes couplés sur un réseau hétérogène (ex. les simulations multi-physiques). Même si les enjeux de la simulation interactive sont aujourd'hui bien perçus, la communauté du calcul scientifique exprime toujours le besoin d'une nouvelle génération d'outils pour le pilotage des simulations numériques sur de environnements distribués. Le domaine de la simulation interactive ou « computational steering » a pour but d'améliorer le processus de simulation numérique (modélisation, calcul, analyse) en le rendant plus interactif.

4.3 La Simulation

La simulation des réseaux de télécommunication consiste à modéliser de façon conforme à la réalité comportement des différents éléments constituants ces réseaux par des outils informatiques afin de récolter des données statistiques. Elle complète souvent la modélisation mathématique et permet de mieux étudier les détails de fonctionnement d'un système complexe.

4.4 L'outil OPNET

OPNET (Optimum Network Performance) est une famille des logiciels de modélisation et de simulation de réseaux s'adressant à différent public tel que les entreprises, les opérateurs et la recherche.

L'environnement OPNET permet la modélisation et la simulation de réseaux de communication grâce à ses bibliothèques de modèles (routeurs, commutateurs, stations de travail, serveurs) et de protocoles (TCP/IP, FTP, FDDI, Ethernet, ATM …).
OPNET permet la simulation des réseaux de radiocommunication : hertzien, téléphonie cellulaire et satellitaire.

Le but de ce projet de fin d'étude est d'aider à la familiarisation avec le logiciel OPNET Modeler, c'est à dire de connaître les actions de base pour la simulation, d'utiliser les principales interfaces et bibliothèques de modèles implantés dans OPNET (modèles standards, matériels, protocolaires et applicatifs).

OPNET est basé sur des modélisations hiérarchiques, cette méthode correspond bien à la structure des réseaux actuels. Il dispose de trois niveaux hiérarchiques imbriqués :

1. le plan de réseau (network Domain).
2. le plan de nœud (node Domain).
3. le plan de processus (process Domain).

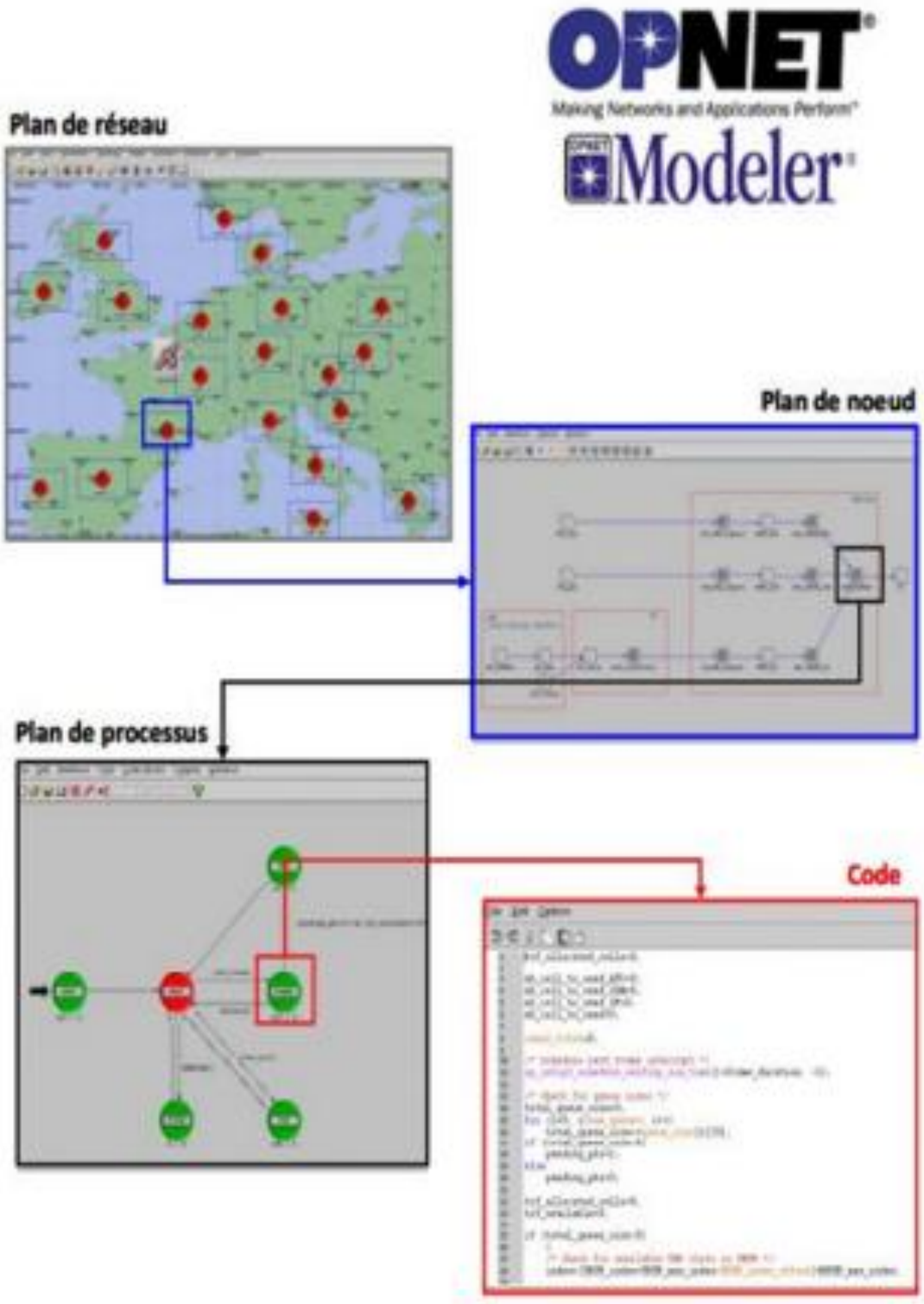


Figure 4.01 : *Modélisation hiérarchique dans l'environnement OPNET.*

OPNET utilise un modèle hiérarchique qui se base sur des frontières physiques et fonctionnelles décrivant d'une façon précise les topologies et les flux échangés dans un système de communication.

Ce modèle hiérarchique présente trois niveaux de description. Pour chaque niveau, en plus de la large bibliothèque d'objets disponible pour l'utilisateur, de nouveaux objets peuvent aussi être créés.

4.4.1 Network Domain

Plan de réseau : est le niveau le plus élevé de la hiérarchie d'OPNET qui présente la topologie physique d'un réseau de communication. Il permet de décrire la topologie générale du réseau étudié.

Le réseau est décrit sous forme d'un ensemble d'éléments de communication (routeurs, stations de travail, hub, etc.) qui sont appelés les nœuds et de liens entre eux. Les utilisateurs peuvent configurer le réseau en paramétrant les attributs associés aux nœuds et aux liens.

4.4.2 Node Domain

Plan de nœud : permet de définir l'architecture des nœuds (routeurs, stations de travail, hub, etc.) en traduisant les flux de données échangés entre les blocs fonctionnels appelés les modules. Les modules peuvent représenter les applications, les couches de protocoles, les buffers, etc. Les modules peuvent communiquer entre eux via des flux des paquets ou via des liens statistiques(échanger des informations de statistiques, par exemple : remplissage de file d'attente, délai limitede transmission, etc.). La fonctionnalité de chaque module est ensuite spécifiée au niveau processus.

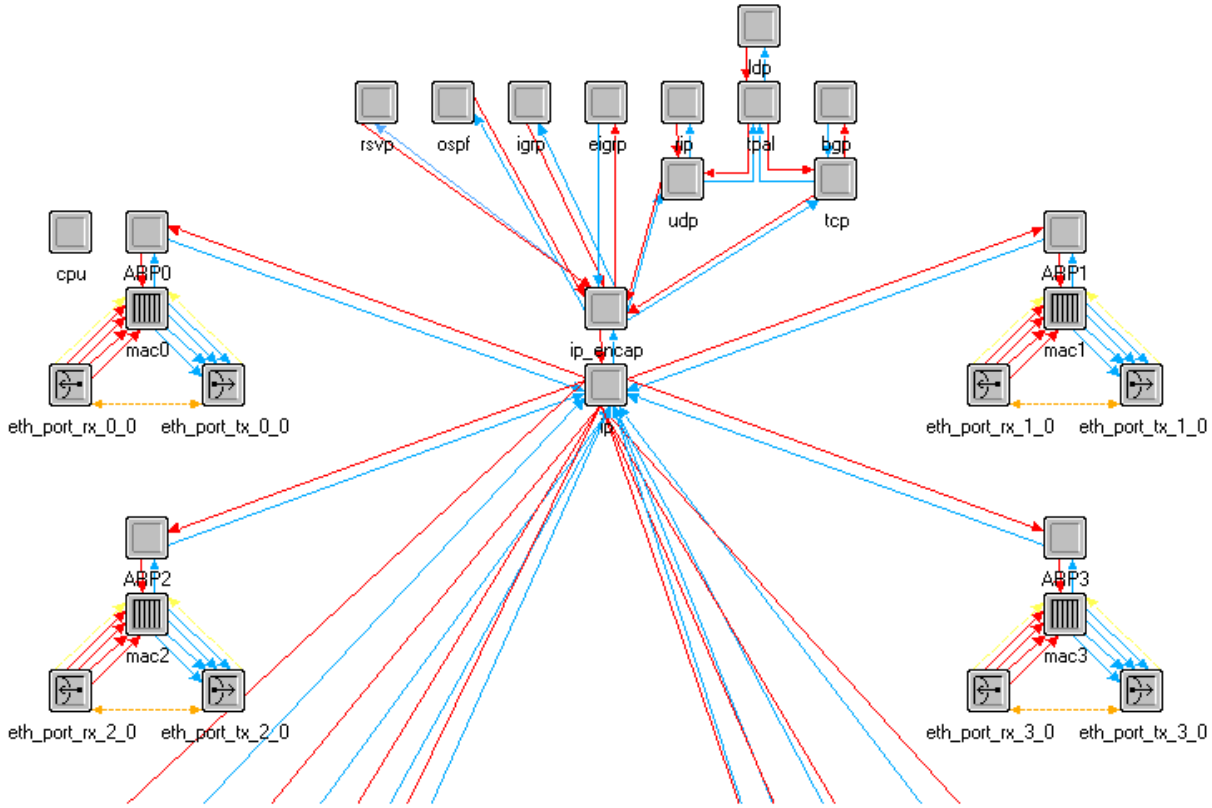


Figure 4.02 : *Node domain sous opnet*

Certains modules sont non programmables : il s'agit principalement des transmitters et des receivers, dont la seule fonction est de s'interfacer entre le nœud et les liens auxquels il est connecté.

Les autres modules sont entièrement programmables : il s'agit des processors et des queues. Les processors sont des modules qui remplissent une tâche bien précise du nœud : ils symbolisent en fait les différentes parties du système d'exploitation d'une machine, et plus principalement les différentes couches réseau implémentées dans le nœud (Ethernet, IP…).

Les processors peuvent communiquer entre eux via des packets streams (flux de paquets), qui permettent de faire transiter un paquet d'une couche à une autre à l'intérieur d'une même machine.

Cette organisation permet d'avoir une vision claire de la pile de protocoles implémentée dans un nœud, et de connaître rapidement leurs interactions.

Par exemple, le module IP est relié, via des streams, aux modules de la couche 4 tels que TCP, UDP, et de la couche 2 (Ethernet).
Les statistic wires constituent le second type de lien permettant une communication entre modules comme leur nom l'indique, ils permettent de faire remonter des informations de statistiques d'un module à l'autre, comme par exemple la taille et le délai des queues des transmitters.

4.4.3 Process Domain

Plan de processus : Les modèles de processus sont représentés par des machines à états finis FSM. Des icônes représentent les états et des liens représentent les transitions entre les états. Les opérations effectuées dans chaque état ou par chaque transition sont décrites par des codes en C ou C++. Un éditeur de processus permet alors de créer des modèles de processus qui contrôlent les fonctionnalités d'un modèle de nœud créé dans l'éditeur de nœuds.
C'est à ce niveau que l'on définit le rôle de chaque module programmable. Un module possède par défaut un processus principal, auquel peuvent s'ajouter des processus fils accomplissant une sous- tâche précise.
OPNET fournit des mécanismes permettant à tous les processus créés à l'intérieur d'un process domain de communiquer entre eux, via un bloc de mémoire partagée, ou l'ordonnancement d'interruptions logicielles. Le rôle d'un module est déterminé par son process model, que l'on décrit sous forme d'une machine à états finis (finite state machine).
Chaque bloc représente un état différent, dans lequel la machine exécute un code déterminé.
Les transitions sont symbolisées par des liens entre blocs et déterminées par des conditions (interruptions, variable ayant une certaine valeur…) Les actions à effectuer sont décrites en langage C, et OPNET fournit une bibliothèque de plus de 400 fonctions propriétaires spécifiques à l'usage des réseaux (création, envoi et réception de paquets, extraction de valeurs contenues dans les différents champs d'une entête…).
Fort heureusement, une aide conséquente permet de trouver facilement les informations dont on a besoin.
En plus de ces trois niveaux de hiérarchie, un modèle de paquet OPNET permet de définir le format et le contenu des échanges d'information. L'éditeur de projets d'OPNET permet, sur un modèle de réseau de récupérer des statistiques et les représenter sous différents types de graphiques ou de les exporter vers d'autres logiciels. Des « sondes » permettant de mesurer des

paramètres préalablement définis sur OPNET peuvent être placées n'importe où dans la hiérarchie présentée précédemment.

4.5 Simulation par l'outil OPNET

OPNET fournit une liste impressionnante d'implémentations de routeurs, de stations de travail, des switchs

On peut donc construire une simulation de réseaux en utilisant principalement deux méthodes :

1. En utilisant les nœuds préprogrammés fournit par la librairie de OPNET.
2. En commençant tout depuis le début et en définissant soi-même un modèle de lien, des process models décrivant des routeurs et des hôtes.

Cette méthode est bien évidemment plus complexe que la première, et nécessite de bonnes connaissances en matière de programmation et de réseaux. Néanmoins elle est indispensable dans le cas où l'on désire expérimenter un algorithme tout nouveau.

Pour chaque niveau hiérarchique présenté ci-dessus, les éditeurs graphiques correspondants sont utilisés pour simplifier la modélisation. De plus, OPNET dispose de beaucoup d'éditeurs/outils supplémentaires (éditeur de paquets, outil de sondes, outil de simulation, etc.) qui permettent facilement et efficacement de simuler et analyser le réseau étudié.

La modélisation et la simulation sous OPNET peuvent se faire de deux manières :

- en utilisant la palette pré-modélisée dans la bibliothèque d'OPNET
- en programmant soi-même les composants suivant l'ordre hiérarchique

Certainement, la première méthode est beaucoup plus rapide et facile que la deuxième car les programmations et les descriptions des éléments sont « transparentes » pour les utilisateurs. Par contre, dans le cas où des nouveaux algorithmes ou protocoles doivent être testés, la deuxième méthode, qui est une étape indispensable, est plus souple et plus facile à adapter que la première.

Principales interfaces

Parmi les nombreuses interfaces que propose OPNET au démarrage, on distingue les interfaces suivantes :

1. Project Editor
2. Network Model Editor

3. Node Model Editor
4. Process Model Editor
5. Antenna Pattern
6. Modulation Curve
7. Simulation Sequence
8. Analysis Configuration

4.5.1 Project Editor

C'est l'interface principale du logiciel. Elle permet d'implanter des modèles issus des bibliothèques

OPNET ainsi que des modèles créés par l'utilisateur. C'est aussi à partir du Project Editor que les simulations peuvent être configurées puis lancées et que les résultats issus de ces simulations peuvent être affichés.

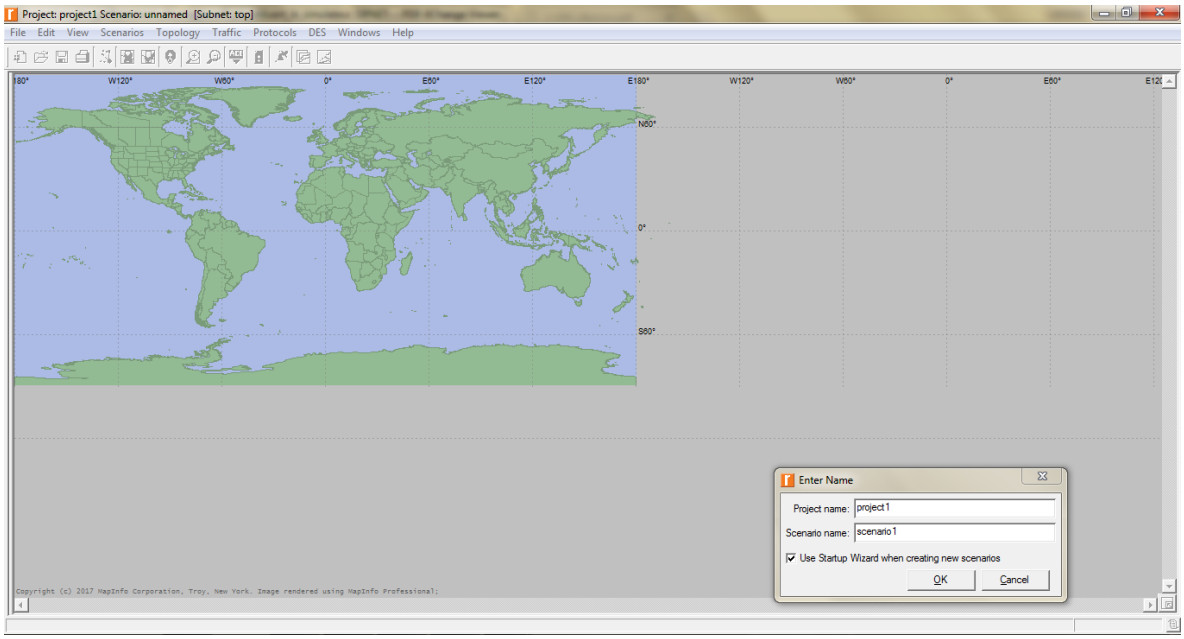


Figure 4.03* : *Interface principale

Les principales fonctions de cette interface sont disponibles sous formes d'icônes.

1 – Ouvrir la palette d'objet

2 – Vérification des liens

3 – Mise en panne d'un appareil ou d'un lien

4 – Remise en marche d'un appareil ou d'un lien

5 – Retour au réseau supérieur

6 / 7 – Zoom + / -

8 – Lancer la simulation

9 – Visualiser les graphiques et statistiques collectés

10 – Visualiser le rapport le plus récent

11 – Visualiser tous les graphiques

4.5.2 Network Model Editor

Permet de représenter la topologie d'un réseau de communication constitué de nœuds et de liens par l'intermédiaire de boîtes de dialogues (palettes et glisser/poser). Cette interface tient compte du contexte géographique (caractéristique physique pour la modélisation).

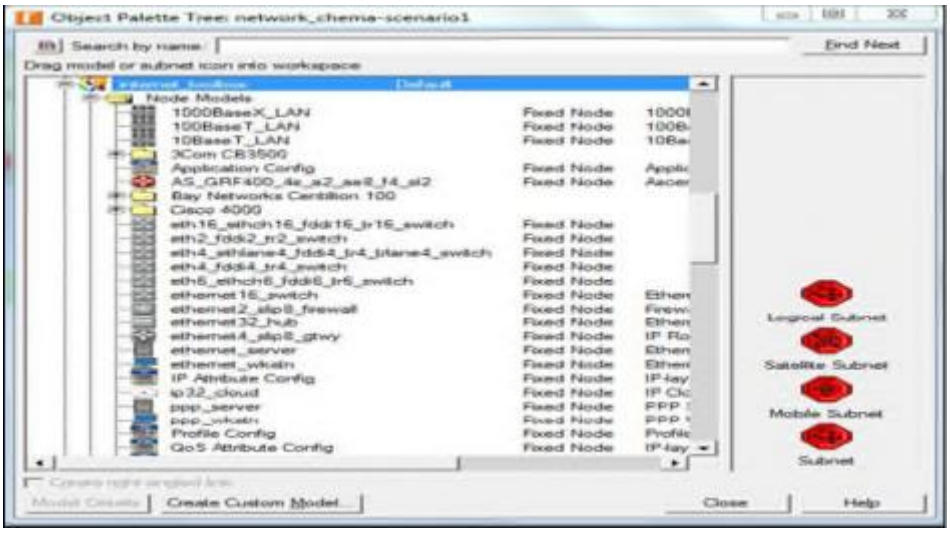


Figure 4.04 : *Editeur des objets*

Affiche une représentation modulaire d'un élément de la bibliothèque on d'un élément créé par l'utilisateur. Chaque module envoie et reçoit des paquets vers d'autres modules. Les modules représentent des applications, des couches protocolaires ou des ressources physiques (buffer, port).

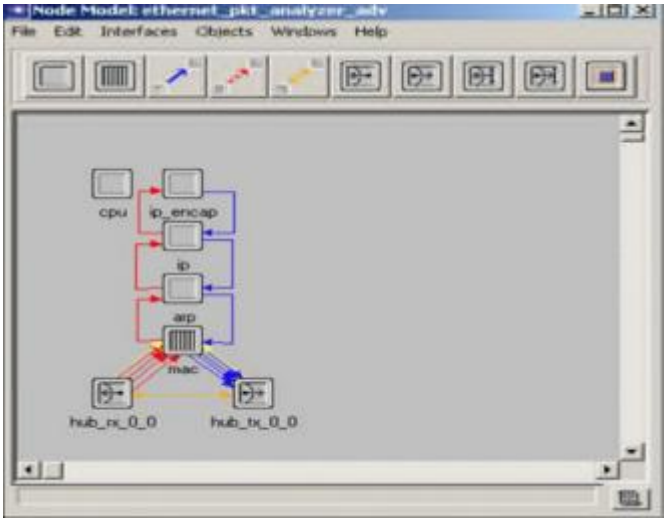


Figure 4.05: Node Model Editor

4.5.3 Process Model Editor

C'est l'interface donne une représentation d'un module par des machines à états finis, chaque état est liés à un autre état par des transitions conditionnelles ou non conditionnelles.

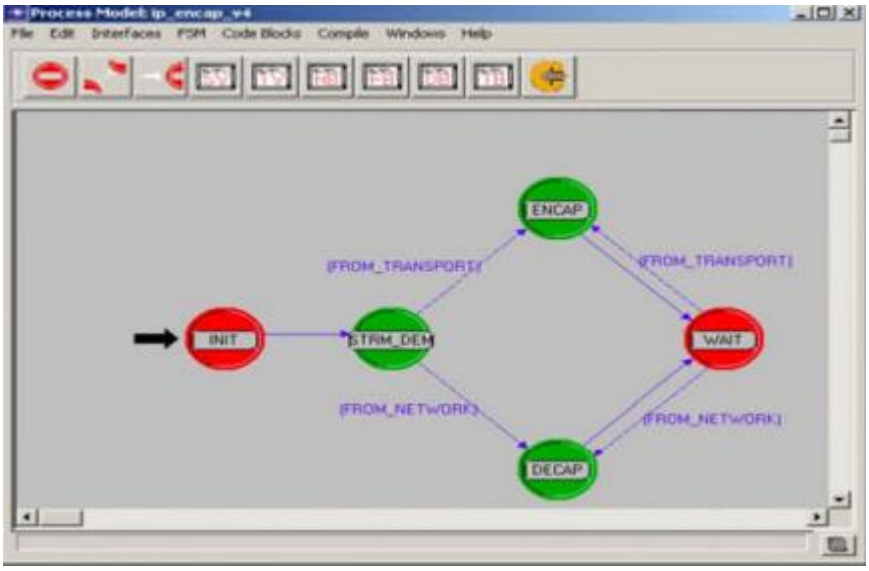


Figure 4.06 : *Process model editor*

4.5.4 Antenna Pattern

Cette interface permet de modéliser une antenne pour radiocommunication par son diagramme de rayonnement 3D, coordonnées polaires.

4.5.5 Simulation Séquence

Permet de paramétrer la ou les simulations OPNET en temps et attributs des modèles (types de liens, d'antenne, de services …).

4.5.6 Analysis Configuration

Pour le stockage des résultats issus des simulations sous différentes formes.

4.6 Simulation et interprétation des résultats

4.6.1 Création d'un nouveau projet

Lorsque l'on crée un nouveau modèle de réseau, on crée un nouveau projet et un scénario associé. Un projet est en fait constitué d'un ensemble de scénario reliés les uns aux autres, chacun montrant un aspect différent du réseau.

Pour créer un réseau, nous allons définir sa topologie initiale, son échelle, sa taille, le lieu et nous allons y associer une palette d'objet.

Pour créer un nouveau projet, on choisit File -> New. La fenêtre suivante s'affiche :

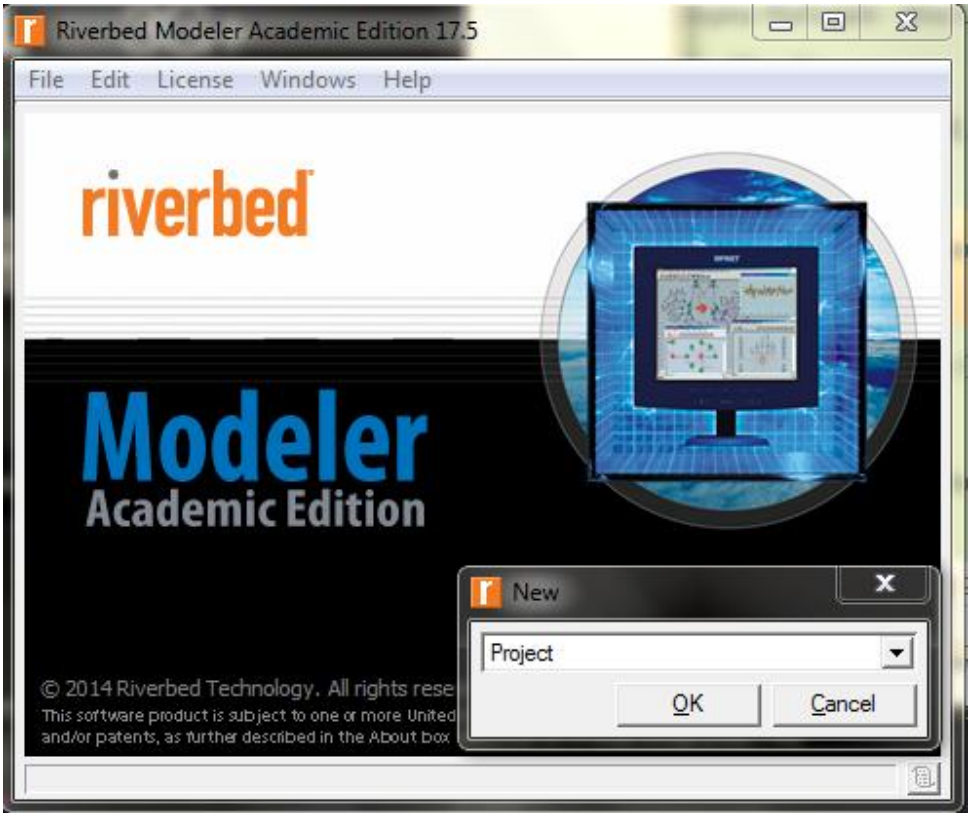


Figure 4.07 : *Création d'un projet*

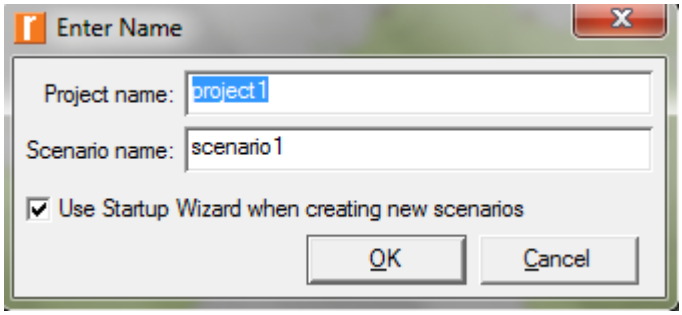


Figure 4.08 : *Création d'un scénario*

Puis on va créer le nom du projet puis le scénario

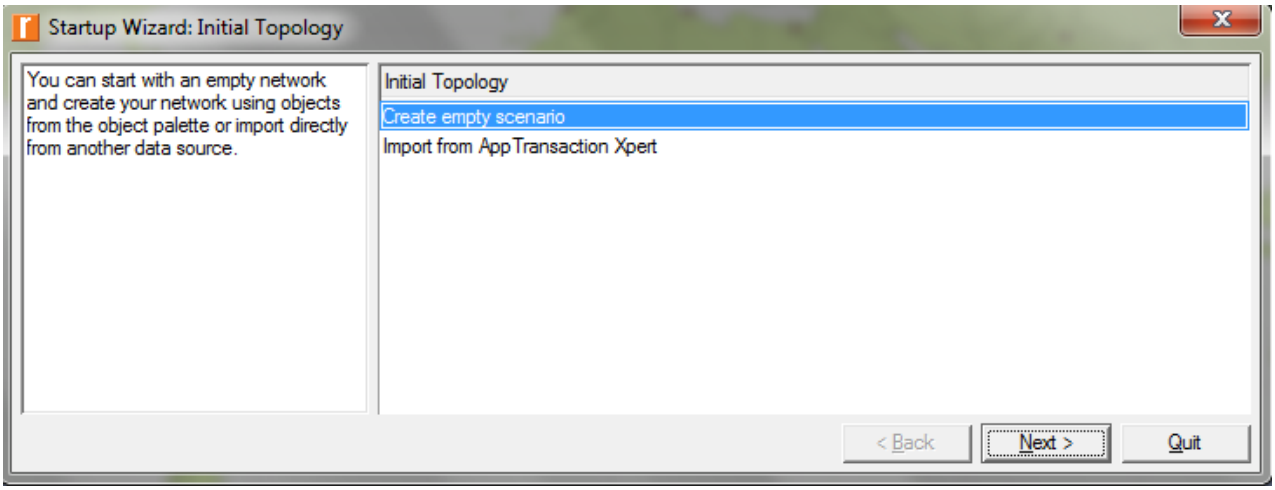


Figure 4.09 : *Création d'un scénario vide*

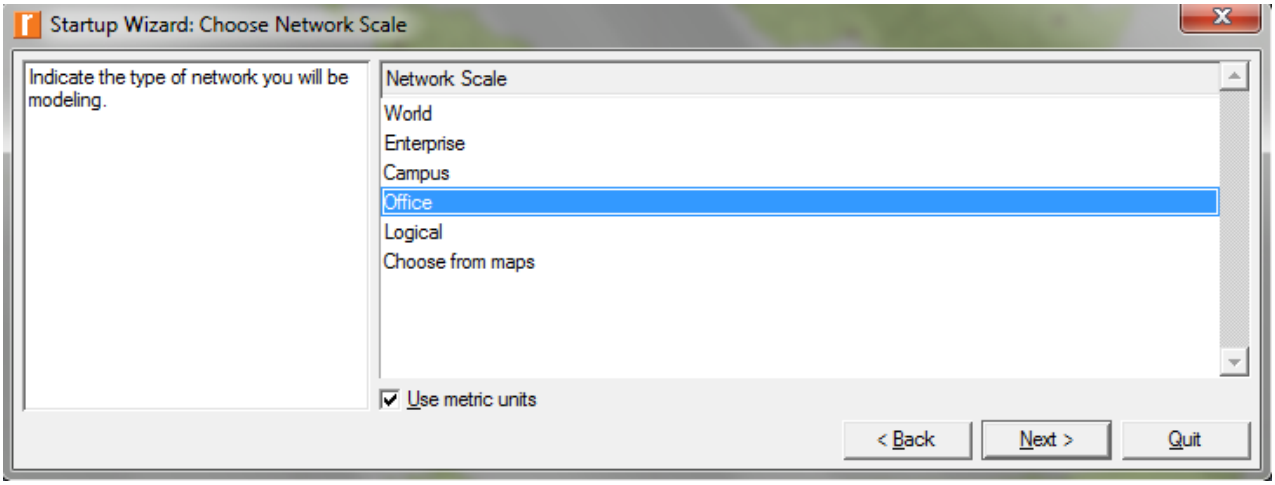


Figure 4.10 : *Type de réseau*

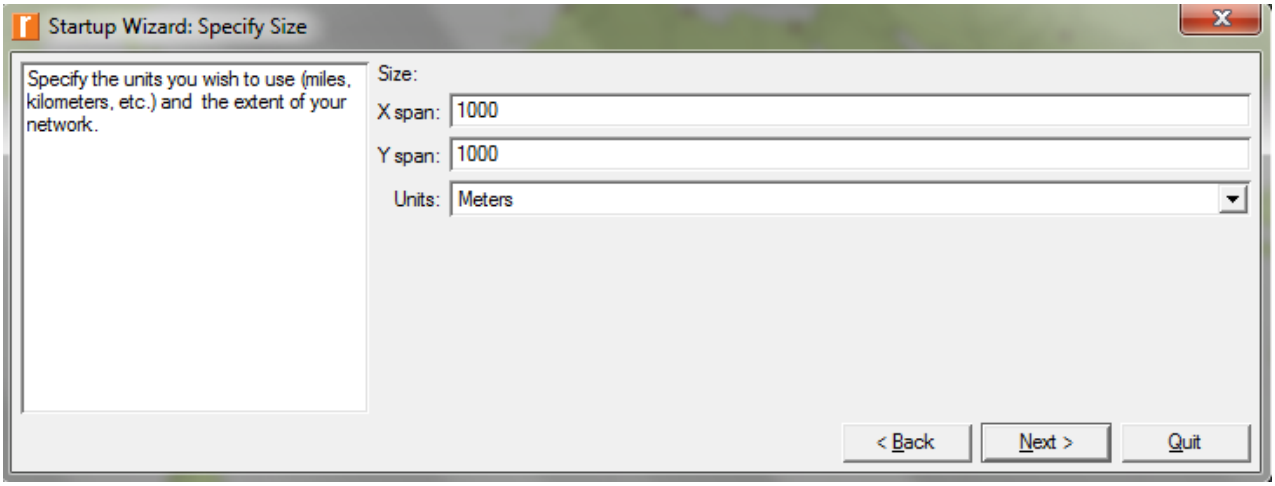


Figure 4.11 : *Position de réseau*

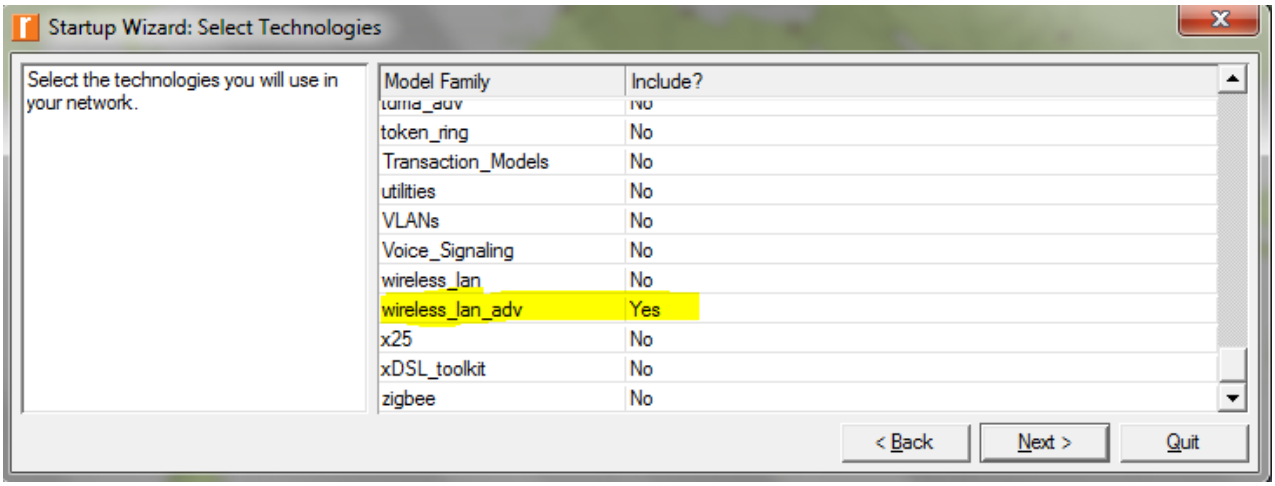


Figure 4.12 : *Type de la technologie du réseau*

Pour faire le network mobile, on a besoin de choisir un utilisateur sous forme mobile station et de poser un point d'accès (Access Point) qui doit être relié par un router ou Gateway qui est lui-même relié par un serveur qui contient notre application.

1. Si elle n'est pas encore ouverte, ouvrir la palette d'objet en cliquant sur l'icône.
2. La première étape c'est créé un point d'accès, on choisir Wireless_lan_adv.
3. Trouver l'objet wlan_ethernet_slip4_adv dans la palette et faites-le glisser dans l'espace de travail.
4. Vous n'avez pas besoin d'autres copies de cet objet. Faites un clic droit pour stopper la création.

Nous avons aussi besoin de connecter le point d'accès au routeur ou Gateway

1. On choisir Ethernet qui contient ethernet4_slip8_gtwy qui est un nœud fixé (fixed nœud) et faites-le glisser dans l'espace de travail.

Puis on a besoin d'un serveur.

2. Trouver l'objet ethernet_server dans la palette et faites-le glisser dans l'espace de travail.
3. Faites un clic droit pour stopper la création.
4. Puis on choisir Wireless_lan_avd et on choisi wlan_wkstn_adv (Works station mobile) parce qu'on a besoin d'un nœud mobile.
5. Un lien de 100BaseT relie alors les trois objets.

Relié Access point au Gateway et Gateway au server.

6. Faites un clic droit pour arrêter la création.

Par exemple quand on a dans la maison et on connecte avec le mobile donc le mobile connecte Access point qui est le modem et le modem lui-même connecte le Gateway qui permet ce dernier de se connecté au serveur qui est par exemple Google ou Yahoo…etc.

7. On va renommer chaque nœud crée par clic droit sur chaque nœud et choisir Set NameChapitre (Access_point, Gateway et http server).

Donc nous avons créé notre réseau.

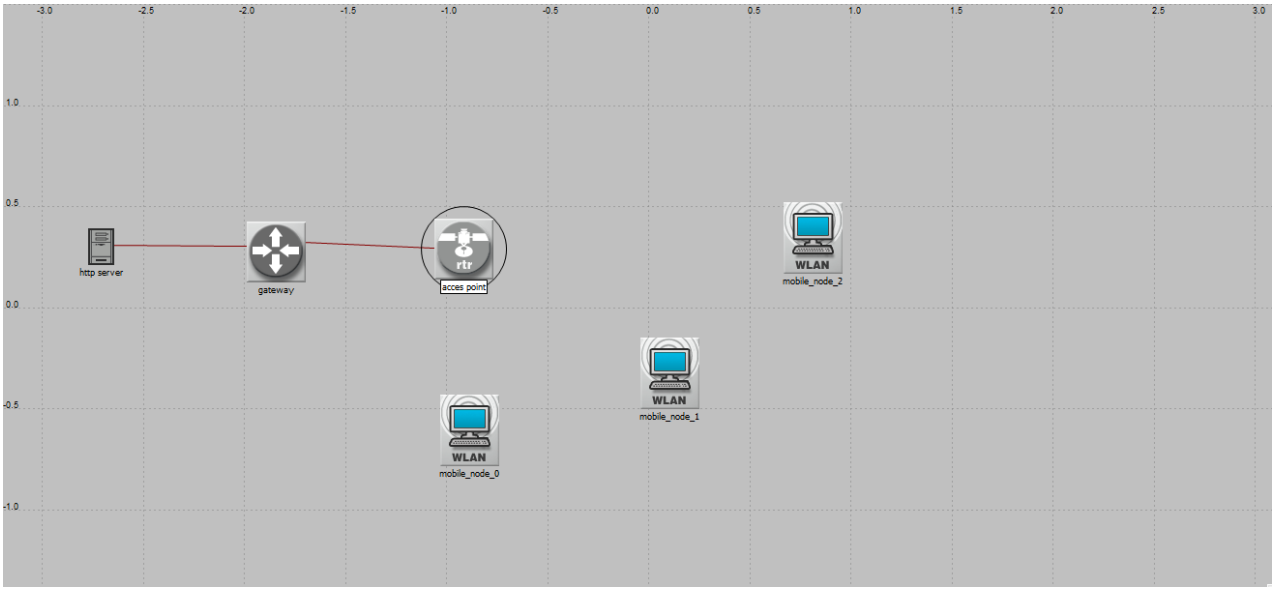


Figure 4.13 : *Architecture de notre réseau*

Nous avons besoin d'ajouter des objets de configuration pour spécifier le trafic des applications qui existent sur le réseau. La configuration des applications peut être très compliquée, c'est pourquoi nous utiliserons les configurations par défaut des applications standard.

Il suffira de placer les objets dans le réseau, cela signifiera que le trafic engendré par les stations de travail sur le réseau sera modélisé.

1. Trouvez l'Application_Config dans la palette et faites-le glisser sur l'espace de travail.
2. Faites un clic droit pour arrêter la création.
3. Trouvez l'objet Profile_Config, le placer sur l'espace de travail puis faire un clic droit
4. Fermez la palette objet.

Application config Définie les applications qui on a donné dans notre réseau.

Par exemple, on va donner application de http pour notre mobile.

1. Faites un clic droit sur l'Application_Config et clic sur edit attributes.

Donc choisir dans le number of rows le nombre 1 qui définis le nombre des applications utilise.

2. Donc elle va demander de donner un nom de votre application. On va le renommé par exemple par http app.
3. Puis définir l'application http par image Brousing

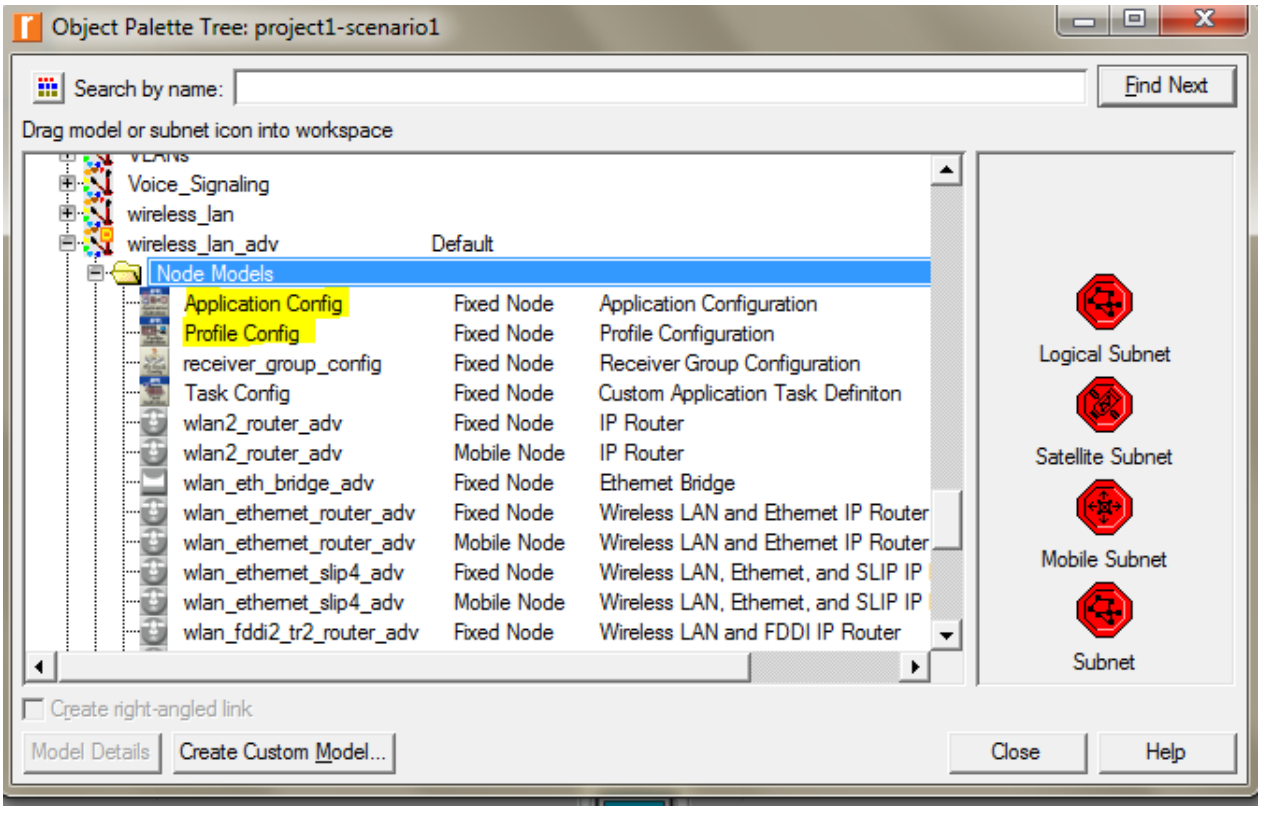


Figure 4.14 : *Editeur des objets*

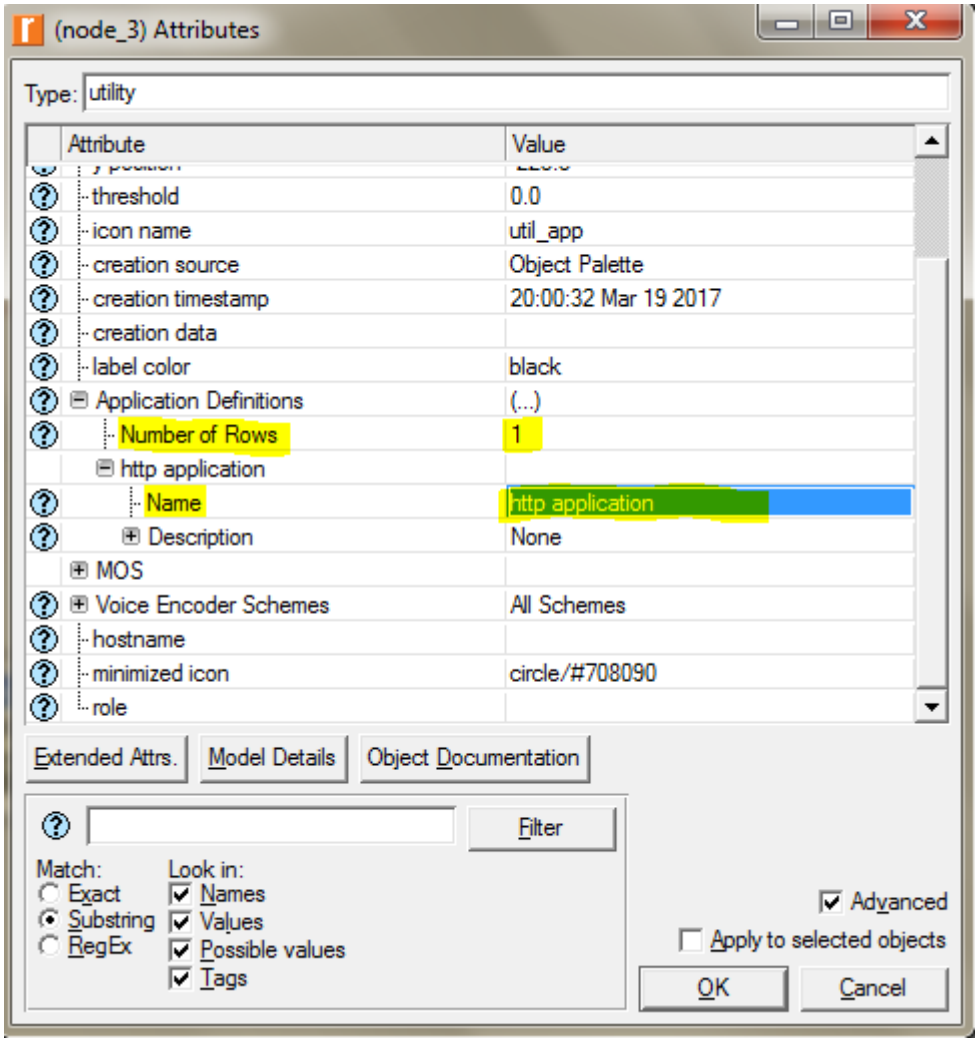


Figure 4.15 : *Configuration application*

Profile config : profile de notre application.

Dans notre exemple :

1. Faites un clic droit sur Profile_Config et clic sur edit attributes.

Choisir dans le number of rows le nombre 1 qui définis le nombre des profils utilisés.

2. Donc elle va demander de donner un nom de votre profil. On va le renommé par exemple par profile1.
3. Puis choisir l'application http qui doit être déjà définie dans Application_Config.

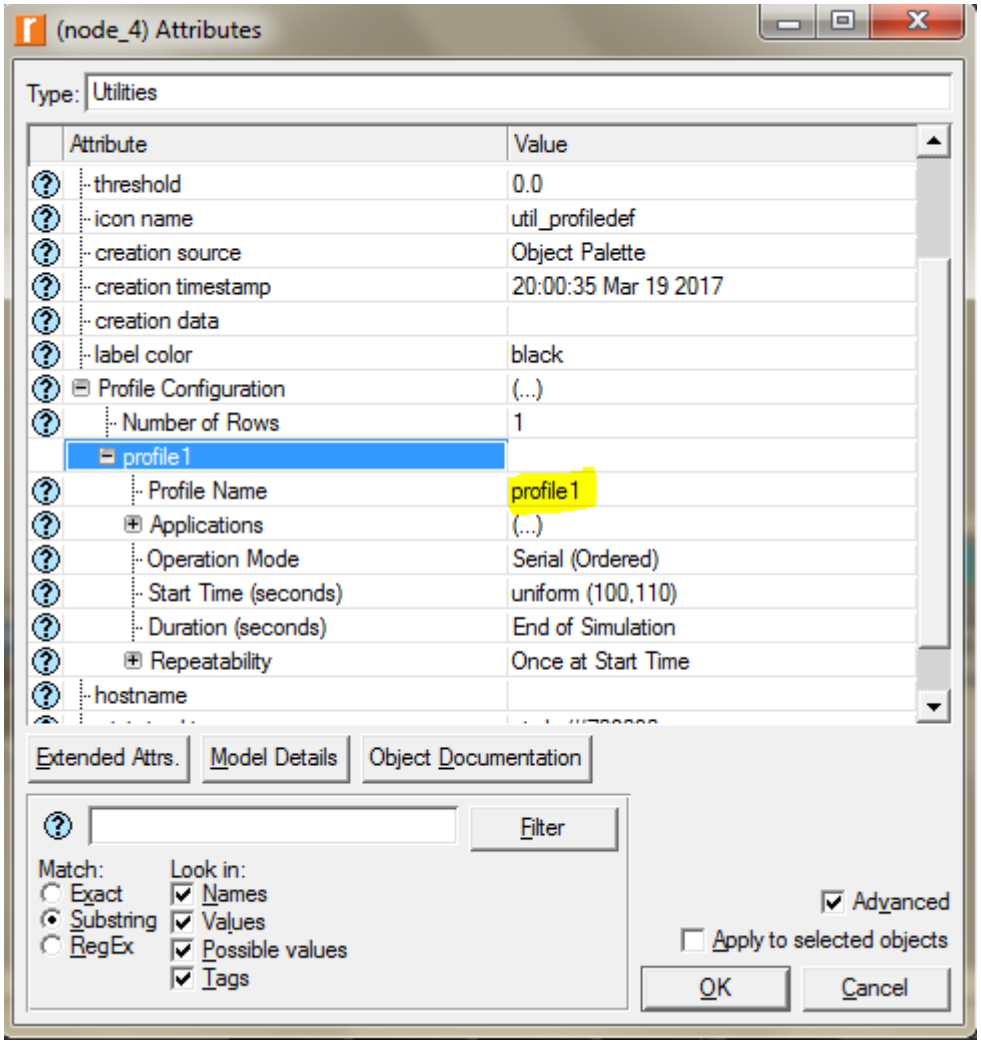


Figure 4.16 : Profile d'application

Le serveur Ethernet

1. Faites un clic droit sur ethernet_server et clic sur edit attributes.

Donc choisir dans Application : supported profiles le nombre 1 qui définis le nombre des profils et les profils utilisés.

2. Puis choisir All dans Application : supported services parce que on a un seul application (http).

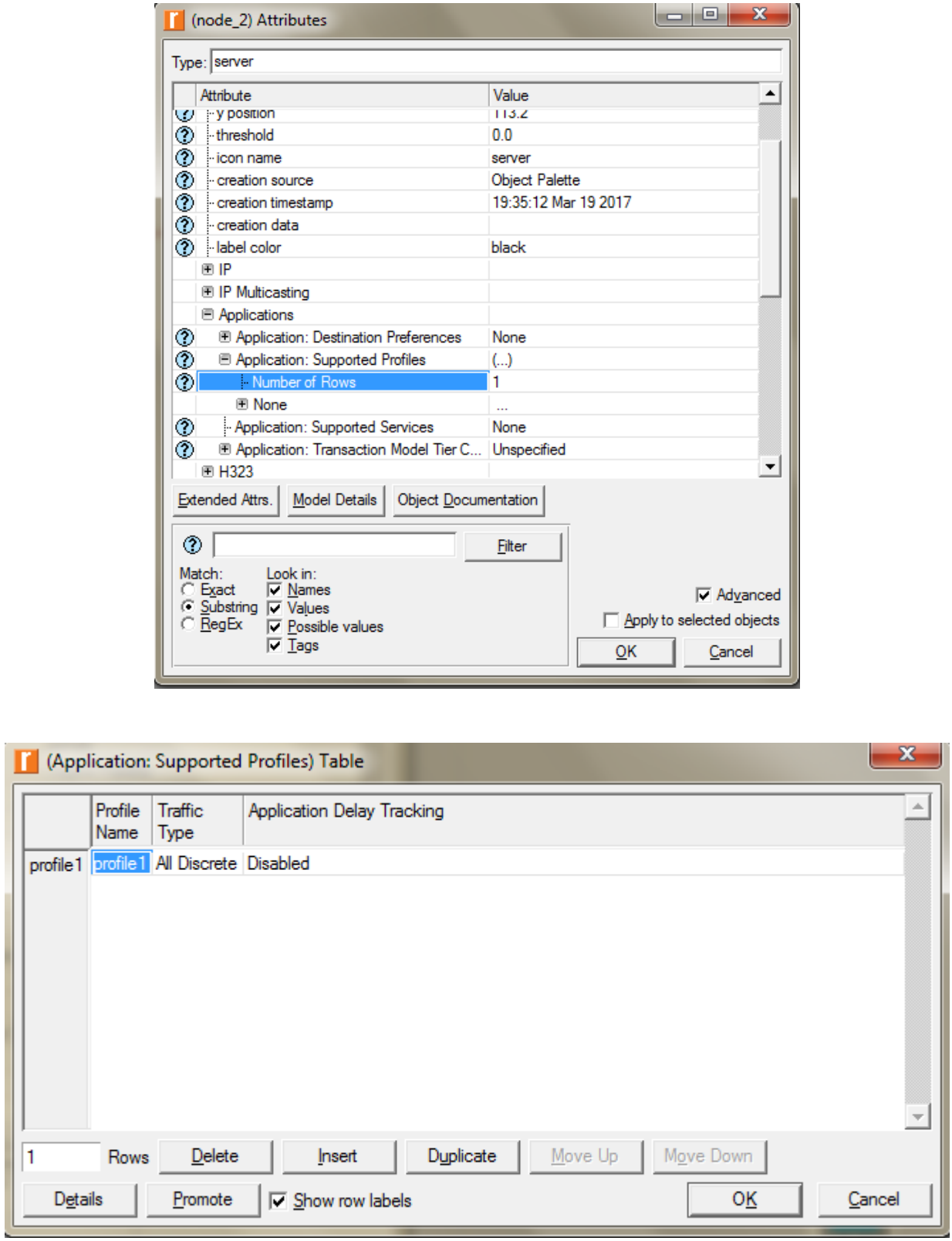


Figure 4.17 : *Configuration de serveur réseau*

Node mobile : Définir quel profil doit être supporté.

1. Faites un clic droit sur mobile_node_0 et clic sur edit attributes.

Donc choisir dans Application : supported profiles le nombre 1 qui définis le nombre profiles et les profiles utiliser.

2. Puis choisir All dans Application : supported services.

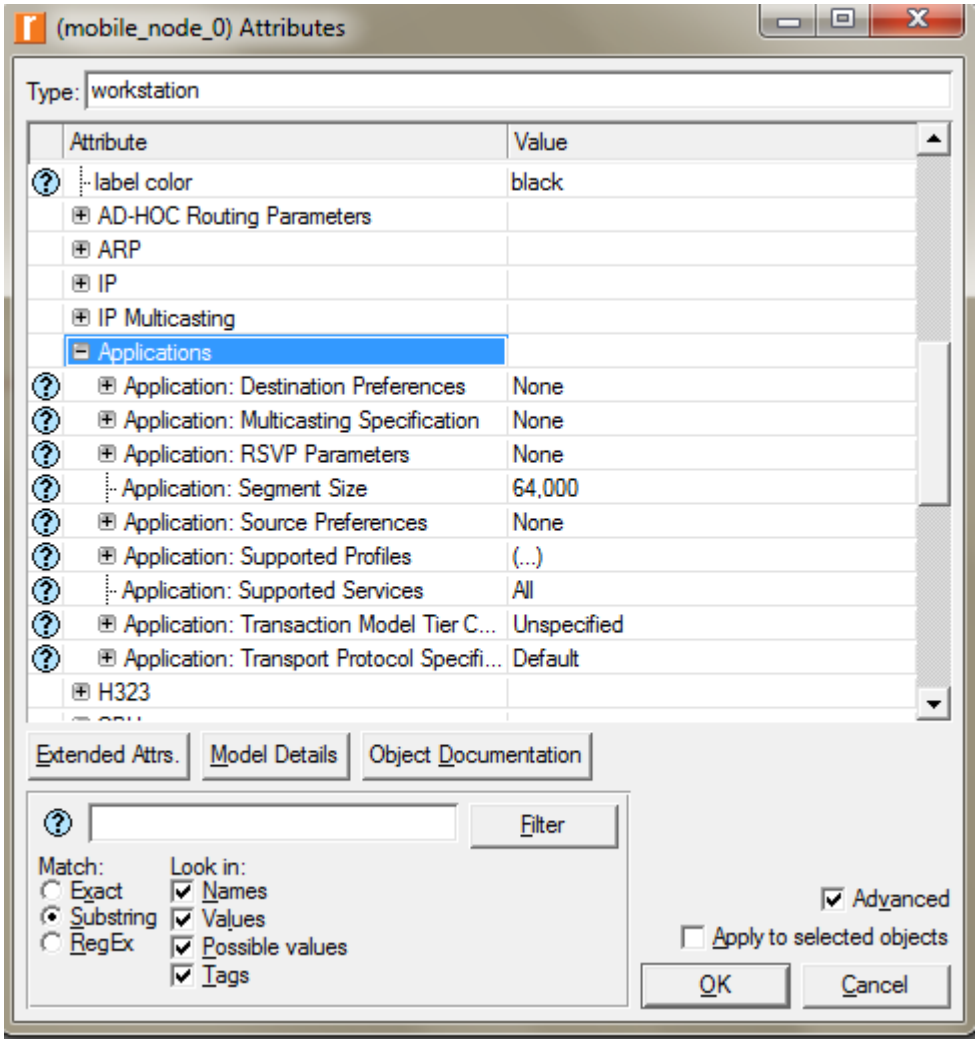


Figure 4.18 : *Configuration nœud mobile*

Access point : Le point d'Accès existe dans un réseau Wifi donc

- Faites un clic droit sur le point d'accès et clic sur edit attributes.

Donc définie dans Wireless Lan l'identifiant de notre point d'accès pour faire la différence entre les autres points d'accès.

On va le renomme par 1.

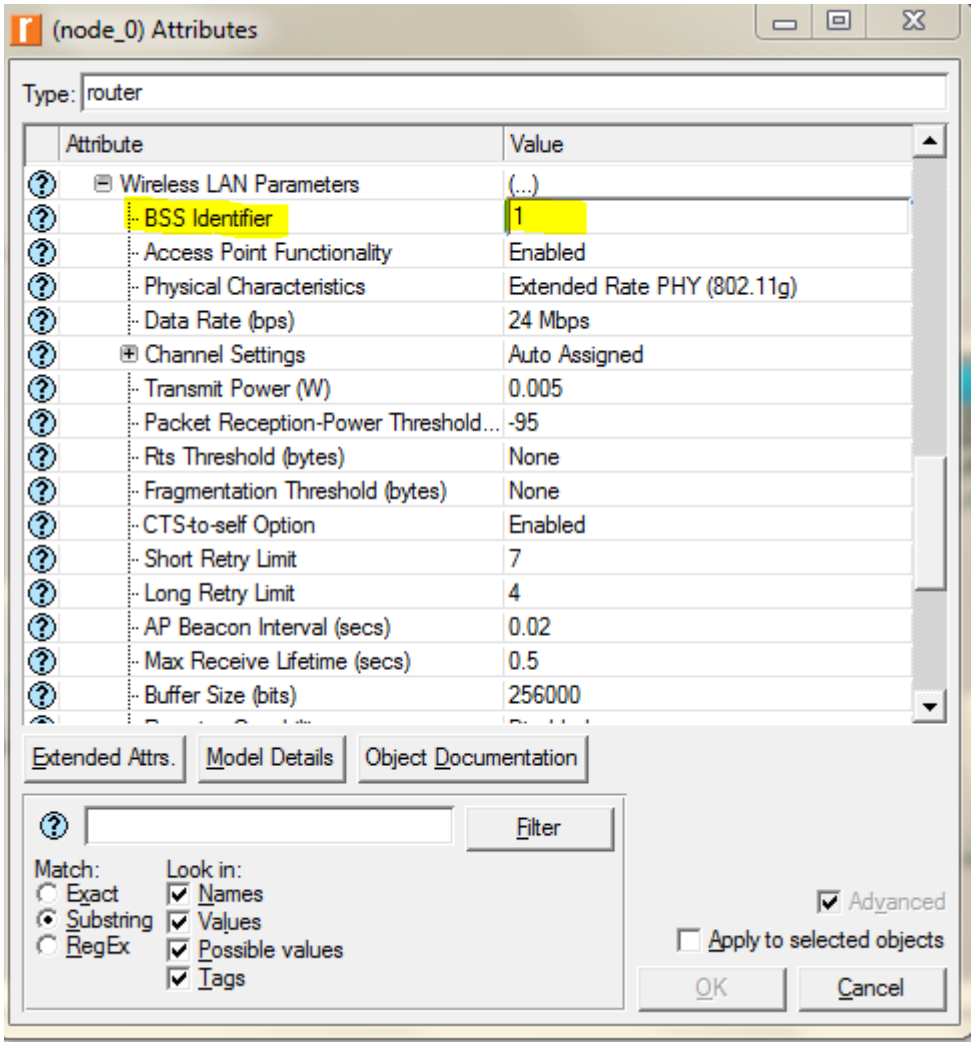


Figure 4.19 : *Configuration du point d'accès*

La même chose pour le node mobile avec changer le Access point functionalitty en mode disable.

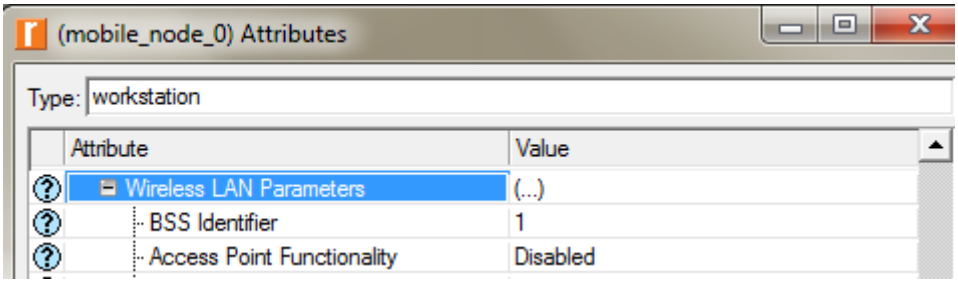


Figure 4.20 : *Configuration fonctionnalité nœud mobile*

Notre mobile (Wireless) doit être bougé autour du point d'accès donc

- Faites un clic droit sur le node mobile et choisir Define trajectory
- On renomme notre trajectoire par wifi trj et mettre le speed en 1km/hSpeed c'est la vitesse de mobile, le maximum c'est 10km/h

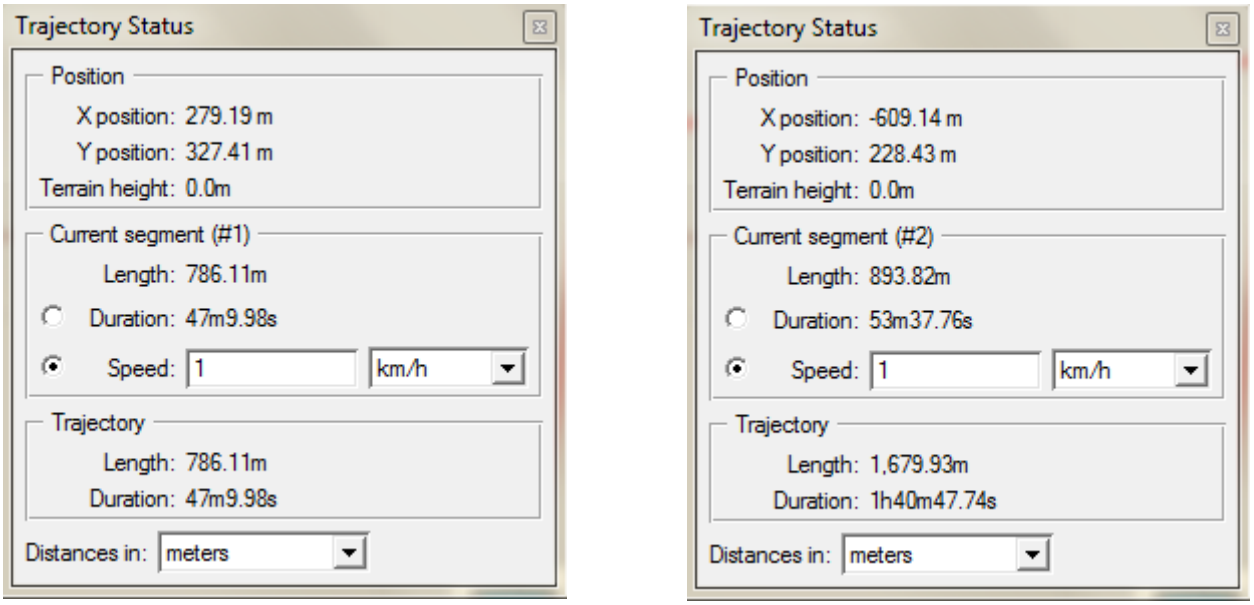


Figure 4.21 : *Configuration de mobilité*

- et en même temps désigne la voie du mobile au tour de point d'accès
- Faites un clic droit sur le node mobile et choisir edit attributes et on modifie notre trajectoire par le nom qui déjà donne et en même temps désigne la voie du mobile autour du point d'accès
- Faites un clic droit sur le node mobile et choisir edit

Donc nous avons créé notre réseau et dessiné la voie du notre mobile. On peut voir la trajectoire du mobile quand elle se déplace en cliquant sur view et choisir show time contrôleur.

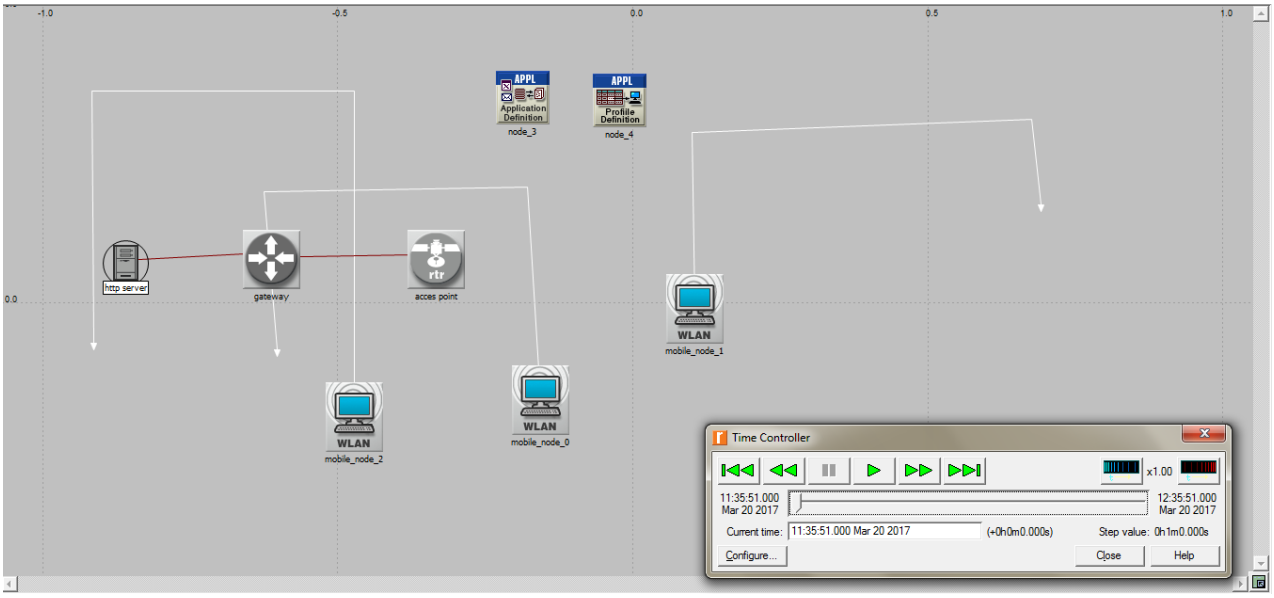


Figure 4.21 : *L'architecture du réseau*

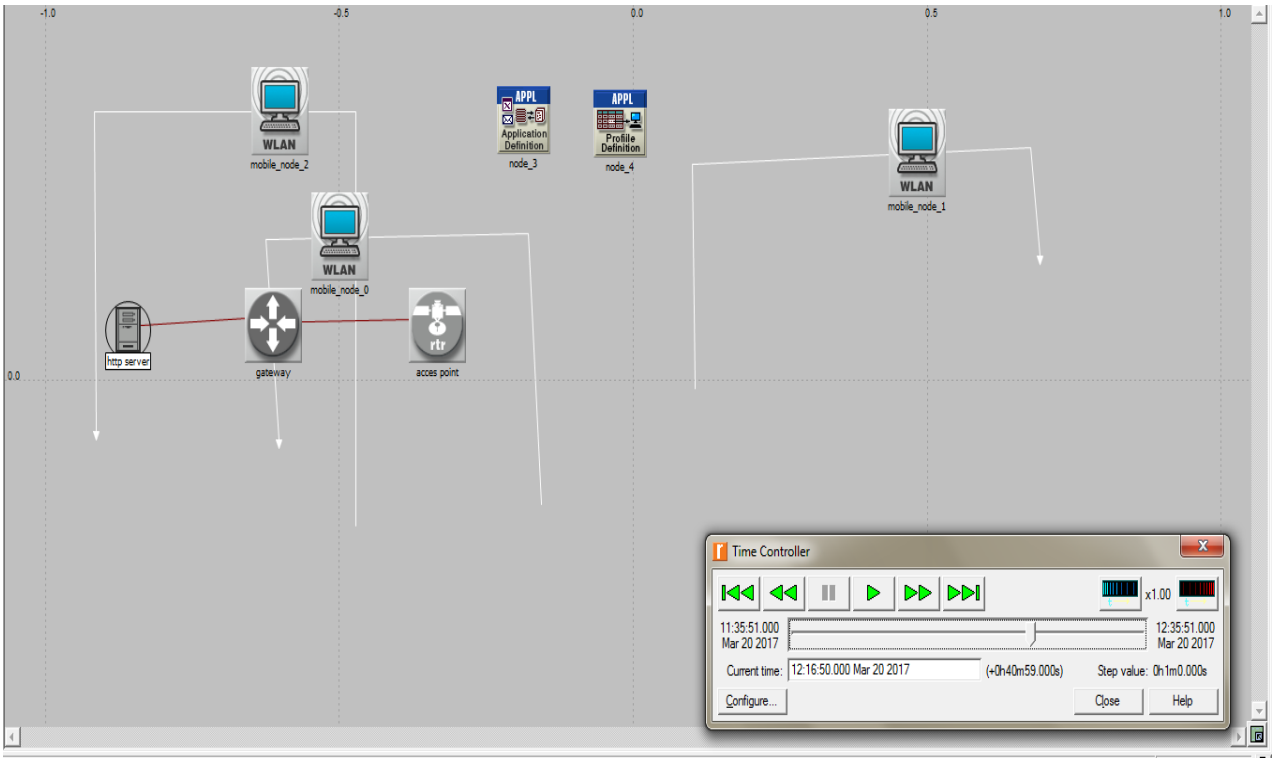


Figure 4.22 : *Le déplacement de station mobile*

Nous sommes maintenant prêts à lancer la collecte des statistiques. La charge du serveur est une statistique clé pour connaître les performances du réseau dans son ensemble.

- Faites un clic droit sur le serveur et choisissez : Choose Individual Statistics dans le menu déroulant.

Cette boîte de dialogue classe hiérarchiquement les statistiques que nous allons collecter. Pour connaître la charge sur le serveur, il faut :

- Cliquez sur le + devant
- Cochez la case server http et Wireless Lan afin que les statistiques concernant cette charge soient collectées.
- Cliquez sur OK.

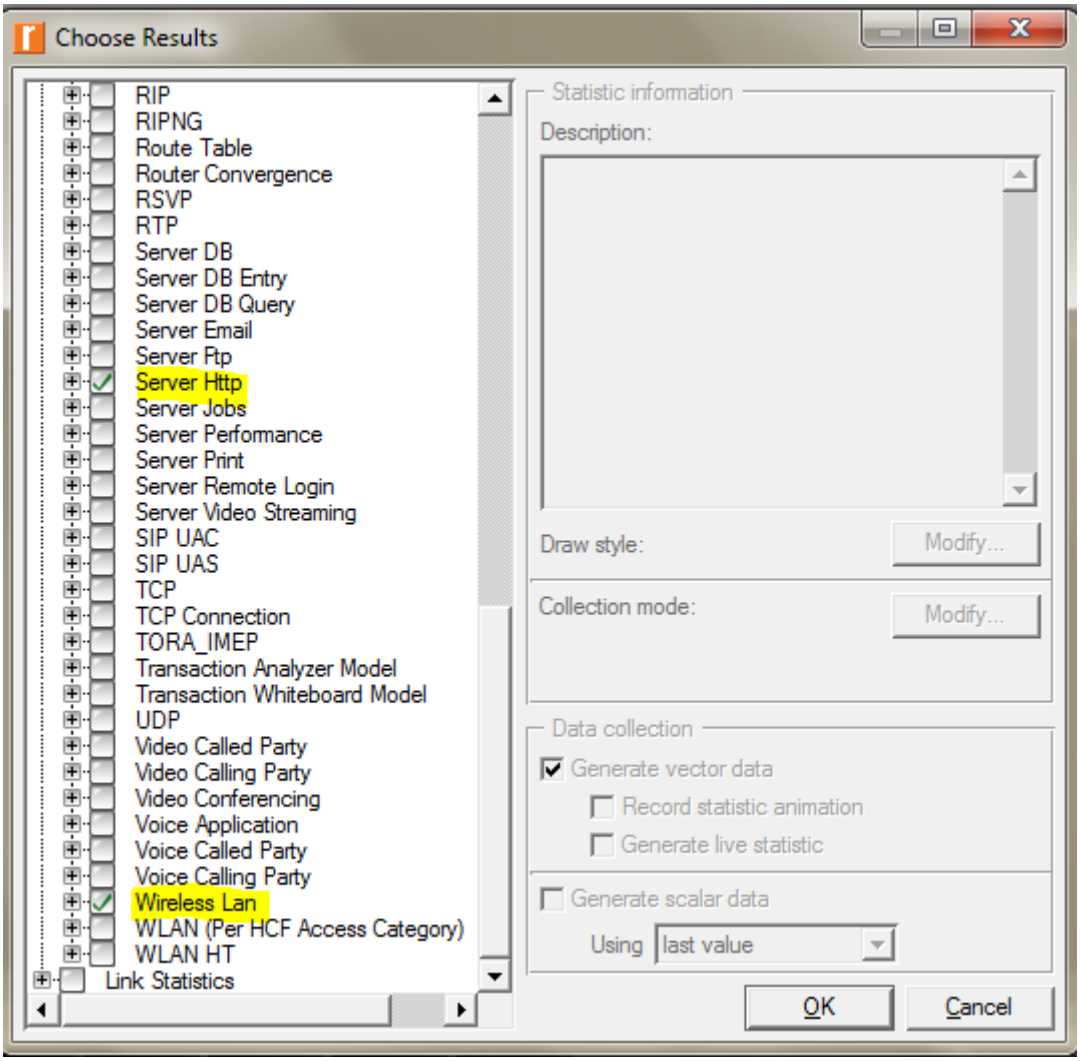
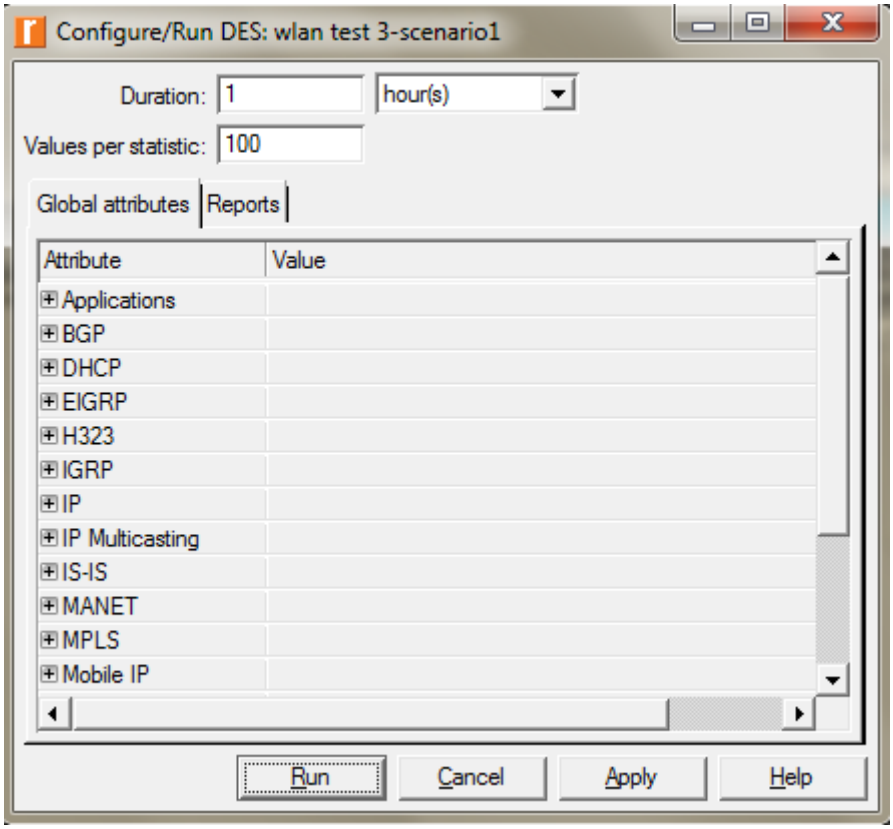


Figure 4.23 : *Configuration service http*

Puis cliquer sur Run



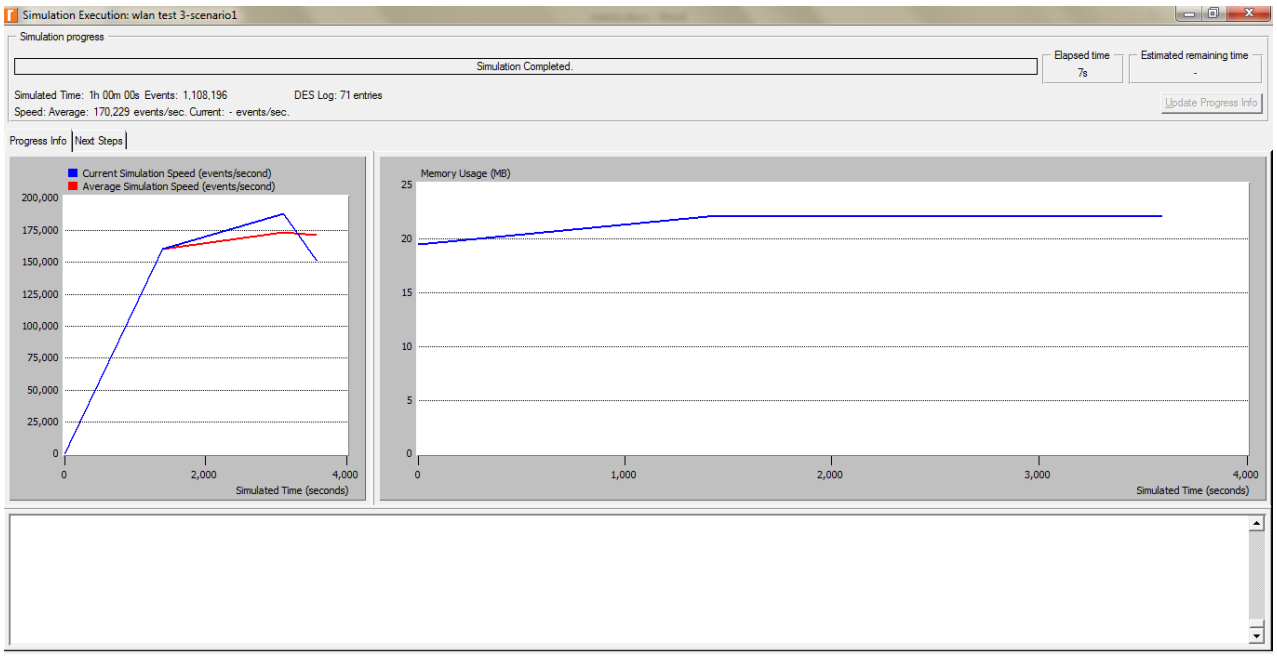


Figure 4.24 : *Lancement de la simulation*

4.6.2 Résultat et interprétation de la simulation :

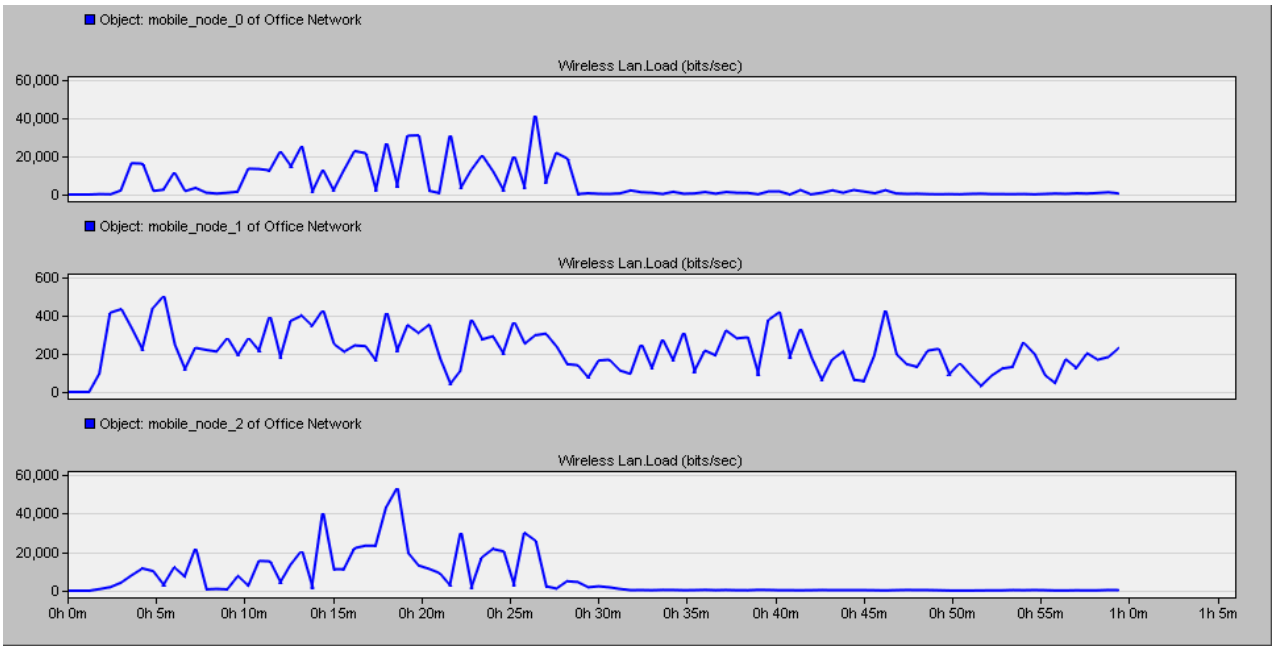


Figure 4.25 : *Charge (bit/sec) de trois stations mobiles*

Nous remarquons qu'une fois les stations proches du point d'accès la charge augmente.

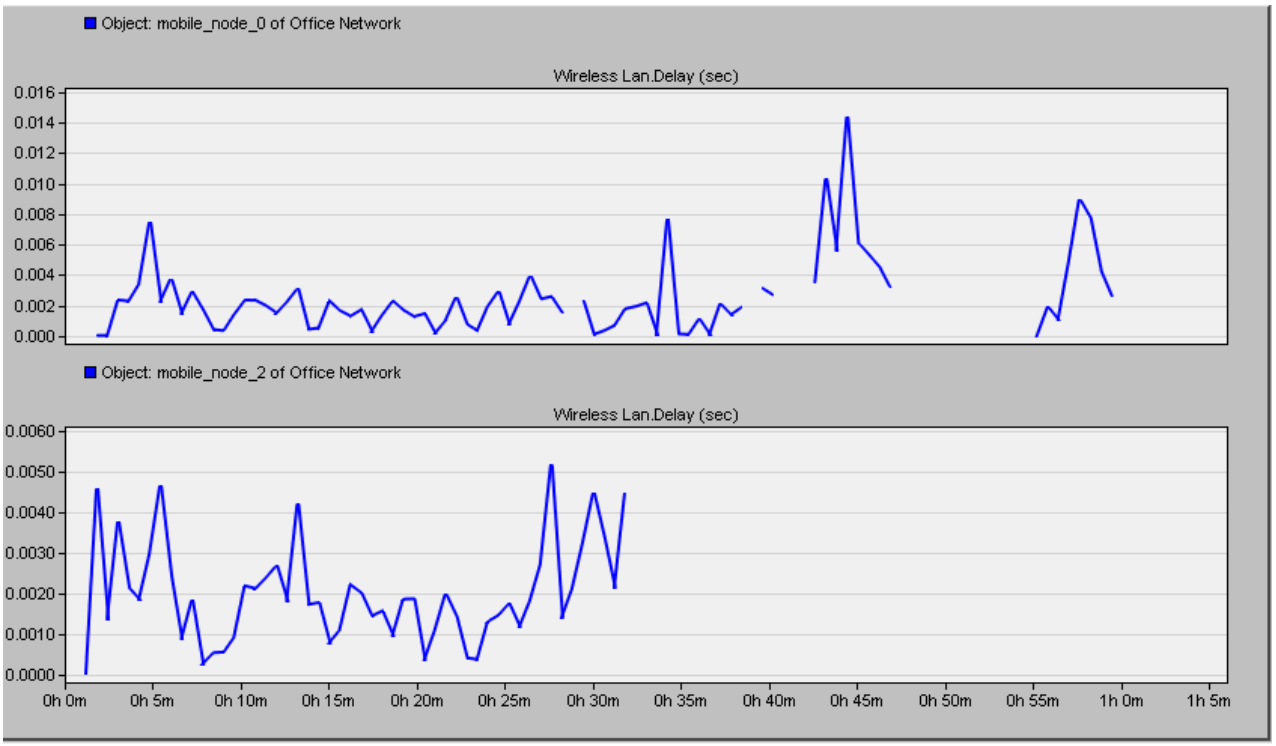


Figure 4.26 : *Délai (sec) de deux stations mobiles*

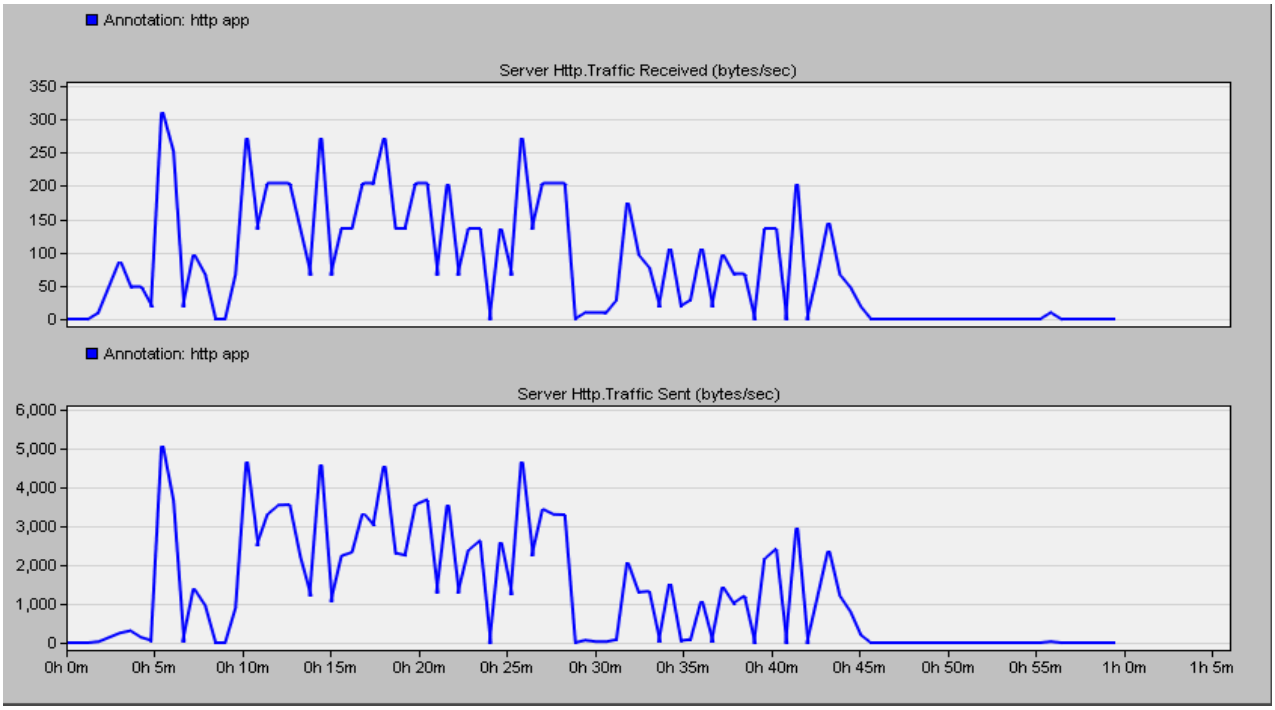


Figure 4.27: *Le trafic reçu et envoyé par le serveur http*

Trafic reçu : 0 à 350bps, le trafic envoyé entre 0 et 6 Kbps

On remarque que le trafic reçu et envoyé augmente quand les stations sont près du point d'accès.

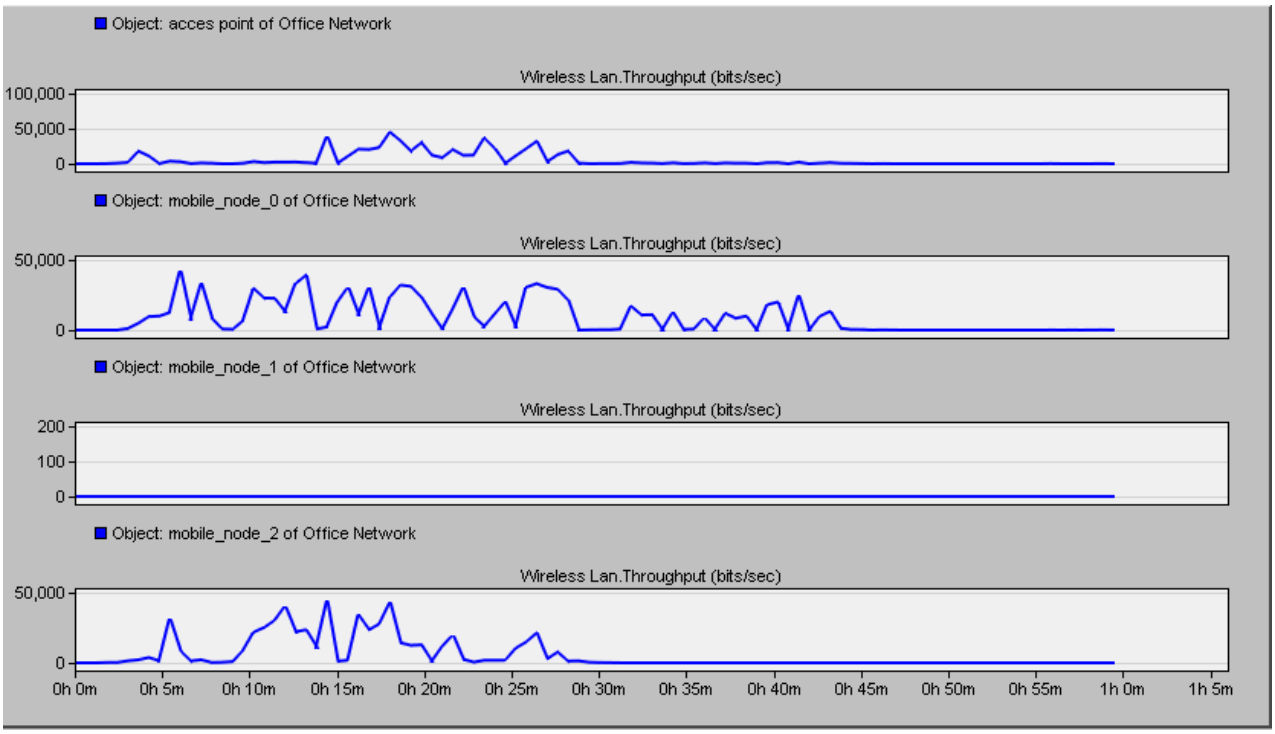


Figure 4.28 : *Le débit des 3 stations mobiles et de l'AP*

Pour le point d'accès, le débit varie de 0 à 50 Kbps, pour le mobile node 0 et 1 il varie de 0 à 50 Kbps et pour le mobile 1 le débit est 0.
Donc le débit du point d'accès des stations mobiles augmente quand les stations sont proches du point accès et il se dégrade quand ils s'éloignent.

4.7 Conclusion

Dans ce chapitre, nous avons étudié les performances du réseau wifi sous opnet dans le cas d'un BSS avec des stations mobiles. Nous avons évalué en termes de délai, de débit, de trafic reçu et envoyé, nous remarquons que les stations mobiles donnent une meilleure qualité de service.

CONCLUSION GENERALE

Dans ce mémoire nous avons étudié les réseaux sans fil, en particulier le wifi. En effet, il est facile de modéliser un réseau sans fil sous la forme d'entités (les nœuds sans fil) et de modéliser les interactions entre elle.

Les simulateurs du réseau offrent beaucoup d'économie de temps et d'argent pour l'accomplissement des tâches et sont également utilisés pour que les concepteurs des réseaux puissent tester les nouveaux protocoles ou modifier les protocoles déjà existants d'une manière contrôlée et productrice.

OPNET est conçu spécifiquement pour le développement et l'analyse des réseaux de communication, et fournit de nombreux détails non disponibles en paquets de simulation simples basées sur les ressources

C'est un outil utilisé pour le dimensionnement des réseaux réduit l'effort nécessaire pour développer une simulation en fournissant un noyau de simulation événementielle efficace, les bibliothèques de blocs de construction, des communications et des compilateurs qui prennent la spécification de conception et génèrent automatiquement une simulation exécutable

Il permet de concevoir et d'étudier des réseaux de communications, des nouvelles technologies, des protocoles et des applications avec facilité et évolutivité.

Donc l'étude de ce mémoire a toutefois dégagé quelques points essentiels qui pourront permettre de traiter et analyser les performances des protocoles de communication dans les réseaux filaire et sans fil en utilisant cet outil de simulation.

ANNEXE

A.1 Les Risques de sécurité de Wi-Fi

Les constructeurs n'activent pas systématiquement par défaut les fonctions de sécurité disponibles sur leurs points d'accès. Il arrive ainsi que certaines personnes déploient des réseaux sans fil sans appliquer les consignes minimales en termes de sécurité. De nombreux outils destinés à l'analyse des réseaux sans fil ont été développés. Les scanners trouvent les réseaux, les sniffers capturent les données et les crackers recouvrent les clés de cryptage WEP.

A.1.1 Dénis de Service

Ces attaques consistent à rendre le réseau inopérant vis-à-vis de l'utilisateur légitime.

- Le brouillage (jamming) : Le brouillage d'un réseau radio est relativement facile à réaliser avec un équipement radio qui émet dans la même bande de fréquence que le réseau Wi-Fi. Il ne présente aucun risque d'intrusion, mais constitue un déni de service efficace. Au-delà d'une certaine puissance, le brouillage peut saturer les équipements physiques du réseau attaqué et le rendre totalement inefficace.
- Accès en rafale : Les attaques DoS, qui ne sont pas propres au sans-fil, consistent à bloquer l'accès au réseau par un trafic ou des connexions malveillantes en rafale (trames d'authentification/association), en dégradant très significativement la qualité des communications ou en générant une charge de traitement sur les équipements réseau ou client (requêtes de probe). Des outils permettent de détecter ce genre de flux, de générer un avertissement et d'aider l'administrateur à localiser la source de l'attaque. Certains commutateurs Wi-Fi sont capables de se défendre d'eux-mêmes en bloquant l'accès Wi-Fi dès détection d'un flux anormal de trafic entrant.
- Des authentifications forcées : Ce type d'attaque consiste à générer des trames qui visent à annuler l'authentification d'un poste mobile. Celui-ci ne peut plus se reconnecter sur le réseau. Une autre attaque consiste à envoyer des trames broadcastées, c'est à dire sans adresse définie, qui attaquent de la même façon tous les postes mobiles à portée.

A.1.2 Intrusions

- L'Intrusion Client : Cette attaque consiste à exploiter les vulnérabilités du client pour accéder au réseau. Comme pour les réseaux câblés, la meilleure protection est la mise en place d'un firewall entre la partie WLAN et le reste de l'infrastructure réseau, qui garantit un niveau de sécurité au moins égal à celui de l'environnement câblé.
- L'Intrusion Réseau : C'est une des attaques les plus critiques. Une intrusion réseau vise à prendre le contrôle des ressources réseau d'une entreprise. Les protections contre ce risque sont les systèmes IDS dédiés au Wi-Fi, qui vont chercher à corréler plusieurs évènements douteux pour déterminer si le réseau ou un système particulier est en train de subir une intrusion.

A.1.3 Falsification des points d'accès

- Le Fake AP ou faux AP : Le faux point d'accès n'est pas un véritable AP, mais une station du réseau. Le PC du hacker joue le rôle de point d'accès en usurpant le SSID du réseau et peut donc récupérer les connexions Wi-Fi des utilisateurs.
- Le Rogue AP ou AP indésirable : La faille de sécurité dite Rogue AP est la plus redoutée en entreprise. L'attaque consiste à brancher sur le réseau un point d'accès pirate qui diffuse dans une zone où peut se trouver le hacker. Elle nécessite certaines complicités au sein de l'entreprise.

A.1.4 Récupération des informations sensibles du réseau

Par « informations sensibles », on entend les informations qui vont permettre au hacker de se connecter au réseau attaqué, à recueillir en clair les informations qui y circulent, d'introduire lui-même ses informations sous forme de virus, de vers, voire de données erronées ou encore de détruire des données :

- L'intrusion par sniffing : Le principe est le même que sur les réseaux Ethernet et utilise un sniffer qui capture les messages d'ouverture de session pour récupérer le nom et le mot de passe. Il suffit au sniffer d'être dans la zone de couverture radio du réseau, soit dans un rayon d'une centaine de mètres autour d'un point d'accès.
- L'écoute malveillante : consiste à observer et décoder le trafic du réseau. Certains modes de cryptage possèdent des faiblesses intrinsèques qui permettent de "craquer" le codage.
- Wardriving : Les ondes radioélectriques des réseaux sans fil se propagent parfois au-delà des limites physiques d'un bâtiment. Bien qu'atténuées, elles restent exploitables de l'extérieur.

Le wardriving consiste à rechercher un réseau sans fil depuis sa voiture grâce à un ordinateur portable et une carte réseau sans fil. Une telle attaque peut aussi être réalisée à pied, on parle alors de' war walking'. Pour lutter contre le war driving, la désactivation des balises ou beacon et le WEP sont très insuffisants mais offrent néanmoins un premier niveau de sécurité.

- Attaque au niveau de la station : Le hacker se connecte à la station et constitue avec elle un réseau « ad-hoc », c'est à dire sans infrastructure de distribution, et peut accéder au réseau de l'entreprise par rebond sur cette station. Ce type d'attaque n'est pas propre au poste mobile.

Des postes fixes équipés d'une option Wi-Fi non désactivée sont tout autant vulnérables.

La figure A4.01 suivante montre une attaque par rebond.

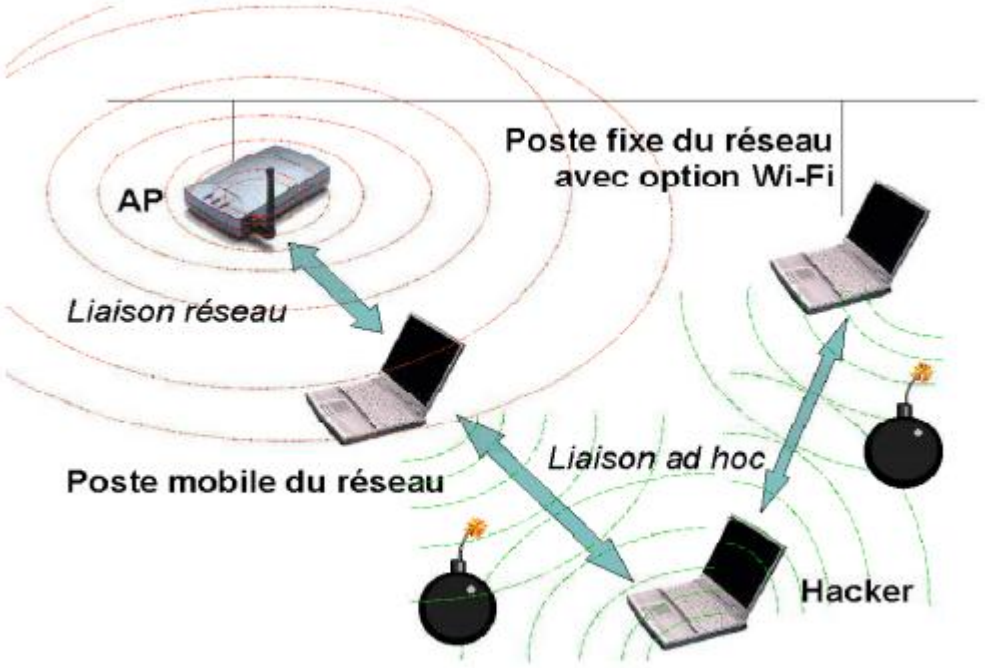


Figure A4.01: *Attaque par rebond*

Une entreprise qui souhaite protéger son réseau Wi-Fi de manière optimale peut le faire mais cela nécessite du temps et des budgets non négligeables.

La prévention des attaques est possible en mettant en place des infrastructures et des mécanismes de sécurité dédiés. Toutefois, la lutte contre les dénis de service reste très délicate car les DoS ne sont pas prévisibles et peuvent s'attaquer au réseau avec des méthodes diverses et variées.

Néanmoins, nous pouvons prévenir les attaques à l'aide de ces quelques manières, à savoir qu'il existe d'autres manières :

- Les réseaux sans fil sont particulièrement sensibles au brouillage radio contre lequel il est difficile d'agir. Pour cela, il est indispensable de maitriser la propagation radio du réseau sans fil ainsi installé en réglant la puissance d'émission des points d'accès au minimum nécessaire.
- Supprimer la configuration par défaut des points d'accès,
- Utilisation de cryptage et chiffrement,
- La mise en place d'un réseau privé virtuel est aussi un moyen supplémentaire permettant d'authentifier l'utilisateur sur le réseau.

A.2 Prévention des attaques

Une entreprise qui souhaite protéger son réseau Wi-Fi de manière optimale peut le faire mais cela nécessite du temps et des budgets non négligeables.

La prévention des attaques est possible en mettant en place des infrastructures et des mécanismes de sécurité dédiés. Toutefois, la lutte contre les dénis de service reste très délicate car les DoS ne sont pas prévisibles et peuvent s'attaquer au réseau avec des méthodes diverses et variées.

Néanmoins, nous pouvons prévenir les attaques à l'aide de ces quelques manières, à savoir qu'il existe d'autres manières

- Les réseaux sans fil sont particulièrement sensibles au brouillage radio contre lequel il est difficile d'agir. Pour cela, il est indispensable de maitriser la propagation radio du réseau sans fil ainsi installé en réglant la puissance d'émission des points d'accès au minimum nécessaire.
- Supprimer la configuration par défaut des points d'accès,
- Utilisation de cryptage et chiffrement,
- La mise en place d'un réseau privé virtuel est aussi un moyen supplémentaire permettant d'authentifier l'utilisateur sur le réseau.

BIBLIOGRAPHIE

[1] Rakotomanantsoa Lova Tiana, «*PLANIFICATION DU RESEAU WIFI D'ENTREPRISE* », Planification du réseaux WIFI d'entreprise AU 2009.

[2] DI Gallo Frédéric, « *WiFi L'essentiel qu'il faut savoir…* », wifi 2003.

[3] Grunenberger Y., « *reseau sans fil »,* technologie wifi 2011.

[4] Mokri Karima Ikram et Sidhom Zineb, « *Evaluation des performances du réseau wifi en utilisant le simulateur OPNET* », évaluation des performances wifi.2014-2015.

[5] http://www.commentcamarche.net/contents/1282-les-modes-de-fonctionnement-du-wifi-802-11-ou-wi-fi.

[6] Kherbache Zeyneb et LARIBI Amina, « *Étude de la Qualité de Service (QoS) dans les réseaux WIFI* », Etude-de-la-Qualite-de-Service(QoS) dans-les-reseaux-WIFI2010-2011

[7] Fluke Networks« *Mise en œuvre de la norme 802 .11ac -révolution ou évolution ?* »5868-livre-blanc-airmagnet-norme-802.11ac 2013.

[8] Riahla Med Amine, « *Généralité sur les réseaux informatiques* », 20_polycope1.2013.

[9] G. Pokra, « *réseaux_ généralités »,* http://www.jaquet.org, février 2017.

[10] Hubert, « *sécurité des systèmes sans fils* », wifi security, 2004.

[11] http://www.memoireonline.com/07/09/2324/m_ Les-technologies-sans-fil-Le-Wi-Fi-et-la-Securite1.html

[12] Runser K, Roche G., Gorce M. J., « *Dimensionnement et planification des réseaux Wi-Fi* », http://ares.insa-lyon.fr, 2007

[13] Males D., Pujolle G., « *Wi-Fi par la pratique* », Eyrolles, 2004.

[14] Anzevui J., « *Les réseaux sans fil* », Les-Reseaux-Sans Fil-Jeremi ANZEVUI1, 2006-2007.

[15] G.Pujolle « Cours réseaux et télécom », Eyrolles 3è Edition 2004.

[16] Muhlethaler P., « 802.11 et les réseaux sans fil », Eyrolles, 2002.

RENSEIGNEMENTS

Nom : RATSIMBAZAFIMANANA

Prénom : Manoela

Adresse : Lot II A23 Antaninandro

Email : manouratsim@gmail.com

Tel : 0330759357

Titre du mémoire : **ETUDE DES PERFORMANCES DU RESEAU WIFI AVEC SIMULATION SUR OPNET**

Nombres de pages : 72

Nombres de tableaux : 2

Nombre de figures : 43

Directeur de mémoire : M. ANDRIAMIASY Zidora, Maitre de Conférences

Andriamiasyzidora@yahoo.fr

0340114121

RESUME

Le réseau wifi est incrusté dans notre vie quotidienne au niveau social, professionnel et scientifique et les utilisateurs demandent des techniques de communications puissantes et adéquates pour combler leur envie de communication et d'échange d'information. Le but de notre mémoire est d'évaluer les performances du réseau wifi en utilisant le simulateur OPNET qui est un logiciel de simulation qui permet de construire graphiquement des topologies avec PC, routeurs, point d'accès et différents types de liaisons tout en fournissant les fonctionnalités nécessaires. Ce logiciel permet de couvrir les points essentiels des cours en réseau.

Mots clés : WIFI, performance, qualité de service, point d'accès, débit.

ABSTRACT

The wifi network is embedded in our daily social, professional and scientific life and users demand powerful and adequate communication techniques to fill their desire for communication and information exchange. The purpose of our paper is to evaluate the performance of the wifi network using the OPNET simulator, which is a simulation software that allows to graphically construct topologies with PCs, routers, access points and different types of links while providing the necessary features. This software allows to cover the essential points of the courses in network.

Keywords: WIFI, performance, quality of service, access point, throughput