

Sommaire

INTRODUCTION GENERAL

Chapitre I : Concepts fondamentaux sur les réseaux informatiques

I.1.Introduction	5
I.2 Principe Modèle	5
I.3 Etude succincte des couches Principales.....	7
I.3.1. La couche physique	7
I.3.1.1.Transmission en bande de base.....	7
I.3.1.2. Transmission en large bande	8
I.3.2. La sous couche MAC	8
I.3.3. La couche liaison LC	8
I.4 Etude succincte des principales implémentations	10
I.4.1. L’anneau à jeton, IEEE 802.5	10
I.4.2. Le jeton adressé ou Token bus, IEEE 802.4	11
I.5. Topologie physique des réseaux	12
I.5.1. Les topologies de base	12
I.5.2. La topologie en bus	12
I.5.3. La topologie en étoile	13
I.5.4. La topologie en anneau	14
I.6. Les support de transmission	14
I.6.1. Paires torsadées	14
I.6.2. Câbles coaxiaux	15
I.6.3. Fibre optique	16
I.6.4.Faisceaux hertziens	16
I.6.5. Les liaisons satellitaires	17
I.7. Routage dans les réseaux sans fils	19
I.8. Conclusion.....	19

Chapitre II : Ethernet et s'évolution sans fil

II.1. Introduction	21
II.2. Ethernet sans fil	21
II.2.1 Réseaux personnels sans fils (WPAN).....	22
II.2.2 Réseaux locaux personnels sans fil (WLAN).....	23
II.2.2.1. Les réseaux 802.11	23
II.2.3. Réseaux métropolitains sans fils (WMAN)	25
II.2.4. Réseaux étendus sans fils (WWAN)	25
II.2.5. Réseaux locaux virtuels (VLAN)	26
II.3. L'architecture générales des réseaux sans fil	26
II.3.1. Réseaux ad-hoc	26
II.3.2 Les réseaux cellulaires	28
II.4. Caractéristiques générales des réseaux Ethernet 802.3	29
II.4.1. Le principe de CSMA/CD	29
II.4.2. Le format des trames Ethernet/IEEE 802.3	29
II.5. Les différentes versions d'Ethernet	30
II.5.1 L'Ethernet épais, IEEE 802.3 10 bas 5	30
II.5.2 L'Ethernet fin, IEEE 802.3 10 bas 2	30
II.5.3 L'Ethernet à 100 Mbit/s	31
II.5.3.1. Couche physique 100 base – T	32
II.5.4 Le Gigabit Ethernet	33
II.6. Conclusion.....	33

Chapitre III : Conception des réseaux WLAN avec Cisco Packet Tracer

III.1 Introduction	35
III.2 Routage statique	35
III.2.1. Réseaux informatique en topologie étoile avec un routeur central.....	35
III.2.1.1. Configuration des routeurs par commandes	36
III.2.1.2. Simulation	40
III.2.2. Réseau informatique en topologie étoile avec 3 routeurs centraux	41

III.2.2.1. Configuration des routeurs par commandes	42
III.2.2.2. Simulation en ligne de commande	44
III.3. Routage dynamique	47
III.3.1. Configuration des routeurs par commandes.....	49
III.3.2. Simulation en mode temps réel	51
III.3.2.1. Simulation de Pc1 vers Pc5	51
III.3.2.2. Simulation de Pc2 vers Pc6	51
III.4. Adressage fixe et dynamique	52
III.4.1. Adressage fixe	53
III.4.1.1. Simulation de Laptop ver PC	54
III.4.2. Adressage dynamique.....	54
III.4.2.1. Paramètres du serveur DHCP.....	55
III.5. WIFI.....	55
III.6. Conclusion	57

CHAPITRE IV : Conception des réseaux filaires par le logiciel OPNET

IV.1 Introduction	59
IV.2. Premier scénario	59
IV.2.1. Eléments de réseau	59
IV.2.2. Duplication du Scenario	61
IV.3. Réseau local avec un routage RIP	63
IV. 3.1. Eléments de réseau.....	63
IV.3.2. Duplication du Scenario	65
IV.3.3. Adresse IP du routeur 1.....	68
IV.4. Réseau RIP d'une topologie étoile	69
IV.5. Modèle de réseau WLAN simple	73
IV.5.1. Application Configuration	74
IV.5.2. Profil Configuration	75
IV.5.3. Client configuration	76
IV.5.4 Server configuration	76
IV.6. Conclusion	78

Annexe 1: Simulation avec Cisco Packet tracer

1. Introduction.....	80
2. Présentation du logiciel.....	80
2.1. Présentation de l'écran principal.....	80
2.2. Spécification des équipements disponibles.....	80
2.3. Spécification des connexions possibles.....	81
2.4. Les commandes et outils CISCO.....	82
2.4.1. Interface graphique sur un poste client (ordinateur basique)	82
2.4.1.1 L'onglet « physical »	82
2.4.1.2. L'onglet « Config »	83
2.4.1.3 L'onglet « Desktop »	83
2.5 Serveur	84
2.5.1. Interface « Physical »	84
2.6. Simulation.....	85
2.6.1 Simulation en temps réel.....	85
2.6.2. Simulation en ligne de commande	85

Annexe 2:

1. Introduction.....	87
2. Présentation générale.....	87
3. Modélisation orientée objet	87
3.1. Objet réseau.....	87
3.2. Objet nœud.....	87
3.3. Objet Paquet	91
3.4. Fonction KERNEL (KP).....	92
4. Editeurs OPNET supplémentaires.....	92
4.1. Editeur de diagramme de rayonnement	92
4.2. Editeur de sondes (Probe editor).....	93
4.3. Prise de statiques.....	94
5. Modélisation Radio.....	95
5.1. Nœud radio.....	95

5.2. Liens radio.....	95
5.3. Antennes.....	96
6. Fenêtre de définition d'une simulation.....	97
7. Fenêtre de définition d'une simulation	98
Conclusion générale	

Introduction Générale

Ethernet est une technologie universelle qui dominait déjà les réseaux locaux bien avant le développement de l'Internet. La clé de la longévité de cette technologie, c'est sa simplicité. Souvent critiquée, elle a toujours été plus facile à utiliser et à mettre en œuvre que ses concurrentes. Ethernet était à l'origine un standard développé par les laboratoires Xerox au tout début des années 1970. Ce standard a d'abord évolué jusqu'à la version Ethernet II aussi appelée DIX ou encore v2.0 avec l'association regroupant Digital. Par la suite, Ethernet a été inclus dans les travaux sur la modélisation OSI au début des années 1980. Depuis cette époque, la technologie Ethernet est totalement indépendante des constructeurs ; c'est un des facteurs importants de sa popularité.

Ce mémoire à la fois une introduction aux normes (IEEE 802.3 – 10Mbps, FastEthernet – 100Mbps, Gigabit Ethernet – 1Gbps, 10Gbps) et une aide à la conception et la réalisation de réseaux locaux.

L'informatique d'entreprise, autrefois dominée par les systèmes centraux (mini-ordinateurs et grands systèmes), a été bouleversée par le développement de la micro-informatique. Celle-ci a apporté à ses utilisateurs– et aux informaticiens – des outils efficaces, plus souples plus confortables et surtout moins onéreux.

Après une phase d'utilisation « individualiste » de la micro – informatique, l'adoption généralisée des réseaux locaux a permis de mieux organiser les informations dispersées, d'améliorer la communication entre les utilisateurs et de réduire les dépenses (en théorie du moins) par le partage des périphériques et des applications.

Un réseau local est un réseau informatique tel que les terminaux qui y participent (ordinateur, etc) s'envoient des trames au niveau de la couche de liaison sans utiliser d'accès à internet. Au niveau de l'adressage IP, un réseau local correspond généralement à un sous-réseau IP(même préfixe d'adresse IP). On interconnecte les réseaux locaux au moyen de routeurs.

Une autre approche consiste à définir le réseau local par sa taille physique. C'est généralement un réseau à une échelle géographique relativement restreinte, par exemple une salle informatique, une habitation particulière, un bâtiment ou un site d'entreprise.

Dans le premier chapitre, nous allons présenter une étude succincte des différentes couches du modèle OSI ou nous nous sommes intéressées plus particulièrement aux couches physique et liaison de données. Le chapitre est terminé par les diverses topologies physiques des réseaux et aussi les différents types de supports de transmission utilisés.

Le deuxième chapitre est entièrement consacré à l'étude des réseaux sans fil. Nous allons présenter ensuite les caractéristiques générales des réseaux Ethernet 802.3 et les différentes versions de ces derniers.

Le troisième chapitre, est concentré à la conception des réseaux locaux en appliquant des techniques de configuration des périphériques des réseaux comme le routage statique et dynamique et l'adressage fixe et dynamique et en terminant par un réseau sans fil de type WIFI. Les résultats de simulation montrent que la connectivité entre les périphériques est bien réalisée.

Enfin, le quatrième chapitre représente les résultats de conception des réseaux locaux simulés par le logiciel OPNET. Ces résultats sont alors présentés et discutés.

Ce mémoire se termine par deux annexes qui donnent une description globale sur les deux logiciels de conception Cisco Packet Tracer et OPNET respectivement et par une conclusion générale des travaux présentés.

I.1. Introduction

Le terme générique « réseau » définit un ensemble d'entités (objets, personnes, etc.) interconnectées les unes avec les autres. Un réseau permet ainsi de faire circuler des éléments matériels ou immatériels entre chacune de ces entités selon des règles bien définies.

Réseau informatique: c'est l'ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques.

Un ordinateur est une machine permettant de manipuler des données. L'homme, en tant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre-deux afin de pouvoir échanger des informations.

Un réseau informatique peut servir plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.).
- La communication entre personnes (courrier électronique, discussion en direct, etc.).
- La communication entre processus (entre des ordinateurs industriels par exemple).
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau).
- Le jeu vidéo multi-joueurs.

I.2. Principe Modèle OSI

Le modèle OSI (Open System Interconnexion - International Standard Organisation) décrit la façon dont une communication entre deux ordinateurs doit se décomposer. Il prévoit sept couches et stipule que chacune de ces couches doit être isolée des autres par une interface bien définie. Chacune des couches correspond à une fonctionnalité particulière d'un réseau.

Les premiers travaux portant sur le modèle OSI datent de 1977. Ils ont été basés sur l'expérience acquise en matière de grands réseaux et de réseaux privés plus petits ; le modèle devait en effet être valable pour tous les types de réseaux. En 1978, l'ISO propose ce modèle sous la norme ISO IS7498. En 1984, 12 constructeurs européens, rejoints en 1985 par les grands constructeurs américains, adoptent le standard.

Chaque couche possède des fonctions, qu'elle met à la disposition des couches supérieures. L'utilisateur ne voit en principe que la couche application du niveau supérieur, alors que le spécialiste du réseau se préoccupera également des autres couches.

Lorsque deux ordinateurs entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes. Cela signifie que les couches se comportent comme si elles étaient en contact direct et non à travers des couches inférieures.

La couche session de la station 1 signale à la couche transport qu'elle souhaiterait faire parvenir un message à son homologue de la station 2 et le lui transmet. La couche transport découpe le message en segments de taille définie, ajoute des informations sur l'adressage et le format et les transmet à la couche suivante. Celle-ci procède de même.

Et ainsi de suite jusqu'à ce que les données soient expédiées vers la station 2. Parvenus au poste destinataire, les paquets de données sont débarrassés des éléments devenus inutiles, intégrés par l'expéditeur dans leur en-tête, et transmis aux couches de niveau supérieur, jusqu'à atteindre leur destination. Cette dernière couche extraira les informations utiles.

Les couches 1, 2, 3 et 4 sont dites basses alors que les couches 5, 6 et 7 sont dites hautes. [1]

Couches hautes	<i>Couche 7</i>	Couche application
	<i>Couche 6</i>	Couche présentation
	<i>Couche 5</i>	Couche session
Couches basses	<i>Couche 4</i>	Couche transport
	<i>Couche 3</i>	Couche réseau
	<i>Couche 2</i>	Couche liaison de données
	<i>Couche 1</i>	Couche physique
<i>Paquet envoyé sous forme de flux de bits</i>		

I.3. Etude succincte des couches principales

I.3.1. La couche physique

La couche physique fournit les moyens mécaniques, électriques, fonctionnels et procéduraux nécessaires à l'activation, au maintien et à la désactivation des connexions physiques destinées à la transmission de bits entre deux entités de liaison de données. Une connexion physique peut mettre en jeu plusieurs systèmes intermédiaires, relayant chacun la transmission des bits dans la couche physique.

Elle se décompose en deux sous niveaux :

Le **PMD** (Physical Medium Dependant, description du média utilisé, câbles, prises...

Le **PHY** (Physical), qui décrit la correspondance entre le signal reçu et son interprétation sous forme binaire (codage). On obtient en sortie de cette couche un flux de données binaire. [3]

I.3.1.1. Transmission en bande de base

On qualifie des systèmes de transmission en bande de base les systèmes qui n'introduisent pas d'écart de fréquence entre les signaux émis et ceux reçus. Cette définition n'exclut nullement des modifications du signal pour mieux l'adapter aux caractéristiques du support de transmission.

On appelle **codage**, l'opération qui fait correspondre à un symbole appartenant à un alphabet, une représentation binaire (codage à la source). On désigne par **transcodage**, ou **codage en ligne**, l'opération qui consiste à substituer au signal numérique (représentation binaire) un signal électrique mieux adapté à la transmission (figure I.2). Cette transformation est réalisée par un codeur/décodeur appelé Émetteur/Récepteur en Bande de Base (ERBdB). [3]

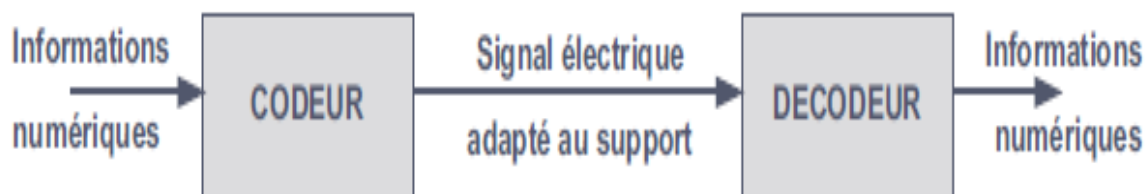


Figure I.2 : Principe du codage en ligne. [3]

I.3.1.2. Transmission en large bande

En transmission large bande, le spectre du signal numérique est traduit autour d'une fréquence centrale appelée **porteuse**. La translation de spectre résout les deux problèmes posés par la transmission en bande de base : dispersion du spectre (étalement du signal) et la monopolisation du support qui interdit le multiplexage. Elle est réalisée par un organe appelé modulateur.

En réception le signal doit subir une transformation inverse, il est démodulé. Le modem, contraction de **modulation/démodulation**, est un équipement qui réalise la modulation des signaux en émission et leur démodulation en réception. [4]

I.3.2. La sous couche MAC

La sous-couche **MAC** (*Medium Access Control*) a pour mission essentielle de gérer l'accès au support physique, elle règle les problèmes d'adressage (adresse MAC) et effectue un contrôle d'erreurs (**FCS**, *Frame Check Sequence*). [5]

I.3.3. La couche liaison LC

La sous-couche **LLC** (*Logical Link Control*) assure un service comparable à celui offert par la couche liaison du modèle de référence. Elle masque à la couche supérieure le type de réseau utilisé (Ethernet, Token Ring...). Les services de la sous-couche LLC sont accessibles à partir d'un point d'accès **LSAP** (*Link Service Access Point* ou point d'accès au service de liaison).

Pour distinguer les deux extrémités de la relation, ces points sont respectivement appelés **DSAP** pour la machine destination (*Destination Service Access Point*) et **SSAP** pour la machine source (*Source Service Access Point*). [5]

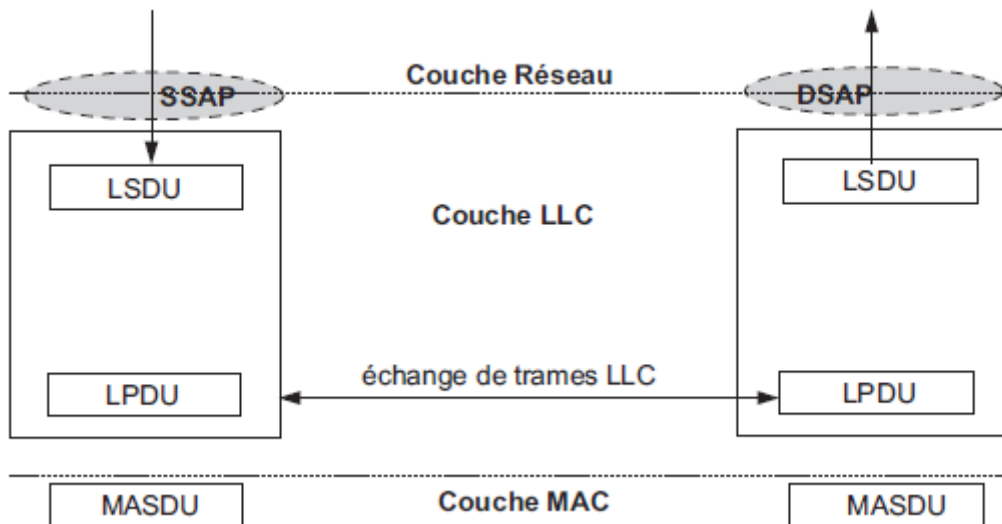


Figure I.3: Notions de point d'accès selon le modèle OSI. [5]

Les unités de données délivrées par ou à la couche supérieure forment des **LSDU** (*Link Service Data Unit*), celles-ci transmettent à la couche liaison les informations nécessaires à l'envoi des données (adresses MAC source et destination, niveau de priorité, données...). Les sous-couches LLC s'échangent des **LPDU** (*Link Protocol Data Unit*) dont le format est similaire à celui des trames d'HDLC. (Figure suivant)[5]

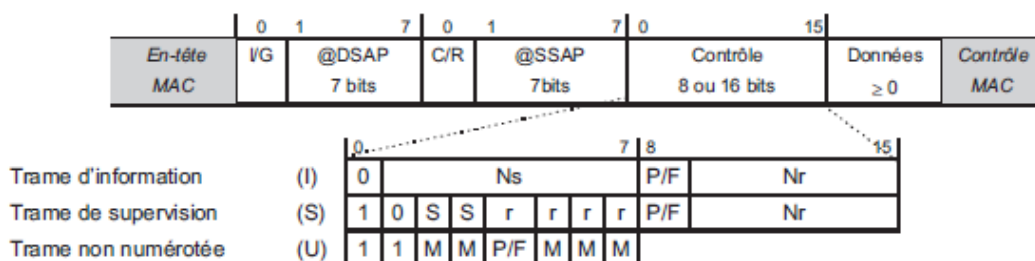


Figure I.4: Format général des trames LLC. [5]

Les adresses DSAP (Destination Service Access Point) et SSAP (Source Service Access Point) sont codées sur 7 bits (128 points d'accès). La notion d'adresse LSAP (Link Service Access Point ou point d'accès au service de liaison) autorise la cohabitation de protocoles différents pour une même carte adaptateur (adresse MAC). Certaines valeurs sont réservées, le tableau de la figure I.5 fournit quelques exemples d'adresses LSAP. [5]

LSAP	Service identifié
0X'00'	Null SAP
0X'02'	LLC Management
0X'06'	Internet ARPA
0X'AA'	SNAP
0X'F0'	NETBIOS
0X'FE'	ISO

Figure I.5 : Exemples d'adresses LSAP. [5]

Le bit I/G indique s'il s'agit d'un DSAP (Destination Service Access Point) individuel (I= 0) ou de groupe (I = 1). Tous les bits du champ adresse à 1 correspondent à l'adresse de diffusion générale (broadcast).

Le bit C/R distingue une trame de commande (C/R = 0) ou de réponse (C/R = 1), identifiant ainsi l'initiateur des échanges, il a une fonction identique au champ adresse de LAP-B(Link Access Protocol, Balanced), il sert à distinguer le bit P du bit F (commande ou Poll C/R = 0 et P = 1, réponse C/R= 1 et F = 1).

À l'instar d'HDLC (High Level Data Link Control, le champ contrôle, sur 8 ou 16 bits, identifie le type de trame (I, S, U), les trames I et S contiennent les compteurs N_s (compteur de trames émises) et N_r (compteur de trames reçues) sur 3 bits (champ de 8 bits, numérotation des trames modulo 8) ou 7 bits (Champ contrôle sur 16 bits, numérotation des trames modulo 128). Les bits r sont réservés pour un usage ultérieur.

La couche LLC offre, selon les besoins, trois types de services : LLC1, LLC2 et LLC3. [5]

I.4.Etude succincte des principales implémentations

I.4.1. L'anneau à jeton, IEEE 802.5

La norme IEEE 802.5 (ISO 8802.5) spécifie un réseau local en boucle (figure I.6) : chaque station est reliée à sa suivante et à sa précédente par un support unidirectionnel. Ce réseau est connu sous le nom de Token Ring. [5]



Figure I.6 : Principe de l'anneau. [5]

Publiée en 1985, la norme IEEE 802.5 fut implémentée par IBM dès 1986. IBM est resté le principal acteur du monde Token Ring. L'implémentation d'IBM diffère quelque peu de la norme d'origine. Notamment, la topologie physique a évolué vers une étoile pour gérer la rupture de l'anneau. Les stations sont reliées à des concentrateurs (**MAU, Multiple Access Unit**) comme le montre la figure I.7. [5]

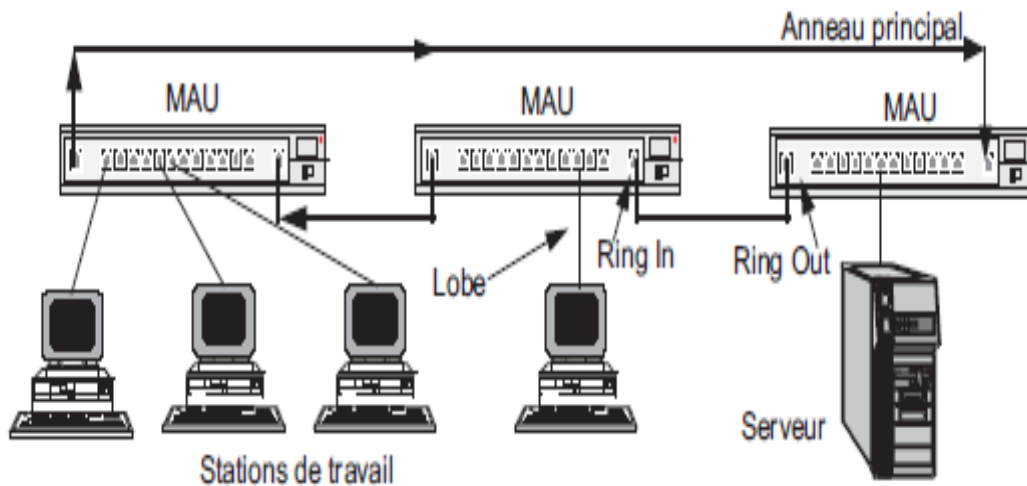


Figure I.7 : Présentation du réseau Token Ring. [5]

I.4.2. Le jeton adressé ou Token bus, IEEE 802.4

Réseau industriel, le Token Bus est aujourd'hui le seul réseau sur support filaire qui utilise un canal large bande (figure I.8). Conçu pour fonctionner en milieu industriel, le Token Bus utilise du câble coaxial (CATV de 75 V), les débits possibles sont 1, 5 et 10 Mbit/s. [5]

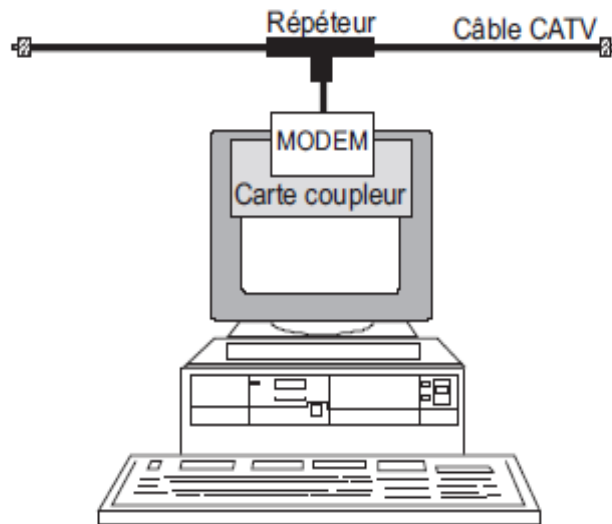


Figure I.8 : Niveau physique de l'IEEE 802.4. [5]

I.5. Topologie physique des réseaux

La topologie d'un réseau décrit la manière dont les nœuds sont connectés. Cependant, on distingue la **topologie physique**, qui décrit comment les machines sont raccordées au réseau, de la **topologie logique** qui renseigne sur le mode d'échange des messages dans le réseau (**topologie d'échange**). [5]

I.5.1. Les topologies de base

Les topologies de bases sont toutes des variantes d'une liaison point à point ou multipoint (figure I.9). [5]



Figure I.9 : Modes de liaisons élémentaires. [5]

I.5.2. La topologie en bus

La plus simple des topologies de base, le **bus** est une variante de la liaison multipoint. Dans ce mode de liaison, l'information émise par une station est diffusée sur tout le réseau. Le réseau en bus est aussi dit **réseau à diffusion** (figure I.10).

Dans ce type de topologie, chaque station accède directement au réseau, d'où des problèmes de conflit d'accès (contentions ou collisions) qui nécessitent de définir une politique d'accès. Celle-ci peut être centralisée (relation dite maître/esclave) ou distribuée comme dans les réseaux locaux.

Les réseaux en bus sont d'un bon rapport performance/prix. Ils autorisent des débits importants (>100 Mbit/s sur 100 m). Il est possible d'y insérer une nouvelle station sans perturber les communications en cours. Cependant, la longueur du bus est limitée par l'affaiblissement du signal, il est nécessaire de régénérer celui-ci régulièrement. La distance entre deux régénérations se nomme « pas de régénération ». [5]

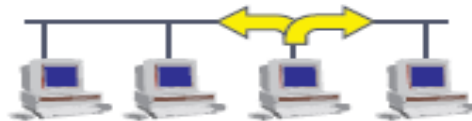


Figure I.10 : topologie bus. [5]

I.5.3. La topologie en étoile

La topologie étoile est une variante de la topologie en point à point. Un nœud central émule n liaisons point à point. Tous les nœuds du réseau sont reliés à un nœud central commun : le concentrateur. Tous les messages transitent par ce point central. Le concentrateur est actif, il examine chaque message reçu et ne le retransmet qu'à son destinataire. Cette topologie correspond, par exemple, au réseau téléphonique privé d'une entreprise où le commutateur téléphonique met en relation les différents postes téléphoniques de l'installation.

La topologie étoile autorise des dialogues entre nœud très performants. La défaillance d'un poste n'entraîne pas celle du réseau, cependant le réseau est très vulnérable à celle du nœud central. [5]

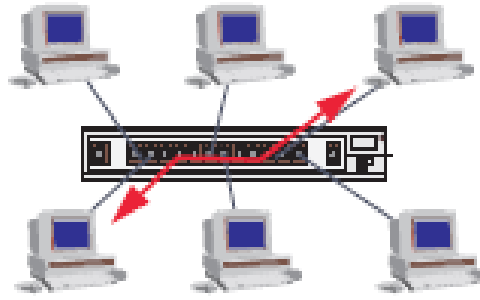


Figure I.11 : topologie étoile

I.5.4. La topologie en anneau

Dans la topologie en anneau, chaque poste est connecté au suivant en point à point. L'information circule dans un seul sens, chaque station reçoit le message et le régénère. Si le message lui est destiné, la station le recopie au passage (au vol). Ce type de connexion autorise des débits élevés et convient aux grandes distances (régénération du signal par chaque station). L'anneau est sensible à la rupture de la boucle. Les conséquences d'une rupture de l'anneau peuvent être prises en compte en réalisant un double anneau. [5]



Figure I.12 : topologie anneau. [5]

I.6. Les support de transmission

I.6.1. Paires torsadées

Une paire torsadée non blindée (UTP, Unshielded Twisted Pair) se compose de deux conducteurs en cuivre, isolés l'un de l'autre et enroulés de façon hélicoïdale autour de l'axe de symétrie longitudinal (voir figure I.13). [6]

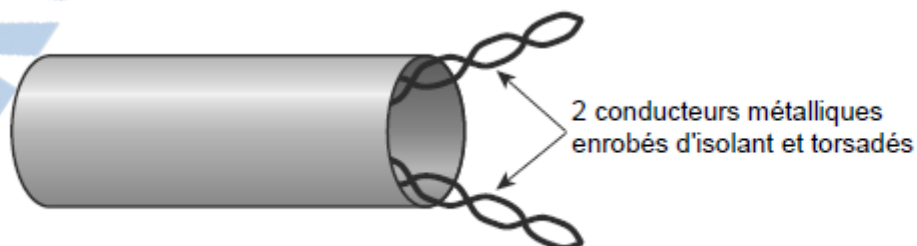


Figure I.13 : Paire torsadée. [6]

L'enroulement réduit les conséquences des inductions électromagnétiques parasites dues à l'environnement. L'utilisation courante de la paire torsadée est le raccordement des usagers au central téléphonique (*la boucle locale*) ou la desserte des usagers de réseaux privés. Son principal inconvénient est l'affaiblissement des courants, d'autant plus important que le diamètre des conducteurs est faible. Les paires torsadées contiennent, à intervalles réguliers, des répéteurs qui régénèrent les signaux. Quand plusieurs paires sont rassemblées dans un même câble, les courants transportés interfèrent les uns avec les autres. Ce phénomène est appelé diaphonie.

La paire torsadée suffit pour les réseaux locaux d'entreprise où les distances se limitent à quelques kilomètres. Ses avantages sont nombreux : technique maîtrisée, facilité de connexion et d'ajout de nouveaux équipements, faible coût. Certains constructeurs proposent des paires torsadées blindées (STP, Shielded Twisted Pair).

Enrobées d'un conducteur cylindrique, elles sont mieux protégées des rayonnements électromagnétiques parasites. Une meilleure protection prévoit un blindage par paire. [6]

I.6.2. Câbles coaxiaux

Pour éviter les perturbations dues aux bruits externes, on utilise deux conducteurs métalliques cylindriques de même axe séparés par un isolant. Le tout forme un *câble coaxial* (voir figure I.14). Ce câble présente de meilleures performances que la paire torsadée : affaiblissement moindre, transmission de signaux de fréquences plus élevées, etc.

La capacité de transmission d'un câble coaxial dépend de sa longueur et des caractéristiques physiques des conducteurs et de l'isolant. Sur 1 km, un débit de plusieurs centaines de Mbit/s peut être atteint. Sur des distances supérieures à 10 km, l'atténuation des signaux réduit considérablement les débits possibles. C'est la raison pour laquelle on utilise désormais les fibres optiques sur les liaisons grandes distances.

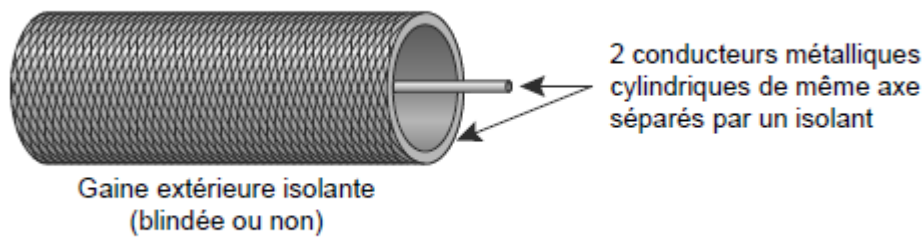


Figure I.14 : Câble coaxial. [6]

I.6.3. Fibre optique

Une fibre optique est constituée d'un fil de verre très fin. Elle comprend un cœur, dans lequel se propage la lumière émise par une diode électroluminescente ou une source laser et une gaine optique dont l'indice de réfraction garantit que le signal lumineux reste dans la fibre. [6]

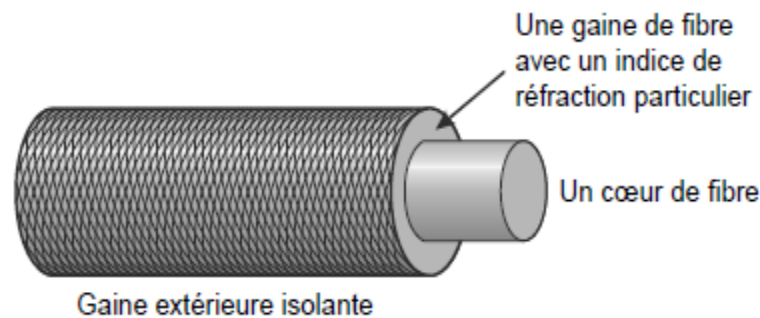


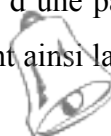
Figure I.15 : Fibre optique. [6]

I.6.4. Faisceaux hertziens

Les ondes radioélectriques peuvent, dans certains cas, remplacer avantageusement les liaisons filaires (cuivre ou optique). Les faisceaux hertziens ou câbles hertziens, par analogie aux réseaux câblés peuvent être analogiques ou numériques. Les débits peuvent atteindre 155 Mbit/s. Ils sont principalement utilisés pour des réseaux :

- de téléphonie (multiplexage fréquentiel ou temporel),
- de transmission de données.
- de diffusion d'émissions télévisées.

Pour diminuer les puissances d'émission, la technique des faisceaux hertziens utilise des antennes très directives. L'antenne réelle est placée au foyer optique d'une parabole qui réfléchit les ondes en un faisceau d'ondes parallèles très concentré, limitant ainsi la dispersion



de l'énergie radioélectrique. En réception, l'antenne est aussi placée au foyer optique de la parabole.

Tous les rayons reçus parallèlement à l'axe optique de la parabole sont réfléchis vers le foyer optique, on recueille ainsi, le maximum d'énergie (figure I.16). [6]

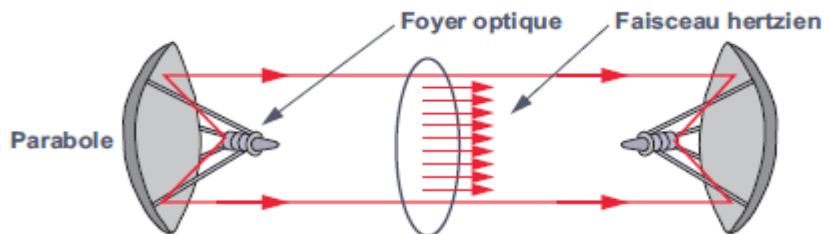


Figure I.16 Principe des faisceaux hertziens. [6]

Les distances franchissables, par les systèmes de transmission hertzienne, peuvent atteindre 100 km. Pour couvrir des distances plus importantes, il faut disposer des relais. Les relais peuvent être passifs ou actifs. Les relais passifs sont utilisés dans les zones où le relief est important ; il s'agit de simples réflecteurs utilisés pour guider l'onde, par exemple pour suivre une vallée. Les relais actifs nécessitent une infrastructure plus complexe, le signal recueilli est remis en forme, amplifié puis retransmis. Les faisceaux hertziens utilisent les bandes de 2 à 15 GHz et autorisent des débits de 155 Mbit/s.

Les faisceaux hertziens sont sensibles aux perturbations atmosphériques et aux interférences électromagnétiques. Une infrastructure hertzienne repose sur l'existence de canaux de secours qu'ils soient hertziens ou filaires.

Les liaisons infrarouges et lasers constituent un cas particulier des liaisons hertziennes. Elles sont généralement utilisées, pour interconnecter deux réseaux privés, sur de courtes distances, de l'ordre de quelques centaines de mètres. [6]

I.6.5. Les liaisons satellitaires

La nécessité de disposer de stations relais rend difficile la réalisation de liaisons hertziennes à très grande distance, notamment pour les liaisons transocéaniques. C'est pourquoi, dès les années 1960, on s'est orienté vers l'utilisation de satellites relais. Ce n'est qu'avec l'apparition de porteurs capables de satelliser sur des orbites d'environ 36000 km qu'il a été possible de réaliser des liaisons permanentes avec des satellites fixes par rapport à un observateur terrestre (satellite géostationnaire). Ces satellites ont une période de révolution

identique à celle de la terre (23 h 56 min), ils sont dits **géosynchrones**. L'orbite équatoriale est de 42 164 km, soit une altitude exacte au-dessus de la Terre de 35 800 km.

Une station terrestre émet vers le satellite un flux d'information (voie montante). Le satellite n'est qu'un simple répéteur, il régénère les signaux reçus et les réémet en direction de la Terre (voie descendante). La figure I.17 illustre le principe d'une liaison satellitaire.

Pour utiliser un satellite comme point nodal d'un réseau terrestre et, non comme simple relais de télécommunication, il est nécessaire d'admettre plusieurs voies montantes. Celles-ci sont alors en compétition pour l'accès au satellite. Plusieurs techniques peuvent être utilisées :

- L'**AMRF** (Accès Multiple à Répartition de Fréquences), consiste à diviser la bande de fréquence du satellite en sous-bandes, chacune réservée à une voie de communication.
- L'**AMRT** (Accès Multiple à Répartition de Temps), la porteuse est commune à tous les canaux de communication, mais chaque canal n'en dispose que durant un intervalle de temps limité. Ce mode d'accès nécessite une synchronisation entre les stations.
- L'**AMRC** (Accès Multiple à Répartition par Code), dans cette technique on attribue à chaque voie de communication un code. Les informations codées sont envoyées simultanément, elles sont extraites du flux par décodage. [5]

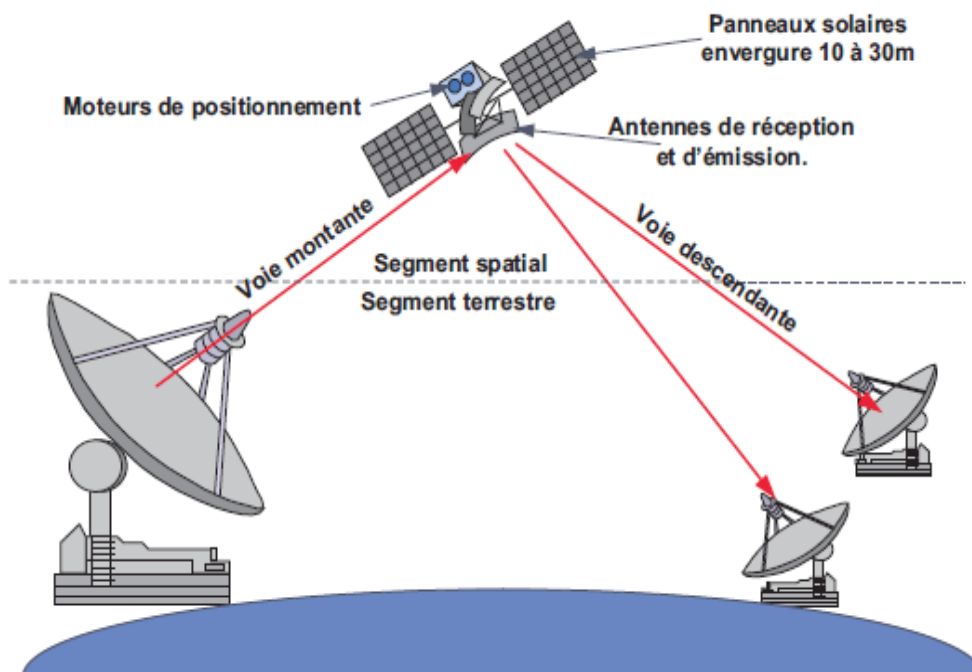


Figure I.17 : Principe d'une liaison satellitaire. [5]

I.7. Routage dans les réseaux sans fils

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème de routage consiste à déterminer un acheminement optimal des paquets à travers le réseau au sens d'un certain critère de performance. Le problème consiste à trouver l'investissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa serviabilité en cas de n'importe quelle panne d'arc ou de nœud.

L'interconnexion a toujours été un facteur d'essor rapide des réseaux, comme en témoigne Internet. L'interconnexion des réseaux sans fil à l'aide de routeurs, et de préférence en évitant de disposer de réseaux câblés, peut ouvrir la porte à de nouvelles applications. C'est en tout cas un sujet qui intéresse particulièrement les militaires américains, qui ont contribué à la création du groupe de travail MANET (Mobile Ad Hoc Network) de l'IETF (Internet Engineering Task Force) sur les réseaux mobiles ad-hoc. Ce groupe travaille à la spécification de protocoles de routage pour réseaux mobiles ad-hoc. [7]

I.8. Conclusion

Tout au long de ce chapitre, nous avons expliqué les concepts fondamentaux sur les réseaux informatiques à partir de leurs composantes et de leurs fonctions ainsi que des règles, normes et standards qui les régissent. Il ressort de cette étude que la principale entité de standardisation est l'ISO. En effet, l'ISO renferme un groupe de normes pour les protocoles qui ont été normalisés dans une structure logique afin d'exécuter des processus réseaux. Cependant, le modèle OSI est souvent considéré comme un modèle conceptuel.

Nous avons aussi étudié, les topologies physiques des réseaux et les différents types des supports de transmission

L'étude d'Ethernet et ses évolutions sans fil fait l'objet du chapitre suivant.

II.1. Introduction

Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet à un utilisateur de changer de place tout en restant connecté. Les communications entre équipements terminaux peuvent s'effectuer directement ou par le biais de stations de base, appelées points d'accès, ou AP (Access Point). Les communications entre points d'accès peuvent être hertziennes ou par câble. Les débits de ces réseaux se comptent en dizaines de mégabits par seconde.

Il faut parler des réseaux Ethernet. Car ce réseau qui reste le plus répandu des réseaux locaux est né des expériences complémentaires de DEC, Intel et surtout Xerox bien avant la normalisation. Ce qui signifie que l'essentiel des protocoles des couches supérieures (2 et 3) n'est pas spécifié.

II.2. Ethernet sans fil

Les réseaux locaux sans fil WLAN s'utilisent comme les réseaux filaires et couvrent quelques centaines de mètres. Les technologies sans fil évoluant très rapidement, on trouve toute une série de normes physiques, repérées par la lettre suivant le terme générique 802.11. Elles se distinguent par la bande de fréquence utilisée, les débits binaires et la portée dans un environnement dégagé. Le *Wi-Fi* (802.11b) est l'une des premières solutions du standard 802.11. Il utilise la bande de fréquence 2,4 GHz sur une portée maximale de 300 mètres.

Les débits disponibles pour les réseaux sans fil varient de 11 Mégabit/s pour le 802.11b à 54 Mégabit/s pour le 802.11g. Deux autres solutions plus récentes coexistent dans la bande des 5 GHz (*Wi-Fi5* ou 802.11a et *HiperLan2* ou 802.11h).

Le protocole d'accès utilisé dans les réseaux locaux sans fil est CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), une variante des algorithmes de la famille CSMA. Ce protocole est destiné à limiter les risques de collisions entre émissions provenant de machines qui ne se « voient » pas, c'est-à-dire entre machines se trouvant hors de portée l'une de l'autre.

L'organisation interne d'un réseau local sans fil est soit indépendante de toute infrastructure (*réseaux ad hoc*), soit elle est structurée en domaines indépendants appelés *cellules* (*réseaux cellulaires*). Dans un réseau ad hoc, les communications sont directes, de

machine à machine (connexions point à point). Les équipements d'un tel réseau sont de ce fait à la fois hôte et relais pour les stations hors de portée ; les règles topologiques des réseaux filaires sont alors inapplicables car la validité d'un itinéraire peut changer brusquement. De plus, les algorithmes de routage ont dû être adaptés pour tenir compte de la bande passante limitée et de la faible durée de vie des batteries.

On distingue habituellement plusieurs catégories de réseaux sans fil, selon le périmètre géographique offrant une connectivité (appelé zone de couverture) : [8]

II.2.1. Réseaux personnels sans fils (WPAN)

Le réseau personnel sans fil (appelé également réseau individuel sans fil 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 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 fil entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN :

- La principale technologie WPAN est la technologie Bluetooth, lancée par Ericsson en 1994, proposant un débit théorique de 1 Mbps pour une portée maximale d'une trentaine de mètres.
- Bluetooth, connu aussi sous le nom IEEE 802.15.1, possède l'avantage d'être très peu gourmand en énergie, ce qui le rend particulièrement adapté à une utilisation au sein de petits périphériques. La version 1.2 réduit notamment les interférences avec les réseaux Wi-Fi.
- HomeRF (Home Radio Frequency), lancée en 1998 par le HomeRF Working Group (formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft) propose un débit théorique de 10 Mbps avec une portée d'environ 50 à 100 mètres sans amplificateur. La norme HomeRF soutenue notamment par Intel, a été abandonnée en Janvier 2003, notamment car les fondateurs de processeurs misent désormais sur les technologies Wi-Fi embarquée (via la technologie Centrino, embarquant au sein d'un même composant un microprocesseur et un adaptateur Wi-Fi).

- La technologie ZigBee (aussi connue sous le nom IEEE 802.15.4) permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégré dans de petits appareils électroniques (appareils électroménagers, hifi, jouets, ...).
- Enfin les liaisons infrarouges permettent de créer des liaisons sans fils de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde. Cette technologie est largement utilisée pour la domotique (télécommandes) mais souffre toutefois des perturbations dues aux interférences lumineuses. L'association irDA (infrared data association) formée en 1995 regroupe plus de 150 membres.

II.2.2. 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 :

- Le **Wifi** (ou IEEE 802.11), soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.
- **hiperLAN2** (High Performance Radio LAN 2.0), norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute), permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 MHz.
- **DECT** (Digital Enhanced Cordless Telecommunication), norme des téléphones sans fils domestiques. Alcatel et Ascom développent pour les environnements industriels, telles les centrales nucléaires, une solution basée sur cette norme qui limite les interférences. Les points d'accès résistent à la poussière et à l'eau. Ils peuvent surveiller les systèmes de sécurité 24/24h et se connecter directement au réseau téléphonique pour avertir le responsable en cas de problème.[8]

II.2.2.1. Les réseaux 802.11

Les réseaux Wi-Fi proviennent de la norme IEEE 802.11, qui définit une architecture cellulaire. Un groupe de terminaux munis d'une carte d'interface réseau 802.11 s'associent pour établir des communications directes. Elles forment alors un BSS (Basic Service Set), à

ne pas confondre avec le BSS (Base Station Subsystem) des réseaux GSM. La zone occupée par les terminaux d'un BSS peut être une BSA (Basic Set Area) ou une cellule.

Comme illustre à la (figure II.1), la norme 802.11 offre deux modes de fonctionnement, le mode infrastructure et le mode ad-hoc. Le mode infrastructure est défini pour fournir aux différentes stations des services spécifiques, sur une zone de couverture déterminée par la taille du réseau. Les réseaux d'infrastructures sont établis en utilisant des points d'accès, qui jouent le rôle de station de base pour un BSS.

Lorsque le réseau est composé de plusieurs BSS, chacun d'eux est relié à un système de distribution, ou DS (Distribution System), par l'intermédiaire de leur point d'accès (AP) respectif. Un système de distribution correspond en règle générale à un réseau Ethernet filaire. Un groupe de BSS interconnectés par un système de distribution forme un ESS (Extended Service Set), qui n'est pas très différent d'un sous-système radio de réseau de mobiles.

Le système de distribution est responsable du transfert des paquets entre différents BSS d'un même ESS. Dans les spécifications du standard, il est implémenté de manière indépendante de la structure hertzienne de la partie sans fil. C'est la raison pour laquelle le système de distribution correspond presque toujours à un réseau Ethernet mais rien n'empêcherait d'utiliser un réseau Token-Ring ou FDDI. Une autre solution est d'utiliser le réseau Wi-Fi lui-même, ce qui donne les « Meshed network », ou réseaux mesh. [9]

En 1997, l'IEEE (Institute of Electrical and Electronics Engineers) adopta le premier standard pour les réseaux locaux sans fil (WLAN), nommé IEEE 802.11 [10] et pouvant atteindre des débits de l'ordre des 2 Mb/sec. Depuis lors, plusieurs groupes de travail (désignés par des lettres) ont été créés afin d'étendre le standard : {IEEE 802.11a : Ce groupe de travail développa une norme pour les WLAN dans la bande des 5 GHz avec un débit théorique de 54Mb/sec grâce à un multiplexage orthogonal en répartition de fréquence (OFDM). Son grand désavantage est d'être incompatible avec les normes 802.11 b/g. {IEEE 802.11b : Ce standard fut publié en 1999 et rencontra un énorme succès. Il douer des débits allant jusqu'à 11 Mb/sec et une portée radio sept fois supérieure à 802.11a dans un espace dégagé. Il exploite une technique de modulation par étalement de spectre (HR-DSSS) et travaille dans la

bande de fréquence des 2,4 GHz. Sa plage de fréquence le rend cependant plus sensible aux interférences des appareils électroménagers qui travaillent dans la même bande. [11]

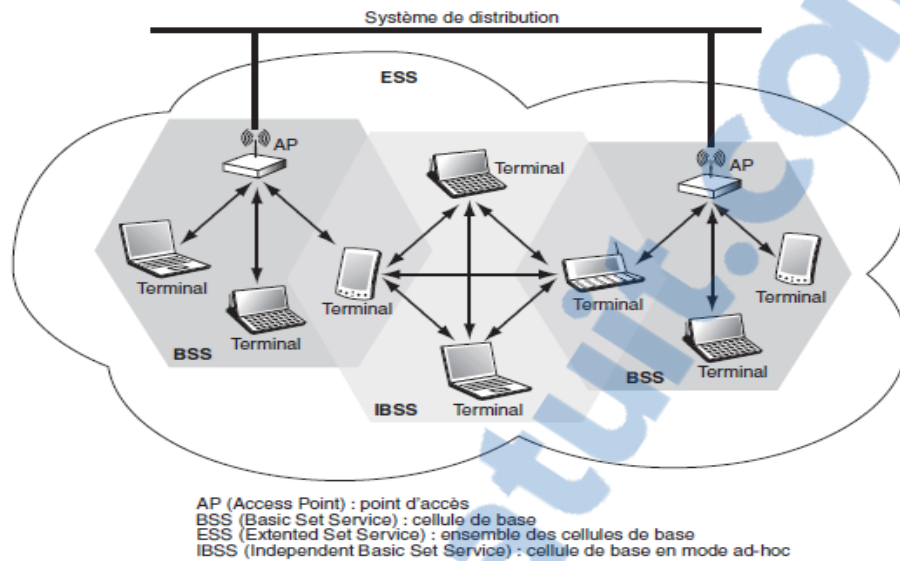


Figure II.1. Architecture d'un réseau Wi-Fi[12]

II.2.3. 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 télécommunications. [8]

II.2.4. 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 fil.

Les principales technologies sont les suivantes :

- GSM (*Global System for Mobile Communication* ou Groupe Spécial Mobile)
- GPRS (*General Packet Radio Service*)
- UMTS (*Universal Mobile Telecommunication System*)
- **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. [8]

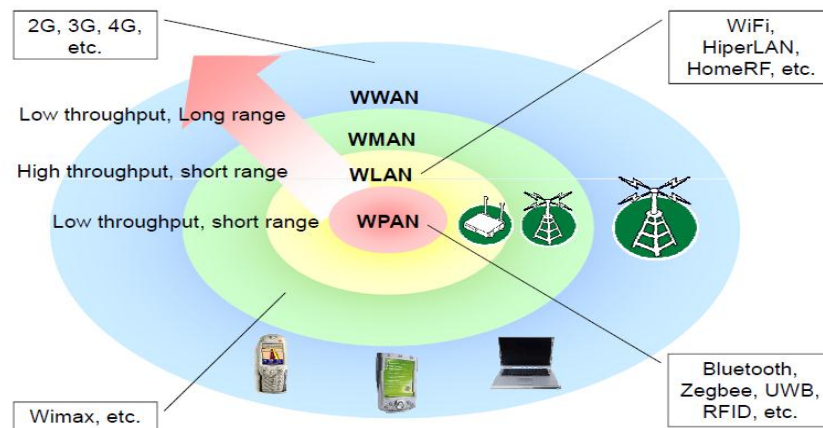


Figure II.2: Catégorie de réseau sans fil [12]

II.2.5. Réseaux locaux virtuels (VLAN)

Un réseau local virtuel est un groupe logique d'unités ou d'utilisateurs qui peuvent être regroupés par fonction, service ou application peu importe l'emplacement de leur segment physique. La configuration d'un réseau local virtuel est effectuée dans le commutateur par un logiciel. Les réseaux locaux virtuels ne sont pas uniformisés et nécessitent l'utilisation d'un logiciel propriétaire vendu par le fournisseur de commutateurs. [8]

II.3. L'architecture générale des réseaux sans fil

II.3.1. Réseaux ad-hoc

Une autre grande catégorie de réseaux sans fil est constituée par les réseaux ad-hoc, dans lesquels l'infrastructure n'est composée que des stations elles-mêmes. Ces dernières acceptent de jouer le rôle de routeur pour permettre le passage de l'information d'un terminal vers un autre, sans que ces terminaux soient reliés directement.

Contrairement aux apparences, les réseaux ad-hoc datent de plusieurs dizaines d'années.

Ils visent à réaliser un environnement de communication qui se déploie sans autre infrastructure que les mobiles eux-mêmes. En d'autres termes, les mobiles peuvent jouer le rôle de passerelle pour permettre une communication d'un mobile à un autre. Deux mobiles trop éloignés l'un de l'autre pour communiquer directement peuvent trouver un mobile intermédiaire capable de jouer le rôle de relais.

La difficulté majeure engendrée par ce type de réseau provient de la définition même de la topologie du réseau : comment déterminer quels sont les noeuds voisins et comment aller d'un noeud vers un autre noeud ? Deux solutions extrêmes peuvent être comparées.

La première est celle d'un réseau ad-hoc dans lequel tous les noeuds peuvent communiquer avec tous les autres, impliquant une longue portée des émetteurs. Dans la seconde solution, au contraire, la portée hertzienne est la plus courte possible : pour effectuer une communication entre deux noeuds, il faut généralement passer par plusieurs machines intermédiaires. L'avantage de la première solution est la sécurité de la transmission, puisqu'on peut aller directement de l'émetteur au récepteur, sans dépendre d'un équipement intermédiaire. Le débit du réseau est minimal, les fréquences ne pouvant être réutilisées.

Dans le second cas, si un terminal tombe en panne ou est éteint, le réseau peut se couper en deux sous-réseaux distincts, sans communication de l'un à l'autre. Bien évidemment, dans ce cas, le débit global est optimisé, puisqu'il peut y avoir une forte réutilisation des fréquences.

Les techniques d'accès sont du même type que dans les réseaux de mobiles. Cependant, du fait que tous les portables jouent le rôle de BSS et qu'ils sont eux-mêmes mobiles, de nouvelles propriétés doivent être apportées à la gestion des adresses des utilisateurs et au contrôle du routage.

La solution développée pour les réseaux ad-hoc prend pour fondement l'environnement IP. Les mobiles qui jouent le rôle de passerelles - le plus souvent l'ensemble des mobiles - implémentent un routeur dans leurs circuits, de telle sorte que les problèmes posés reviennent essentiellement à des problèmes de routage dans Internet, la mobilité étant gérée par le protocole IP Mobile.

Les avantages des réseaux ad-hoc sont leurs extensions très simples, leurs couvertures physiques et leurs coûts. Toutefois, pour en bénéficier pleinement, un certain nombre d'écueils sont à surmonter, telles les qualités de service et la sécurité, du fait de la mobilité des noeuds. [13]

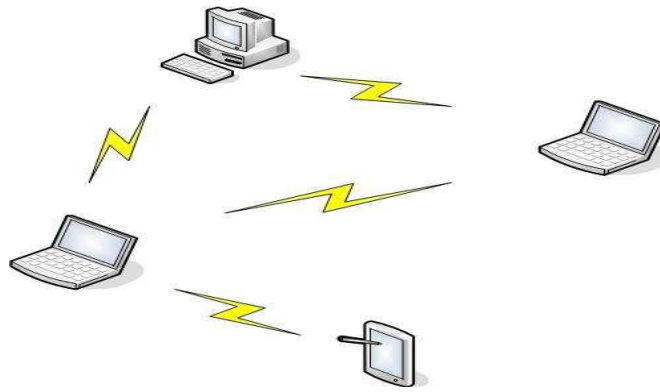


Figure II.3: Le mode Ad Hoc

II.3.2. Réseaux cellulaires

Les réseaux cellulaires sont généralement décomposés en deux ensembles d'entités distinctes, les sites fixes appartenant à un réseau filaire classique, et les sites mobiles. Certains sites fixes appelés stations support mobile (Mobile support station) ou station de base (SB) sont munis d'une interface de communication sans fil pour la communication directe avec les unités mobiles (UM) localisées dans une zone géographique limitée appelée cellule (figure II.3).

A chaque station de base correspond une cellule à partir de laquelle des unités mobiles peuvent émettre et recevoir des messages via des liaisons sans fils ayant une bande passante limitée qui réduit sévèrement le volume d'informations échangées. Toutefois, l'ensemble des stations de base sont connectées entre eux par un réseau de communication filaire, généralement fiable et d'un débit élevé.

A un instant donné, une unité mobile n'est directement connectée qu'à une seule station de base. Elle peut communiquer avec les autres sites à travers la station de base à laquelle elle est directement rattachée. Dès lors, et pour envoyer un message d'une unité mobile UM1 à une autre unité mobile UM2, UM1 doit envoyer le message à sa station de base SB1 à travers le réseau sans fil qui le transmet à la station de base de l'unité UM2 appelée SB2, qui à son tour le transmet à UM2.[14]

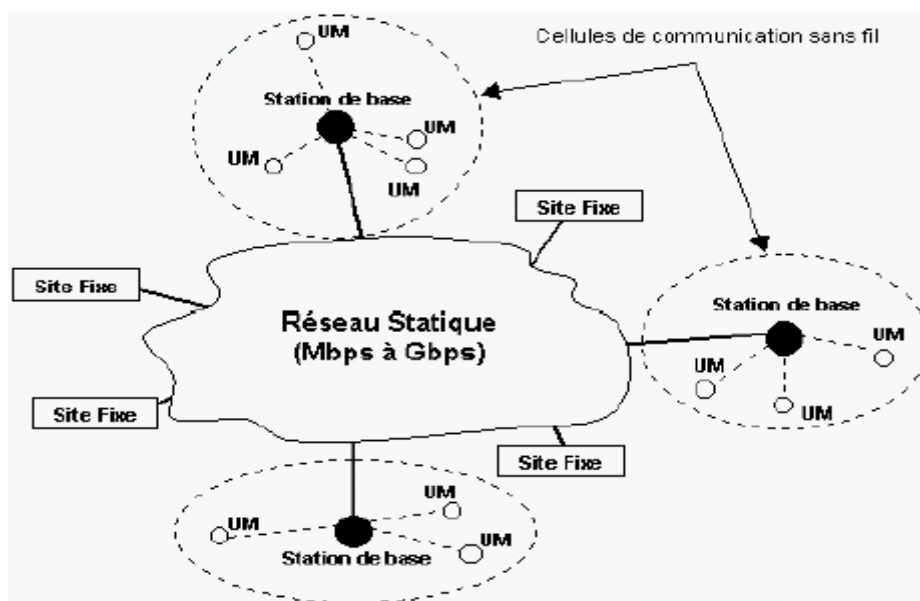


Figure II.4: Modèle des réseaux cellulaires

II.4. Caractéristiques générales des réseaux Ethernet 802.3

II.4.1. Principe de CSMA/CD

Dans les méthodes de type CSMA, pour *Carrier Sense Multiple Access*, (IEEE 802.3), les stations s'émettent à l'écoute du canal et attendent qu'il soit libre pour émettre. Les transmissions ne sont pas instantanées par suite des délais de propagation, et une collision peut se produire au moment où une station émet, même si elle a écouté le canal au préalable et n'a rien entendu. Plus le délai de propagation est grand, plus le risque de collision est important.

Il existe différentes variantes du protocole. La plus classique est celle des réseaux 802.3 : CSMA/CD, pour CSMA with *Collision Detection*. Sa particularité est que la station *continue* à écouter le canal après le début de l'émission et *arrête* immédiatement l'émission si une collision est détectée. Le temps pendant lequel on écoute ainsi, alors qu'on est en train de transmettre, est limité à quelques microsecondes (temps de propagation aller-retour entre les deux stations les plus éloignées). La durée de la collision est ainsi réduite au minimum. Le temps nécessaire pour émettre une trame ne peut pas être garanti avec le CSMA/CD. En effet, les retransmissions sont effectuées après une durée aléatoire qui dépend du nombre de tentatives et après 16 tentatives infructueuses, on abandonne. L'intérêt de cette technique est qu'elle ne nécessite pas la présence d'une station maîtresse. [15]

II.4.2. Format des trames Ethernet/IEEE 802.3

La norme IEEE802.3 est représentée en (figure II.4.). Le codage est du type Manchester. Un préambule de 7 octets permet la synchronisation bit. La synchronisation caractère est assurée par le fanion de début de trame (SFD, Start Frame Delimitator), les deux bits à «1» marque le début de la trame. Les champs adresses (2 ou 6 octets) contiennent les adresses MAC destination et source.

Un pointeur, sur 2 octets, indique la longueur utile du champ données. Le champ données est suivi d'un contrôle d'erreur de type CRC: le FCS (Frame check Sequence) sur 4 octets. [16]

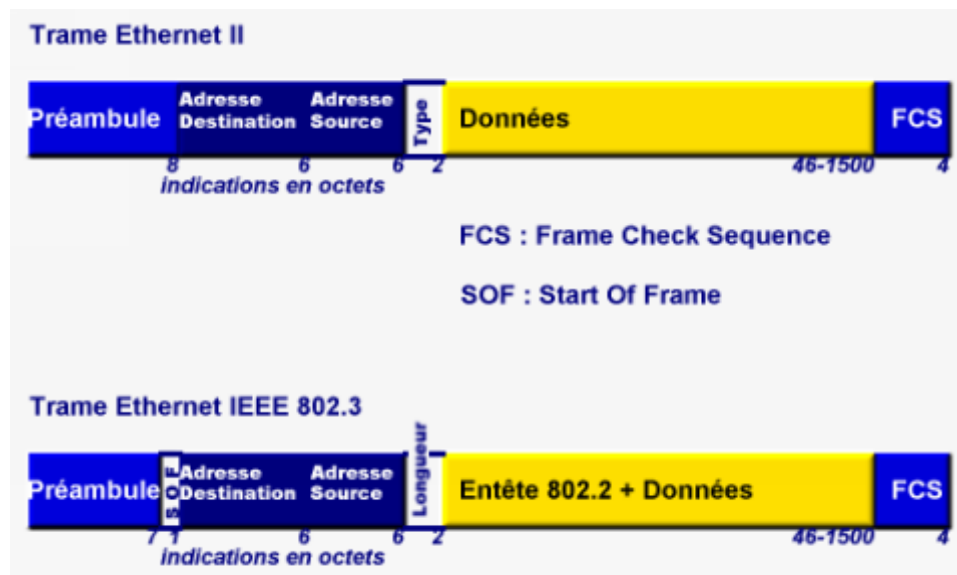


Figure II.5: Format des trames Ethernet 802.3 [17]

II.5. Différentes versions d'Ethernet

II.5.1. L'Ethernet épais, IEEE 802.3 10 bas 5

Appellations	10Base5, Thick Ethernet
Support	câble coaxial 50 Ohms associé à une connectique N-BNC
Longueur Maximum	500 m par brin. Les câbles doivent avoir une longueur multiple de 23,4m (généralement 117m) pour que les réflexions produites sur les raccords soient superposées déphasées
Distance entre connexions	au moins 2,50m (points repérés sur le câble)
Nombre maximum de	au plus 100 connexions par brin

connexions	
------------	--

Tableau II.1 : Ethernet IEEE 802.3 10 bas 5

II.5.2 L'Ethernet fin, IEEE 802.3 10 bas 2

Appellations	10Base2, Thinnet ou Thin Ethernet
Support	câble coaxial 50 Ohms (RG58) associé à une connectique BNC
Longueur maximum	185m
Distance entre connexions	50cm
Nombre maximum de connexions	30 stations

Tableau II.2 : Ethernet Fin [17].

II.5.3 L'Ethernet à 100 Mbit/s

Au début des années 90, face à un besoin de plus en plus croissant de bande passante, la « haute autorité » de l'IEEE décida de faire travailler le comité 802.3 sur l'élaboration d'un réseau LAN à haut débit. Suite à de nombreux échanges entre le comité et les différents acteurs du marché (3com, Cisco, etc...) 2 propositions émergèrent :

- Faire évoluer l'Ethernet 10Mbit/s.
- Redéfinition plus complète de la norme : Le 100VG Anylan (soutenu par HP & IBM).

La première proposition fut retenue pour des raisons évidentes de compatibilité ascendante avec tous les produits déjà existants et conformes à la norme 802.3. Parallèlement, les partisans du 100VG AnyLan créèrent leur propre standard.

Caractéristiques communes avec Ethernet :

- Reprise du protocole CSMA/CD donc compatibilité totale.
- Maintient de la taille des trames (de 64 à 1518 octets).

- Même topologie en étoile que le 10Base-T. La topologie Bus associée à l'utilisation du coaxial est abandonnée.

Principales différences/évolutions :

- Fenêtre de collision ou TC (tranche canal) diminuée proportionnellement au débit:

On passe de 51,2 μ s à 5,12 μ s. Implicitement, le diamètre maximum du réseau est fortement diminué (distance maximale entre les stations les plus éloignées) et passe à environ à 200m au lieu de 2500m. Cette solution a été préférée à l'augmentation de la taille minimum de la trame. La logique aurait voulu que l'on évolue de 64 octets à 640 octets mais dans ce cas précis, une partie de la bande passante aurait été perdue.

- Le silence inter-frames (IFG : Inter Frame Gap) diminue également proportionnellement et passe à 0,96ns.
- De nouvelles fonctions de management font leur apparition au niveau de la couche physique.
- Enfin, même si techniquement il était possible d'implémenter Fast Ethernet sur du coaxial, cette solution n'a pas été retenue et la seule et unique topologie retenue est la topologie en étoile avec un câblage paires torsadées ou Fibre optique.

La norme 100Base-T se décline en 2 sous-ensembles: Le 100Base-T4 basé sur l'utilisation de 4 paires torsadées et le 100Base-TX qui se décline à nouveau en 2 sous-ensembles, le 100Base-TX (2 paires torsadées) et le 100Base-FX (sur fibre optique).

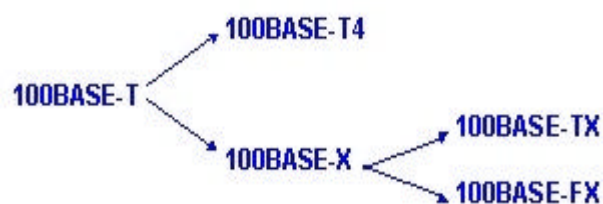


Figure II.6: Norme 100Base T.

Dans l'architecture étoilée qui caractérise le 100Base-T, il existe 2 types de hub partagés :

- Les hubs de **classe I** qui ne supportent pas la présence des autres hubs. Pour accroître la taille du réseau il faut faire appel à des ponts, routeurs ou commutateurs...

- Les hubs de **classe II** qui autorisent une cascade de 2 hubs du même type. Leur raccordement ne permet pas d'étendre la taille maxi du réseau mais surtout d'accroître le nombre de stations connectées.

La plupart des hubs sont équipés d'un protocole d'auto-négociation du débit. Grâce à des signaux de type *Fast Link Pulse* le hub négocie avec chaque station le mode de communication le plus intéressant : 100Base-TX full duplex, 100Base-T4, 100Base-TX, 10Base-TX, etc...

II.5.3.1. couche physique 100Base-T

La norme 100Base-T supporte 3 types de supports physiques :

appellation	Type câble	Long. station/hub	Etendue maximale du réseau	Remarque
100Base-T4	4 paires torsadées cat.3 ou 4 UTP	100 m	~ 200 m	Duplex asymétrique 100Mbit/s et 25Mbit/s
100Base-TX	2 paires torsadées cat.5 UTP ou STP.	100 m	~ 200 m	Duplex symétrique à 100Mbit/s
100Base-FX	2 fibres optiques Multicode (MMF) diamètre 125µm.	400 m	~ 318 m	Duplex symétrique à 100Mbit/s

Tableau II.3: couche physique 100Base-T [18]

II.5.4. Gigabit Ethernet

Comme les câbles en paires torsadées de catégorie 5 sont certifiés pour des fréquences allant jusqu'à 100MHz, le passage à 1000Mbps pose des difficultés nouvelles par rapport aux évolutions précédentes. La couche physique a été entièrement revue. La nouvelle définition est une « fusion » de deux technologies : l'Ethernet IEEE802.3 et le Fibre Channel ANSI X3/T11.

Cette fusion reprend le format de trame Ethernet 802.3 et la méthode d'accès CSMA/CD full-duplex pour conserver la compatibilité avec les couches supérieures du réseau et elle bénéficie du débit élevé de l'interface physique Fibre Channel.

Comme pour la famille Fast Ethernet, il existe plusieurs variantes 1000BaseX [18]

II.6. Conclusion

Dans ce chapitre, nous avons dans un premier temps nous avons décrit les informations nécessaires pour comprendre la suite de ce manuscrit à savoir quelques informations générales sur les réseaux technologie Ethernet. Puis, nous avons intéressé aux réseaux locaux filaires et sans fils pour lesquels nous allons détailler ses types de réseaux afin de pouvoir à la suite simulés quelques exemples avec Cisco Packet Tracer et OPNET.

III.1. Introduction

Dans ce chapitre nous avons présente brièvement quelques exemple pour les réseaux informatique utile .Ensuite nous somme présente les différentes topologies avec le logiciel Cisco Packet tracer.

III.2. Routage statique

III.2.1. Réseaux informatique en topologie étoile avec un routeur centrale

Le réseau informatique est composé de 6 sous réseaux reliés par un routeur central selon la figure III.1. Il faut en premier temps configurer la partie réseau (adresse IP et routage) et puis vérifier la connectivité entre les périphériques à fin d'assurer un bon fonctionnement du réseau. [19]

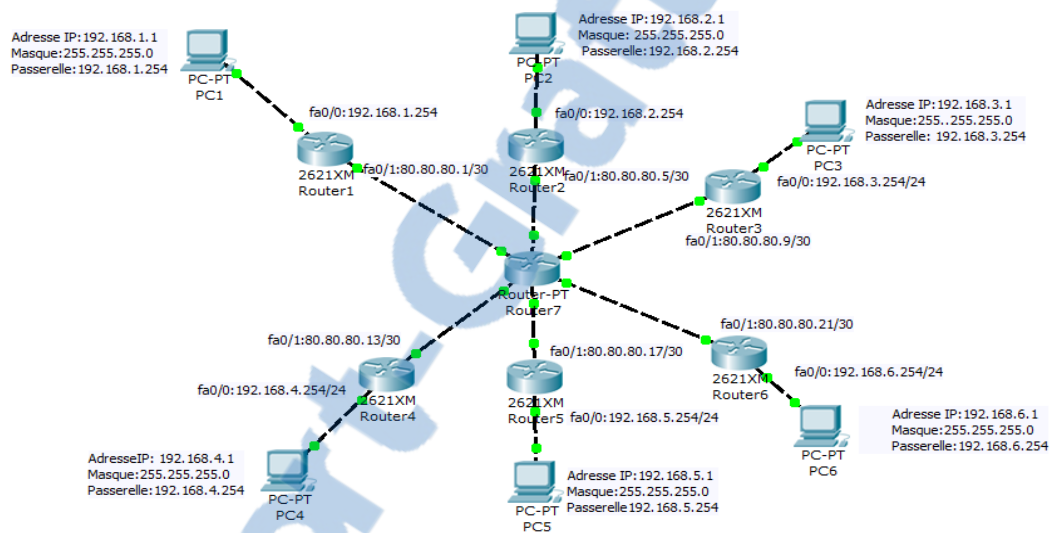


Figure III.1 : Topologie étoile avec un routeur central. [19]

Le tableau suivant présent les adresses IP des ordinateur et les interfaces des routeurs.

Machines	Int	@IP	Masque
PC1	Carte réseau	192.168.1.1	255.255.255.0
PC2	Carte réseau	192.168.2.1	255.255.255.0
PC3	Carte réseau	192.168.3.1	255.255.255.0
PC4	Carte réseau	192.168.4.1	255.255.255.0
PC5	Carte réseau	192.168.5.1	255.255.255.0
PC6	Carte réseau	192.168.6.1	255.255.255.0
Router 1	Fa0/0	192.168.1.254	255.255.255.0

	Fa0/1	80.80.80.1	255.255.255.252
Router 2	Fa0/0	192.168.2.254	255.255.255.0
	Fa0/1	80.80.80.5	255.255.255.252
Router 3	Fa0/0	192.168.3.254	255.255.255.0
	Fa0/1	80.80.80.9	255.255.255.252
Router 4	Fa0/0	192.168.4.254	255.255.255.0
	Fa0/1	80.80.80.13	255.255.255.252
Router 5	Fa0/0	192.168.5.254	255.255.255.0
	Fa0/1	80.80.80.17	255.255.255.252
Router 6	Fa0/0	192.168.6.254	255.255.255.0
	Fa0/1	80.80.80.21	255.255.255.252
Router 7 (centrale)	Fa0/0	80.80.80.6	255.255.255.252
	Fa0/1	80.80.80.2	255.255.255.252
	Fa0/2	80.80.80.10	255.255.255.252
	Fa0/3	80.80.80.14	255.255.255.252
	Fa0/4	80.80.80.18	255.255.255.252
	Fa0/5	80.80.80.22	255.255.255.252

Tableau III.1.Table de routage de réseau proposé

III.2.1.1. Configuration des routeurs par commandes

En premier lieu, nous allons configurer les éléments (routeurs, ordinateurs) du réseau informatique proposé, en indiquant tous les @ IP des interfaces utilisés. Ensuite, nous allons ajouter les routes statiques dans chaque routeur.

Routeur1

On commence la configuration du Routeur1 par lui donner un nom. Celui-ci va permettre de ne pas se perdre entre les différents routeurs. Tapez la commande suivante :

```
Router # configure terminal
Router (config)#no ip domain-lookup
Router (config)#hostname Routeur1
```

Nous configurons ensuite l'interface fastethernet 0/0, pour lui donner l'adresse ip "192.168.1.254/24".

```
Routeur1(config)#interface fastEthernet 0/0
Routeur1(config-if)#ip address 192.168.1.254 255.255.255.0
Routeur1(config-if)#no shutdown Routeur1(config-if)#exit
```

Puis nous configurons l'interface fastethernet 0/1, pour lui donner l'adresse ip "80.80.80.1/30".

```
Routeur1(config)#interface fastEthernet 0/1

Routeur1(config-if)#ip address 80.80.80.1 255.255.255.252

Routeur1(config-if)#no shutdown

Routeur1(config-if)#exit
```

Pour finir nous configurons le routeur statique.

```
Routeur1(config)#ip route 192.168.0.0 255.255.0.0 80.80.80.2

Routeur1(config)#exit
```

Nous allons suivre les mêmes étapes pour configurer les autres routeurs.

a- Routeur2

```
Routeur2(config)#interface fastEthernet 0/0

Routeur2(config-if)#ip address 192.168.2.254 255.255.255.0

Routeur2(config-if)#no shutdown

Routeur2(config-if)#exit

Routeur2(config)#interface fastEthernet 0/1

Routeur2(config-if)#ip address 80.80.80.5 255.255.255.252

Routeur2(config-if)#no shutdown

Routeur2(config-if)#exit

Routeur2(config)#ip route 192.168.0.0 255.255.0.0 80.80.80.6

Routeur2(config)#exit
```

b- Routeur3

```
Router#configure terminal

Router(config)#no ipdomain-lookup

Router(config)#hostname Routeur3

Routeur3(config)#interface fastEthernet 0/0

Routeur3(config-if)#ip address 192.168.3.254 255.255.255.0

Routeur3(config-if)#no shutdown

Routeur3(config-if)#exit

Routeur3(config)#interface fastEthernet 0/1

Routeur3(config-if)#ip address 80.80.80.9 255.255.255.252

Routeur3(config-if)#no shutdown

Routeur3(config-if)#exit

Routeur3(config)#ip route 192.168.0.0 255.255.0.0 80.80.80.10

Routeur3(config)#exit
```


c- Routeur4

```
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#hostname Routeur4
Routeur4(config)#interface fastEthernet 0/0
Routeur4(config-if)#ip address 192.168.4.254 255.255.255.0
Routeur4 (config-if)#no shutdown
Routeur4 (config-if)#exit
Routeur4 (config)#interface fastEthernet 0/1
Routeur4 (config-if)#ip address 80.80.80.13 255.255.255.252
Routeur4 (config-if)#no shutdown
Routeur4 (config-if)#exit
Pour finir nous configurons le routeur statique.
Routeur3(config)#ip route 192.168.0.0 255.255.0.0 80.80.80.10
```

d- Routeur5

```
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#hostname Routeur5
Routeur5 (config)#interface fastEthernet 0/0
Routeur5 (config-if)#ip address 192.168.5.254 255.255.255.0
Routeur5 (config-if)#no shutdown Routeur5 (config-if)#exit
Routeur5 (config)#interface fastEthernet 0/1
Routeur5 (config-if)#ip address 80.80.80.17 255.255.255.252
Routeur5 (config-if)#no shutdown
Routeur5 (config-if)#exit
Routeur5 (config)#ip route 192.168.0.0 255.255.0.0 80.80.80.18
```

```
Routeur5(config)#exit
```

e- Routeur6

```
Router#configure terminal
Router (config)#no ipdomain-lookup
Router (config)#hostname Routeur6
Routeur6 (config)#interface fastEthernet 0/0
Routeur6 (config-if)#ip address 192.168.6.254 255.255.255.0
Routeur6 (config-if)#no shutdown
Routeur6 (config-if)#exit
Routeur6 (config)#interface fastEthernet 0/1
Routeur6 (config-if)#ip address 80.80.80.21 255.255.255.252
Routeur6 (config-if)#no shutdown
Routeur6 (config-if)#exit
Routeur6(config)#ip route 192.168.0.0 255.255.0.0 80.80.80
Routeur6 (config)#exit
```

f- Routeur7 (central)

```
Router#configure terminal
```

```
Router(config)#no ipdomain-lookup
Router(config)#hostname Routeur-Central
```

Nous configurons maintenant nos interfaces :

```
Interface fa 1/0 :
Routeur-Central(config)#interface fastEthernet 1/0
Routeur-Central(config-if)#ip address 80.80.80.2 255.255.255.252
Routeur-Central(config-if)#no shutdown
Routeur-Central(config-if)#exit
```

```
Interface fa 2/0 :
Routeur-Central (config)#interface fastEthernet 2/0
Routeur-Central(config-if)#ip address 80.80.80.6 255.255.255.252
Routeur-Central(config-if)#no shutdown
Routeur-Central(config-if)#exit
```

```
Interface fa 3/0 :
Routeur-Central (config)#interface fastEthernet 3/0
Routeur-Central (config-if)#ip address 80.80.80.10 255.255.255.252
Routeur-Central (config-if)#no shutdown
Routeur-Central (config-if)#exit
```

```
Interface fa 4/0 :
Routeur-Central (config)#interface fastEthernet 4/0
Routeur-Central (config-if)#ip address 80.80.80.14 255.255.255.252
Routeur-Central (config-if)#no shutdown
Routeur-Central (config-if)#exit
```

```
Interface fa 5/0 :
Routeur-Central (config)#interface fastEthernet 5/0
Routeur-Central (config-if)#ip address 80.80.80.18 255.255.255.252
Routeur-Central (config-if)#no shutdown
Routeur-Central (config-if)#exit
```

Interface fa 6/0 :

```
Routeur-Central (config)#interface fastEthernet 6/0
```

```
Routeur-Central (config-if)#ip address 80.80.80.22 255.255.255.252
```

```
Routeur-Central (config-if)#no shutdown
```

```
Routeur-Central (config-if)#exit
```

Pour finir nous configurons les routeurs statiques.

```
Routeur-Central(config)#ip route 192.168.1.0 255.255.255.0 80.80.80.1
```

```
Routeur-Central(config)#ip route 192.168.2.0 255.255.255.0 80.80.80.5
```

```
Routeur-Central(config)#ip route 192.168.3.0 255.255.255.0 80.80.80.9
```

```
Routeur-Central(config)#ip route 192.168.4.0 255.255.255.0 80.80.80.13
```

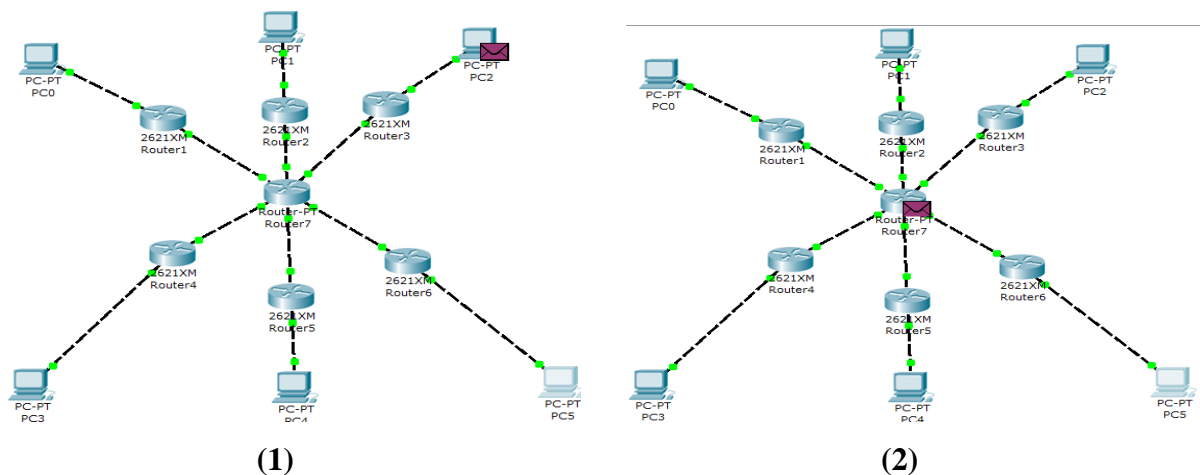
```
Routeur-Central(config)#ip route 192.168.5.0 255.255.255.0 80.80.80.17
```

```
Routeur-Central(config)#ip route 192.168.6.0 255.255.255.0 80.80.80.2
```

```
Routeur-Central(config)#exit
```

III.2.1.2. Simulation

Il est important de commencer à assurer la connectivité entre les périphériques. Nous allons tester par le mode simulation (PDU) les deux stations PC2 et PC5.



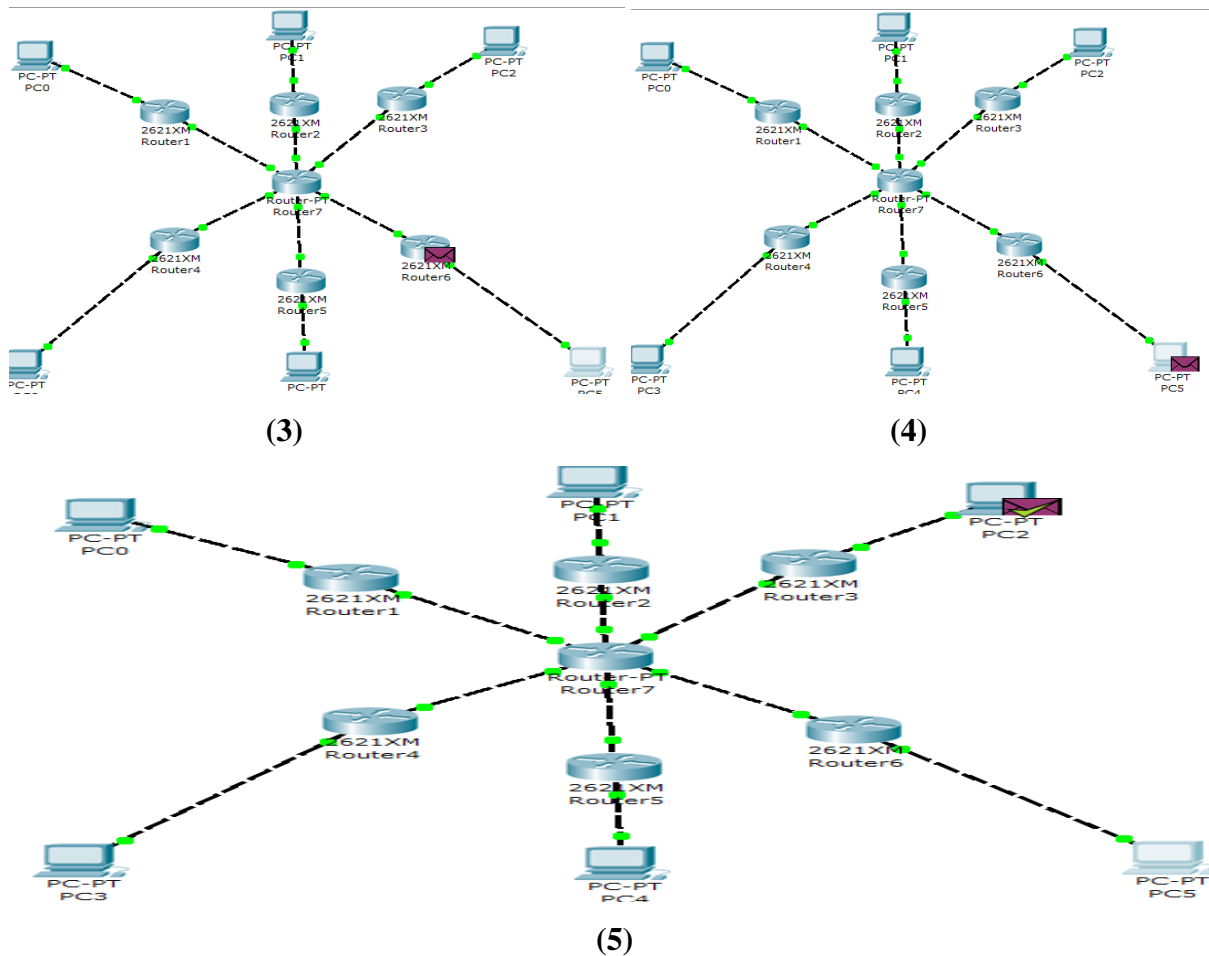


Figure III.2.Etapes de simulation de PC2 vers PC5. [19]

En activant le mode simulation les échanges de trames sont simulés par des déplacements d’enveloppes sur le schéma. Les manipulations peuvent être les mêmes qu’un mode temps réel mais des animations visuelles montrent le cheminement des informations.

Nous remarquons que l’enveloppe est dirigée de la station émettrice PC2 vers la station réceptrice PC5 sans aucunes erreurs. L’enveloppe cochée verte reçue par la station PC2 montre encore que la connectivité entre ces deux stations est correcte(étape 5).

Nous avons vérifié aussi la connectivité entre la station PC2 vers les autres stations (PC0, PC1, PC3, PC4) par le mode simulation.

Dans ce cas, le réseau fonctionne correctement en introduisant la technique de routage statique insérée dans les différents routeurs de la topologie choisie.

III.2.2 Réseau informatique en topologie étoile avec 3 routeurs centraux

Le réseau de la figure ci-dessous est composé de cinq routeurs, six PCs et quatre commutateur .Les types des composants utilisés sont les suivants : Des routeurs Cisco

modèle 2621 XM et des commutateurs Cisco modèle 2950. Ce réseau comporte 6 sous réseaux reliés ensemble par des routeurs.

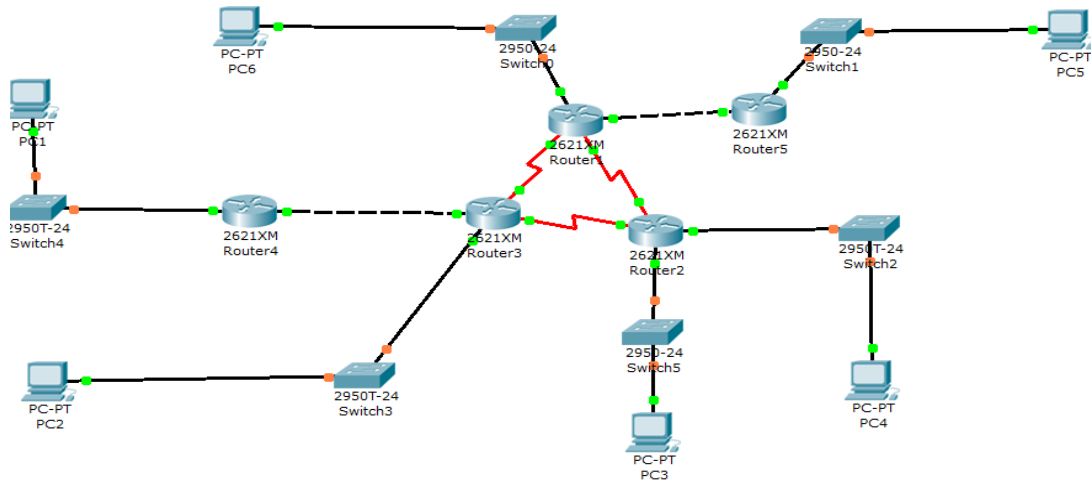


Figure III.3 : Topologie étoile avec 3 routeurs centraux. [20]

Le tableau suivant présent les adresses IP des stations et des interfaces des routeurs.

Les machines	Interface	Adresse IP	Masque de sous-réseau
Pc1	Carte réseau	192.168.1.2	255.255.255.0
Pc2	Carte réseau	192.168.2.2	255.255.255.0
Pc3	Carte réseau	192.168.3.2	255.255.255.0
Pc4	Carte réseau	192.168.4.2	255.255.255.0
Pc5	Carte réseau	192.168.5.2	255.255.255.0
Pc6	Carte réseau	192.168.6.2	255.255.255.0
Router1	Fa0/0	192.168.0.17	255.255.255.252
	Fa0/1	192.168.6.1	255.255.255.0
	Se0/0	192.168.0.1	255.255.255.252
	Se0/1	192.168.0.5	255.255.255.252
Router2	Fa0/0	192.168.3.1	255.255.255.0
	Fa0/1	192.168.4.1	255.255.255.0
	Se0/0	192.168.0.2	255.255.255.0

	Se0/1	192.168.0.10	255.255.255.252
Router3	Fa0/0	192.168.0.13	255.255.255.252
	Fa0/1	192.168.2.1	255.255.255.0
	Se0/0	192.168.0.6	255.255.255.252
	Se0/1	192.168.0.9	255.255.255.252
Router4	Fa0/0	192.168.1.1	255.255.255.0
	Fa0/1	192.168.0.14	255.255.255.252
Router5	Fa0/0	192.168.5.1	255.255.255.0
	Fa0/1	192.168.0.18	255.255.255.252

Tableau III.2 : Table de routage de la topologie proposée. [20]

III.2.2.1. Configuration des routeurs par commandes

On commence la configuration du Routeur1 par lui donner un nom. Celui-ci va permettre de ne pas se perdre entre les différents routeurs. Tapez la commande suivante :

a- Routeur 1

```
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#hostname Routeur1
Nous configurons ensuite l'interface fastethernet 0/0.
Routeur1(config)#interface fastEthernet 0/0
Routeur1(config-if)#ip address 192.168.0.17 255.255.255.252
Routeur1(config-if)#no shutdown
Routeur1(config-if)#exit
```

Puis nous configurons l'interface fastethernet 0/1, pour lui donner l'adresse ip 192.168.6.1

```
Routeur1(config)#interface fastEthernet 0/1
Routeur1(config-if)#ip address 192.168.6.1 255.255.255.0
Routeur1(config-if)#no shutdown
```

```
Routeur1(config-if)#exit
```

Nous configurons maintenant nos interfaces sérial 0/0 et sérial0/1 :

```
Routeur1(config)#interface serial 0/0
Routeur1(config-if)#ip address 192.168.0.1 255.255.255.252
Routeur1(config-if)#no shutdown
Routeur1(config-if)# encapsulation ppp
Routeur1(config-if)#clock rate 64000
Routeur1(config-if)#exit
Routeur1(config)#interface serial 0/1
Routeur1 (config-if)#ip address 192.168.0.5 255.255.255.252
Routeur1 (config-if) #no shutdown
Routeur1(config-if)# encapsulation ppp
Routeur1(config-if)#clock rate 64000
Routeur1 (config-if) #exit
```

Pour finir nous configurons les routeurs statiques.

```
Router1 (config)#ip route 192.168.5.0 255.255.255.0 192.168.0.18
Router1 (config)#ip route 192.168.3.0 255.255.255.0 192.168.0.2
Router1 (config)#ip route 192.168.4.0 255.255.255.0 192.168.0.2
Router1 (config)#ip route 192.168.2.0 255.255.255.0 192.168.0.6
Router1 (config)#ip route 192.168.1.0 255.255.255.0 192.168.0.6
```

Les mêmes étapes sont répétées pour configurer les autres routeurs. On présente maintenant les chemine des routes statiques dans les routeurs suivants :

a- Router2

Network Address
192.168.1.0/24 via 192.168.0.9
192.168.6.0/24 via 192.168.0.1
192.168.5.0/24 via 192.168.0.1

b- Router3

Network Address
192.168.1.0/24 via 192.168.0.14
192.168.4.0/24 via 192.168.0.10
192.168.3.0/24 via 192.168.0.10
192.168.6.0/24 via 192.168.0.5
192.168.5.0/24 via 192.168.0.5

c- Router4

Network Address
192.168.2.0/24 via 192.168.0.13
192.168.3.0/24 via 192.168.0.13
192.168.4.0/24 via 192.168.0.13
192.168.5.0/24 via 192.168.0.13
192.168.6.0/24 via 192.168.0.13

d- Router5

Network Address
192.168.6.0/24 via 192.168.0.17
192.168.2.0/24 via 192.168.0.17
192.168.3.0/24 via 192.168.0.17
192.168.4.0/24 via 192.168.0.17
192.168.1.0/24 via 192.168.0.17

III.2.2.2. Simulation en ligne de commande

L'invite de commandes permet d'exécuter un ensemble de commandes relatives au réseau. La liste est accessible en tapant help. En particulier, les commandes ping, arp, tracert et ipconfig sont accessibles

Pour tester le bon fonctionnement des liaisons de réseau, il est possible d'ouvrir une invite de commandes ping suivi d'une adresse IP de la station destinataire. Les résultats de simulation en ligne de commande entre les périphériques sont présentés par les figures suivantes :

a- Ping entre PC1 et les autres PCs

```

PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 10ms, Average = 10ms

```

(a) :PC1 vers PC2

```

PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=16ms TTL=125
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 16ms, Average = 13ms

```

(b) :PC1 vers PC3

```

PC>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=12ms TTL=125
Reply from 192.168.4.2: bytes=32 time=12ms TTL=125
Reply from 192.168.4.2: bytes=32 time=12ms TTL=125
Reply from 192.168.4.2: bytes=32 time=12ms TTL=125

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 12ms, Average = 12ms

```

(c) :PC1 vers PC4

```

PC>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.5.2: bytes=32 time=15ms TTL=123
Reply from 192.168.5.2: bytes=32 time=14ms TTL=124
Reply from 192.168.5.2: bytes=32 time=15ms TTL=123
Reply from 192.168.5.2: bytes=32 time=14ms TTL=124

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 15ms, Average = 14ms

```

(d) :PC1 vers PC5

```

PC>ping 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:

Reply from 192.168.6.2: bytes=32 time=12ms TTL=125
Reply from 192.168.6.2: bytes=32 time=13ms TTL=124
Reply from 192.168.6.2: bytes=32 time=12ms TTL=125
Reply from 192.168.6.2: bytes=32 time=13ms TTL=124

Ping statistics for 192.168.6.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 13ms, Average = 12ms

```

(d) :PC1 vers PC5

Figure III.4. Résultats de simulation entre PC1 et les autres PCs

b- Ping entre PC3 et les autres PCs

```

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=12ms TTL=125
Reply from 192.168.1.2: bytes=32 time=12ms TTL=125
Reply from 192.168.1.2: bytes=32 time=12ms TTL=125
Reply from 192.168.1.2: bytes=32 time=12ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 12ms, Average = 12ms

```

(a) :PC3 vers PC1

```

PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 10ms, Average = 10ms

```

(b) :PC3 vers PC2

```

PC>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=8ms TTL=127
Reply from 192.168.4.2: bytes=32 time=8ms TTL=127
Reply from 192.168.4.2: bytes=32 time=8ms TTL=127
Reply from 192.168.4.2: bytes=32 time=8ms TTL=127

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 8ms, Average = 8ms

```

(c) :PC3 vers PC4

```

PC>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Reply from 192.168.5.2: bytes=32 time=12ms TTL=125
Reply from 192.168.5.2: bytes=32 time=12ms TTL=125
Reply from 192.168.5.2: bytes=32 time=12ms TTL=125
Reply from 192.168.5.2: bytes=32 time=12ms TTL=125

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 12ms, Average = 12ms

```

(d) :PC3 vers PC5

```

PC>ping 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:

Reply from 192.168.6.2: bytes=32 time=10ms TTL=126
Reply from 192.168.6.2: bytes=32 time=10ms TTL=126
Reply from 192.168.6.2: bytes=32 time=10ms TTL=126
Reply from 192.168.6.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.6.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 10ms, Average = 10ms

```

(e) :PC3vers PC6

Figure III.5 : Résultats de simulation entre PC3 et les autres PCs

c- Ping entre PC5 et les autres PCs

```

Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=14ms TTL=124
Reply from 192.168.1.2: bytes=32 time=14ms TTL=124
Reply from 192.168.1.2: bytes=32 time=14ms TTL=124
Reply from 192.168.1.2: bytes=32 time=14ms TTL=124

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 14ms, Maximum = 14ms, Average = 14ms

```

(a) :PC5 vers PC1

```

PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=12ms TTL=125
Reply from 192.168.2.2: bytes=32 time=12ms TTL=125
Reply from 192.168.2.2: bytes=32 time=12ms TTL=125
Reply from 192.168.2.2: bytes=32 time=12ms TTL=125

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 12ms, Average = 12ms

```

(b) :PC5 vers PC2

```

PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=12ms TTL=125
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125
Reply from 192.168.3.2: bytes=32 time=12ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 12ms, Average = 12ms

```

(c) :PC5 vers PC3

```

PC>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time=12ms TTL=125
Reply from 192.168.4.2: bytes=32 time=12ms TTL=125
Reply from 192.168.4.2: bytes=32 time=12ms TTL=125
Reply from 192.168.4.2: bytes=32 time=12ms TTL=125

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 12ms, Average = 12ms

```

(d) :PC5 vers PC4

```

PC>ping 192.168.6.2

Pinging 192.168.6.2 with 32 bytes of data:

Reply from 192.168.6.2: bytes=32 time=10ms TTL=126
Reply from 192.168.6.2: bytes=32 time=10ms TTL=126
Reply from 192.168.6.2: bytes=32 time=10ms TTL=126
Reply from 192.168.6.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.6.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 10ms, Average = 10ms

```

(a) :PC5 vers PC6

Figure III.6 : Résultats de simulation entre PC5 T les autres PCs

D’après les résultats de simulations, nous remarquons que les nombres des paquets envoyés sont égaux aux nombres des paquets reçus et que les paquets perdus sont nuls. Ceu-ci monter que la connectivité est bien vérifiée entre les différents éléments constituant la topologie choisie.

III.3. Routage dynamique

Nous somme basé sur le même réseau précédent schématisé par la figure III.3 sous Packet Tracer, ou nous allons introduire la technique de routage dynamique qui est plus simple et plus pratique que le routage statique. Le réseau est composé de cinq routeurs de types router-PT, de six commutateurs de série 2950T et six PCs reliés avec des câbles appropriés. [21]

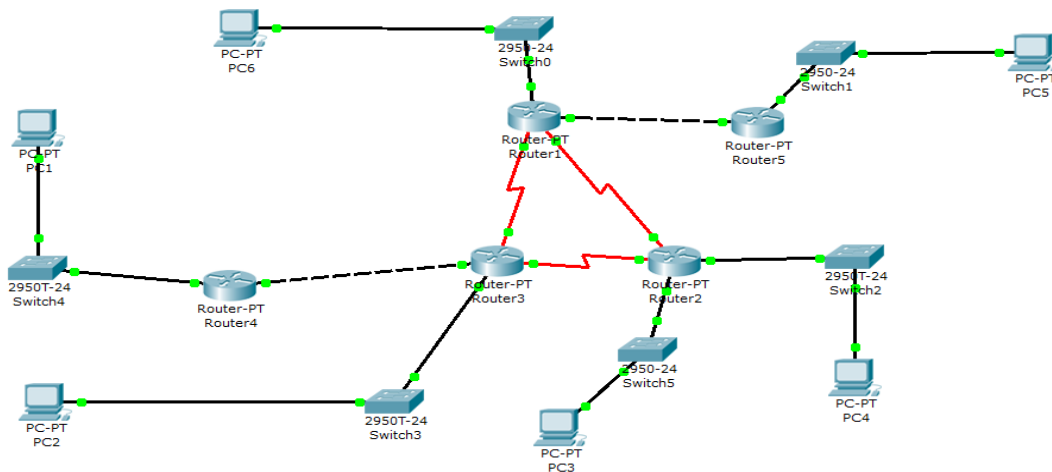


Figure III.7 : Réseau proposé avec la technique de routage dynamique. [21]

Le tableau suivant présent les adresses IP des PCs et des interfaces des routeurs.

Les routeurs	FastEthernet	Ip address
--------------	--------------	------------

Pc1	Carte réseau	192.168.1.2
Pc2	Carte réseau	192.168.2.2
Pc3	Carte réseau	192.168.3.2
Pc4	Carte réseau	192.168.4.2
Pc5	Carte réseau	192.168.5.2
Pc6	Carte réseau	192.168.6.2
Routeur 1	Fa0/0	192.168.0.17
	Fa0/1	192.168.6.1
	Se0/0	192.168.0.1
	Se0/1	192.168.0.5
Routeur 2	Fa0/0	192.168.3.1
	Fa0/1	192.168.4.1
	Se0/0	192.168.0.10
	Se0/1	192.168.0.2
Routeur 3	Fa0/0	192.168.0.13
	Fa0/1	192.168.2.1
	Se0/0	192.168.0.6
	Se0/1	192.168.0.9
Routeur 4	Fa0/0	192.168.0.14
	Fa0/1	192.168.1.1
Routeur 5	Fa0/0	192.168.0.18
	Fa0/1	192.168.5.1

Tableau III.3 : Table de routage de réseau choisi. [21]

III.3.1. Configuration des routeurs par commandes

Pour configurer le routeur1 nous avons utilisé les commandes suivantes :

```
Router>enable

Router#configure terminal

Router1(config)#no ip domain-lookup

Router1(config)#hostname Routeur1

Routeur1(config)#interface fastEthernet 0/0

Routeur1(config-if)#ip address 192.168.0.17 255.255.255.252

Routeur1(config-if)#no shutdown

Routeur1(config-if)#exit
```

Puis nous configurons l'interface fastethernet 0/1, pour lui donner l'adresse ip 192.168.6.1

```
Routeur1(config)#interface fastEthernet 0/1

Routeur1(config-if)#ip address 192.168.6.1 255.255.255.0

Routeur1(config-if)#no shutdown

Routeur1(config-if)#exit
```

Nous configurons maintenant nos interfaces sérial 0/0 et sérial0/1 :

```
Routeur1(config)#interface serial 0/0
Routeur1(config-if)#ip address 192.168.0.1 255.255.255.252
Routeur1(config-if)#no shutdown
Routeur1(config-if)# encapsulation ppp
Routeur1(config-if)#clock rate 64000
Routeur1(config-if)#exit
Routeur1(config)#interface serial 0/1
Routeur1(config-if)#ip address 192.168.0.5 255.255.255.252
Routeur1 (config-if) #no shutdown
Routeur1(config-if)# encapsulation ppp
```

```
Routeur1(config-if)#clock rate 64000
Routeur1 (config-if) #exit
```

Pour finir nous configurons le routeur dynamique.

```
Router(config)#router rip
Router(config-router)# network 192.168.0.0
Router(config-router)# network 192.168.1.0
Router(config-router)# network 192.168.2.0
Router(config-router)# network 192.168.3.0
Router(config-router)# network 192.168.4.0
Router(config-router)# network 192.168.5.0
Router(config-router)# network 192.168.6.0
Router5(config-router)#exit
```

On procédé de la même manière pour la configurer les autres routeurs avec les routes dynamiques suivantes indiquées pour chaque routeur.

a- Routeur2

Network Address
192.168.0.0
192.168.3.0
192.168.4.0

b- Routeur3

Network Address
192.168.0.0
192.168.2.0

c- Routeur4

Network Address
192.168.0.0
192.168.1.0

d- Routeur5

Network Address
192.168.0.0
192.168.5.0

III.3.2. Simulation en mode temps réel

Pour vérifier le bon fonctionnement du réseau on teste les stations par la simulation en mode temps réel.

III.3.2.1. Simulation de Pc1 vers Pc5

Sur les figures suivantes, on représente les étapes de simulation de PC1 vers PC5.

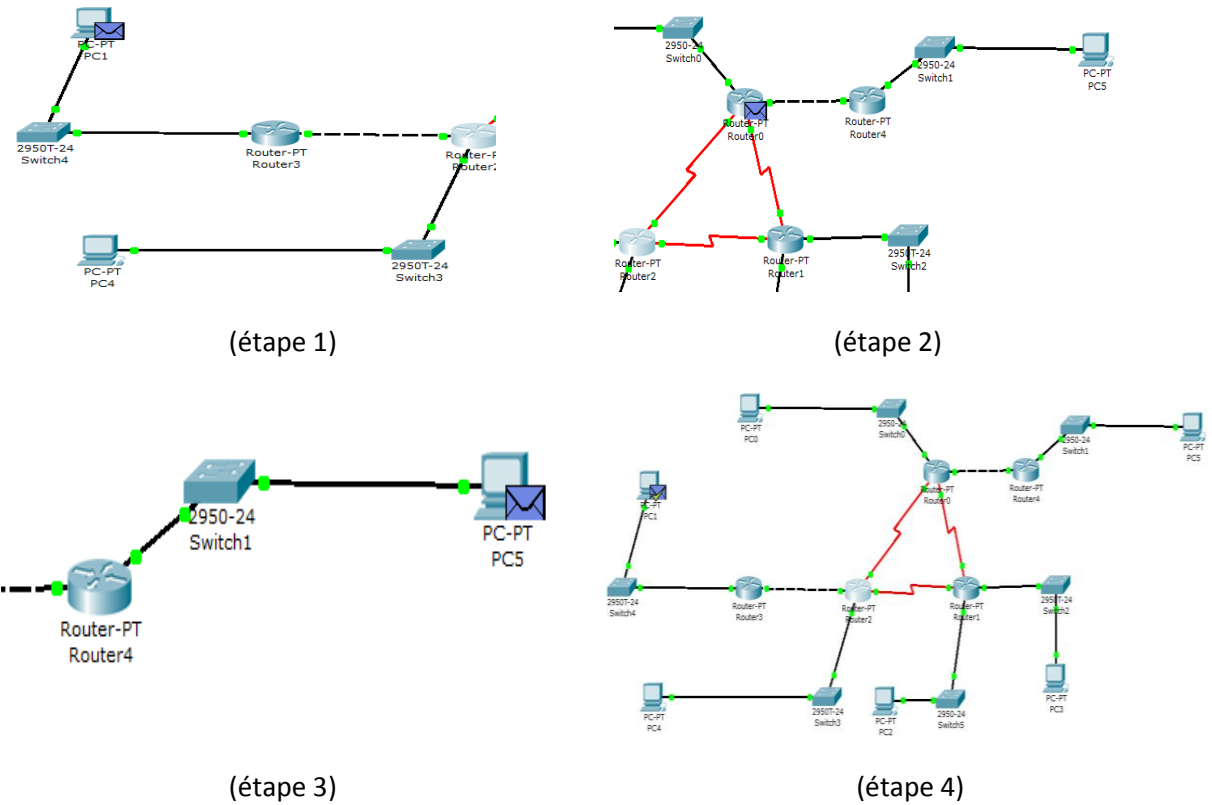


Figure III.8 :Etapes de simulation de PC1 vers PC5

l’enveloppe suivre le chemin le plus court pour arriver au destination (PC5) comme représente la figure III.8.Ceux –ci montrent que la configuration des périphériques

(PC1,routeur 4,routeur 3,routeur 1,routeur 5,PC5) est bien réalisé et que les paquets sont envoyés sans aucunes erreurs.

III.3.2.2. Simulation de Pc2 vers Pc6

Sur les figures suivantes, on représente les étapes de simulation de PC2 vers PC6.

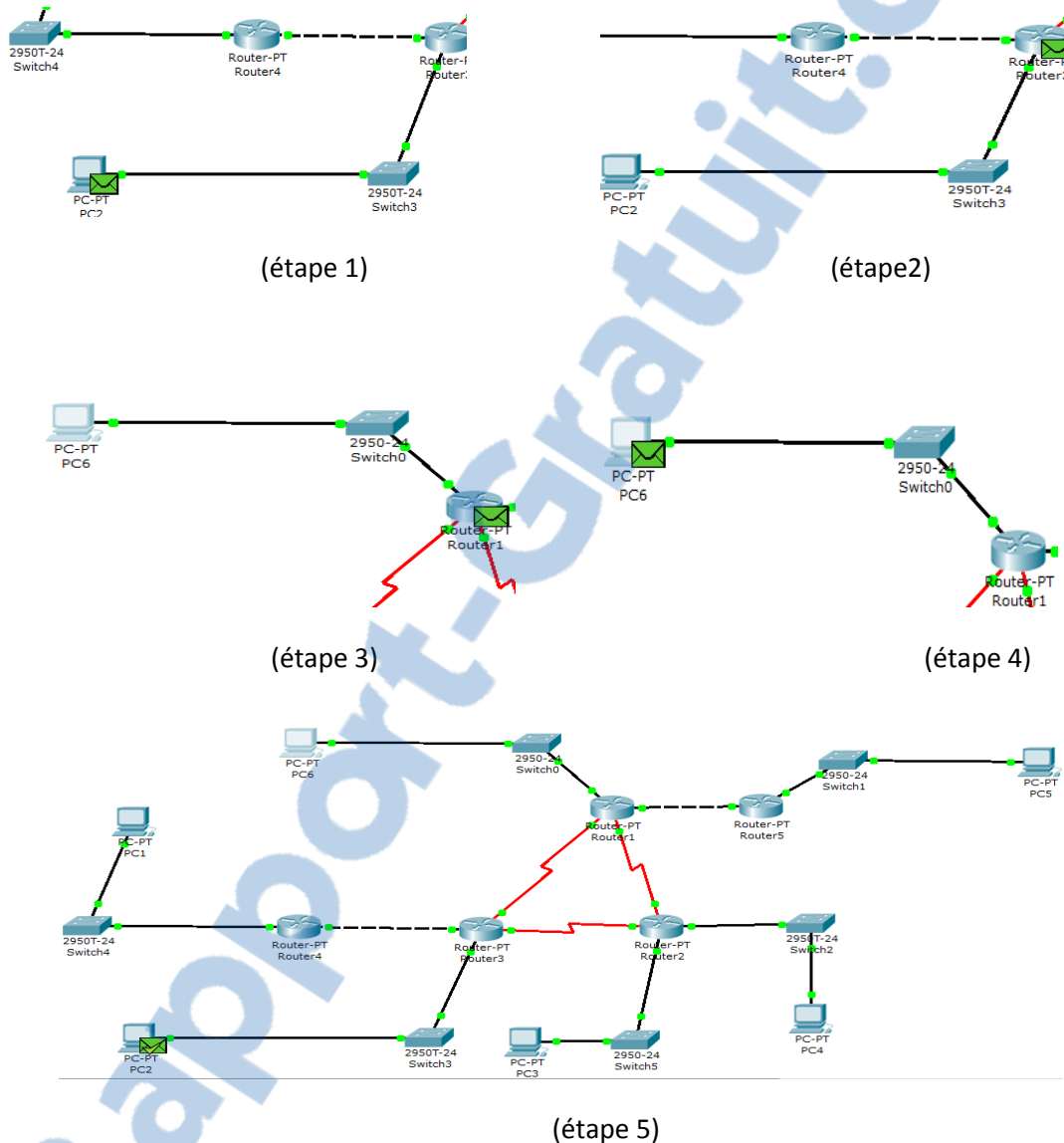


Figure III.9 :Etapes de simulation de PC1 vers PC6

A partir de l'étape 5,nous observons que la station émettrice (PC2) engendre une enveloppe cochée en vert .Donc la communication entre PC2 et PC6 est bien établie.

III.4. Adressage fixe et dynamique

A l'aide de l'outil « Packet Tracer » schématiser le réseau de la figure ci-dessous composé d'un Wireless Router, 15 PC et un commutateur, deux ordinateurs portables et quarts hub PT, le commutateur Cisco modèle 2950. [21]

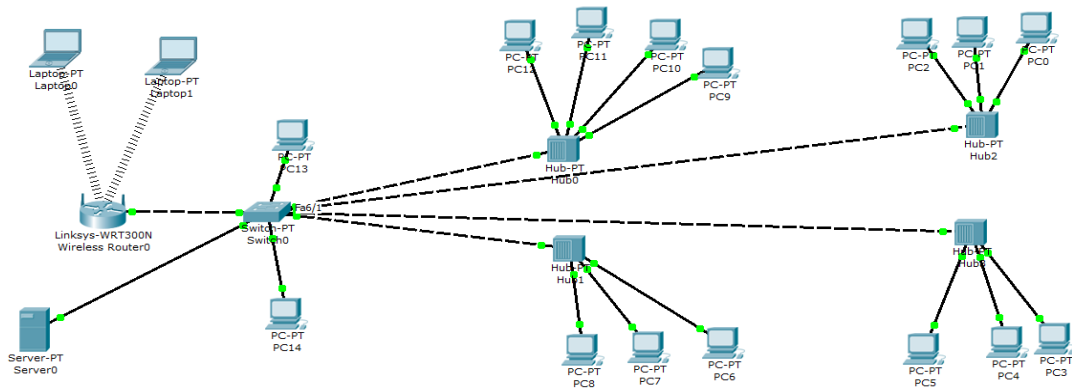


Figure III.10 : Réseau informatique d'entreprise.[21]

III.4.1.Adressage fixe

La table de routage du réseau informatique est présenté par le tableau III.4

Les machines	Adresse IP	Masque de sous-réseau
Laptop1	192.168.0.100	255.255.255.0
Laptop2	192.168.0.101	255.255.255.0
PC0	192.168.1.1	255.255.255.0
PC1	192.168.1.2	255.255.255.0
PC2	192.168.1.3	255.255.255.0
PC3	192.168.1.4	255.255.255.0
PC4	192.168.1.5	255.255.255.0
PC5	192.168.1.6	255.255.255.0
PC6	192.168.1.7	255.255.255.0
PC7	192.168.1.8	255.255.255.0
PC8	192.168.1.9	255.255.255.0
PC9	192.168.1.10	255.255.255.0
PC10	192.168.1.11	255.255.255.0

PC11	192.168.1.12	255.255.255.0
PC12	192.168.1.13	255.255.255.0
PC13	192.168.1.14	255.255.255.0

Tableau III.4 : Table de routage. [21]

En adressage fixe, il faut intervenir manuellement pour configurer l'adresse IP, la passerelle et le serveur DNS.

III.4.1.1.Simulation de Laptop ver PC12

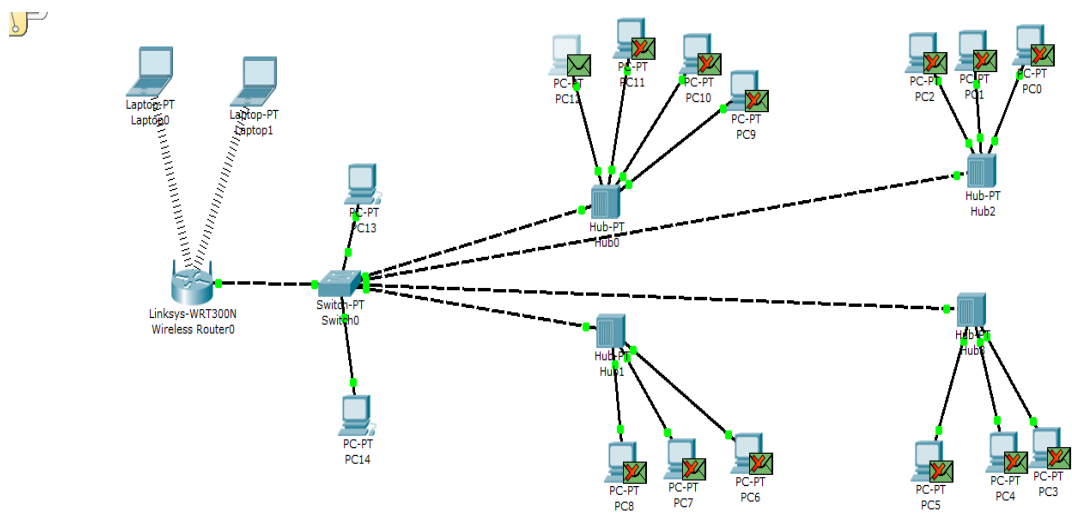


Figure III.11. Etapes de simulation de Laptop1 vers PC1(Adressage fixe)

III.4.2.Adressage dynamique

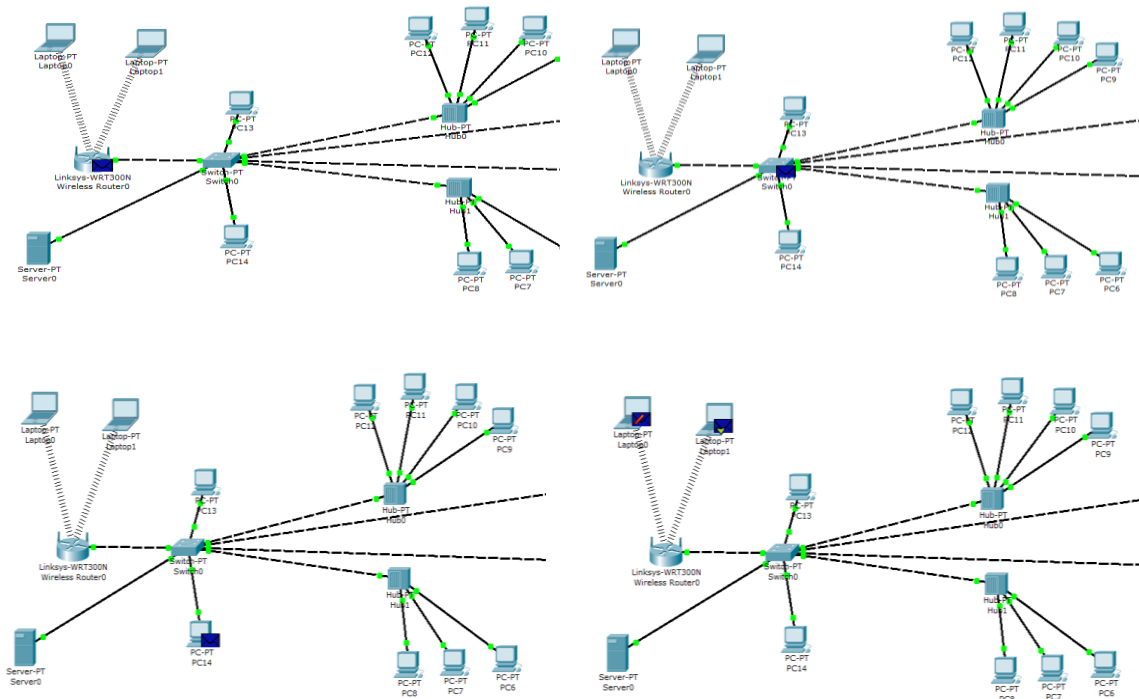


Figure III.12 : Etapes de simulation de Laptop1 vers PC1

Pour l'adressage dynamique on doit configurer les paramètres du serveur DHCP au lieu de configurer les adresse IP des périphériques .Cette technique est plus simple et plus rapide que la méthode de l'adressage fixe.D'après les résultats de simulation, nous pouvons déduire que la communication entre les différentes stations est bien réalisée.

III.4.2.1. Paramètres du serveur DHCP

Paramètres du serveur DHCP	
Adresse IP de départ	10.4.4.1
Masque de sous réseau	255.0.0.0
Passerelle par défaut	10.0.0.1
Serveur DNS	10.0.0.2

Tableau III.5 : Paramètres du serveur DHCP

III.5.Wifi

A l'aide de l'outil « Packet Tracer » nous avons créé et simulé un réseau WIFI constitué de trois ordinateurs portables, d'un serveur, de deux points d'accès WIFI et deux

commutateurs. Les commutateurs sont de types Cisco modèle 2960. Le réseau proposé est schématisé par la figure suivante :

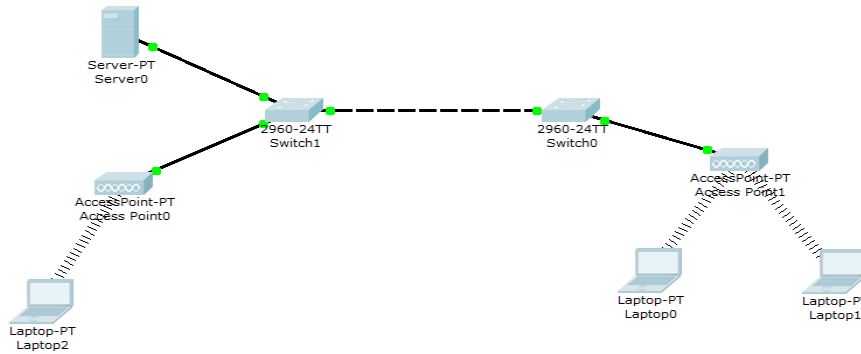


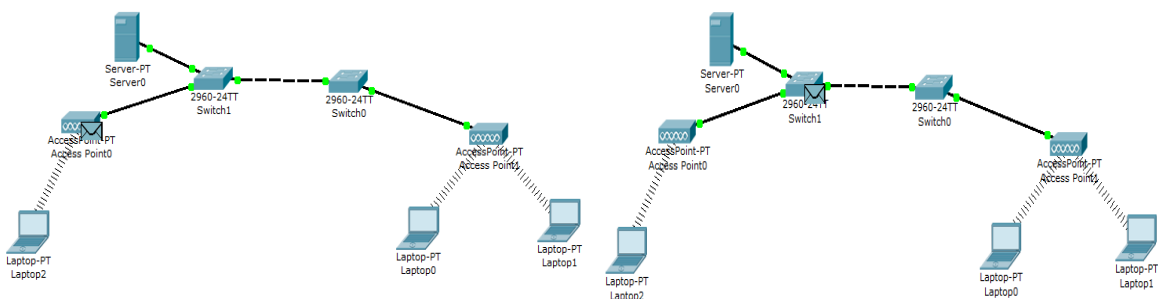
Figure III.13 : Réseau WIFI proposé. [21]

Dans le tableau suivant, nous allons présenter les @ IP et les masques des ordinateurs portables et de server.

Configuration		
Poste	Adresse IP	Masque de sous réseau
Laptop0	192.168.2.4	255.255.255.0
Laptop1	192.168.2.5	255.255.255.0
Laptop2	192.168.2.3	255.255.255.0
Server-PT	192.168.2.6	255.255.255.0

Tableau III.6 : Table de routage de réseau WIFI.

III.5.1. Simulation entre Pc1 et Pc2



(étape 1)

(étape 2)

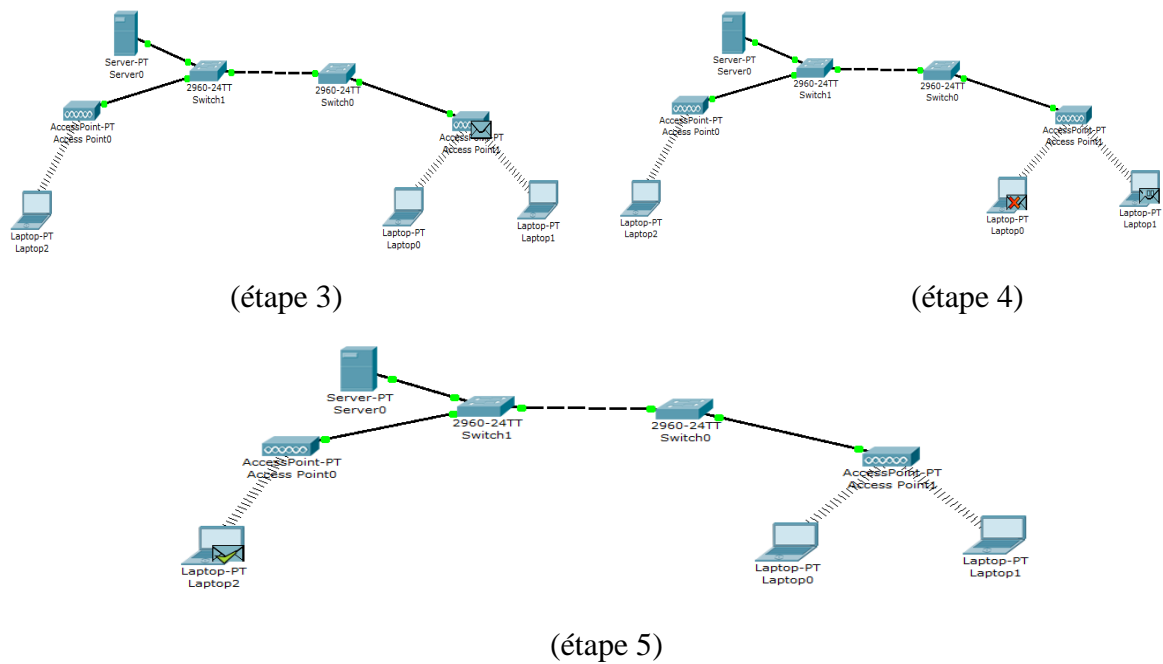
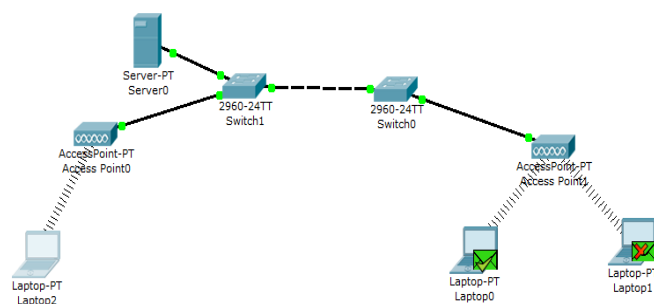


Figure III.14 : Etape de simulation de PC1 vers PC2

A la fin de la simulation, une enveloppe cochée en vert est observée au niveau du PC2. Nous pouvons déduire que la configuration de réseau WIFI est bien faite et précisément les liens sans fil établis entre les Access Points et les Laptops.



L'enveloppe qui coche verte montre que la communication entre les PC bien établie.

III.6. Conclusion :

Dans ce chapitre, nous avons utilisé l'outil de simulation Cisco Packet Tracer pour simuler des réseaux informatiques locaux. Dans lesquels nous avons appliqué divers algorithmes tels que l'algorithme de routage statique et dynamique, l'algorithme de l'adressage fixe et dynamique. Comme nous avons conçu un réseau informatique sans fil de

type WIFI. Les résultats de simulation montrent que la connectivité entre les différents périphériques est bien établie et que les réseaux proposés sont bien configurés sans aucune erreur aux niveaux des éléments constituant le réseau choisi.

Dans le chapitre suivant, nous allons concevoir quelques réseaux locaux avec le logiciel OPNET Modeler.

IV.1.Introduction

L'environnement OPNET permet la modélisation et la simulation des réseaux de communications grâce à des modèles bibliothèques (Routeurs, Commutateurs, Stations de travail, Serveurs ...) et de protocoles (TCP/IP, FTP, FDDI, Ethernet, ATM ...). Le module Radio OPNET permet la simulation des réseaux de radiocommunications : hertzien, téléphonie cellulaire et satellitaire. Le but de ce projet 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 interfaces principales et les modèles bibliothèques de implantés dans OPNET (modèles standards, matériels, protocolaires et applicatifs).

IV.2. Premier scénario

Nous allons créer un modèle de réseau initial qui est composé de 16 stations et d'un commutateur. Ceci constitue un réseau initial qui sera le premier scénario nommé « OnlyHub »

Le tableau suivant montre les valeurs essentielles qu'on doit les écrire dans les zones de dialogue de *Statup Wizard*. [22]

Dialog Box Name	Value
Initial Topology	Select the default value : Create Empty Scenario.
Choose Network Scale	Select Office . Select the Use metric units checkbox.
Specity Size	Select the Fault size: 100 m x 100 m
Review	Chek values, then click Finish

Tableau IV.1 : Valeurs indiquées dans le Startup Wizard.

IV.2.1. Eléments de réseau

Pour créer le premier réseau en utilisant *Rapid Configuration*

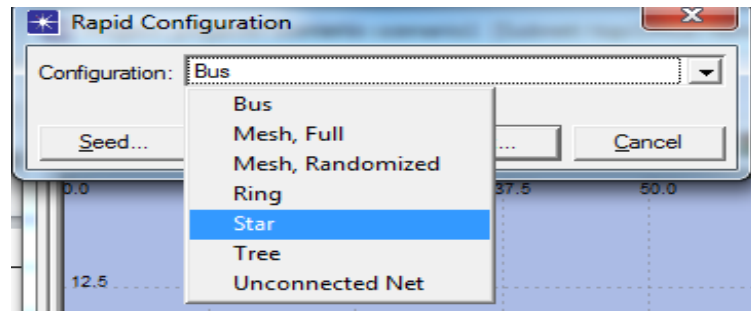


Figure IV.1 : Choix de la topologie étoile à partir du menu déroulant.

Les nœuds et les liens employés pour établir le premier réseau sont résumés dans la figure IV.2.

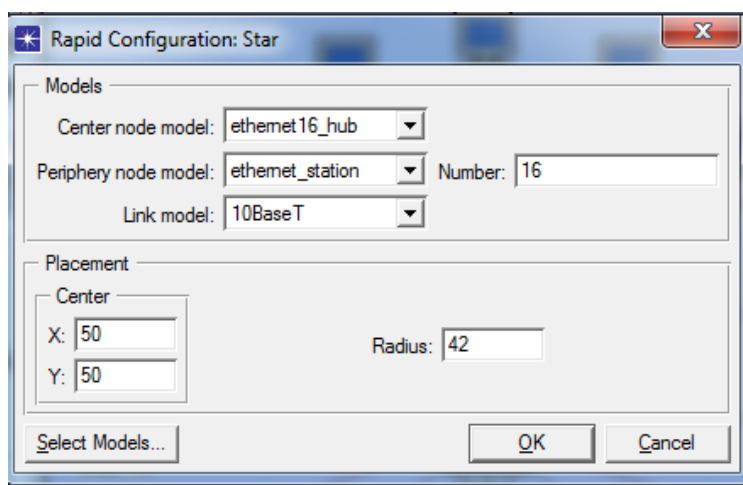


Figure IV.2 : Zone de dialogue Rapide Configuration.

Le réseau est maintenant établi comme représente la figure suivante.

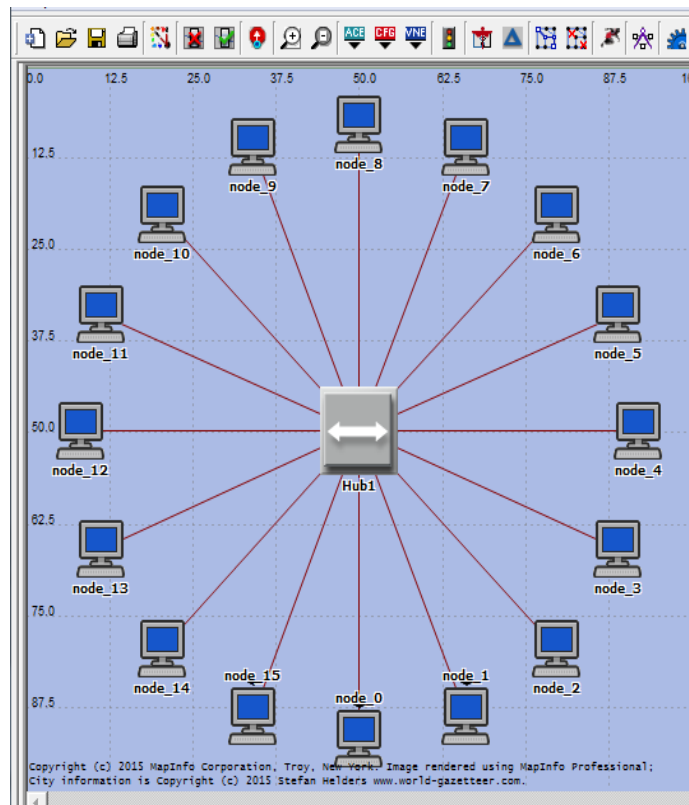


Figure IV.3 : Premier scénario.

IV.2.2. Duplication du Scénario

Le réseau que nous avons créé utilise seulement un moyen pour relier les 16 postes. Nous allons créer un autre réseau qui utilise un changement et voir si cela affectera la performance du réseau. Pour créer un double du réseau courant, On choisi **Duplicate Scenario** du menu et on lui donne le nom HubAndSwitch . [22]

Le réseau est maintenant établi comme représente la figure suivante.

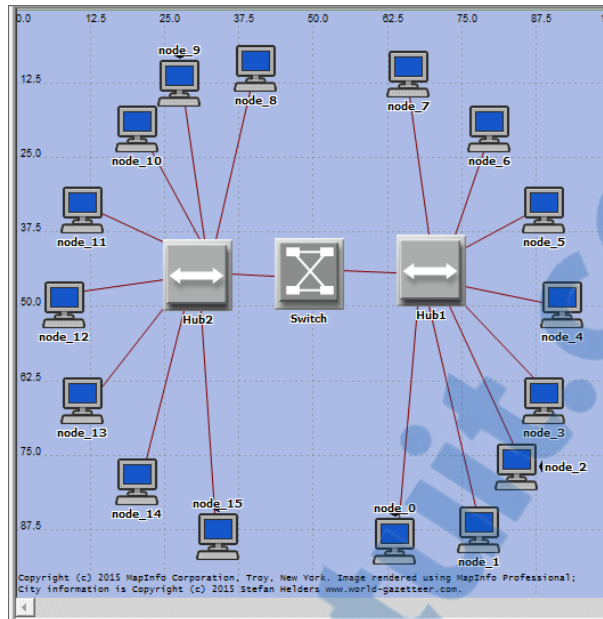


Figure IV.4 : Scénario HubAndSwitch. [22]

Pour chaque scénario, la durée de simulation d'entrée est 2min avec 100 échantillons par statique.

Les résultats de simulation des deux scénarios sont montrés dans les figures suivantes :

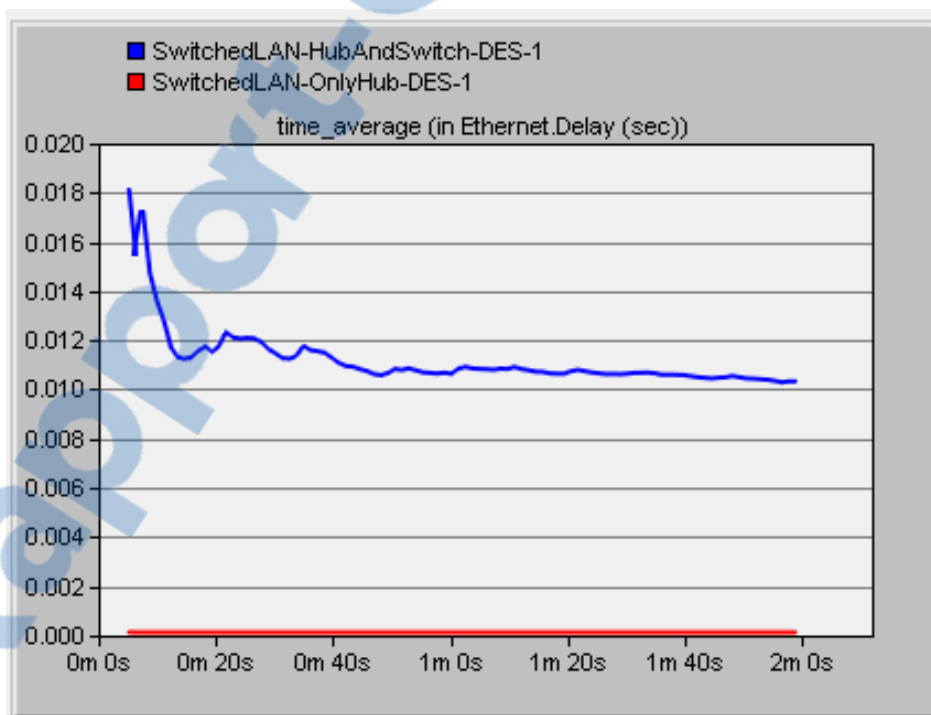


Figure IV.5 : Délai maximum à travers le réseau (delay) en sec.

Nous remarquons que le délai maximum pour le deuxième scénario est autour de 0.011 par rapport au premier scénario qui presque nul.

Le graphique résultant devrait ressembler à celui-ci-dessous le trafic envoyé dans les deux scénarios est presque identique.

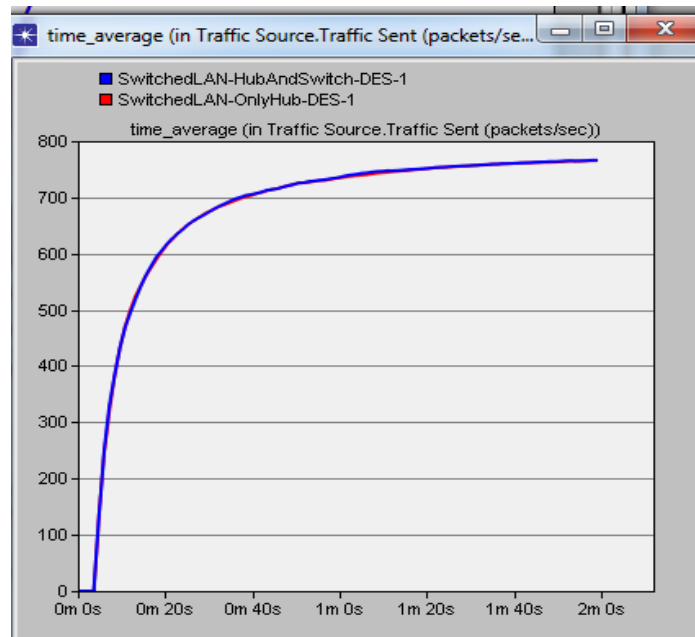


Figure IV.6 : Trafic envoyé

Comme vous voyez, le trafic reçu avec le deuxième scénario, HubAndSwitch, est plus haut que du celui scénario OnlyHub.

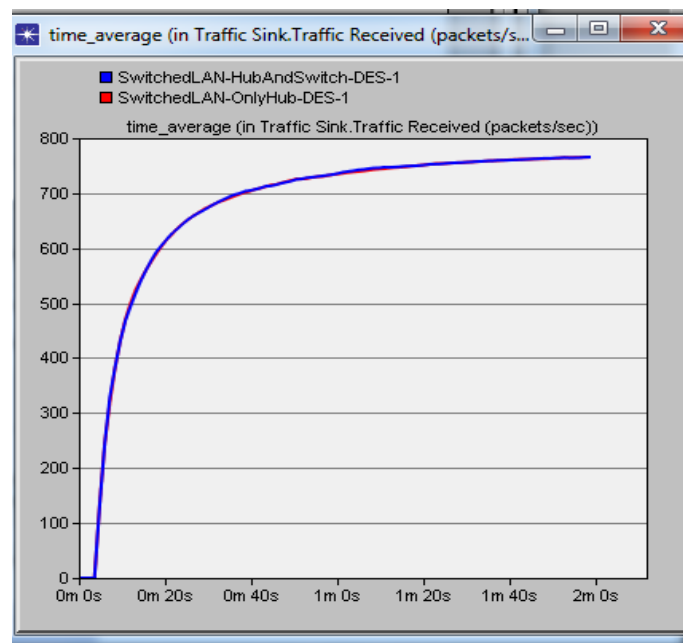


Figure IV.7 : Trafic reçu

IV.3. Réseau local avec un routage RIP

Le réseau proposé est composé de quatre Routeurs ou chacun est relié avec deux sous réseaux de type 100 base T.

Le tableau suivant montre les valeurs essentielles qu'on doit les écrire dans les zones de dialogue de *Startup Wizard*. [23]

Dialog Box Name	Value
Initial Topology	Select the default value : Create Empty Scenario.
Choose Network Scale	Select Campus . Select the Use metric units checkbox.
Specity Size	Select the Fault size: 10 km x 10 km
Review	Chek values, then click Finis

Tableau IV.2 : Valeurs indiquées dans le Startup Wizard

IV. 3.1. Eléments de réseau

Nous avons ajouté à l'espace du travail du projet les objets suivants (100 Base T LAN et Ethernet 4 – slip 8) de la palette pour créer un réseau. Nous allons reliez entre les routeurs avec PPP_DS3 et les routeurs et les réseaux avec 100BaseT.

Le réseau est maintenant établi comme représente la figure suivante.

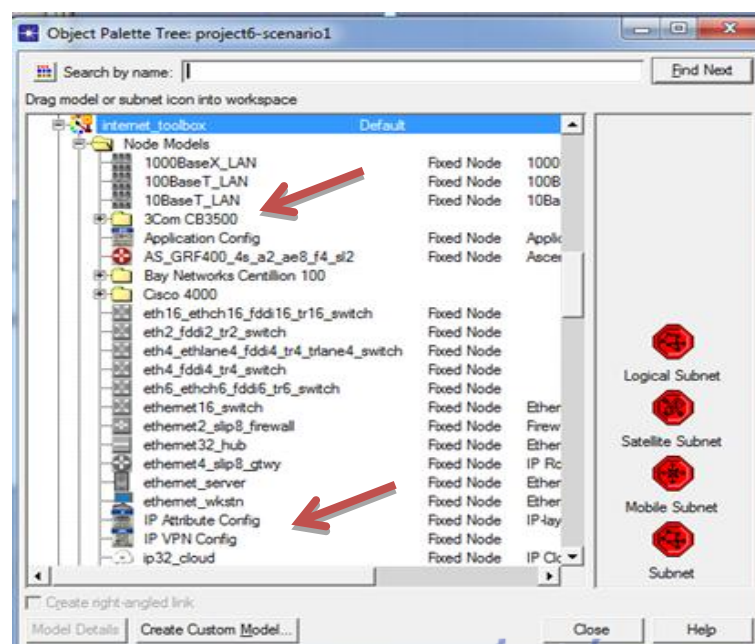


Figure IV.8 : Palette d'objet



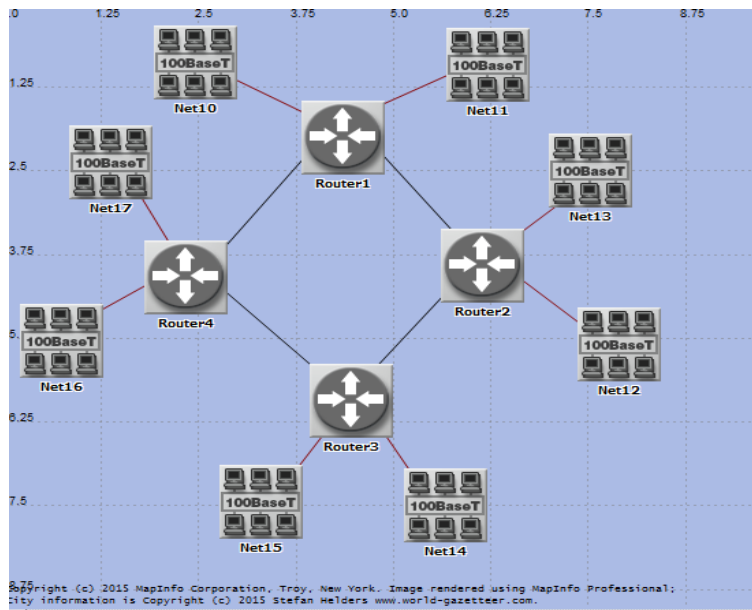


Figure IV.9 : Réseau NO_ Failure.

Nous avons besoin de configurer quelques paramètres de la simulation avec une durée de simulation 10 minutes selon la figure IV .10. Ces paramètres sont les suivants :

- IP interface Addressing Mode: Auto Addressed /Export.
- RIP Sim Efficiency: Disabeld

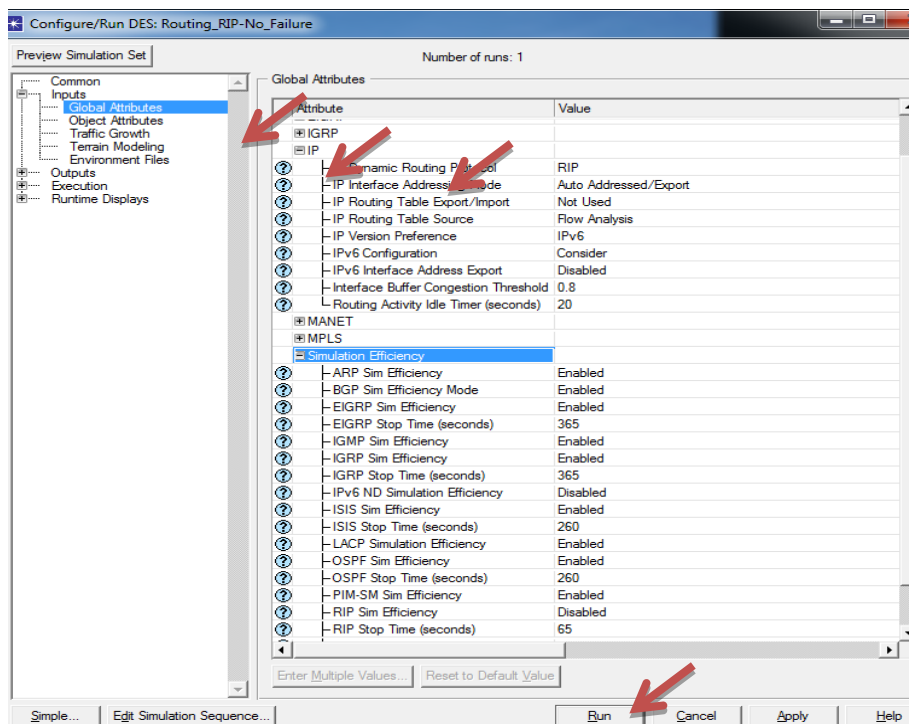


Figure IV.10 : Configuration des paramètres la Simulation

IV.3.2. Duplication du Scenario

L'objectif de ce projet est comparer le comportement des routeurs dans les deux scénarios. (NO – Failure et Failure). [23]

Pour configurer le deuxième scénario, On applique les étapes suivantes :

1. Choisi **Duplicate Scenario** du menu **Scenarios** et le nommer **Failure**.
2. Ouvrir la palette l'objet et Sélectionnez le palette **Utilities** en bas du menu.
3. Ajoute un **Failure Recovery** et proteste contre votre allure des travaux et le nommer **Failure**.

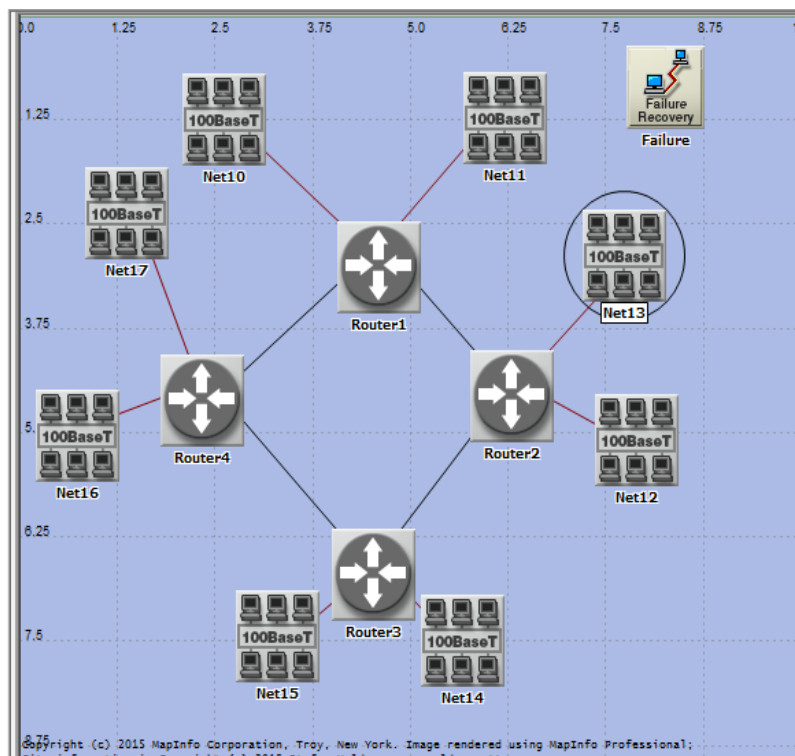


Figure IV. 11 : Réseau Failure

Pour configurer le **Failure** nous changeons quelques paramètres :

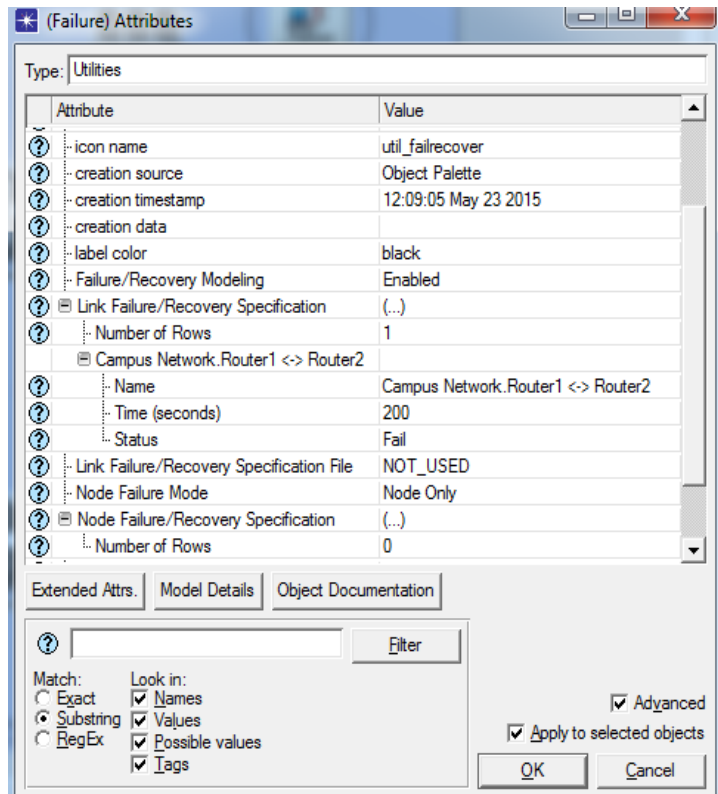


Figure IV. 12 : Configuration de Failure.

Les résultats de simulation des deux scénarios sont montrés dans les figures suivantes :

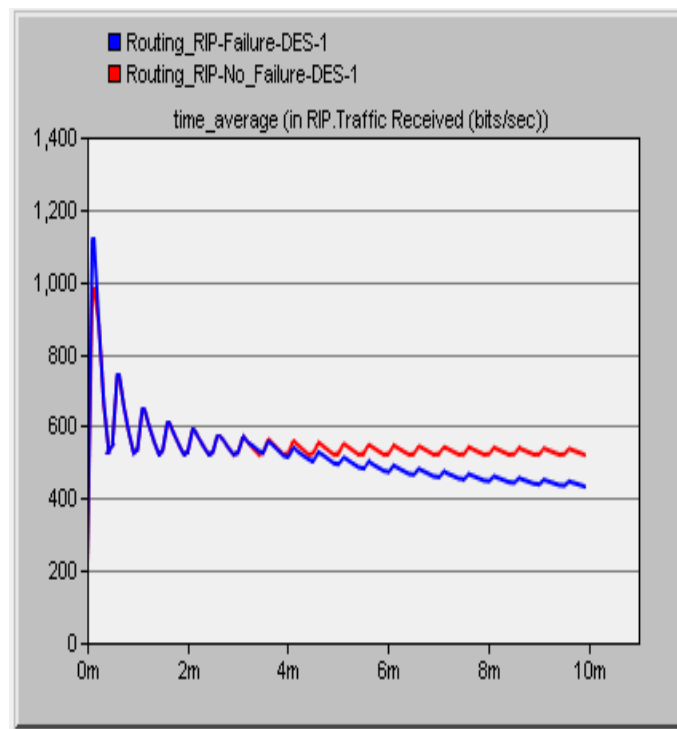


Figure IV. 13 : Trafic reçu

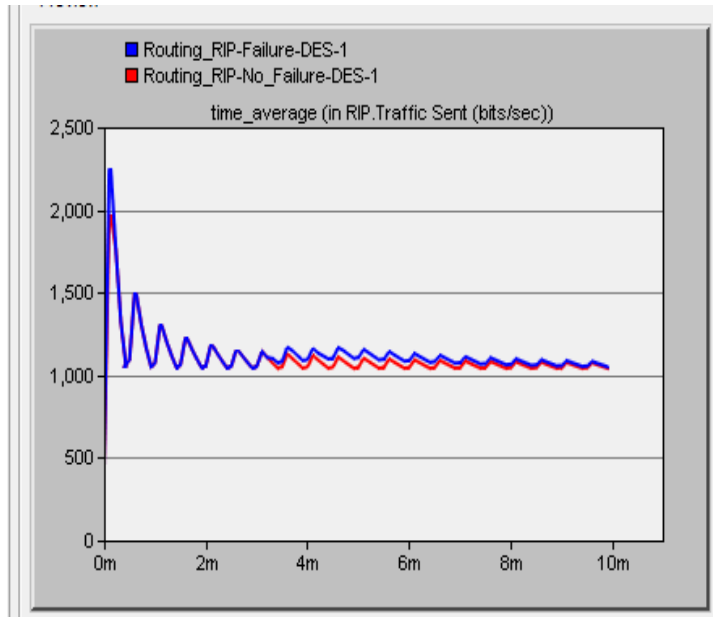


Figure IV. 14 : Trafic a envoyé(bit/sec)

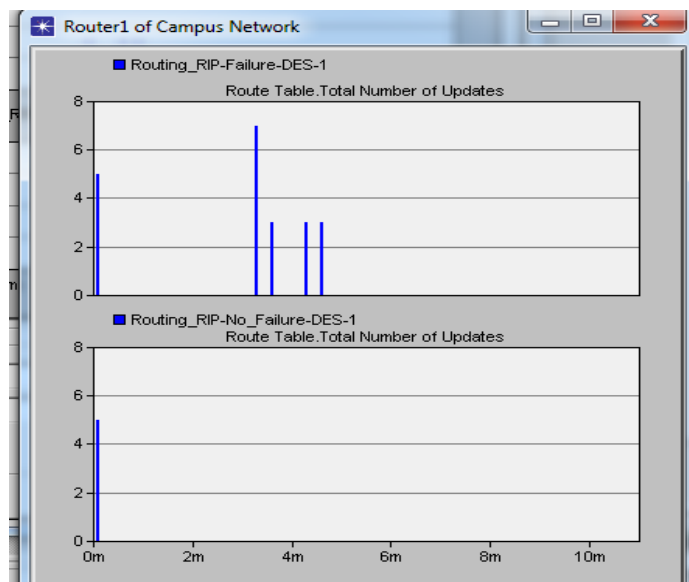


Figure IV. 15 : Nombre total de Mise à jour de Routeur1.

Le trafic a envoyé pour le premier scénario (NO – Failure) est un peu plus faible que le trafic a envoyé par le scénario dupliqué et c'est le contraire pour le trafic reçu. Nous remarquons aussi que le nombre total de mise à jour du routeur1, présenté dans le deuxième scénario est plus important que le scénario NO-Failure. Ceci revient à la complexité du deuxième scénario par rapport au premier

IV.3.3. Adresse IP du routeur 1

Dans la figure IV.14 et IV.15, on présente respectivement les adresses IP des interfaces du routeur 1 ainsi que sa table de routage.

```

Generic Data File: Routing_RIP-No_Failure-DES-1-ip_addresses
File Edit Options Windows Help

1 #
2 # Purpose:  Contains IP address information for all active
3 #           interfaces in the current network model.
4 #           (created by exporting this information from the model.)
5 #
6
7 # Node Name: Campus Network.Router1
8 # Iface Name      IP Address      Subnet Mask      Connected Link
9 # -----
10 IF0               192.0.0.1       255.255.255.0   Campus Network.Net11 <-> Router1
11 IF1               192.0.1.1       255.255.255.0   Campus Network.Net10 <-> Router1
12 IF10              192.0.2.1       255.255.255.0   Campus Network.Router1 <-> Router2
13 IF11              192.0.3.1       255.255.255.0   Campus Network.Router4 <-> Router1
14

```

Figure IV. 16: Addresses IP NO_Failure

Performance.IP Forwarding Table at End of Simulation for Campus Network.Router1

	Destination	Source Protocol	Route Preference	Metric	Next Hop Address	Next Hop Node	Outgoing Interface	Outgoing LSP	Insertion Time (secs)
1	192.0.0.0/24	Direct	0	0	192.0.0.1	Campus Network.Router1	IF0	N/A	0.000
2	192.0.1.0/24	Direct	0	0	192.0.1.1	Campus Network.Router1	IF1	N/A	0.000
3	192.0.2.0/24	Direct	0	0	192.0.2.1	Campus Network.Router1	IF10	N/A	0.000
4	192.0.3.0/24	Direct	0	0	192.0.3.1	Campus Network.Router1	IF11	N/A	0.000
5	192.0.4.0/24	RIP	120	1	192.0.2.2	Campus Network.Router2	IF10	N/A	5.850
6	192.0.5.0/24	RIP	120	1	192.0.2.2	Campus Network.Router2	IF10	N/A	5.850
7	192.0.6.0/24	RIP	120	1	192.0.2.2	Campus Network.Router2	IF10	N/A	5.850
8	192.0.7.0/24	RIP	120	2	192.0.3.2	Campus Network.Router4	IF11	N/A	9.361
9	192.0.8.0/24	RIP	120	2	192.0.3.2	Campus Network.Router4	IF11	N/A	9.361
10	192.0.9.0/24	RIP	120	1	192.0.3.2	Campus Network.Router4	IF11	N/A	9.361
11	192.0.10.0/24	RIP	120	1	192.0.3.2	Campus Network.Router4	IF11	N/A	9.361
12	192.0.11.0/24	RIP	120	1	192.0.3.2	Campus Network.Router4	IF11	N/A	9.361
13									
14	Gateway of last resort is	not set							
15									

Figure IV. 17: Table de routage du routeur 1

IV.4. Réseau RIP d'une topologie étoile

Nous avons basé sur le même réseau informatique de la figure III.1 ou nous volons le concevoir avec le logiciel OPNET Modeler. Pour réaliser ce réseau, nous avons procédé de la même manière que le réseau précédent. On utilise dans ce cas sept routeurs et six stations de types ethernet-wktns reliés par les câbles PPP-DS3 et 100 Base T.

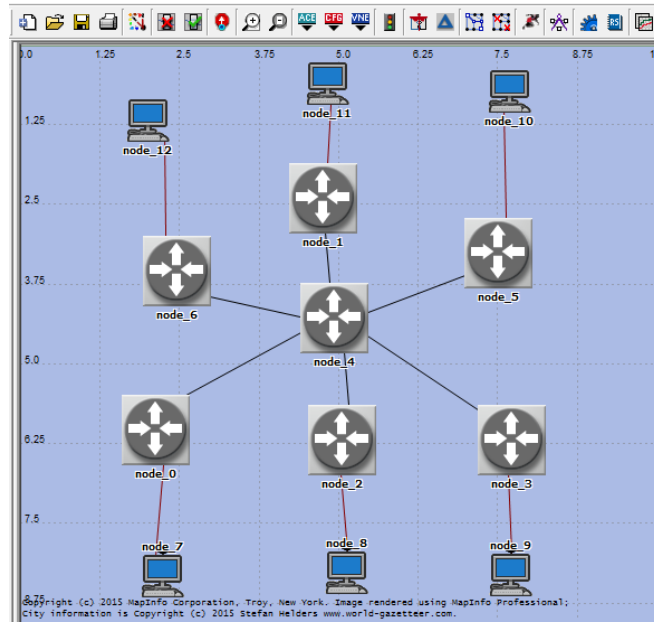


Figure IV.18 : Réseau initial (Routage).

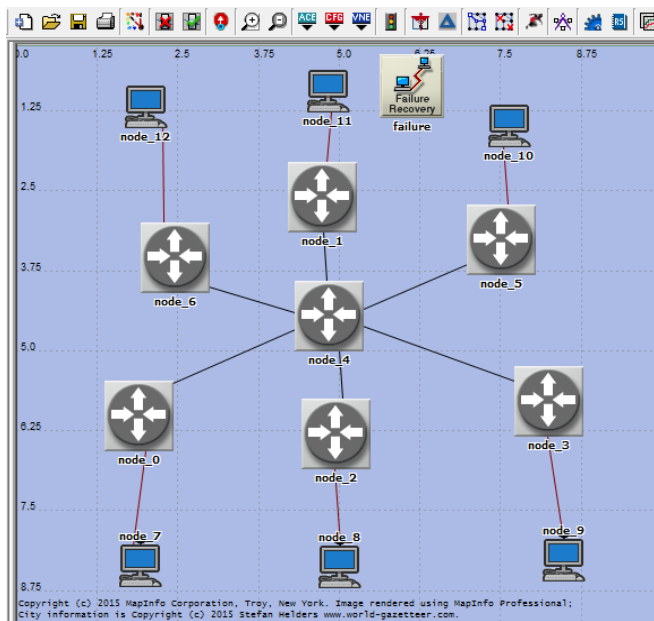


Figure IV.19 : Réseau dupliqué

Sur les figures IV. (20,21,22), On présente respectivement le trafic envoyé et reçu ainsi que le nombre total de mise à jour du routeur centrale (node – 4). La durée de simulation est de 10 minutes.

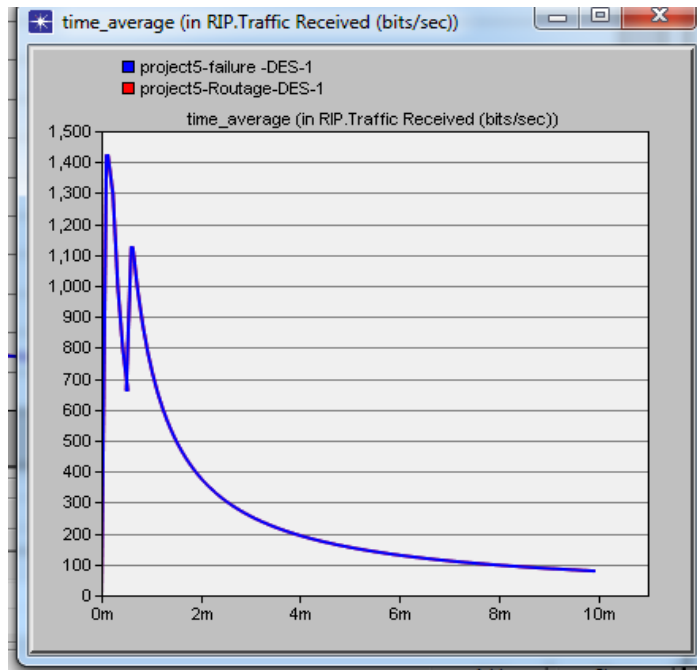


Figure IV.20: Trafic reçu (bits/sec).

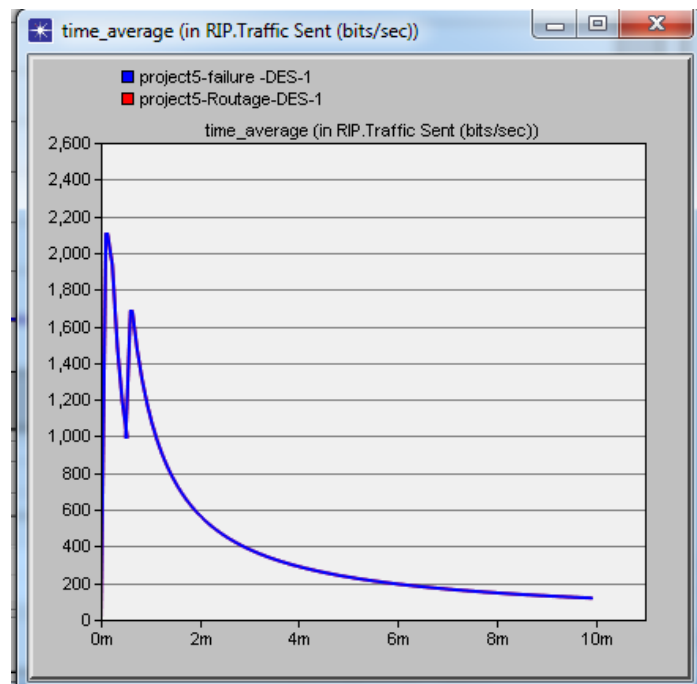


Figure IV.21 : Trafic a envoyé (bit/sec).

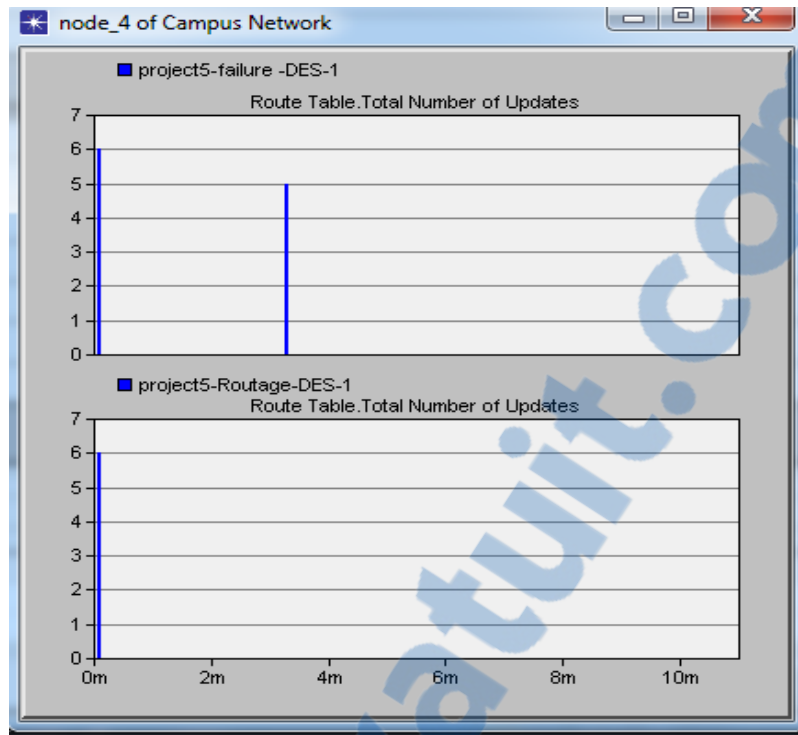


Figure IV. 22 : Nombre total de Mise à jour du routeur central

Les trafics envoyés et reçus sont bien identiques pour les deux scénario initial et dupliqué respectivement. Nous observons aussi que le trafic reçu est plus faible que le trafic envoyé selon les figures IV. (20,21)

Le nombre total de mise à jour du scénario final (Faiture) est plus important que le nombre total de mise à jour du scénario initial (Routage) du routeur central.

- **Adresses IP des routeurs**

```

7 # Node Name: Campus Network.node_0
8 # Iface Name      IP Address      Subnet Mask      Connected Link
9 # -----
10 IF0               192.0.0.1       255.255.255.0   Campus Network.node_0 <-> node_7
11 IF10              192.0.1.1       255.255.255.0   Campus Network.node_4 <-> node_0
12
13
14 # Node Name: Campus Network.node_1
15 # Iface Name      IP Address      Subnet Mask      Connected Link
16 # -----
17 IF0               192.0.2.1       255.255.255.0   Campus Network.node_1 <-> node_11
18 IF10              192.0.3.1       255.255.255.0   Campus Network.node_1 <-> node_4
19
20
21 # Node Name: Campus Network.node_2
22 # Iface Name      IP Address      Subnet Mask      Connected Link
23 # -----
24 IF0               192.0.4.1       255.255.255.0   Campus Network.node_2 <-> node_8
25 IF10              192.0.5.1       255.255.255.0   Campus Network.node_4 <-> node_2
26
27
28 # Node Name: Campus Network.node_3
29 # Iface Name      IP Address      Subnet Mask      Connected Link
30 # -----
31 IF0               192.0.6.1       255.255.255.0   Campus Network.node_3 <-> node_9
32 IF10              192.0.7.1       255.255.255.0   Campus Network.node_4 <-> node_3
33
34
35 # Node Name: Campus Network.node_4
36 # Iface Name      IP Address      Subnet Mask      Connected Link
37 # -----
38 IF4               192.0.7.2       255.255.255.0   Campus Network.node_4 <-> node_3
39 IF5               192.0.5.2       255.255.255.0   Campus Network.node_4 <-> node_2
40 IF6               192.0.1.2       255.255.255.0   Campus Network.node_4 <-> node_0
41 IF7               192.0.8.1       255.255.255.0   Campus Network.node_6 <-> node_4
42 IF10              192.0.3.2       255.255.255.0   Campus Network.node_1 <-> node_4
43 IF11              192.0.9.1       255.255.255.0   Campus Network.node_5 <-> node_4
44
45

```

Figure IV. 23 : Adresses IP des routeurs.

- **Table de routage du routeur central**

	Destination	Source Protocol	Route Preference	Metric	Next Hop Address	Next Hop Node	Outgoing Interface	Outgoing LSP	Insertion Time (secs)
1	192.0.0.0/24	RIP	120	1	192.0.1.1	Campus Network.node_0	IF6	N/A	6.971
2	192.0.1.0/24	Direct	0	0	192.0.1.2	Campus Network.node_4	IF6	N/A	0.000
3	192.0.4.0/24	RIP	120	1	192.0.5.1	Campus Network.node_2	IF5	N/A	6.975
4	192.0.5.0/24	Direct	0	0	192.0.5.2	Campus Network.node_4	IF5	N/A	0.000
5	192.0.6.0/24	RIP	120	1	192.0.7.1	Campus Network.node_3	IF4	N/A	6.923
6	192.0.7.0/24	Direct	0	0	192.0.7.2	Campus Network.node_4	IF4	N/A	0.000
7	192.0.8.0/24	Direct	0	0	192.0.8.1	Campus Network.node_4	IF7	N/A	0.000
8	192.0.9.0/24	Direct	0	0	192.0.9.1	Campus Network.node_4	IF11	N/A	0.000
9	192.0.10.0/24	RIP	120	1	192.0.9.2	Campus Network.node_5	IF11	N/A	9.295
10	192.0.11.0/24	RIP	120	1	192.0.8.2	Campus Network.node_6	IF7	N/A	9.148
11									
12	Gateway of last resort is not set								
13									

Figure IV. 24 : Table de routage du node - 4

IV.5. Modèle de réseau WLAN simple

Sous OPNET Modeler, nous avons configuré un réseau sans fil WLAN (dimensions de ce réseau : 100 m x 100 m), celui-ci est composé d'un poste de travail en liaison sans fil

avec un point d'accès. Ce dernier est connecté à un Switch ainsi qu'un serveur qui fournit des applications utilisées pour la station de travail. [24]

Les paramètres de WLAN (accès point, poste de travail) sont :

- Mode d'opération : 802,11g.
- Débit : 45Mbps.
- La puissance de transmission : 0.005W.

Maintenant que nous avons défini notre topologie, nous devons générer un trafic sur notre réseau. Il existe plusieurs manières proposées par OPNET Modeler pour représenter ce trafic : l'une consiste à importer le trafic et l'autre consiste à modéliser le trafic d'application en installant diverses applications.

Pour la seconde méthode, OPNET Modeler fournit les objets « globaux » afin de définir des profils et des applications. L'avantage d'employer un objet global est qu'un fois qu'il a été défini, il peut être réutilisé pour la topologie entière. Ces objets globaux sont des entités portatives qui sont indépendamment définis. Par conséquent, les objets globaux d'un projet peuvent être récupérés et réutilisés sur plusieurs scénarios. [24]

Nous devons alors définir deux nœuds pour les applications et les profils comme représente la figure IV.25.

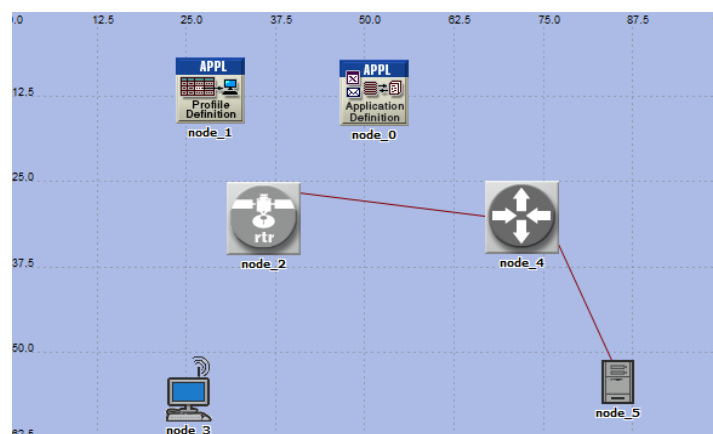


Figure IV.25 : Topologie d'un réseau WLAN.

Pour configuration un poste de travail, on doit définir leur comportement. Le comportement ou le « profil » d'un utilisateur peut être décrit par les applications employées.

IV.5.1. Application Configuration

Un profil est construit en utilisant différentes applications pour chaque définition d'application, on peut indiquer des paramètres d'utilisation tels que l'heure de départ, la durée et la répétitivité.

Le logiciel permet d'indiquer un profil d'utilisateur se composant de plusieurs applications (applications standards : FTP, http, Email...etc.) sont déjà prédéfinies à aide d'attributs représentés dans la figure ci-dessous.

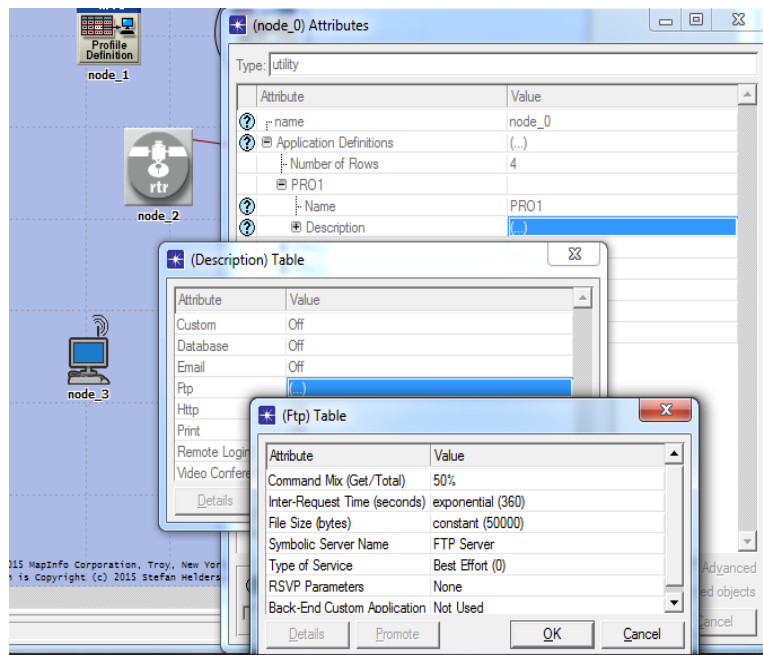


Figure IV.26 : Configuration d'une application.

Le scénario établi consiste à une application de transfert de fichier entre la station de travail équipée de carte WiFi et le server. A noter, pour déclarer de nouvelles applications, il suffit d'augmenter l'attribut « Row » encadré en bleu sur la figure ci-dessus.

La quatrième fenêtre nous permet de configurer les caractéristiques d'échanges entre le client et le serveur.

IV.5.2. Profil Configuration

Les profils décrivent les modèles d'activités d'un utilisateur, ou d'un groupe d'utilisateurs, en termes d'applications utilisées sur une période de temps définie. Les profils peuvent

s'exécuter à plusieurs reprises sur le même nœud, OPNET Modeler nous permet de configurer des répétitions de profil pour être simulé simultanément ou en série (l'une après l'autre). Les profils contiennent une liste d'applications que l'on peut configurer de la façon suivante. [24]

Simultaneous ;

Serial ordered : successivement, dans un ordre défini ;

Serial random : successivement, dans un ordre aléatoire ;

L'objet de définition du profil définit l'ensemble des profils qui peuvent être employés dans un scénario. Seuls des profils qui ont dans cet objet peuvent être appliqués aux stations. Ceci est valable également pour les applications qui ont été définies dans l'objet de définition d'application.

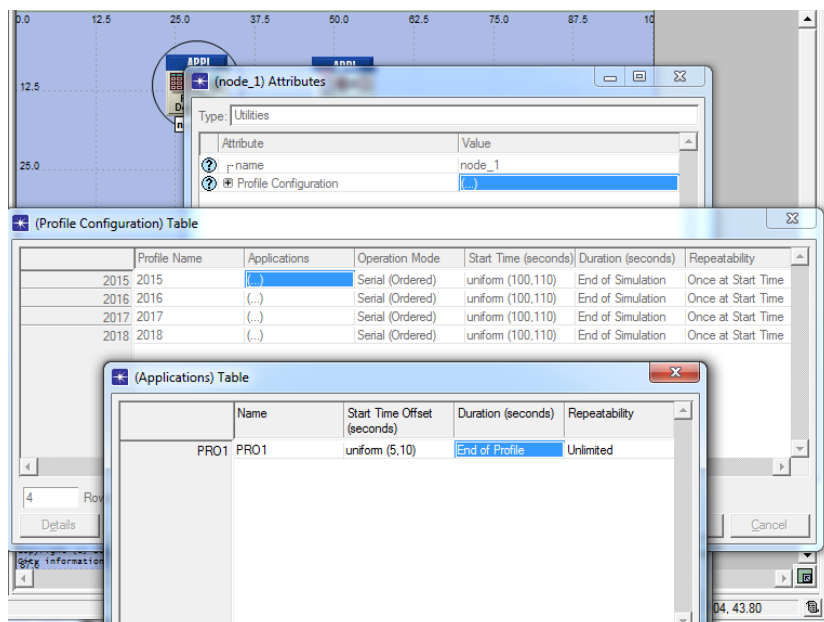


Figure IV.27 : Configuration d'un profil.

Les différentes fenêtres représentent le type de profil que l'on attribue à nos stations. Toujours dans un souci de simplicité, nous avons créé un seul type de profil, 2015. Ce profil sera supporté par la station de travail et leur permettra de générer le FTP.

Une fois que l'on a configuré les applications et les profils, nous devons les déployer sur les postes de travail et le serveur.

IV.5.3. Client configuration

Le profil établi, 2015, doit être indiqué sur la station de travail. Celui-ci permet à la station de supporter l'application FTP, et donc de créer des sources de trafic. La figure ci-dessous représente le monde opératoire pour indiquer le profil aux stations. Cependant, étant donné que la station est équipée d'une carte Wifi, nous devons régler également certains paramètres WLAN. [24]

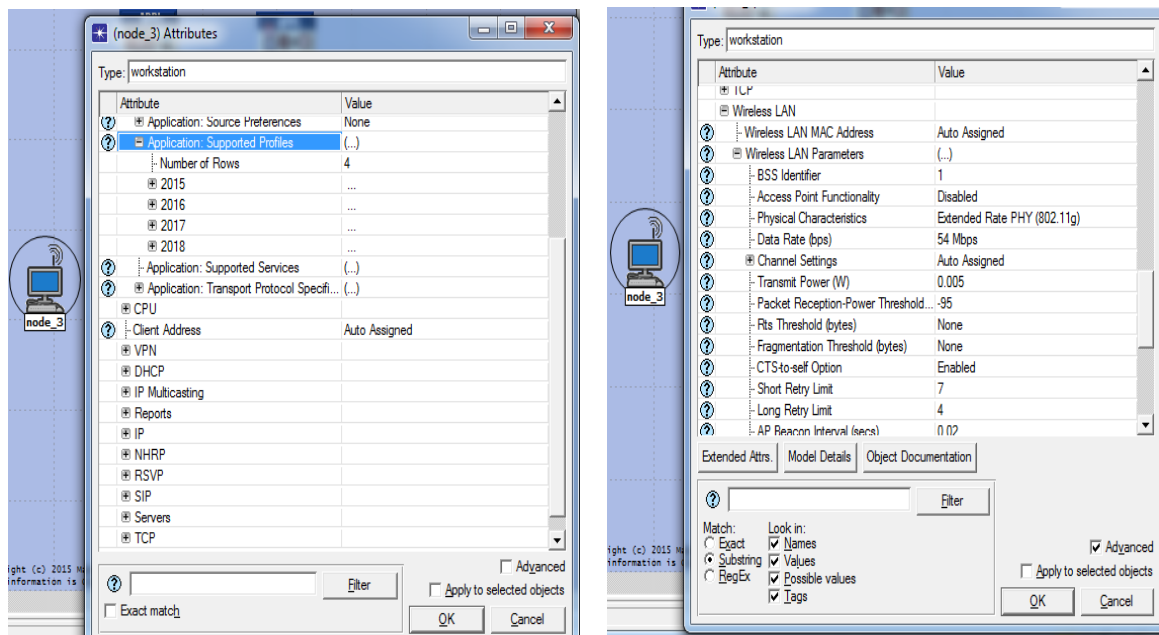


Figure IV.28 : Configuration d'un client.

IV.5.4 Server configuration

Une fois que le profil est installé sur les postes de travail, On doit configurer le serveur pour qu'il puisse supporter l'application souhaitée.

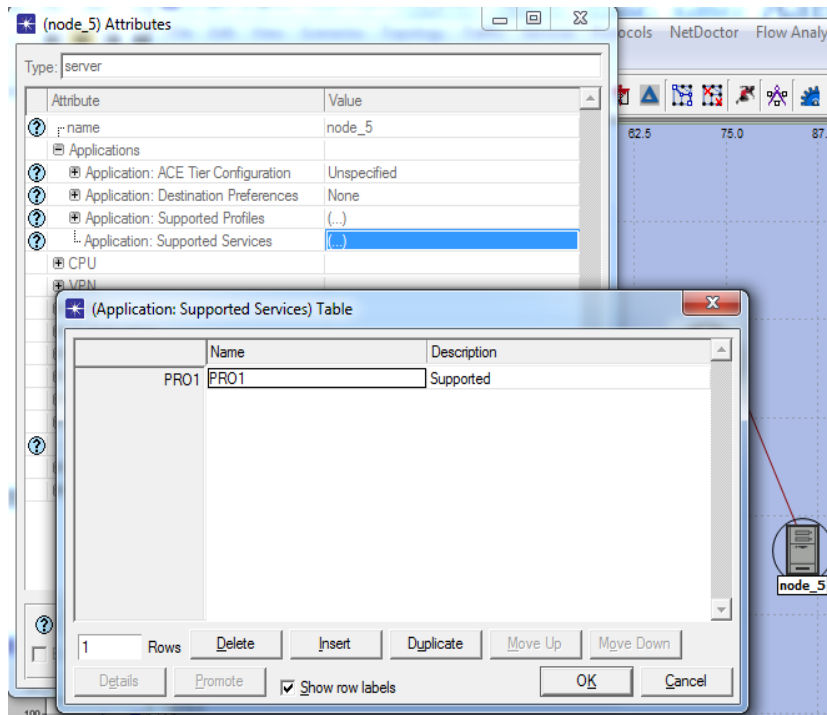


Figure IV.29 : configuration d'un serveur.

Dans notre cas (figure IV.29), les configurations d'applications sont les suivantes :
Email, FTP, Web Browsing, Print (le tout avec load).

La durée de la simulation :3.5 heures

Les résultats de simulation sont indiqués par la figure IV.22.

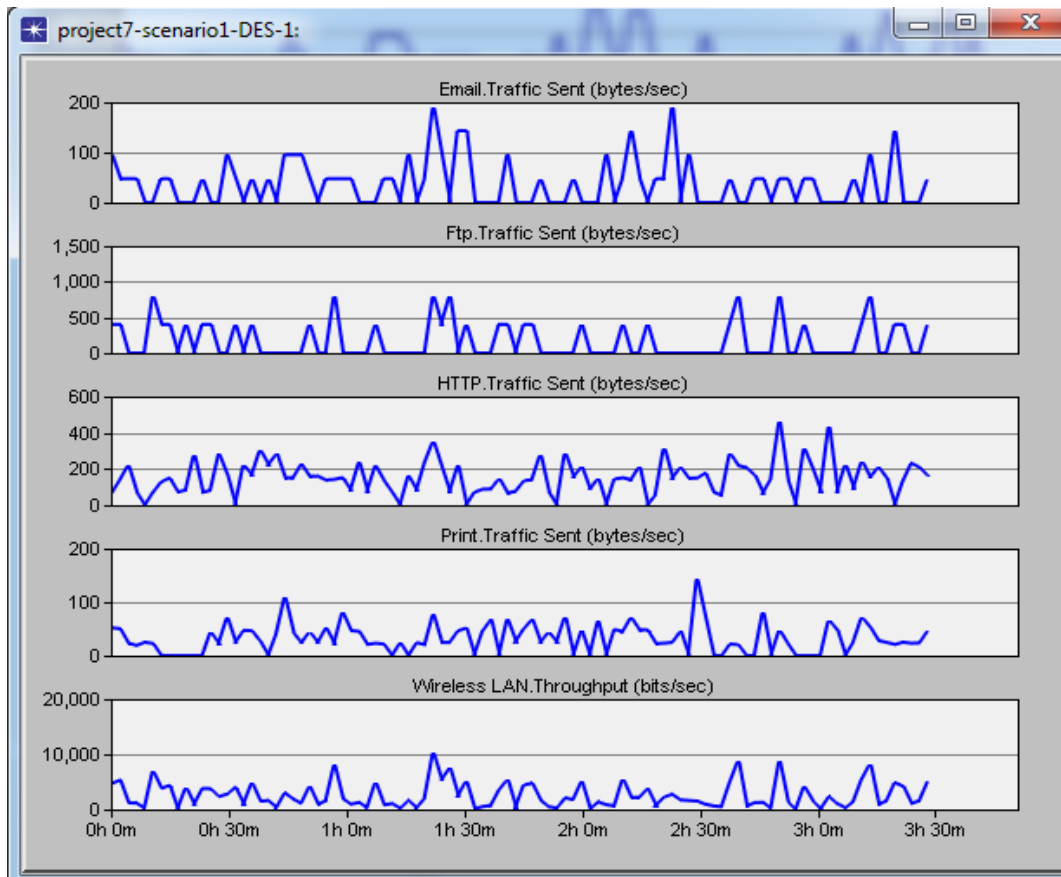


Figure IV.30 : Débit pour chaque application.

A partir des graphes ci-dessous, nous pouvons lire la valeur de débit pour chaque application. Par exemple pour l'Email, le débit est autour de 100bytes/sec et pour transfert de fichier est dans l'ordre de 500 bytes/sec, ect. Pour le dernier graphe, le débit du réseau entier est de 6 Kbps qui reste négligeable par rapport au débit de la norme 802.11g qui est choisie comme un mode d'opération. Ceci revient à la simplicité de la topologie proposée.

IV.6. Conclusion

Dans le but de trouver un autre outil fiable pour modéliser des réseaux locaux informatique et donc l'évaluation de ses performances, Ce chapitre exploite l'outil OPNET Modeler pour concevoir quelques réseaux locaux filaires et sans fil. Plusieurs réseaux informatiques topologie étoile ont été proposés, La convergence des résultats à la réalité a confirmé la bonne modélisation de ces derniers par cet outil. Les résultats de simulation sont alors présentés et discutés.

1. Introduction

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc. . . .

2. Présentation du logiciel

2.1. Présentation de l'écran principal

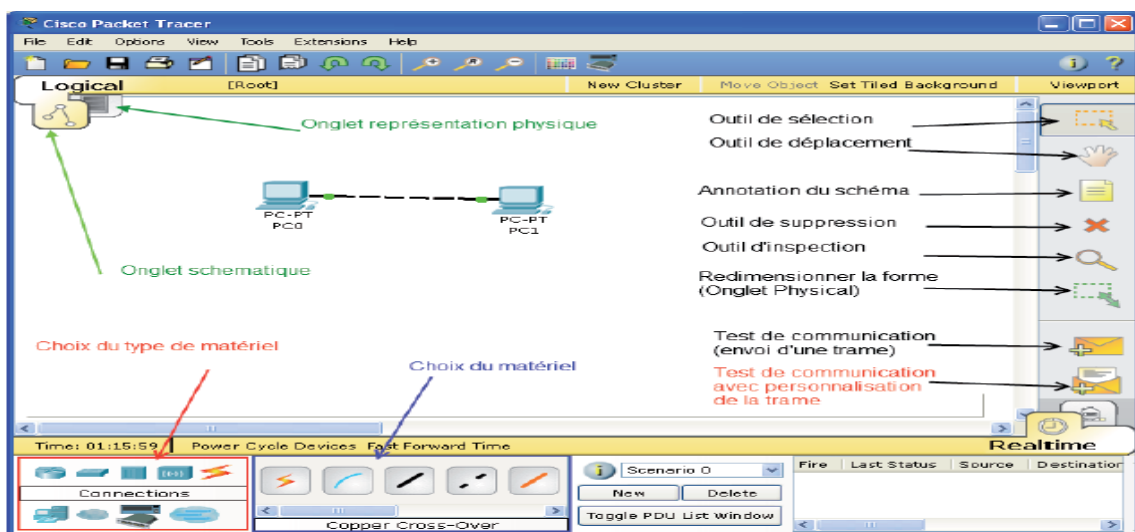


Figure 1 : Interface de logiciel Cisco Packet tracer

- Il dispose d'une barre de menu classique
- D'une barre d'outils principale comportant les fonctionnalités de base de gestion de fichier, d'impression, etc....
- D'une barre d'outils à droite comportant les outils minimaux nécessaires
- Ainsi que trois boîtes à outils :
 - ✓ Choix du type de matériel (ordinateur, routeurs, etc...)
 - ✓ Choix du matériel en fonction du type
 - ✓ Résultats de l'échange de données

2.2. Spécification des équipements disponibles

Les différents types d'appareils disponibles dans la boîte à outils de la zone 2 sont les suivants :

1. Les routeurs.

2. Les commutateurs (Switches).
3. Les concentrateurs (hubs).
4. Les bornes sans fils (wifi).
5. Les connexions.
6. Les ordinateurs.
7. Les réseaux étendus (Wan).
8. Des appareils divers.
9. Les connexions multi usagers.

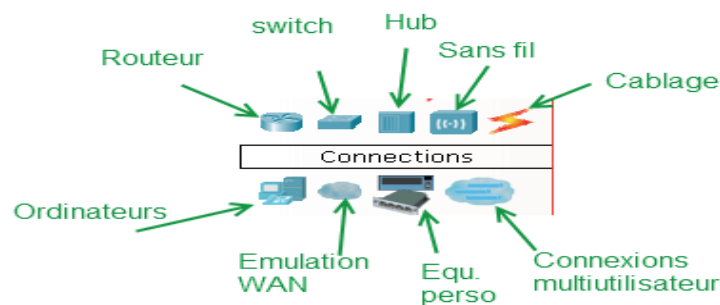


Figure 2: Types d'équipements. [25]


Chaque équipement possède une vue physique comprenant des modules à ajouter, une vue configuration pour configurer les principales options via une interface graphique et une vue permettant la configuration CLI.[25]


2.3. Spécification des connexions possibles


Packet Tracer propose les principales connexions possibles entre les différents équipements réseaux.





Figure 3: Les différentes connexions proposées. [25]


 Câble Console (connexion PC-Switch) : les connexions console peuvent être établies entre PCs et routeurs ou commutateurs. Elles servent principalement à configurer les équipements.


 Câble droit : standard Ethernet pour connecter les équipements opérant dans les différentes couches du modèle OSI. Packet Tracer supporte le 10, 100 et 1000 Mbps.

 Câble croisé : standard Ethernet pour connecter les équipements opérant dans les mêmes couches du modèle OSI. Packet Tracer supporte le 10, 100 et 1000 Mbps.

 Fibre optique : les connexions fibres peuvent être établies si les équipements possèdent les ports fibre adéquates. Packet Tracer supporte le 100 et 1000 Mbps.

 Ligne téléphonique : Les connexions téléphoniques ne sont disponibles qu'entre les équipements possédant des ports modem. Ces connexions se font généralement à travers un nuage réseau.

 Câble Coaxial : Même chose que pour la ligne téléphonique, sauf que les ports utilisés sont des ports coaxiales.

 Câbles DCE et DTE : les connexions sériales se font entre 2 ports séries. Elles sont souvent utilisées pour simuler des liens WAN. Le clocking doit être activé sur le câble DCE pour activer la connexion. En fonction du premier câble sélectionné (DTE ou DCE) le deuxième sera forcément de l'autre type afin d'assurer la connexion.

Il existe aussi la possibilité de connecter les équipements en wifi pour ceux possédant les modules wifi compatibles. Un module wifi correspond à une connexion wifi. C'est-à-dire qu'un équipement possédant un module de type A ne pourra se connecter qu'au point d'accès qui possédera ce même type de module. [25]

2.4. Les commandes et outils CISCO

2.4.1. Interface graphique sur un poste client (ordinateur basique)

2.4.1.1 L'onglet « physical »

Cet onglet permet de rajouter des modules, c'est-à-dire des cartes matériels afin d'ajouter des ports Ethernet, une carte wifi etc.

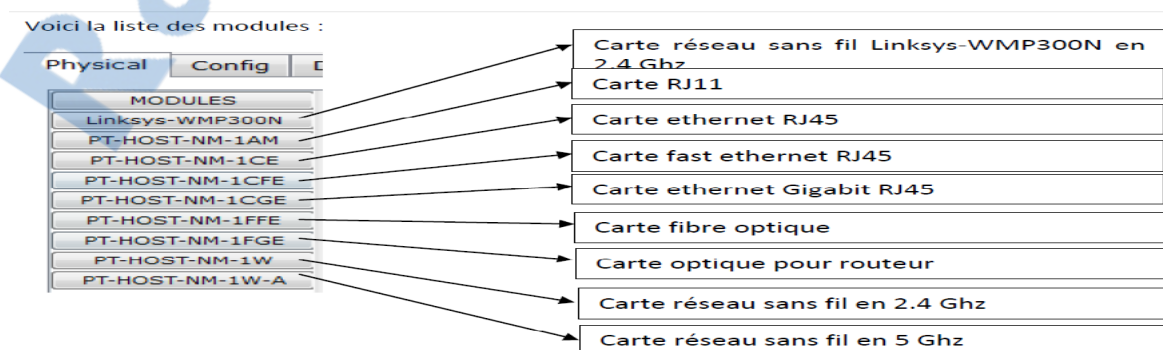


Figure 4 : Onglet physical. [25]

2.4.1.2. L'onglet « Config »

Cet onglet permet de configurer essentiellement les paramètres réseau de l'ordinateur.

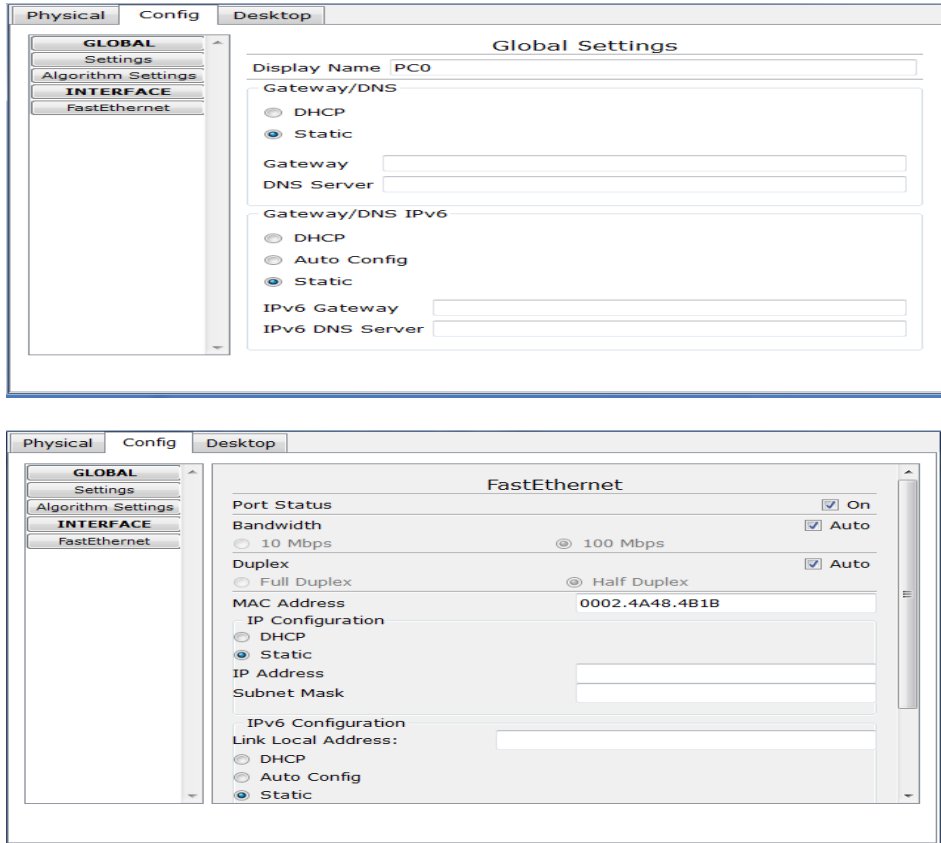


Figure 5 : Onglet config. [26]

2.4.1.3 L'onglet « Desktop »

L'onglet Desktop met à la disposition de l'utilisateur les outils logiciels habituels des équipements.

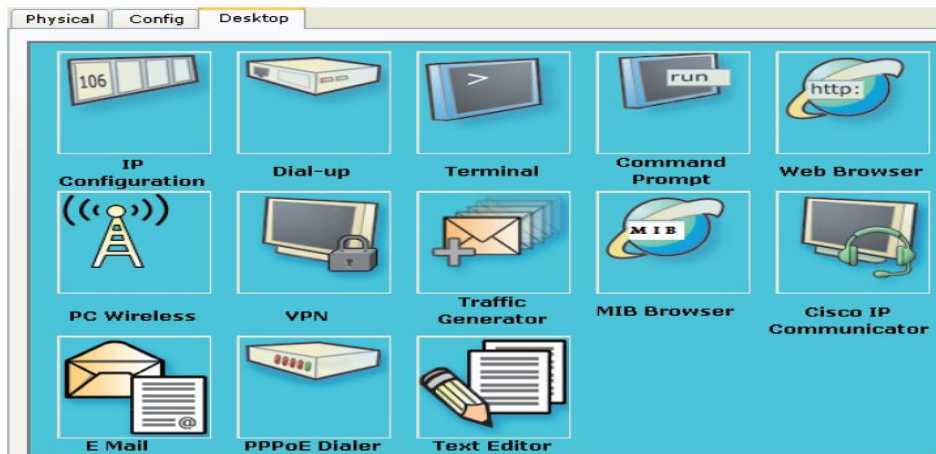


Figure 6 : Onglet Desktop. [26]

- **IP configuration** permet de configurer les paramètres réseau de la machine
- **Dial-Up** permet de configurer un modem s'il est présent dans l'équipement
- **Terminal** permet d'accéder à une fenêtre de programmation (HyperTerminal)
- **Command prompt** est la fenêtre DOS classique permettant de lancer des commandes en ligne de commande (PING, IPCONFIG, ARP, etc...)
- **WEB Browser** : il s'agit d'un navigateur Internet
- **PC Wireless** : permet de configurer une carte WIFI si elle est présente dans l'équipement
- **VPN** : permet de configurer un canal VPN sécurisé au sein du réseau.
- **Traffic generator** : permet pour la simulation et l'équipement considéré de paramétrer des trames de communications particulières (exemple : requête FTP vers une machine spécifiée).
- **MIB Browser** : permet par l'analyse des fichiers MIB d'analyser les performances du réseau.
- **CISCO IP Communicator** : permet de simuler l'application logicielle de téléphonie développée par CISCO.
- **Email** : client de messagerie.
- **PPPoE Dialer** : pour une liaison Point à Point (Point to Point Protocol).
- **Text Editor** : éditeur de texte.

2.5 Serveur

2.5.1. Interface « Physical »

Les modules sont les mêmes que pour un poste client.

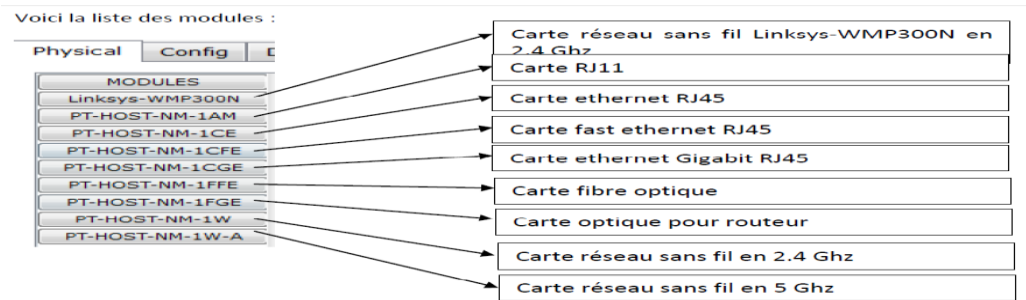


Figure 7 : Interface Physical. [26]

2.6. Simulation

Packet Tracer permet de simuler le fonctionnement d'un réseau par l'échange de trames Ethernet et la visualisation de celles-ci.

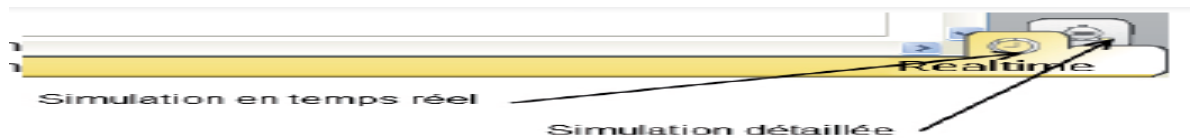


Figure 8 : Présentation des modes de simulation

Il existe deux modes de simulation :

- la simulation en temps réel (**REALTIME**): elle visionne immédiatement tous les séquences qui se produisent en temps réel.
- la simulation permet de visualiser les séquences au ralenti entre deux ou plusieurs équipements.

2.6.1 Simulation en temps réel

Réalisation d'un PING

Un ping fait appel au protocole ICMP avec le message n°8. Packet Tracer permet de faire un ping rapidement avec l'outil **Add Simple PDU**.



- Sélectionner l'outil
- Cliquer sur l'ordinateur émetteur du PING
- Cliquer ensuite sur l'ordinateur Destinataire du PING
- La fenêtre d'état informera de la réussite (Successfull) ou de l'échec (Failed) de la transaction

2.6.2. Simulation en ligne de commande

Comme sur un vrai ordinateur, il est possible par ligne de commande de saisir des commandes réseau (IPCONFIG, PING, ARP...). [26]

- Ouvrir la fenêtre de configuration de l'ordinateur en cliquant sur sa représentation.
- Choisir l'onglet Desktop.
- Sélectionner l'outil *Command Prompt*.
- Saisir la commande souhaitée.
- Valider par la touche ENTREE.

1. INTRODUCTION

Ce chapitre explique le fonctionnement général du logiciel OPNET en présentant chaque éditeur utilisé. Puis dans un deuxième temps, les procédures suivies pour améliorer cette version d'OPNET sont décrites à savoir l'intégration d'un diagramme de rayonnement complexe et le couplage avec un logiciel de propagation développé au sein du laboratoire.

Puis pour terminer, nous traitons un exemple des systèmes de communication afin de démontrer l'utilité d'un tel outil

2. PRESENTATION GENERALE

OPNET est un environnement graphique créé pour permettre de concevoir, étudier des réseaux numériques, et des protocoles de communication avec une grande flexibilité.

Il travaille sur toutes les couches du modèle OSI et permet de récupérer une grande quantité d'informations tant que l'on reste au niveau de granularité égale au paquet. Il permet également de simuler un bon nombre de matériels existant comme les routeurs, les serveurs d'application etc... Grâce à cela, toutes les configurations de réseaux deviennent très faciles à modéliser et simuler.

3. Modélisation orientée objet

Son approche est orientée objet pour le développement et dispose d'une interface graphique simple dans laquelle on place les différents composants du réseau à étudier. OPNET supporte tous les types et toutes les technologies de réseaux.

3.1 Objet réseau

Rappelons tout d'abord qu'un réseau est un ensemble complexe constitué de matériels, logiciels et supports de transmissions, c'est à dire un ensemble de nœuds et de liens, interconnectés entre eux pour communiquer.

OPNET dispose de deux types de nœuds - fixes (serveurs, stations de travail, routeurs...) ou mobiles (téléphones portables, satellites...) - et de trois types de liens - point à point, bus ou radio.

3.2. Objet nœud

Un nœud est formé d'un ensemble de blocs fonctionnels appelés modules de processus qui peuvent être des processeurs, des files d'attente, des générateurs, des émetteurs, des

récepteurs ou bien des antennes. Ils sont liés entre eux par des connexions de type flux de paquets (pour le transport des données) ou de type fil statistique (pour la transmission de valeurs).

Les éléments précédents sont assemblés grâce à l'éditeur de nœuds (figure 1) appelé « Node Editor » afin de créer des éléments de réseau comme un routeur, un ordinateur, etc.

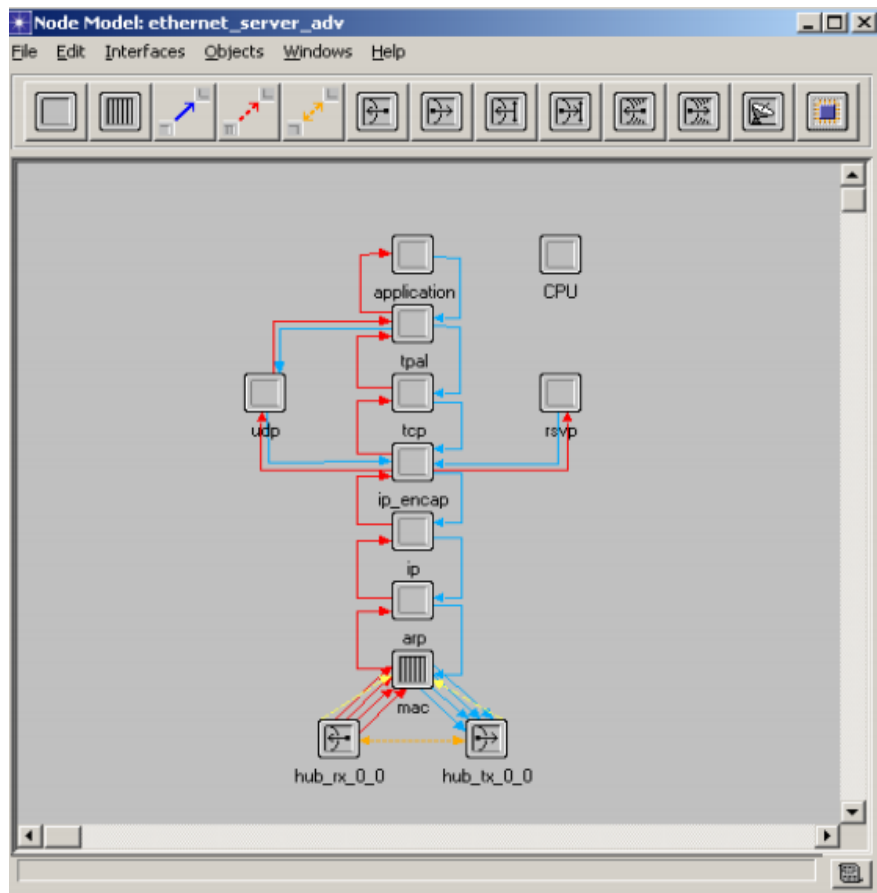


Figure 1: Exemple de nœud construit avec l'éditeur de nœuds

La figure 25 montre un exemple de nœud à savoir un serveur Ethernet avec toutes les couches utilisées par celui-ci (Application, TCP, IP, etc...).

Objet processus

Un processus définit le comportement d'un module appartenant à un nœud. Construit à partir de l'éditeur de processus (Process Editor), il est décrit par un diagramme de transitions et d'états. Chacun de ces états est programmé en langage C ou C++.

La figure 2 illustre un diagramme d'état à l'intérieur d'un processus.

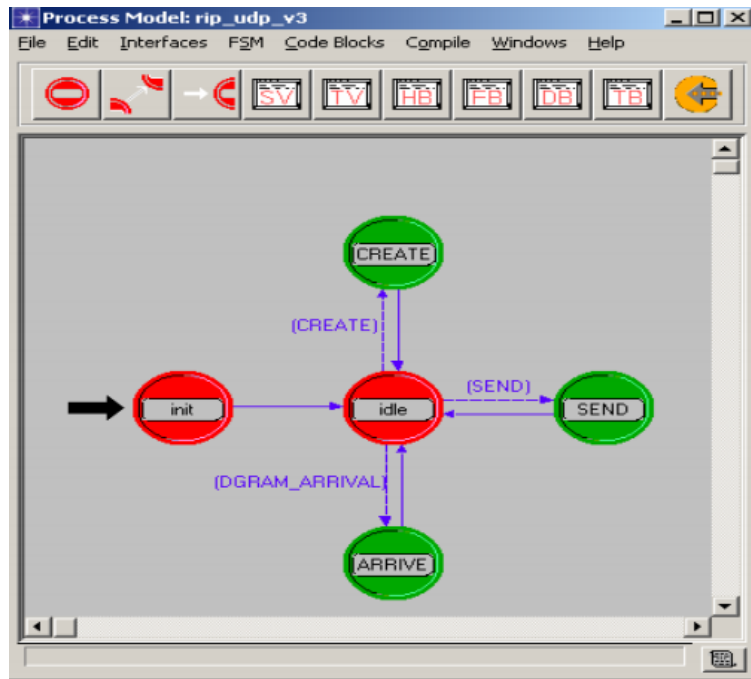


Figure 2: Editeur de processus avec le diagramme d'état

Les états d'un modèle de processus sont de l'un des trois types suivants :

- état initial : état dans lequel se trouve un processus en début de simulation,
- état forcé (vert) : état dans lequel un processus ne peut pas interrompre son activité durant la simulation c'est-à-dire qu'il exécute en une seule fois toutes ses lignes de code,
- état non forcé (rouge) : état dans lequel un processus exécute une première partie de son code C, s'interrompt pour passer le relais au noyau de simulation ou à un autre module puis redevient actif lorsqu'il reprend la main.

Chaque état comporte deux blocs d'exécution : celui d'entrée (Enter Excès) qui s'exécute lorsque le processus entre dans cet état et celui de sortie qui se déroule avant que le processus ne le quitte. Les différents états sont reliés entre eux par des transitions qui décrivent la possibilité pour un processus de passer d'un état à un autre. Elles sont évaluées après l'exécution du code de sortie d'un état, en vue de ne sélectionner que celle dont la condition est vraie. [27]

Une fois le processus construit, il est alors nécessaire de le compiler afin de le rendre exécutable et utilisable dans un modèle de nœud. La simulation de ce dernier est ensuite gérée par un outil appelé noyau de simulation (Simulation Kernel) qui coordonne les différents processus mis en jeu. A chaque exécution du code d'un état, il y a programmation dans une

liste, connue sous le nom d'échéancier, d'un ou de plusieurs événements appelés interruptions. Le noyau de simulation, qui gère cet échéancier, passe donc le contrôle de la simulation à un module donné, en lui envoyant l'interruption qui arrive à la tête de cette liste.

L'événement suivant prend alors la place de l'interruption précédente.

Résumé et principe de développement d'un projet

Lorsque l'on crée un nouveau projet, il faut dans un premier temps définir les nœuds qui vont intervenir dans le réseau (ordinateurs, routeur, etc...). Chacun de ces nœuds, comme vu précédemment, va être composé de différents modules (files d'attente, générateur de paquets, etc...) qui eux même sont composés d'un processus réalisé avec un diagramme d'état. Ce diagramme d'état doit définir quel état prend le processus (donc le module) en fonction de l'évènement (arrivée d'un paquet par exemple) généré par le noyau de simulation.

Afin de clarifier ce principe, nous allons examiner en détail une simple communication entre deux machines à savoir la création et la transmission d'un seul paquet entre la machine numéro 0 et le numéro 1.

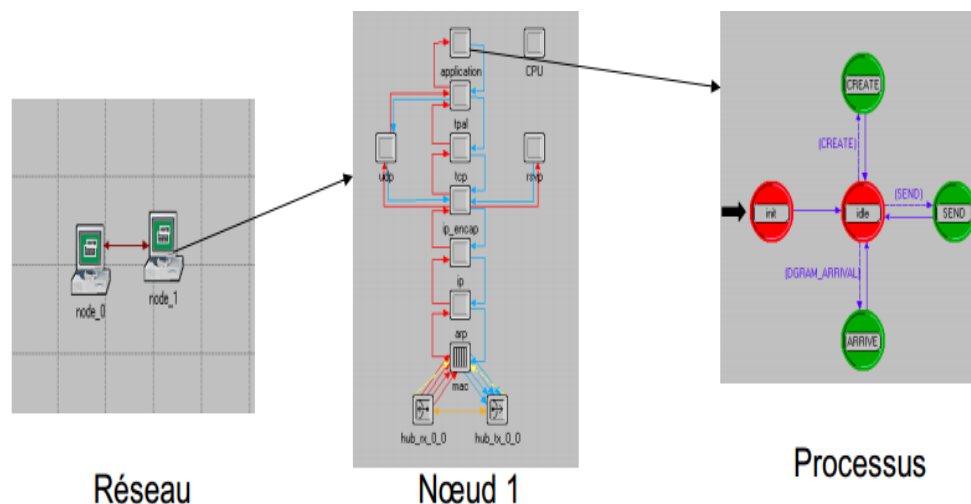


Figure 3 : Analyse d'une simulation simple.

Tout d'abord, il faut créer le paquet dans la machine numéro 0 à savoir le nœud 0 au début de la simulation. Le paquet est donc créé dans le processus nommé ici application appartenant au nœud 0 au début de la simulation (figure 3).

Ce paquet est ensuite transmis au module suivant par l'intermédiaire d'une connexion de type flux de paquets afin de subir certains traitements que nous ne détaillerons pas ici (figure 3).

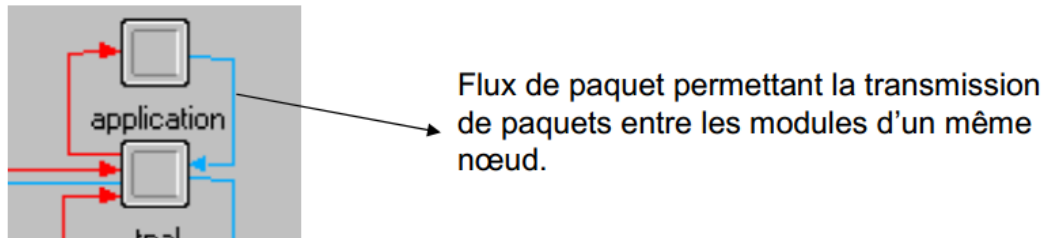


Figure 4 : Transmission du paquet entre les modules

Il finira par arriver aux modules de transmission qui le feront parvenir au nœud numéro 1 (machine 1).

A ce moment-là, le noyau de simulation va créer un événement dans les processus de réception du nœud numéro 1. Ces processus vont ensuite se placer dans l'état prévu lorsque ils reçoivent un paquet et le traiter comme le développeur l'a programmé (le détruire, le transmettre à un autre nœud, etc...).

On a montré ici que le logiciel permet une modélisation très fine des différents éléments d'un réseau. Le développeur peut donc modéliser le comportement de différentes machines d'un réseau quelconque et analyser le fonctionnement de ce dernier.

3.3. Objet Paquet

Comme nous l'avons vu brièvement ci-dessus, l'unité d'échange de données dans les simulations OPNET est le paquet. Ce dernier, structuré en plusieurs champs, permet de transmettre des informations entre les divers objets d'un modèle. Il est créé puis détruit au cours d'une simulation.

Son format est défini grâce à l'éditeur OPNET appelé Packet Format Editor (figure 5).

Chaque champ est représenté par des boîtes rectangulaires proportionnelles à la taille (en bits, en octets...) que l'utilisateur spécifie.[27]

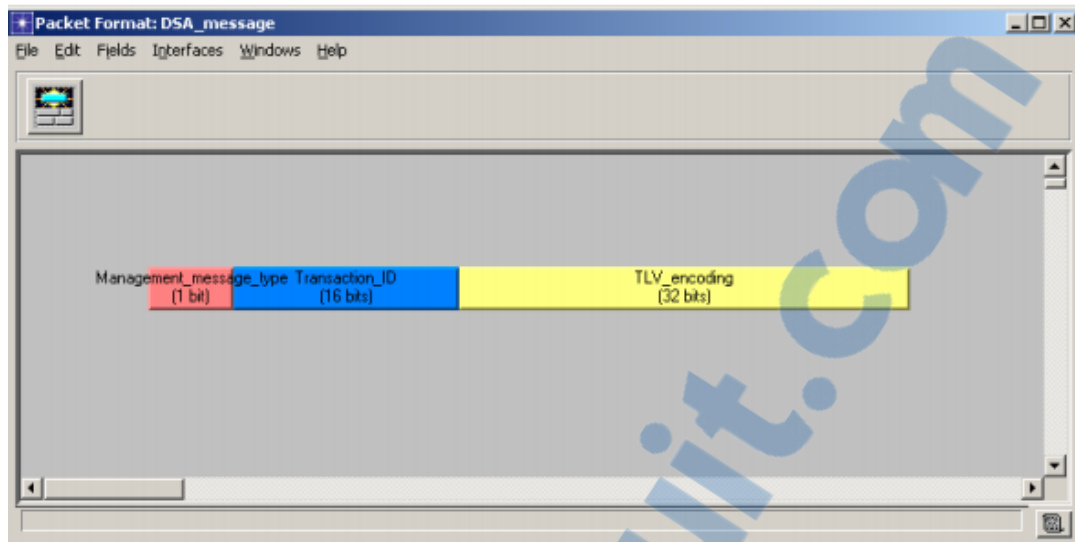


Figure 5 : Exemple de format de paquet construit avec l'éditeur OPNET

Par exemple, la figure 29 montre un paquet utilisé pour transmettre les informations de management avec ses différents champs.

3.4. Fonctions KERNEL (KP)

Afin de faciliter la tâche du développeur, OPNET fournit un certain nombre de fonctions appelées procédures KERNEL (KP). Ces fonctions, écrites en langage, permettent de réaliser des opérations fréquentes, complexes ou fastidieuses. Ainsi, existent par exemple des fonctions de gestion de la mémoire, de traitement de paquets ou de résultats.

Elles peuvent être appelées par le code source C de certains modules (comme les processus) mais aussi par d'autres fichiers C (comme les Transceiver Pipelines). Par exemple, pour transmettre un paquet comme vu précédemment, on utilise la KP « op_pk_send (paquet)».

4. Editeurs OPNET supplémentaires

Outre les quatre éditeurs précédemment cités (Project-Node-Process-Packet Editors), OPNET en comporte dix autres parmi lesquels deux méritent un peu plus d'attention.

4.1. Editeur de diagramme de rayonnement

Cet outil (figure 6) permet de modéliser le gain d'une antenne dans différentes directions par une saisie point à point des valeurs de gain dans différents plans et de visualiser en trois dimensions le diagramme de rayonnement réalisé. [28]

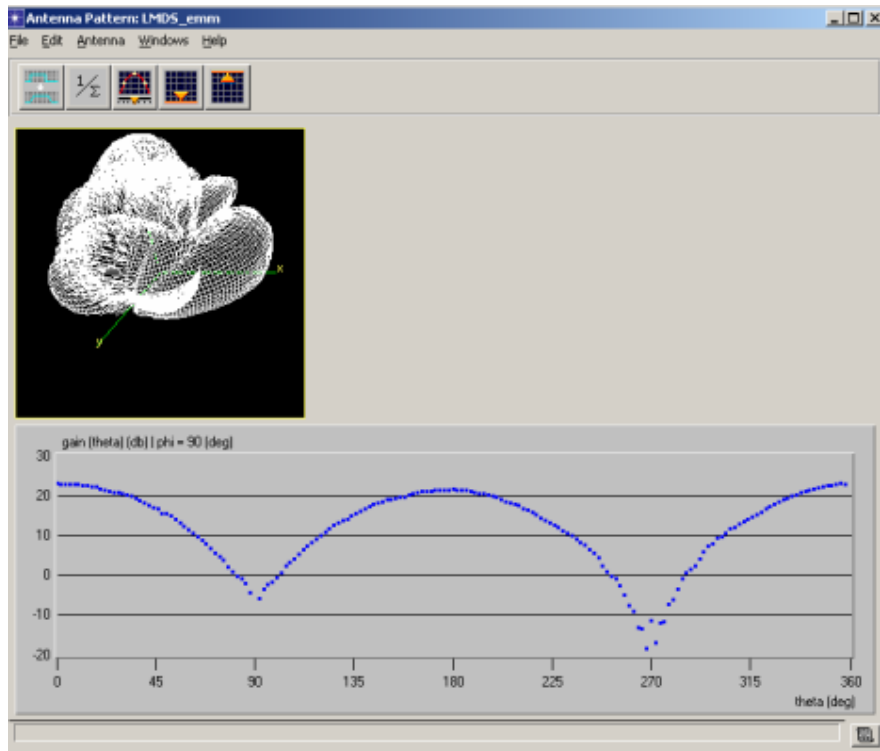


Figure 6: Editeur de diagramme

Sur la figure 30, nous voyons la représentation en 3 dimensions du diagramme édité puis la valeur du gain pour un angle phi donné en fonction de l'angle teta.

4.2. Editeur de sondes (*Probe editor*)

Cet éditeur (figure 7) permet de choisir les statistiques qui seront seules collectées lors de la simulation. Il existe différentes sortes de statistiques mais les deux plus utilisées sont :

- les statistiques globales qui concernent le réseau dans son ensemble,
- les statistiques locales qui sont spécifiques à un objet (lien ou nœud) particulier du réseau.

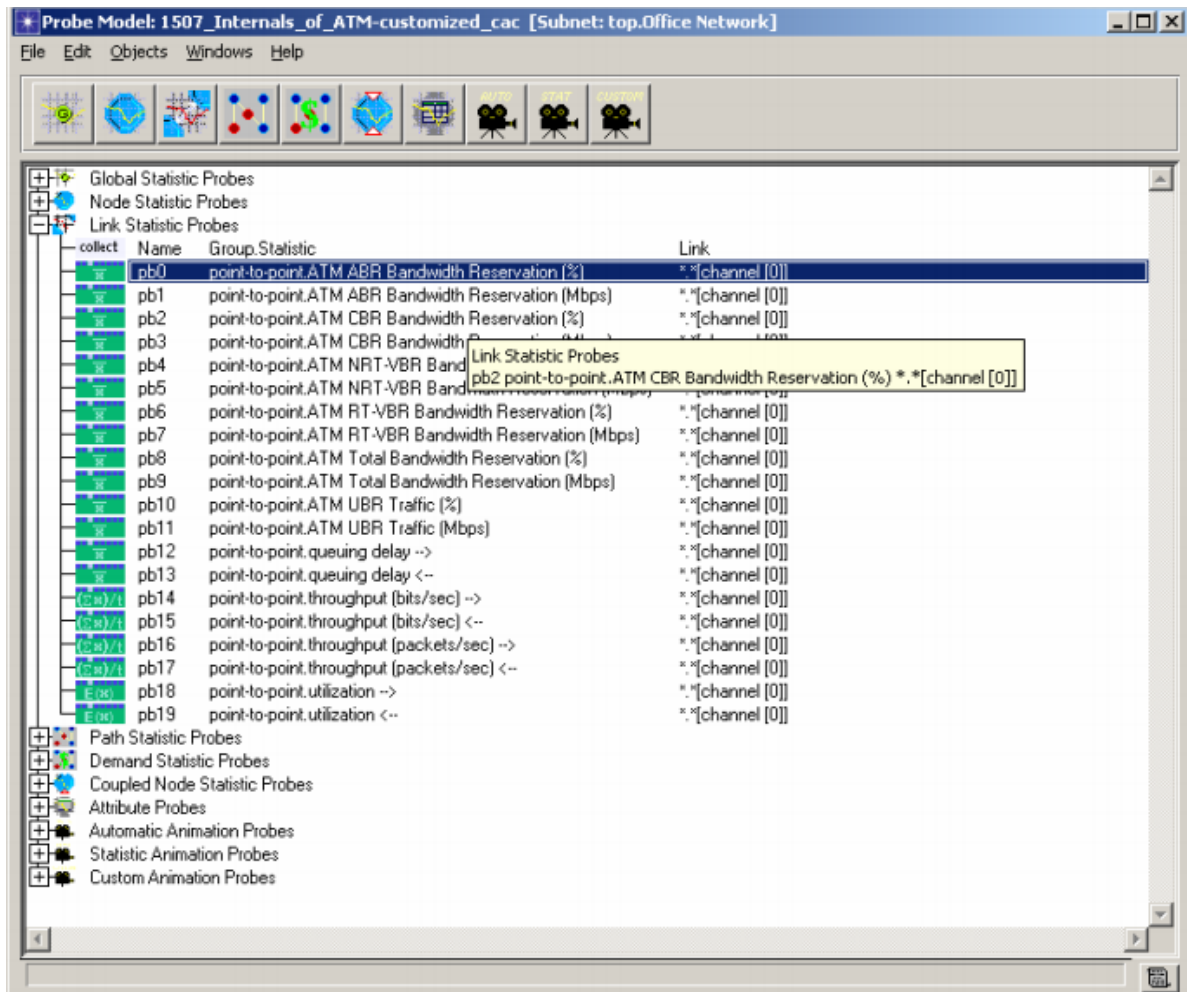


Figure 7 : Editeur de sondes

La figure 7 montre un exemple de configuration des sondes avec l'éditeur. On peut y voir que la sonde pb0 mesure la bande passante d'une liaison point à point particulière.

4.3. Prise de statistiques

Le réseau étant établi, il est nécessaire de choisir les différentes statistiques qui devront être récoltées au cours de la simulation.

Certaines statistiques, telles que le temps de réponse ou le taux d'utilisation d'un serveur sont prédéfinies. Cependant, l'utilisateur peut en créer d'autres afin de caractériser au mieux son réseau.

Ces nouvelles statistiques sont alors déclarées dans les différents modèles de processus de manière à pouvoir être sondées. [28]

5. Modélisation Radio

La présentation qui va suivre concerne l'aspect radio offert par la version du logiciel OPNET dont nous disposons. Elle traite plus particulièrement de la procédure d'établissement d'un lien radio entre deux nœuds.

Chaque procédure sera décrite par un nœud radio, un lien radio, et une antenne. Le rôle de ces procédures va maintenant être détaillé. [28]

5.1. Nœud radio

OPNET Modeler/Radio permet de modéliser plusieurs types de réseaux de communications sans fil, que ce soit un réseau d'antennes fixes comme le réseau TV, un réseau mobile comme celui des téléphones portables ou bien un réseau satellitaire.

En effet, il permet d'utiliser trois catégories de nœuds adaptés à chacun de ces réseaux: des nœuds fixes, mobiles et satellites. Les premiers sont repérés dans l'espace par trois coordonnées (x, y, altitude) constantes au cours du temps. Les seconds, modélisant des composants de réseau terrestre comme des automobiles, des avions ou des bateaux, ont par définition une position variant au cours de la simulation. Ils sont caractérisés par (x, y, altitude) mais aussi par une trajectoire définie par l'utilisateur. Les nœuds satellites, quant à eux, modélisent des éléments de réseau en orbite autour de la Terre, comme des satellites ou des vaisseaux spatiaux. [28]

5.2. Liens radio

Lors d'une liaison radio, il y a propagation des ondes émises dans l'air. Cette diffusion à l'ensemble du réseau fait qu'un lien radio est susceptible d'exister entre toute paire émetteur/récepteur. Chaque lien, n'existant pas en tant qu'objet physique, est établi dynamiquement au cours de la simulation entre chaque paire potentielle, mais n'est effectif que si certains paramètres tels que les bandes de fréquence, le type de modulation, la puissance émise, la distance et la direction des antennes le permettent.

Pour caractériser une liaison radio, il est nécessaire d'associer aux antennes d'émission et de réception respectivement un émetteur et un récepteur radio. Ils sont représentés par la figure 8 :

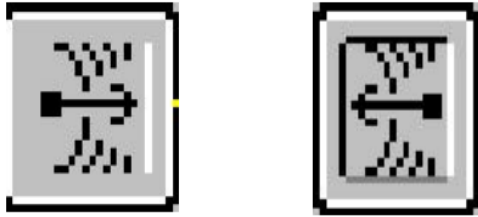


Figure 8 : Icône de réception et émission radio

Ceux-ci regroupent différents paramètres déterminants pour l'existence ou non du lien à un moment donné. Ces paramètres sont :

- Channel: caractérise les attributs du ou des canaux radio par les paramètres suivants:
 - data rate (bps) : débit d'émission ou de réception des données,
 - packet format: type de paquet qu'un canal peut émettre ou recevoir,
 - bandwidth (kHz):largeur de bande du canal,
 - Min frequency (MHz): fréquence basse du canal,
 - spreading code : utilisé pour spécifier du code utilisateur,
 - power (W):puissance d'émission des paquets émis sur le canal (d'émission seulement),
 - processing gain : gain du canal de réception spécifié par l'utilisateur (donc seulement en réception).
- Modulation: nom de la table de modulation utilisée, calculant le taux d'erreur (BER) en fonction du rapport signal à bruit (SNR).
- Noise figure : représentation de l'effet du bruit thermique sur la transmission radio (réception seulement).
- Ecc_threshold (en bits): proportion maximale de bits en erreur pour laquelle un paquet peut être accepté par un récepteur (réception seulement).
- model : attributs du modèle de communication, c'est à dire étapes du Transceiver Pipeline.

5.3. Antennes

Elles permettent soit de rayonner, soit de capter des informations transmises dans l'espace.

Chaque antenne modélisée sous OPNET possède divers attributs :

- Pattern: nom du diagramme de rayonnement défini au moyen de l'éditeur Antenna Pattern,
- Pointing ref. phi et pointing ref. theta : angles définissant le point du diagramme de rayonnement à pointer vers un récepteur donné appelé cible (ils sont pris dans le repère de l'éditeur précité donc : $0^\circ < \text{phi} < 180^\circ$ et $0^\circ < \text{theta} < 360^\circ$).
- Target latitude, target longitude et target altitude : paramètres définissant la position de la cible dans l'espace et servant à orienter l'antenne vers celle-ci.

La procédure appelée Transceiver Pipeline modélise l'émission de paquets à travers le canal de communication en implémentant les caractéristiques de la couche physique. Elle est divisée en 14 étapes décrites en annexe 1, chacune modélisant un aspect particulier du canal. Six d'entre elles sont associées à l'émetteur, les huit autres au récepteur. [28]

6. Fenêtre de définition d'une simulation

Juste avant d'exécuter une simulation, on ouvre une fenêtre « Simulation Set » semblable à :

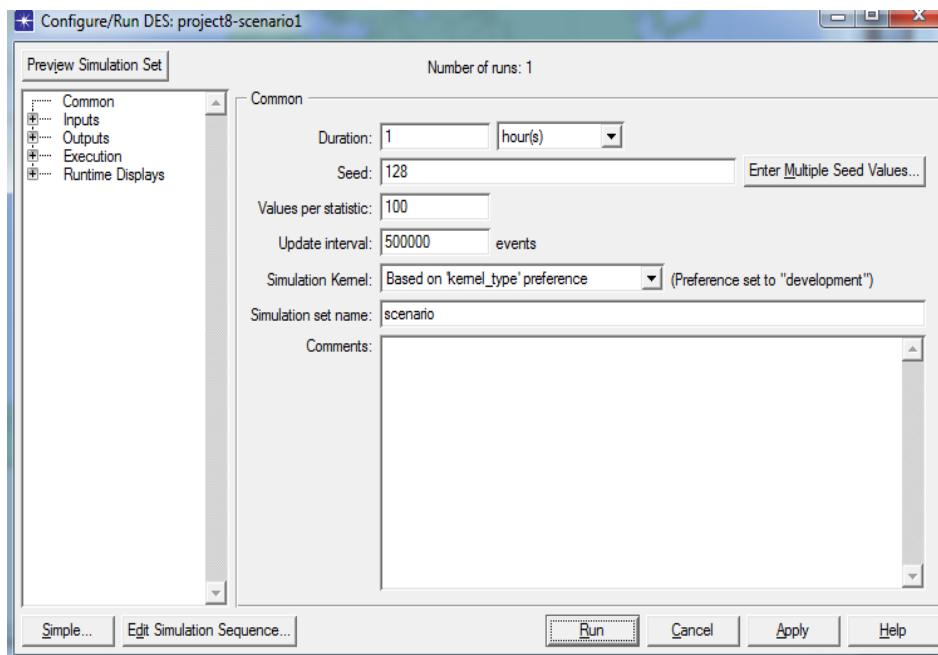


Figure 9 : Fenêtre de définition d'une simulation.

Son accès se fait en partant du projet par la rubrique 'configure simulation (Advanced)' de la simulation, puis en éditant les attributs du scénario.

On y trouve des informations comme le nom du réseau à soumettre à la simulation, le nom du fichier de stockage des résultats, la durée de la simulation (selon la puissance de l'ordinateur, une simulation programmée pour une durée de quelques heures peut s'exécuter en quelques secondes).

Dans certains projets, des paramètres ne sont pas définis car on leur prévoit plusieurs valeurs possibles, ce paramètre est déclaré « promoted » à la construction du modèle du réseau. C'est dans la fenêtre de simulation que l'on affectera les valeurs à utiliser séquentiellement pour les paramètres « promoted » : pour N valeurs différentes du paramètre, il y aura N simulations de durée t. cette façon de simuler est intéressante lorsque l'on souhaite un résultat graphique en fonction d'un paramètre qui n'est pas temps. [28]

7. Fenêtre de définition d'une simulation

Une fenêtre très utilisée est celle présentations graphique des résultats. son accès se fait en choisissant « Resultat Browser» à la place de « project » dans le champ ouvert par le menu File...new.

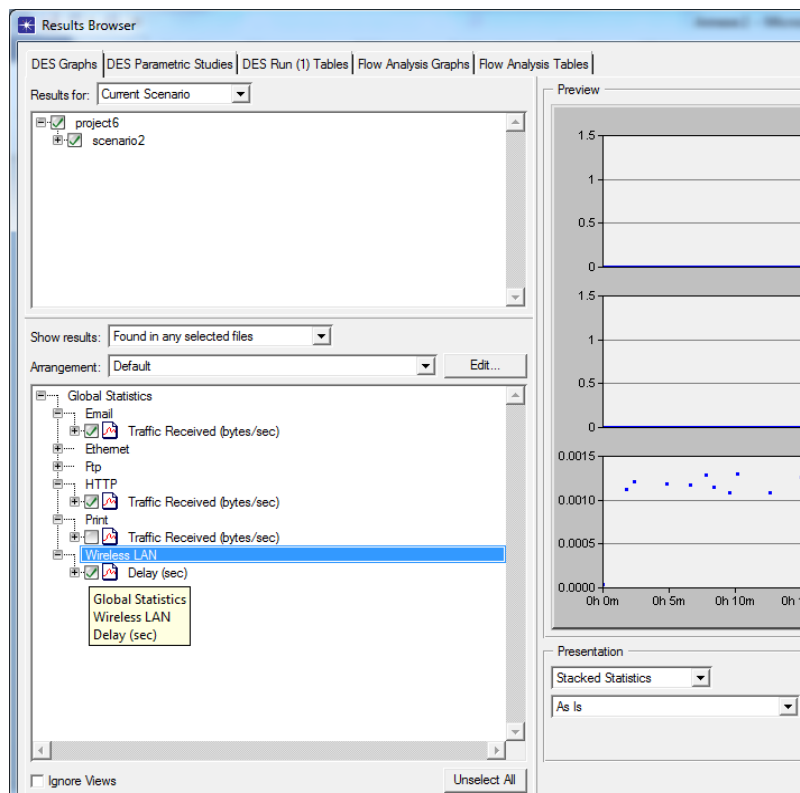


Figure 10 : Fenêtre de présentation des résultats de simulation.

La diversité des statistiques collectées lors de la simulation ainsi que la façon de les présenter nécessitent des choix sur ce que l'on veut voir afficher.

Après l'affichage des résultats, l'utilisateur d'OPNET modeler aura à :

- Faire des interprétations.
- Exercer un esprit critique.
- Tirer une conclusion

Conclusion Générale

Ethernet n'a cessé depuis lors de se développer et c'est aujourd'hui la technologie de réseau local la plus déployée dans le monde. Trois facteurs fondamentaux permettent d'expliquer le succès de cette technologie : Invente chez Xerox, Ethernet devient une norme industrielle en 1980 (standard 10Mbps du consortium DIX), puis un standard (IEEE 802.3) adopté comme tel par l'ISO. C'est une technologie sûre et largement éprouvée, basée sur un mécanisme de transmission à la fois simple et robuste. L'adoption très large des standards Ethernet a conduit à une diminution du coût des équipements.

Les réseaux locaux informatique (en anglais LAN, *Local Area Network*) sont destinés principalement aux communications locales, généralement au sein d'une même entité (entreprise, administration, etc), sur de courtes distances (quelques kilomètres au maximum). Un réseau local permet la connexion d'un ensemble de postes afin d'échanger ou de partager des informations. Il permet aussi le partage de ressource (disque, imprimante,...).

Premièrement nous avons familiarisé la lecture des réseaux locaux informatiques et en particulier à ceux définissant les couches MAC et physique d'un modèle OSI. Dans un deuxième temps, nous avons présenté l'étude succincte des principales implémentations et aussi les différents types de supports de transmission utilisée.

Les différents types des réseaux sans fil ont été introduits dans la deuxième partie, ainsi que leurs architectures générales de ces derniers. Ensuite, nous avons finalisé ceux-ci par les différentes versions de la technologie Ethernet.

La conception des réseaux locaux informatiques d'entreprises par l'outil de simulation Cisco Packet Tracer montre que les divers réseaux proposée en appliquant certaines techniques de configuration assurent un bon fonctionnement pour chaque réseau.

La dernière partie représente et décrit les étapes suivis pour concevoir des réseaux locaux informatiques et rentre progressivement dans les détails pour expliquer les travaux proposés durant la conception. Ces réseaux ont été simulés par le logiciel OPNET et les résultats de simulation sont alors présentés et discutés.

Enfin ce mémoire permet de collecter plusieurs informations sur les réseaux locaux informatiques et surtout côté simulation de ces derniers par les logiciels Cisco Packet Tracer.

Liste des Tableaux

Chapitre I

Chapitre II

Table II.1.Ethernet IEEE 802.3	30
Table II.2.Ethernet fin	30
Table II.3.Couche physique 100Base -T	32

Chapitre III

Table III.1. Table de routage de réseau proposé	36
Table III.2. Table de routage de la topologie proposée	42
Table III.3. Table de routage de réseau choisi.....	48
Table III.4.Table de routage	53
Table III.5. Paramètres du serveur DHCP	55
Table III.6. Table de routage de réseau WIFI.....	55

Chapitre IV

Tableau IV.1 : Valeurs indiquées dans le Startup Wizard.

Annexe 1

Annexe 2

Liste des Figures

	Chapitre I
Figure I.1. Les couches du modèle OSI.....	6
Figure I.2. Principe du codage en lign.....	7
Figure I.3. Notions de point d'accès selon le modèle OSI	9
Figure I.4. Format général des trames LLC.....	9
Figure I.5. Exemple d'adresse LSAP.....	10
Figure I.6. Principe de l'anneau.....	11
Figure I.7. Présentation du réseau Token Ring.....	11
Figure I.8. Niveau physique de l'IEEE 802.4.....	12
Figure I.9. Les modes de liaison élémentaire.....	12
Figure I.10. Topologie en bus.....	13
Figure I.11. Topologie en étoile.....	14
Figure I.12. Topologie en anneau.....	14
Figure I.13. Paire torsadée.....	14
Figure I.14. Câble coaxial.....	16
Figure I.15. Fibre optique.....	16
Figure I.16. Principe des faisceaux hertziens.....	17
Figure I.17. Principe d'une liaison satellitaire.....	18
	Chapitre II
Figure II.1. Architecture d'un réseau Wi-Fi	25
Figure II.2. Catégorie de réseau sans fil.....	26
Figure II.3. Le mode Ad Hoc	28

Figure II.4. Modèle des réseaux cellulaires	29
Figure II.5. Format des trames Ethernet 802.3	30
Figure II.6. Norme 100Base T.....	32

Chapitre III

Figure III.1. Topologie étoile avec routeur central	35
Figure III.2 .Etapes de simulation de PC2 vers PC5.....	41
Figure III.3. Topologie étoile avec 3 routeurs centraux	42
Figure III.4. Résultats de simulation entre PC1 et les autres PCs	45
Figure III.5. Résultats de simulation entre PC3 et les autres PCs	46
Figure III.6. Résultats de simulation entre PC5 et les autres PCs	47
Figure III.7. Réseau proposé avec la technique de routage dynamique.....	48
Figure III.8. Etapes de simulation de PC1 vers PC5	51
Figure III.9. Etapes de simulation de PC1 vers PC6	52
Figure III.10. Réseau informatique d'entreprise	53
Figure III.11. Etapes de simulation de Laptop1 vers PC1(Adressage fixe)	54
Figure III.12. Etapes de simulation de Laptop1 vers PC1.(Adressage dynamique)	54
Figure III.13. Réseau WIFI proposé	55
Figure III.14. Etape de simulation de PC1 vers PC2	56

Chapitre IV

Figure IV.1 : Choix de la topologie étoile à partir du menu déroulant.....	59
Figure IV.2 : Zone de dialogue Rapide Configuration.....	60
Figure IV.3 : Premier scénario.....	60
Figure IV.4 : Scénario HubAndSwitch.....	61

Figure IV.5 : Délai maximum à travers le réseau (delay) en sec.....	62
Figure IV.6 : Trafic envoyé.....	62
Figure IV.7 : Trafic reçu.....	63
Figure IV.8 : Palette d'objet.....	64
Figure IV.9 : Réseau NO_ Failure.....	64
Figure IV.10 : Configuration des paramètres la Simulation.....	65
Figure IV. 11 : Réseau Failure.....	66
Figure IV. 12 : Configuration de Failure.....	66
Figure IV. 13 : Trafic reçu.....	67
Figure IV. 14 : Trafic a envoyé(bit/sec).....	68
Figure IV. 15 : Nombre total de Mise à jour de Routeur1.....	68
Figure IV. 16: Adresses IP NO_ Failure.....	69
Figure IV. 17: Table de routage du routeur 1.....	69
Figure IV.18 : Réseau initial (Routage).....	70
Figure IV.19 : Réseau dupliqué.....	70
Figure IV.20: Trafic reçu (bits/sec).....	71
Figure IV.21 : Trafic a envoyé (bit/sec).....	71
Figure IV. 22 : Nombre total de Mise à jour du routeur central.....	72
Figure IV. 23 : Adresses IP des routeurs.....	72
Figure IV. 24 : Table de routage du node – 4.....	73
Figure IV.25 : Topologie d'un réseau WLAN.....	74
Figure IV.26 : Configuration d'une application.....	75
Figure IV.27 : Configuration d'un profil.....	76

Figure IV.28 : Configuration d'un client.....	76
Figure IV.29 : configuration d'un serveur.....	77
Figure IV.30 : Débit pour chaque application.....	78

Annexe 1

Figure 1. Interface de logiciel Cisco Packet tracer.....	80
Figure 2. Types d'équipements.....	81
Figure 3. Les différentes connexions proposées.....	81
Figure 4. Onglet physical.....	82
Figure 5. Onglet config.....	83
Figure 6. Onglet Desktop.....	83
Figure 7. Interface Physical	84
Figure 8. Présentation des modes de simulation.....	85

Annexe 2

Figure 1. Exemple de nœud d construit avec l'éditeur de nœuds.....	87
Figure 2. Editeur de processus avec le diagramme d'état.....	88
Figure 3. Analyse d'une simulation simple.....	89
Figure 4. Transmission du paquet entre les modules.....	90
Figure 4. Transmission du paquet entre les modules	91
Figure 6. Editeur de diagramme	92
Figure 7. Editeur de sondes	93
Figure 8. Icône de réception et émission radio	95
Figure 9. Fenêtre de définition d'une simulation.....	96
Figure 10. Fenêtre de présentation des résultats de simulation.....	97

Sigles et abréviations

A

AMRC	Accès Multiple à Répartition par Code
AMRF	Accès Multiple à Répartition de Fréquences
AMRT	Accès Multiple à Répartition de Temps

B

BSA	Basic Set Area
BSS	Base Station Subsystem

C

CSMA/CA	Carrier Sense Multiple Access /Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access /Collision Detection

D

DS	Distribution System
DSAP	Destination Service Access Point

E

ESS	Extented Service Set
------------	-----------------------------

F

FH/TDD	Frequency Hopping /Time Division Duplex
---------------	---

G

H

HDLC	High Data Link Control
-------------	-------------------------------

I

IP Internet **P**rotocol

G

GPRS General Packet Radio Services

GSM **G**lobal **S**ystem for **M**obile communications

K

L

LC **L**ate_ **C**ounter

LLC **L**ogical **L**ink **C**ontrol

LSAP **L**ink **S**ervice **A**ccess **P**oint

LPDU **L**ink **P**rotocol **D**ata **U**nits

LSDU **L**ink **S**ervice **D**ata **U**nits

M

MAC **M**edium **A**ccess **C**ontrol

MAU **M**ultiple **A**ccess **U**nits

N

O

P

PHY **P**hysical

PMD **P**hysical **M**edium **D**ependant

Q

R

S

SFD Start **F**rame **D**elimiter

STP Shielded **T**wisted **P**air

SSAP Source **S**ervice **A**ccess **P**oint

T

U

UMTS Universal **M**obile **T**elecommunication
System

UTP Unshielded **T**wisted **P**airs

V

VLAN Virtual **L**ocal **A**rea **N**etwork

W

WPAN Wireless **P**ersonal **N**etwork

WLAN Wireless **L**ocal **A**rea **N**etwork

WMAN Wireless **M**etropolitan **A**rea **N**etwork

WWAN Wireless **W**ide **A**rea **N**etwork

[1] Réseaux informatique, 2010.

[2] Note de AL Combaire basées sur le cours d'Alain Bawin, 01-04-2014.

- [3] Cours réseau, Pascal Urien ,2011.
- [4] Réseaux et télécommunication, Dominique SERET, 2005.
- [5] Réseaux et télécoms cours et exercices corrigés, Claude Servin 2009.
- [6] Architecture des réseaux, Daniel Dromard, 2010.
- [7] 802.11 et les réseaux sans fil, Paul Mühlethaler, Groupe Eyrolles, 2002.
- [8] site commenta Marche.net ‘les réseaux sans fil’ et ‘WiFi’ tyon- François Pillon.
- [9] IEEE 8802.11-1999, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1999.
- [10] <http://www.metz.supelec.fr>.
- [11] Introduction à informatique - U.Lg. 2006 H.P. Garnir et F. Monjoie
- [12] Réseaux et TELECOMMUNICATIONS Domique SERFT Ahmed MEHAOUA DORTA 2005-2006.
- [13] Les Réseaux Gey Pujolle 2008.
- [14] O.derhab, Le problème d’exclusion mutuelle dans les réseaux mobiles Ad Hoc, thèse de magistère, université des sciences et de la technologie houari Boumediene, 2003.
- [15] C. Venkatramani and T. Chiueh. Supporting Real-Time Traffic on Ethernet. InProceedings of IEEE Real-Time Systems Symposium, San Juan, Puerto Rico, 1994.
- [16] RESEAUX &TELECOMS Claude SERVIN 2006.
- [17] Technologie Ethernet Philippe Latu 2000.
- [18] Guide Pratique des Réseaux Ethernet. Charles Spurgeon, Vuibert 1998.
- [19] Routage statique, N SALMON
- [20] Protocoles et concepts de routage, ENI Editions – MOHA Anisa
- [21] Routage Cisco, vinel Emmanuel /Slimane amine ,2009.
- [22] Simulation du réseau, Prof Morgan Kaufmann 2003.

[23] B. Wu. "Simulation Based Performance Analyses on RIPv2, EIGRP, and OSPF Using OPNET."

[24] Charley BATAILLE, Sofia DJERROUD, Sasid ALLAH, Christine PHAMPANG, Virginie ROCHE, ING5 TR, «PROJET DE FIN D'ETUDES : Réalisation d'un réseau wifi sous OPNET et implémentation de mécanismes de sécurité », Ecole centrale d'électronique, Groupe ECE

[25] Doc Packet Tracer PDF

[26] Utilisation Packet Tracer, IUT Nice coté d'Azur, 2012.2013

[27] MIL3 Inc, « OPNET Medeling Concepts »,2001.

[28] David CARSENAT, « Contribution à l'étude de réseaux de communication sans fil, Application au LMDS », Thèse de Doctorat en Télécommunications 15 Octobre 2003.

Résumé

Ce travail est consacré à la conception des réseaux locaux informatiques avec les logiciels Cisco packet tracer et OPNET Modeler.

Un réseau numérique ou informatique permet l'échange entre machines distantes de données qui sont si nécessaire relayées de liaison en liaison par les machines intermédiaires.

Différentes techniques de configuration des périphériques des réseaux locaux ont été présentées afin de pouvoir tester la connectivité et vérifier le bon fonctionnement entre des réseaux distants en utilisant l'outil Cisco packet tracer.

Ce projet de fin d'étude s'intéresse aussi à connaître les performances des réseaux locaux informatiques en utilisant un autre logiciel commercial OPNET qui permet de concevoir des infrastructures réseaux et recueillir des statistiques au sujet des performances de ces derniers.

Mots clés : Réseaux locaux, Cisco Packet Tracer, OPNET Modeler.

Abstract

This work is dedicated to the conception of the computer local networks with the software Cisco packet to draw and OPNET Modeler.

A numeric or computer network permits the exchange between distant machines of data that are so necessary relieved of link in link by the intermediate machines.

Different techniques of configuration of the peripherals of the local networks have been presented in order to be able to test the connectivity and to verify the good working between distant networks while using the tool Cisco packet to draw.

This project of survey end is also interested in to know the performances of the computer local networks while using another software commercial OPNET that permits to conceive some infrastructures networks and to collect statistics about the performances of these last.

Keywords: Local area networks, Design, Cisco packet tracer, OPNET modeler.