TABLE DES MATIERES

LISTE DES ABREVIATIONS

ACL	Access Control List
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BECN	Backward Explicit Congestion Notification
BGP	Border Gateway Protocol
CIDR	Classless Inter Domain Routing
CIR	Committed Information Rate
CLI	Command-Line Interface
CRC	Cyclic Redundancy Check
CSU/DSU	Circuit Service Unit/Data Service Unit
CV	Circuit Virtuel
DE	Discard Eligibility
DEL	Diode Electroluminescent
DHCP	Dynamic Host Configuration Protocol
DLCI	Data Link Connection Identifier
DNS	Domain Name System
DoD	Department of defense
EGP	Exterior Gateway Protocol
EIGRP	Enhanced IGRP
EIR	Excess Information Rate
ETCD	Equipement de terminaison de circuit de données
ETTD	Equipement terminal de traitement de données
FAI	Fournisseur d'Accès à Internet
FCS	Frame Check Sequence
FECN	Forward Explicit Congestion Notification
FQDN	Full Qualified Domain
FRAD	Frame Relay Access Device
HDLC	High-Level Data Link Control
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
InARP	Inverse ARP
InterNIC	Internet Network Information Center
IOS	Internetwork Operating System
IP	Internet Protocol
IPX	Internetwork Packet eXchange
ISO	International Standardization Organization
LAN	Local Area Network
LASER	Light Amplification by Stimulated Emission Radiation
LMI	Local Management Interface
LS	Lignes Spécialisées
MAC	Medium Access Control
MAN	Metropolitan Area Network
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NBNS	NetBIOS Name Service
NIC	Network Interface Card
NM	Network module
NVRAM	Non Volatile RAM
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PABX	Private Automatic Branch eXchange
PAT	Port Address Translation
PC	Personal Computer
PDU	Protocol Data Unit
POP	Point Of Presence
PVC	Permanent Virtual Circuit
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol

RFC	Requests For Comments
RIP	Routing Information Protocol
RNIS	Réseau Numérique à Intégration de Services
RTPC	Réseau Téléphonique Public Commuté
SC	Subscriber Connecter
ST	Straight Tip
STP	Shielded Twisted Pair
SVC	Switched Virtual Circuit
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UIT-T	Union Internationale des Télécommunications-Télécommunication
UTP	Unshielded Twisted Pair
VLAN	Virtual LAN
VLSM	Variable Length Subnet Masks
VPN	Virtual Private Network
WAN	World Area Network
WIC	WAN Interface Card
WINS	Windows Internet Naming Service
WLAN	Wireless Local Area Network
xDSL	x désigne la famille et DSL Digital Subscriber Line

INTRODUCTION GENERALE

Un réseau est par définition un ensemble d'entités communicant entre elles dont le but est de se partager des ressources. Il existe différentes sortes de réseau mais dans notre cas nous allons nous intéresser au réseau informatique. Ce dernier est apparu suite à une demande des entreprises qui recherchaient une méthode pour éviter la duplication des imprimantes et une simplification des communications de données entre des équipements informatiques.

Cependant, sa mise en place requiert une étude approfondie et planifiée quelle que soit sa taille. Par ailleurs, plus le temps passe, plus l'entreprise évolue, et le réseau doit toujours répondre à ses besoins. En effet, une petite entreprise initialement conçue qui trouve son essor cherchera à étendre ses services en installant des succursales au niveau national ou même international. La fiabilité et la performance du réseau doivent être à la hauteur des enjeux qu'il supporte.

Dans le cadre de ce mémoire, nous allons effectivement répondre à cette problématique qui se résume en la mise en place d'un réseau d'entreprise en plein développement capable d'interconnecter son siège à ses différentes succursales locales et distantes. Il est alors nécessaire de connaître les technologies de communication. Ce mémoire a notamment pour objectif d'offrir aux amateurs de réseau, tels que les étudiants intéressés au sujet, les connaissances de base qu'il faut avoir en tant que concepteur et administrateur de réseau. En outre, comme il est difficile de manipuler des équipements physiques pour tester la conception de réseau surtout si l'on veut tester une connectivité à distance, nous devons utiliser un logiciel de simulation. Une fois que la conception du réseau simulé est vérifiée, on aboutit à un prototype pouvant être mis en place réellement.

Ce travail s'intitulant « Prototypage d'un réseau d'entreprise utilisant la technologie Frame Relay » se divise en cinq chapitres : en premier lieu, nous allons parler des généralités sur les réseaux telles que des vocabulaires fréquemment utilisés en terme de réseau, les différents types de réseau informatique, les unités de base utilisés ; dans le chapitre deux nous allons entrer en détail avec les deux types de modèles sur lesquels se reposent le fonctionnement du réseau; dans le troisième chapitre nous allons aborder le concept de routage voire ses différents types, les divers protocoles de routage. L'avant dernier chapitre concerne les réseaux de transport c'est-à-dire qu'on va parler du principe d'interconnexion dans le réseau WAN; nous allons terminer notre travail avec une simulation d'un réseau d'une entreprise fictive en appliquant toutes les notions apprises dans les chapitres précédents.

CHAPITRE 1
GENERALITES SUR LES RESEAUX

1.1 Quelques définitions

1.1.1 Hôte, serveur, client

Un hôte est un terme utilisé pour désigner toute machine qui offre un service à des utilisateurs : ordinateur personnel, station de travail, mini-ordinateur…

Un serveur est toute machine sur laquelle tourne un logiciel serveur offrant des services à des logiciels utilisateurs. C'est à la fois un ensemble de logiciels et d'ordinateur les hébergeant qui répond de manière automatique à des services demandés par des clients.

Un client est tout logiciel utilisateur utilisant les services des logiciels serveurs c'est-à-dire que c'est le logiciel qui envoie des demandes à un serveur ; il peut bien être aussi l'ordinateur depuis lequel ces demandes ont été envoyées. [1]

1.1.2 Protocole, service

On peut définir un protocole comme étant :

- un ensemble de règles ou de conventions qui déterminent le format et la transmission de données.
- un dialogue connu par deux réseaux entre deux couches du même niveau ; seules deux couches de même niveau peuvent se dialoguer entre elles.

  Exemples : la couche « transport » utilise comme protocoles le TCP (Transmission Control Protocol) et l'UDP (User Datagram Protocol) ; la couche « réseau » utilise le protocole IP (Internet Protocol).

Un service est l'ensemble des fonctions que doivent remplir une couche fournissant l'interface pour transmettre des données de la couche n à la couche (n+1). [2]

1.1.3 Bande passante numérique, le débit et le taux de transfert de données

Une bande passante numérique est la quantité d'informations (de données) pouvant circuler d'un endroit à un autre pendant une unité de temps. L'unité de la bande passante (BP) est le bit par seconde (bps). Elle présente d'énormes importances dans le cadre d'un réseau, en effet :

- Elle est finie c'est-à-dire qu'elle est limitée par des lois et des conditions physiques.
- De ce fait, elle permet de réaliser des économies.

- C’est une mesure clé de la conception et des performances du réseau : la bande passante reste l’un des principaux aspects de la conception de nouveaux réseaux.
- Elle est essentielle à la bonne compréhension de l’Internet du fait d’envoyer des millions et des billions de bits en une seconde entre des ordinateurs n’importe où dans le monde et à n’importe quel moment.
- La demande en bande passante augmente sans cesse.

  Voici quelques exemples de bande passante maximale prise en charge par des différents médias :

Type de medias	**Bande passante**
Câble coaxial de 50 Ohms (Ethernet 10BASE2 fin, 10BASE5 épais)	10 à 100 Mbps
Paire torsadée non blindée de catégorie 5 (Ethernet 10BASE-T, 100BASE-TX)	10 Mbps
Paire torsadée non blindée renforcée de catégorie 5 (Ethernet 10BASE-T, Fast Ethernet 100BASE-TX et 1000BASE-T)	100 Mbps
Fibre optique multimode (100BASE-FX)	100 Mbps
Fibre optique monomode (100BASE-LX)	1000 Mbps (1Gbps)
Sans fil	11 Mbps

Tableau 1.01: *Exemples de bande passante*

Le débit de données est la bande passante réelle mesurée à un moment précis de la journée sur des routes internet données, lors d’un téléchargement d’un fichier particulier. Pour diverses raisons, le débit est inférieur à la bande passante maximale que peut atteindre un média. En voici ces facteurs :

- La topologie du réseau
- Les unités d’interconnexions de réseaux
- Les autres utilisateurs utilisant le réseau, leur nombre, leurs ordinateurs
- Le type de données transmises
- L’ordinateur serveur
- Les coupures d’électricité et autres pannes causées par les intempéries

- Le routage à l'intérieur du « nuage »

Il est alors à noter que lors de la conception d'un réseau, il convient de tenir compte de la bande passante théorique. Le réseau ne sera plus rapide que ne le permet le média. Ainsi, on peut prévoir si le débit du réseau dans le temps réel est convenable à l'utilisateur. [3]
Le taux de transfert de données est donné par les formules du tableau suivant :

Taux de transfert maximal	$T = \frac{F}{BP}$
Taux de transfert type	$T = \frac{F}{D}$
BP	Bande passante théorique maximale de la liaison entre l'hôte source et l'hôte de destination en Bps
D	Débit réel au moment du transfert en Bps
T	Durée du transfert des fichiers en seconds (s)
F	Taille de fichier en bits

Tableau 1.02: *Formule du taux de transfert de données*

1.2 Différents types de réseau

Il existe trois types de réseau suivant les distances entre les communicants :

- Les réseaux LAN
- Les réseaux MAN
- Les réseaux WAN

1.2.1 Réseaux LAN (Local Area Network)

Les réseaux locaux couvrent jusqu'à 1km de région : cas dans une salle de classe, dans un bâtiment ou un campus.... Leurs caractéristiques sont les suivants :

- Ils fonctionnent dans une région géographique limitée.
- Ils permettent à de nombreux utilisateurs d'accéder à des médias à haut débit.
- Ils assurent une connectivité continue aux services locaux.
- Ils interconnectent physiquement des unités adjacentes.

1.2.2 Réseaux MAN (Metropolitan Area Network)

Ces réseaux connectent un ou plusieurs LAN dans une même région géographique. Ce type de réseau est en émergence du fait du développement des réseaux Wireless. On les trouve souvent en ville, situés dans les endroits publics.

1.2.3 Réseaux WAN (World Area Network)

Ce sont des réseaux couvrant une vaste espace, reliant des villes et des pays. Ce type de réseau a été conçu pour relier les réseaux locaux pour faire ainsi circuler les informations rapidement et efficacement entre les entreprises d'un même ou de divers pays. Leurs caractéristiques sont de :

- Couvrir une large région géographique.
- Permettre l'accès par des interfaces séries plus lentes.
- Assurer une connectivité continue et intermittente (irrégulière).
- Relier des unités dispersées à une échelle planétaire.

1.3 Unités LAN de base

1.3.1 Topologie d'enseignement

Le terme topologie peut être interprété comme l'étude d'emplacement. La topologie permet de définir la structure d'un réseau. Elle comprend deux parties :

- La topologie physique : elle représente la disposition effective des fils ou des médias, elle décrit le plan de câblage des équipements physiques.
  On trouve : la topologie en bus, la topologie en anneau, la topologie en étoile, la topologie en étoile étendu, la topologie hiérarchique et la topologie maillée. [3]

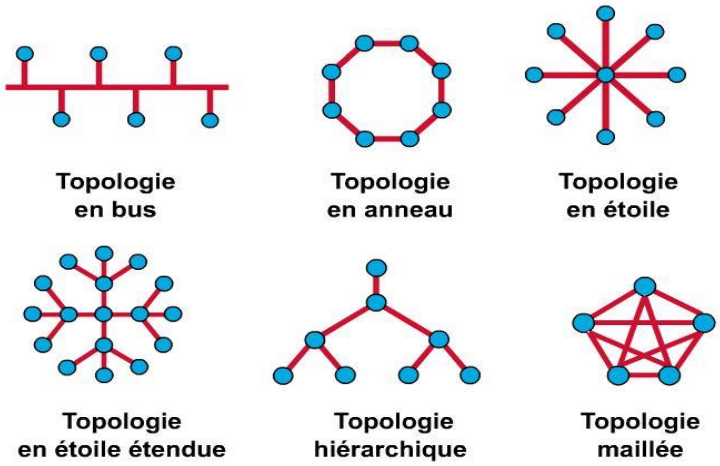


Figure 1.01 : *Les différents types de topologie physique*

- La topologie logique : c'est la méthode qu'utilisent les hôtes pour communiquer par le média. Elle permet de savoir comment circulent les informations dans le réseau afin de déterminer les emplacements où les collisions peuvent se produire.

  Les deux types de topologie logique les plus courants sont le broadcast et le passage de jeton.

  Le principe du broadcast est que chaque hôte envoie ses données à tous les autres hôtes présents sur le média du réseau.

  Pour le passage de jeton, l'accès au réseau est contrôlé en passant un jeton électronique de manière séquentielle à chaque hôte ; lorsqu'un hôte reçoit un jeton il peut transmettre de données sur le réseau, s'il n'a pas de données à transmettre il passe le jeton à l'hôte suivant et le processus se répète.

1.3.2 Médias

Les médias permettent la liaison entre deux équipements et assurent ainsi la transmission des informations (des données) entre eux. Un bloc d'information est un élément binaire connu sous le nom de bit ou impulsion. Il existe une représentation de ce bit dans le média physique. En effet, dans un milieu électrique, un bit correspond, par exemple, à 0 (zéro) volts pour un 0 binaire et à +5 volts pour un 1 binaire, mais on trouve aussi d'autre codage plus complexe.

Dans la mesure où le but est de transmettre des quantités gigantesques de bits à travers un média, il est important de prendre en compte et de ne pas négliger ses paramètres car le moindre défaut peut avoir des énormes conséquences sur la qualité de la transmission.

Il faut aussi savoir qu'une liaison entre deux équipements A et B peut être :

- Simple (unidirectionnelle) : A est toujours l'émetteur et B le récepteur (comme entre un banc de mesure et un ordinateur recueillant les données mesurées.
- Half-duplex (bidirectionnelle à l'alternat) : le rôle de A et B peut changer, la communication change de sens à tour de rôle (principe du talkie-walkie).
- Full-duplex (bidirectionnelle simultanée) : A et B peuvent émettre et recevoir en même temps (dans le cas du téléphone). [13]

Il existe alors plusieurs catégories de médias : les médias de cuivre, les médias optiques et les médias sans fils.

1.3.2.1 Médias de cuivre

❖ *Câble à paires torsadées non blindées ou UTP (Unshielded Twisted Pair) [4]*

Descriptions	Avantages	Inconvénients
- 4 paires de fils torsadés 2 à 2 - impédance : 100 ohms - vitesse et débit : 10 à 100 Mbits/s -diamètre extérieur : 0.43 cm - longueur maximale : 100m - Connecteur : RJ-45	- Facilité d'installation - Peu coûteux -Petit diamètre -effet d'annulation : limite la perturbation électromagnétique et l'interférence radioélectrique	- Sensible aux interférences - Longueur maximale courte

Tableau 1.03: *Câble à paires torsadées non blindées*

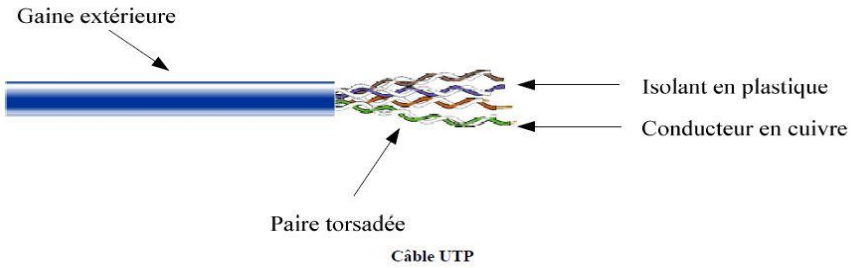


Figure 1.02 : *Câble à paires torsadées non blindées*

❖ *Câble à paires torsadées blindées ou STP (Shielded Twisted Pair)*

Descriptions	Avantages	Inconvénients
- 4 paires de fils torsadés 2 à 2 avec blindages - impédance : 150 ohms - vitesse et débit : 10 à 100 Mbits/s -Taille du connecteur/média : moyen à gros - longueur maximale : 100m - Connecteur : STP	- Coût moyen - Alliance des techniques de blindage, d'annulation et de torsion de fils. - Une plus grande protection contre tous les types d'interférence externe	- Longueur maximale courte - Moins facile à installer que l'UTP - Apparition de plusieurs problèmes en cas de non mis à la terre correcte du blindage

Tableau 1.04: *Câble à paires torsadées blindées*

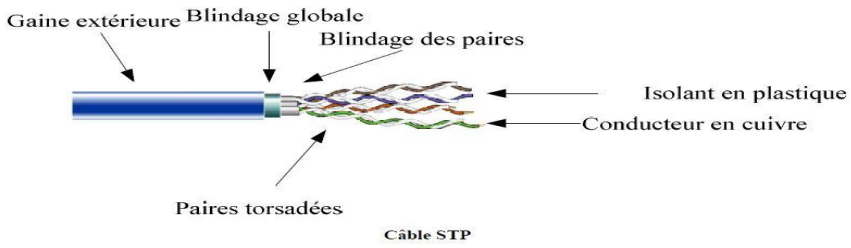


Figure 1.03 : *Câble à paires torsadées blindées*

❖ *Câble coaxial [6]*

Descriptions	Avantages	Inconvénients
- le fil intérieur est constitué de 2 éléments conducteurs : un conducteur central en cuivre et une torsade de cuivre jouant un rôle de blindage - vitesse et débit : 10 à 100 Mbits/s -Taille du connecteur/média : moyen - longueur maximale : 200 à 500m - plusieurs variantes : le Thicknet, le Thinnet, le Cheapernet - Connecteur : BNC	-Peu coûteux surtout pour le Cheapernet - Un plus grand recouvrement entre des nœuds réseaux surtout pour le Thicknet - Réduction des interférences externes grâce à la deuxième couche de conducteur (blindage) - Souplesse pour le Thinnet.	- Moins facile à installer dans le cas du Thicknet (épais, large diamètre) - Apparition de plusieurs problèmes en cas de non mis à la terre correcte du blindage surtout dans le cas du Thinnet.

Tableau 1.05: *Câble coaxial*

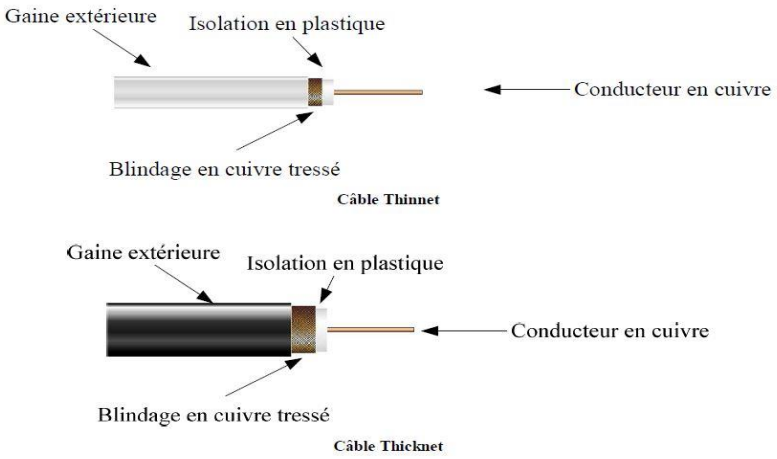


Figure 1.04 : *Câbles coaxiaux*

1.3.2.2 Médias optiques

Contrairement aux câbles de cuivre qui transportent des impulsions électriques, les câbles à fibre optiques transportent des impulsions lumineuses. Les signaux représentant les bits sont alors convertis en faisceaux lumineux. Il y a deux types de source de lumière :

- DEL (diode électroluminescente) : produit de la lumière infrarouge de longueur d'onde de 850 nm ou 1310 nm
- LASER (Light Amplification by Stimulated Emission Radiation) : produit des rayons étroits de lumière infrarouge de longueur d'onde de 1310 ou 1550 nm [4]

Une fibre optique transmet des données dans un sens seulement. Un câble optique doit alors contenir deux fibres pour communiquer en full-duplex : l'une pour la transmission et l'autre pour la réception.

Descriptions	Avantages	Inconvénients
- câble constitué de 2 fibres logées dans des enveloppes distinctes - vitesse et débit : plus de 100 Mbits/s -Taille du connecteur/média : petit - Monomode, longueur maximale : jusqu'à 3000m - Multimode, longueur maximale : jusqu'à 2000m - Monomode : un faisceau de lumière LASER - Multimode : plusieurs faisceaux de lumière LED - Connecteurs : ST (Straight Tip) pour la monomode et SC (Subscriber Connecter) pour la multimode	- Insensible aux interférences électromagnétiques. - Débit de données très élevé -Avantageux pour les communications à longue distance	-Coût moyen par nœud le plus cher -Fibre optique plus onéreuse : difficulté d'installation

Tableau 1.06: *Médias optiques*

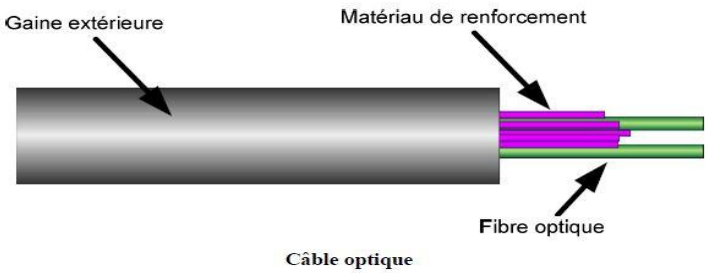


Figure 1.05 : *Câble optique*

1.3.2.3 Médias sans fils

Les réseaux sans fil ou WLAN (Wireless Local Area Network) réussissent à conjuguer tous les avantages d'un réseau filaire traditionnel mais sans limitation de câbles. En effet, les signaux sans fil sont des ondes électromagnétiques qui peuvent circuler dans le vide de l'espace ou dans les médias tels que l'air c'est-à-dire sans intervention d'un média physique.

Ainsi, au lieu des câbles à paires torsadées, par exemple, un WLAN utilise des fréquences radio. Les réseaux sans fil sont conformes aux normes IEEE 802.11. Ils peuvent fonctionner selon la technologie utilisée : soit aux alentours de 2400 MHz (2.4 GHz) pour le 802.11b et le 802.11g ; soit aux alentours de 5000 MHz (5 GHz) pour le 802.11a.

Norme	802.11b	802.11g	802.11a
Bande de fréquence	2.4 GHz	2.4 GHz	5 GHz
Débit maximum	11 Mbps	54 Mbps	54 Mbps

Tableau 1.07: *Caractéristiques des médias sans fils*

Les lois de la radio sont comme suit :

- Un débit plus grand signifie une couverture plus faible
- Une puissance d'émission élevée signifie une couverture plus grande mais une durée de vie des batteries faible
- Fréquence élevée signifie couverture plus faible mais débit élevé

1.3.3 Equipements

A part les médias qu'on a vus précédemment, il existe plusieurs équipements utilisés dans un réseau. [2]

- Le répéteur : c'est un composant actif (il tire l'énergie d'un bloc d'alimentation pour régénérer les signaux réseaux). Il permet de régénérer et de resynchroniser le signal afin de pouvoir étendre la portée des câbles. Il est à un seul port d'entrée et à un seul port de sortie. Il peut être symbolisé comme suit :

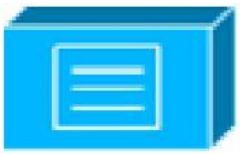


Figure 1.06 : *Symbole d'un répéteur*

- Le concentrateur : c'est un répéteur multi ports. Il reprend le fonctionnement du répéteur en ajoutant une fonctionnalité de connectivité. En effet, il dispose de plusieurs ports permettant d'interconnecter plusieurs équipements réseau. Chaque signal arrivant sur un port est régénéré, resynchronisé et réémis à travers tous les autres ports.

Figure 1.07 : *Concentrateur et son symbole*

Ces deux premiers équipements créent et manipulent des bits. Ils ne reconnaissent aucune information dans les bits, ni les adresses, ni les données. Leur fonction se limite seulement à déplacer les bits. Ce sont des équipements de la couche 1 du modèle OSI que l'on va retrouver ultérieurement.

- L'émetteur/récepteur : en anglais « Transceiver », convertit un signal en un autre. Il est souvent intégré aux cartes réseau.

- Le pont : Il se définit par son filtrage de trames de couche 2 et par la manière dont celui-ci est vraiment réalisé. Il est conçu pour connecter deux segments LAN : il permet de filtrer le trafic sur un LAN. Comme chaque unité réseau possède une adresse MAC unique sur la carte NIC, le pont effectue le suivi des adresses MAC se trouvant chacun de ses côtés et prend les décisions en fonction de cette liste d'adresses. C'est une unité à un seul port d'entrée et à un seul port de sortie.

Figure 1.08 : *Symbole du pont*

- Le commutateur : il est aussi appelé pont multiport. La différence entre le concentrateur et le commutateur est que ce dernier prend des décisions en fonction des adresses MAC. Il effectue cela en 'commutant' les données uniquement au port auquel le bon hôte est

connecté. Il vise à concentrer la connectivité tout en accroissant l'efficacité de la transmission de données.

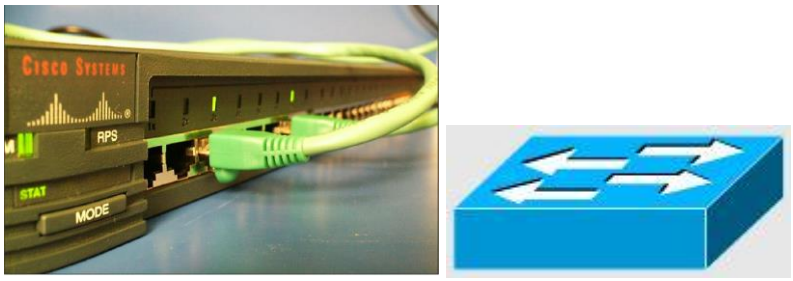


Figure 1.09 : *Commutateur et son symbole*

- Le routeur : c'est un équipement permettant d'interconnecter deux réseaux ou plus en se basant sur les adresses de couche 3 du modèle OSI. Son rôle consiste à examiner les paquets entrants, à choisir le meilleur chemin pour les transporter sur le réseau et à les commuter ensuite au port de sortie approprié.

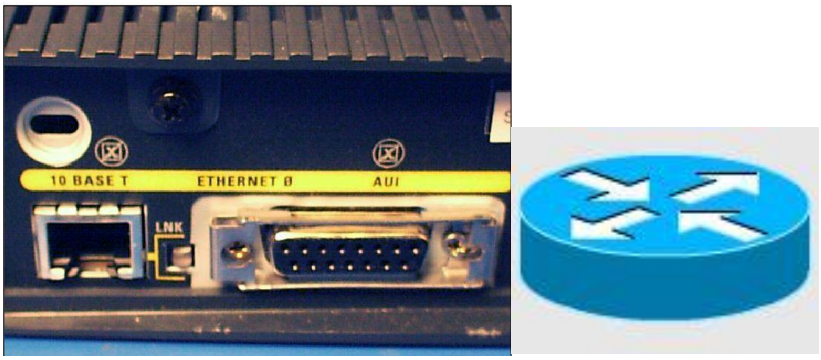


Figure 1.10 : *Routeur et son symbole*

1.4 Conclusion

Dans ce premier chapitre, nous avons appris la signification d'un hôte, un client, un serveur ; la différence entre un protocole et un service. Nous avons vu aussi qu'il existe plusieurs types de réseaux selon leurs portées géographiques. Enfin, nous avons des notions sur la structure d'un réseau, les différents médias qui assurent la transmission des données et les différents équipements qui entrent en jeu au sein d'un réseau informatique.

Dans le chapitre suivant, nous allons entrer plus en détails sur les bases de fonctionnement d'un réseau et les concepts à savoir pour réaliser un réseau viable dans une entreprise.

CHAPITRE 2
MODELES OSI ET DoD

Pour que les différents équipements des différentes entreprises puissent se connecter, des normes ont été adoptées par l'ISO et l'UIT-T. Il s'agit de la mise en place d'un modèle de réseau basé sur la notion de couches afin d'assurer l'interopérabilité des différents systèmes. Il existe deux modèles : le modèle de référence OSI et le modèle DoD.

2.1 Modèle de référence OSI

2.1.1 Description du modèle

L'OSI (Open System Interconnection) est un système modèle de référence pour interconnecter des systèmes ouverts. Il définit une architecture en couches normalisées adoptées conjointement par l'ISO et l'UIT-T pour les réseaux informatiques, téléinformatiques et télématiques. Cette architecture est constituée de sept couches dont la liaison réelle entre couches adjacentes se fait à partir des «services » ; pour deux systèmes en communication, la relation logique entre les couches se fait à partir des « protocoles ». Ces sept couches sont :

- Couche application
- Couche présentation
- Couche session
- Couche transport
- Couche réseau
- Couche liaison de données
- Couche physique [1] [2]

Le tableau ci-dessous décrit cette architecture :

Couche	Unité de données	Fonctions	Equipements utilisés
7-Application	Donnée	Services réseaux fournis aux processus d'application : synchronisation ; contrôle d'intégrité de données.	hôte

Couche	Unité de données	Fonctions	Equipements utilisés
6-Présentation	Donnée	Représentation de données : Lisibilité, format, structure des données (utilisation de format commun).	hôte
5-Session	Donnée	Communication entre les hôtes : Etablissement, gestion et fermeture de sessions entre applications.	hôte
4-Transport	Segment	Communication de bout en bout : Transport des données, fiabilité du transport ; établissement, maintien et fermeture des circuits virtuels ; détection des pannes et reprise ; contrôle de flux d'informations.	Hôte, nuage (possibilité de se connecter à un autre réseau ou internet en entier)
3-Réseau	Paquet	Adressage et sélection du meilleur chemin : connectivité et sélection du meilleur chemin, domaine de routage	Routeur
2-Liaison de données	Trame	Accès au média : Transfert fiable de données par le média, adressage physique et topologie de réseau, notification des erreurs et contrôle de flux	Pont, commutateur, carte réseau(NIC)
1-Physique	Bits	Transmission binaire : Spécifications électriques et mécaniques pour maintenir la liaison physique des systèmes d'extrémité : fils, connecteurs, tension, débit	Emetteur-récepteur, câble (média réseau), répéteur, concentrateur

Tableau 2.01: *Modèle OSI*

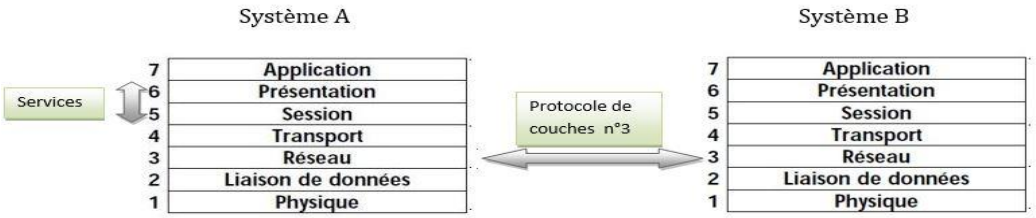


Figure 2.01 : *Liaisons entre deux couches adjacentes et deux couches de même niveau*

2.1.2 Encapsulation de données

Au sein d'un réseau, toutes les communications partent d'une source, puis acheminées vers une destination et les informations envoyées sur le réseau sont appelées données ou paquets de données. Si un ordinateur (hôte A) veut envoyer des données à un autre ordinateur (hôte B), les données doivent d'abord être préparées grâce à un processus appelé encapsulation. Ce processus conditionne les données en leur ajoutant des informations relatives au protocole avant de les transmettre dans le réseau. Ainsi, en descendant dans les couches du modèle OSI, les données reçoivent des en-têtes, des en-queues et d'autres informations. Pour comprendre comment se produit l'encapsulation, examinons la manière dont les données traversent les couches. Comme la montre la figure ci-dessous, les données qui sont envoyées par l'ordinateur source traversent la couche application et les autres couches. La présentation et le flux de données échangées subissent des changements au fur et à mesure que les réseaux fournissent leurs services aux utilisateurs.

Les réseaux doivent effectuer les cinq étapes de conversion suivants afin d'encapsuler les données :

a) Construction des données : lorsqu'un utilisateur envoie un message électronique, les caractères alphanumériques qu'il contient sont convertis en données pouvant circuler dans l'inter-réseau.

b) Préparation des données pour le transport de bout en bout : les données sont préparées pour le transport inter-réseau. En utilisant des segments (type de donnée dans la couche transport), la fonction de transport assure que les systèmes hôtes situés à chaque extrémité du système de messagerie peuvent communiquer de façon fiable.

c) Ajout de l'adresse réseau à l'en-tête : les données sont organisées en paquets, ou datagrammes, contenant un en-tête réseau constitué des adresses logiques d'origine et de destination. Ces adresses aident les unités réseau à acheminer les paquets dans le réseau suivant un chemin déterminé.

d) Ajout de l'adresse locale à l'en-tête de liaison : chaque unité réseau doit placer le paquet dans une trame. La trame permet d'établir la connexion avec la prochaine unité réseau

directement connectée dans la liaison. Dans l'en-tête de la trame se trouve les adresses physiques de la source et de la destination.

e) Conversion en bits pour la transmission : La trame doit être convertie en une série de un et de zéro (bits) pour la transmission sur le média. Une fonction de synchronisation permet aux unités de distinguer ces bits lorsqu'ils circulent sur le média. Tout au long du trajet suivi dans l'inter-réseau physique, le média peut varier. Ainsi, le message électronique peut provenir d'un réseau local, traverser le backbone d'un campus, sortir par une liaison WAN pour atteindre sa destination sur un autre LAN éloigné. Les en-têtes et en-queues sont ajoutés au fur et à mesure que les données descendent dans les couches du modèle OSI. [3]

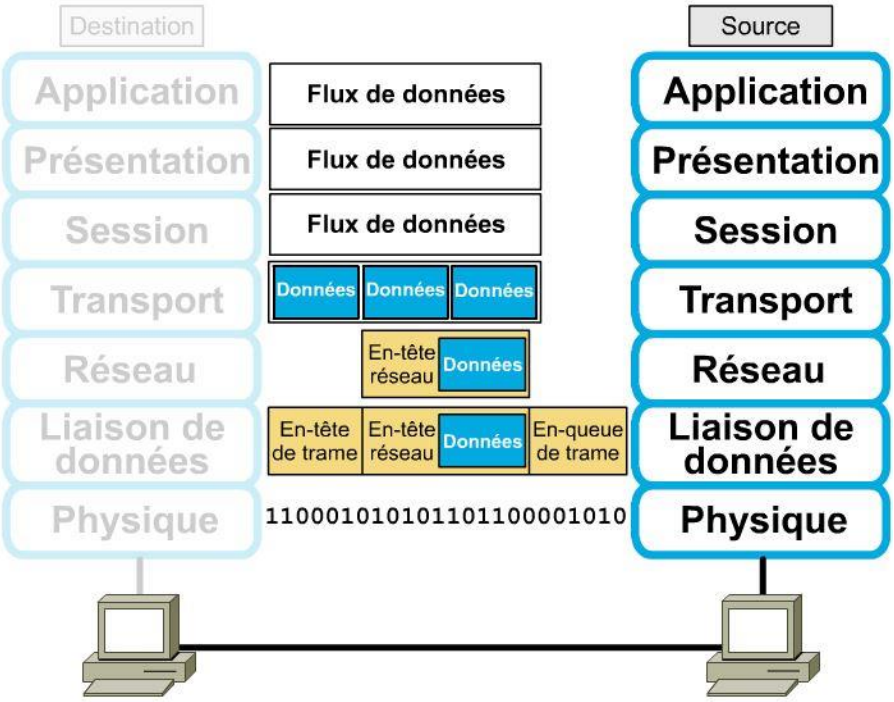


Figure 2.02 : *Encapsulation de données dans l'inter-réseau*

A la réception, des procédures inverses sont effectués aux données en traversant les couches inférieures jusqu'à la couche application, c'est la désencapsulation.

2.2 Modèle DoD

Le ministère de la défense (DoD) a développé le modèle de référence TCP/IP dont le but d'avoir un réseau qui résiste à toutes les situations. Ce modèle est inspiré du modèle OSI, il reprend l'approche modulaire (utilisation de modules ou couches) mais il est constitué de seulement quatre couches :

- Couche Application

- Couche Transport
- Couche Internet
- Couche Accès réseau

Depuis lors, ce modèle s'est imposé comme la norme Internet. [1]

Le tableau suivant décrit l'architecture du modèle DoD :

Couche	Unités de données	Fonctions
Application	Donnée	Gestion des protocoles de haut niveau, des questions de présentation, assure le code et le contrôle de dialogue.
Transport	Segment	Fiabilité des communications réseaux ; établissement d'un dialogue entre ordinateur source et ordinateur destination ; contrôle de flux et correction des erreurs.
Internet	Paquet	Identification de meilleur chemin pour l'envoi des paquets sources ; commutation de paquets.
Accès au réseau	Trame - bits	Etablissement de liaison physique pour un paquet physique. Elle comprend les détails dans les couches physiques et liaison de donnée du modèle OSI

Tableau 2.02: *Modèle DoD*

2.3 Comparaison entre les deux modèles

2.3.1 Similitudes

- Tous les deux comportent des couches.
- Ils comportent une couche application bien que chacune fournisse des services très différents.
- Les deux comportent des couches réseau et transport comparables.
- Ils supposent l'utilisation de la technologie de commutation de paquets et non de commutation de circuits.

2.3.2 Différences

- TCP/IP intègre la couche présentation et la couche session dans sa couche application.
- TCP/IP regroupe les couches physiques et liaison de données OSI au sein d'une seule couche.

- TCP/IP présente moins de couches et semble plus simple.
- Les protocoles TCP/IP constituent la norme sur laquelle s'est développé Internet.

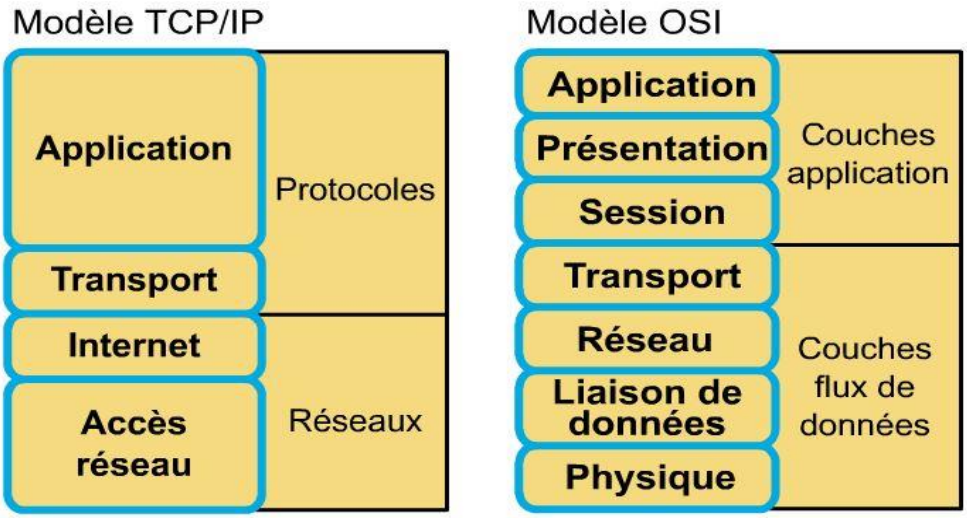


Figure 2.03 : *Comparaison des deux modèles*

2.4 Principes fondamentaux dans la conception des réseaux informatiques

2.4.1 Objectifs fondamentaux de conceptions

Après analyse et examen des exigences attendues par les réseaux informatiques, les concepteurs et techniciens réseau doivent tenir compte des principaux points suivants lors de la conception d'un nouveau réseau :

- Extensibilité : qui permet au réseau d'accueillir de nouveaux groupes d'utilisateurs, de sites distants, et de prendre en charge de nouvelles applications sans affecter le niveau de service fourni aux utilisateurs existants.
- Disponibilité : le réseau doit être disponible à tout moment avec des performances stables et fiables même en cas de panne d'équipements ou de problème de liaisons.
- Sécurité : la conception de réseau doit inclure à l'avance sa sécurisation en assurant la planification de l'emplacement des dispositifs de sécurité, des filtres et des pare-feu pour la protection des ressources du réseau.
- Facilité de gestion : le personnel en charge du réseau doit être capable de le gérer pour son bon fonctionnement. [5]

2.4.2 Réseau hiérarchique et ses avantages

Il existe deux structures de modèles de réseau : le modèle hiérarchique et le modèle maillé. Dans une structure maillée, la topologie du réseau est linéaire. Tous les routeurs remplissent essentiellement les mêmes fonctions et il n'existe généralement pas de définition précise des fonctions exécutées par chaque routeur. L'expansion du réseau s'effectue par hasard et de façon arbitraire.

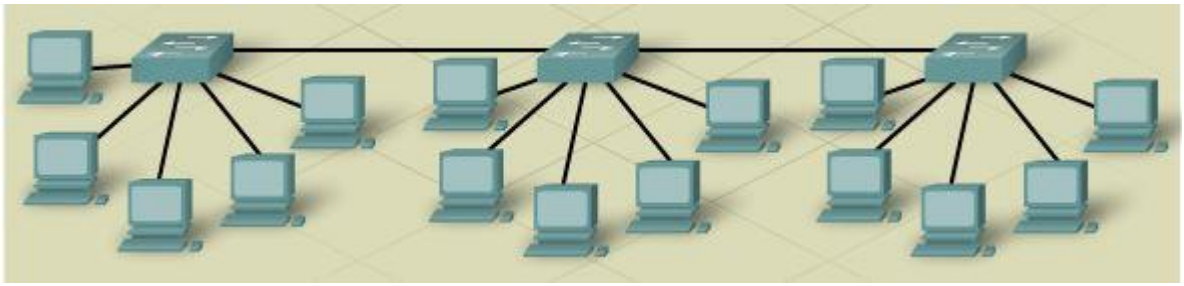


Figure 2.04 : *Réseau maillé*

Dans une structure hiérarchique, on regroupe les périphériques en un certain nombre de réseaux distincts qui sont organisés en couches. Une ou plusieurs fonctions précises sont associées à chaque couche. Le modèle de conception hiérarchique possède trois couches de base :

- Couche Cœur du réseau
- Couche de Distribution
- Couche d'Accès

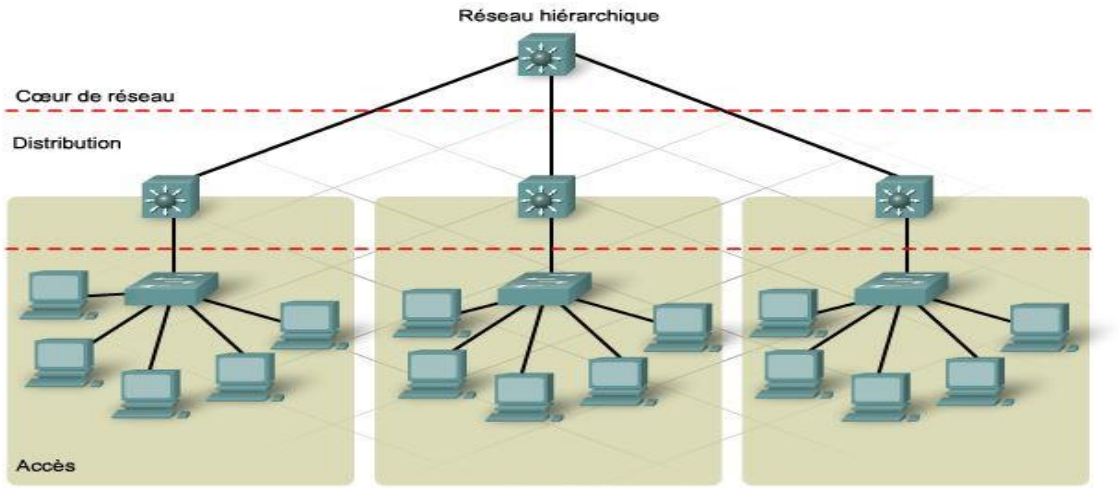


Figure 2.05 : *Réseau hiérarchique*

Cependant, pour assurer les objectifs fondamentaux cités précédemment, le réseau hiérarchique présente plusieurs atouts par rapport au réseau maillé pour la conception d'un réseau flexible et viable.

2.4.2.1 Avantages du réseau hiérarchique

- Evolutivité : possibilité d'une forte croissance du réseau sans effet négatif sur le contrôle et la facilité de gestion. En effet, les fonctionnalités sont localisées et il est plus facile de détecter les problèmes éventuels.
- Facilité de mis en œuvre : celle-ci est due à l'attribution des fonctionnalités précises à chaque couche.
- La facilité de dépannage : on peut isoler les problèmes qui peuvent survenir au réseau puisque ce dernier est modulaire ; il est aussi facile de segmenter temporairement le réseau pour réduire l'étendue du problème.
- La prévisibilité : on peut comprendre et prévoir le comportement d'un réseau utilisant des couches fonctionnelles ; la planification de la capacité de croissance du réseau et la modélisation de ses performances peuvent être simplifiées.
- La prise en charge des protocoles : l'organisation logique de l'infrastructure sous-jacente sur le réseau permet la facilité de combiner les applications et les protocoles actuels et futurs.
- La facilité de gestion

2.4.2.2 Couche Cœur du réseau

Cette couche cœur de réseau appelée aussi réseau fédérateur relie les périphériques de la couche distribution. Les routeurs et les commutateurs de cette couche offrent une connectivité haute vitesse. Elle contient une ou plusieurs liaisons vers les périphériques de la périphérie du réseau pour la prise en charge de l'accès à Internet, aux réseaux privés virtuels (VPN), à l'extranet et au réseau étendu (WAN). Ainsi, on conçoit la couche cœur de réseau afin de transférer efficacement et rapidement des données entre deux sections de réseau ; faciliter la croissance du réseau et sa gestion. Toutefois, elle ne s'occupe pas du filtrage ou de la sécurité et une défaillance au niveau de cette couche entraine un problème de grande échelle au niveau du réseau global.

Les technologies utilisées au niveau de cette couche sont les routeurs ou commutateurs multicouches, la redondance pour la continuité de service en cas de panne, les liaisons de haute

vitesse, les protocoles de routage tels qu'EIGRP et OSPF ayant des fonctionnalités importantes telles qu'une convergence rapide et le partage de charge.

2.4.2.3 Couche Distribution

La couche de distribution est une frontière de routage entre la couche d'accès et la couche cœur de réseau ; c'est aussi le point de connexion entre les sites distants et la couche cœur de réseau. Elle assure le filtrage (ACL ou Access Control List), la gestion de flux de trafic et le routage des VLAN ; elle permet aussi d'isoler la couche cœur de réseau par rapport aux pannes ou interruptions de service au niveau de la couche d'accès.

La couche de distribution est créée à partir des périphériques de couche 3 tels que les routeurs ou les commutateurs multicouches. Ces périphériques gèrent les files d'attente et la hiérarchisation du trafic avant la transmission vers la couche cœur. Ils présentent aussi des liaisons agrégées et redondantes pouvant être configurées pour un équilibrage de charge, augmentant ainsi la bande passante disponible pour les applications. Cette couche est câblée selon une topologie à maillage partielle tout comme la couche cœur de réseau.

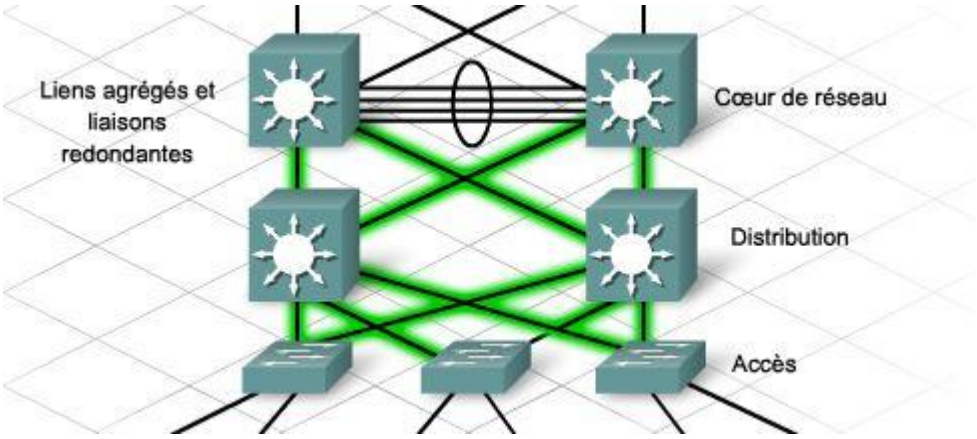


Figure 2.06 : *Topologie à maillage partielle*

2.4.2.4 Couche d'Accès

Cette couche est habituellement un LAN ou un groupe de LAN, de type Ethernet ou Token Ring, qui assure aux utilisateurs un accès de première ligne aux services réseau. C'est au niveau de cette couche que la plupart des hôtes, tels que tous les serveurs et les stations de travail des utilisateurs, sont reliés au réseau. Les services et les périphériques de cette couche sont situés dans chaque bâtiment de campus, chaque site distant et à la périphérie du réseau d'entreprise.

La topologie de la couche d'accès peut être en étoile ou à maillage globale. Elle utilise la technologie de commutation de couche 2. L'accès peut se faire à partir d'une infrastructure câblée permanente ou de points d'accès sans fil.

L'emplacement physique des équipements représente alors l'une des plus grandes préoccupations lors de la conception d'une couche d'accès.

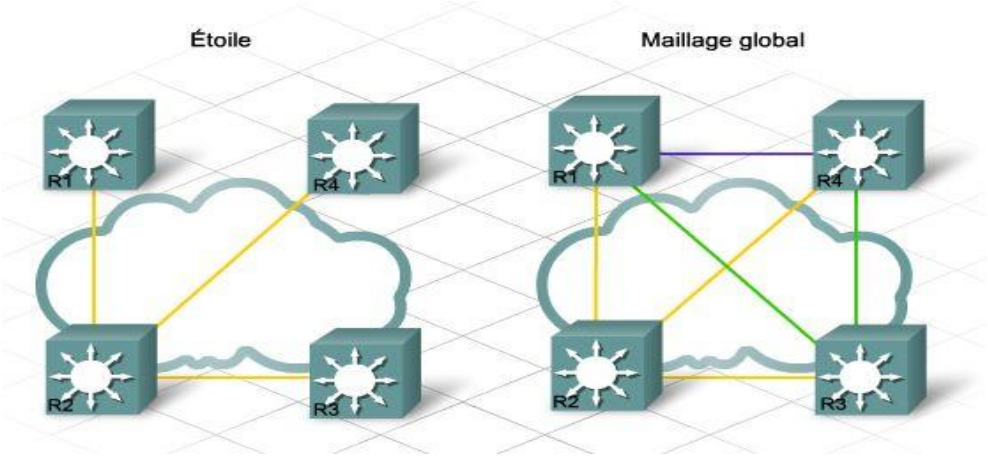


Figure 2.07 : *Exemple de topologie en étoile et à maillage globale*

2.4.3 Méthodologies de conception de réseau

Pour concevoir un réseau d'entreprise de grande envergure, il faut passer par les trois étapes suivantes :

Etape 1 : Identification des besoins du réseau

Etape 2 : Caractéristiques du réseau actuel

Etape 3 : Conception de la topologie et des solutions du réseau

- L'identification des besoins du réseau se résume par la détermination des objectifs commerciaux de l'entreprise qu'il faut atteindre et les spécifications techniques attendues dans la mise en œuvre du réseau
- Les Caractéristiques du réseau actuel : c'est l'étude comparative entre le réseau existant et le nouveau réseau au niveau des équipements et des protocoles.
- La conception de la topologie et des solutions du réseau : utilisation de la stratégie de l'approche descendante qui est une méthode de test de réseau pour prendre en charge des réseaux spécifiques et répondre à des exigences de qualité de service de la part des clients.

Un prototype ou un test de démonstration de faisabilité est effectué à la fin de a conception pour vérifier le bon fonctionnement du nouveau réseau à mettre en place. [5]

2.5 Conclusion

On a vu que tant avec le fonctionnement interne d'un réseau qu'à sa mise en place, l'utilisation d'un concept modulaire ou un système en couches s'avère avantageuse. Le réseau se repose sur un modèle de référence OSI de sept couches, le modèle TCP/IP de quatre couches vient ensuite ; tous deux bien que similaires présentent des différences surtout au niveau des fonctions de chaque couche. Par ailleurs, la mise en œuvre d'un réseau d'entreprise nécessite des exigences et des techniques de conception à prendre en compte.

Dans le chapitre qui va suivre, nous allons nous concentrer sur les concepts de routage d'un réseau afin de mieux comprendre le principe de transmissions des paquets dans un réseau.

CHAPITRE 3
CONCEPT DE ROUTAGE

3.1 Adresse IP

La présence d'une multitude d'équipements terminaux oblige à définir un système d'identification cohérent au sein du réseau pour les différencier : c'est la fonction d'adressage. [6]

Dans un réseau TCP/IP, tous les hôtes connectés possèdent des adresses qui peuvent les identifier au sein du réseau et par les autres réseaux. Pour la communication entre des machines du même réseau, elles utilisent leurs adresses MAC qui sont encapsulées dans l'en-tête et l'en-queue de la trame de la couche liaison de données du modèle OSI. Cette adresse MAC est une adresse physique ; elle est composée de 48 bits représentée par des nombres hexadécimaux. L'adresse MAC unique de chaque machine se trouve sur sa carte réseau.

Tandis que pour faire communiquer deux machines appartenant à deux différents réseaux, on a besoin des adresses IP. C'est une adresse souvent dite logique ; c'est un identifiant unique attribué à chaque interface et associé à une machine (ordinateur, routeur,…). Cette adresse se trouve dans l'en-tête des paquets échangées.

Une adresse IP est composée de 32 bits représentés par 4 octets séparés par des points et notés en décimal.

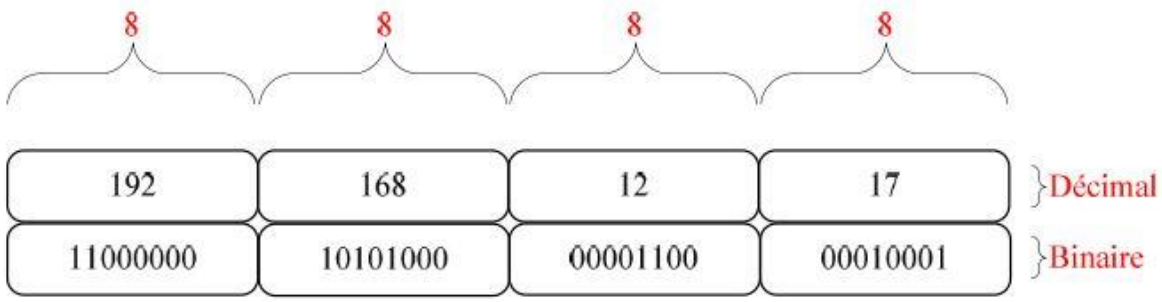


Figure 3.01 : *Exemple d'adresse IP*

Une adresse IP est décomposée en deux parties [7]:

- Une partie qui identifie le réseau dans lequel se trouve l'hôte ; c'est le netID
- Une partie qui identifie le numéro de l'hôte dans le réseau ; c'est le hostID

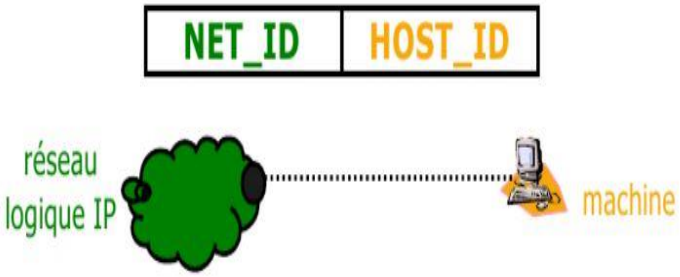


Figure 3.02 : *Les deux parties d'une adresse IP*

Seules les machines appartenant à un même réseau peuvent se communiquer directement, c'est-à-dire ayant le même netID. Dans le cas contraire, elles pourront le faire à partir d'une passerelle qui est souvent un routeur.

Il existe deux versions de l'adresse IP :

- L'IPv4 qui utilise les adresses codées en 32bits comme précédemment permet d'adresser 2^{32} machines soit 4 294 967 296 adresses possibles. Actuellement, cette version n'arrive plus à répondre à l'énorme croissance des hôtes au sein des différents réseaux mais elle reste la plus utilisée.
- L'IPv6 permet de coder les adresses IP en 128 bits sous forme de 8 nombres hexadécimaux séparés de « : ». L'IPv6 permet alors d'adresser 2^{128} machines, c'est une version qui commence à faire son essor pour résoudre le déficit de l'IPv4 et assurer les futurs besoins des nouveaux réseaux.

3.1.1 Format de paquet IP

On sait que les données venant des couches supérieures du modèle OSI subissent une encapsulation en paquet IP dans la couche 3 ou couche réseau. Les adresses IP de la source et de la destination du message à envoyer se trouvent dans l'en-tête de ce paquet IP dont le format est décrit ci-dessous :

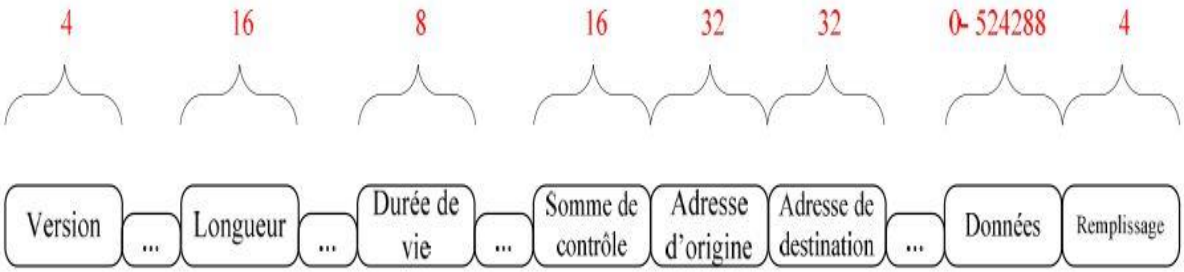


Figure 3.03 : *Format du paquet IP*

Champ	Définition
Version	Indique la version de protocole IP Soit IPv4 soit IPv6
Longueur totale	Indique la longueur totale du paquet IP dont les données et l'en-tête
Durée de vie	C'est un compteur qui décroît par décrémentation. Le paquet est supprimé quand elle atteint 0
Adresse d'origine	Indique l'adresse de l'hôte source ou émetteur
Adresse de destination	Indique l'adresse de l'hôte récepteur
Somme de contrôle	Assure l'intégrité de l'en-tête IP
Données	Contient les informations des couches supérieures (64Ko maximum)
Remplissage	Ajoute des zéros pour que l'en-tête IP soit multiple de 32 bits

Tableau 3.01: ***Champs de paquet IP***

3.1.2 Adresses IP avec classe

On distingue deux types de réseaux qu'on peut adresser en IP [7]:

- Le réseau public Internet où chaque équipement connecté possède une adresse unique et enregistrée au niveau mondial.
- Les réseaux privés dans lesquels le choix des adresses de chaque réseau est libre et que les adresses ne sont uniques que dans ce réseau.

Les adresses IP avec classes concernent les adresses privées. Il existe cinq classes d'adresses IP qui sont attribuées par l'organisme InterNIC (Internet Network Information Center), aujourd'hui remplacé par l'IANA (Internet Assigned Numbers Authority). Ces classes d'adresses se diffèrent par les bits de poids fort qui les composent (ce sont les premiers bits de l'octet le plus à gauche de l'adresse). Pour ne pas confondre les adresses publiques des privées, ces dernières sont résumées avec les plages correspondantes dans le tableau suivant :

Classe	Plage	
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Tableau 3.02: ***Les différentes classes d'adresses IP***

Pour différencier la partie réseau et la partie hôte de l'adresse IP on utilise ce qu'on appelle masque de réseau. Le masque de réseau est de la forme d'une adresse IP mais elle est constituée d'une suite non interrompue de bits 1 suivis de bits 0. A chaque classe correspond alors à un masque de réseau. Dans la classe A, le premier octet à gauche reste constant et les plages 0.0.0.0 et 127.0.0.0 ne sont pas utilisables car la première n'est pas reconnue par le réseau et la deuxième est utilisée pour la boucle locale. Son masque de réseau est 255.0.0.0 ou /8 en notation CIDR et elle est utilisée dans les réseaux de grande taille. Dans la classe B, les deux premiers octets restent inchangés et il a pour masque 255.255.0.0 ou /16; ces adresses sont utilisées dans le cas des réseaux de taille moyenne. Pour la classe C, seul le dernier octet qui varie et son masque de réseau est 255.255.255.0 ou /24; elle permet d'adresser les réseaux de petite taille. Les classes D et E ne possèdent pas de masque de réseau : la classe D est utilisée dans la diffusion multicast et la classe E est encore non utilisée à ce jour mais sert à des fins expérimentales par le groupe IETF (Internet Engineering Task Force).

Dans un réseau, il existe deux adresses particulières et réservées : une adresse réseau dont les bits hôtes sont tous des 0, cette adresse permet d'identifier le réseau lui-même ; une adresse de broadcast, dont les bits hôtes sont tous des 1, permet de diffuser les paquets à toutes les adresses des équipements.

3.1.3 Sous réseaux et masques de sous réseau

Afin d'améliorer la capacité et mieux gérer le trafic, maîtriser l'adressage au sein du réseau et assurer sa sécurité, il est possible de subdiviser les grands réseaux en plusieurs segments ou sous-réseaux de petites tailles.

Le principe de création des sous-réseaux est le suivant : emprunter des bits à la partie hôte de l'adresse IP; la partie hôte originale est alors divisée en deux pour avoir le champ de sous-réseau (subnetID) et la nouvelle partie machine (hôte). Le nombre minimal de bits à emprunter est deux et le nombre maximal est le nombre restant en laissant 2 bits à la partie hôte.

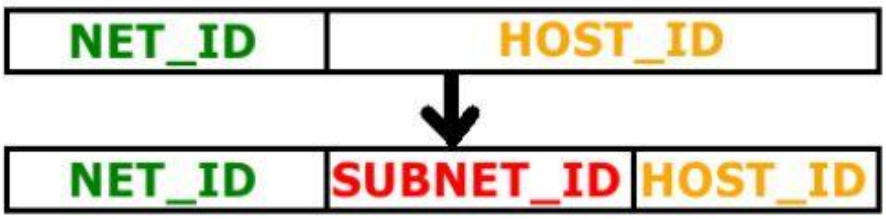


Figure 3.04 : *Création de sous-réseaux*

De la même façon que pour un réseau entier, le découpage en sous-réseaux nécessite l'utilisation de masques de sous-réseaux. Le masque de sous réseau englobe alors la partie netID initiale et la partie subnetID.

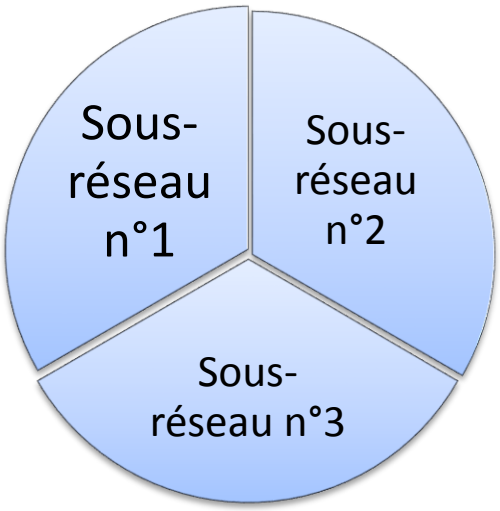


Figure 3.05 : *Un réseau divisé en 3 sous-réseaux*

Cependant, il faut noter que le mécanisme de la création de sous-réseaux entraine une perte d'adresses. En effet, il faut suivre les règles suivantes : [8]

- Règle du 2^n-2 : ne pas utiliser le premier et le dernier sous-réseau (RFC 950)
- Règle du 2^n-1 : ne pas utiliser le premier sous-réseau car l'adresse du premier sous-réseau correspond à l'adresse réseau de la plage réseau toute entière (RFC 1878)
- Règle du 2^n : utiliser tous les sous-réseaux (RFC 1878)

L'application d'une règle par rapport à une autre dépend des capacités techniques des équipements. L'important à retenir est qu'à chaque sous-réseau créé, il existe toujours l'adresse réseau et l'adresse broadcast à ne pas utiliser et même le premier sous-réseau et le dernier sous-réseau eux-mêmes sont inutilisables. On a alors un grand gaspillage d'adresses.

3.1.4 Adresses IP sans classe – CIDR et VLSM

On sait que pour pouvoir accéder à Internet un équipement d'une entreprise a besoin d'une adresse publique, les adresses privées, quant à elles, sont affectées aux autres machines afin de pouvoir se communiquer de façon interne. Les adresses publiques sont attribuées par un FAI (Fournisseur d'Accès Internet).

Pour résoudre la pénurie en adresses publiques due à l'évolution exponentielle de l'Internet et au découpage fixe de l'espace d'adressage d'IPv4 (notion de classe), à part l'élaboration de la nouvelle version IPv6 des adresses IP, on utilise l'adressage sans classe (classless) qui permet d'envoyer le masque de sous-réseau utilisé sur les autres équipements afin de créer des sous-réseaux de tailles différentes.

Le CIDR (Classless Inter Domain Routing) et le VLSM (Variable Length Subnet Masks) sont deux procédures différentes mais complémentaires de l'adressage classless. Le VLSM permet de résoudre le problème de gaspillage d'adresses au sein d'une entreprise à partir des masques de sous-réseaux de tailles variables ; le CIDR permet de réduire les nombreuses entrées des tables de routage (qu'on va expliquer ultérieurement), dues aux différents sous-réseaux à gérer, en utilisant des agrégations des routes.

Le principe d'agrégation de routes se fait en conservant la partie réseau en commun de toutes les adresses des sous-réseaux à combiner et en remplaçant par 0 les bits restants ; on obtient ainsi l'adresse agrégée et le nouveau masque de sous-réseau à utiliser dans la table de routage. C'est la notion de résumé de routes ou supernetting.

Le VLSM quant à lui permet de subdiviser une adresse déjà divisée en sous réseaux. Il repose aussi sur le principe d'agrégation. En général, on décompose alors l'adresse de classe C en plusieurs sous-réseaux de tailles variables : de grands sous-réseaux pour les LAN et de très petits pour les liaisons WAN.

3.1.5 NAT

Une machine à l'intérieur d'un réseau ne peut pas accéder au réseau externe ou Internet à partir de son adresse privée. Il lui faut l'adresse publique de l'entreprise attribuée par le FAI. Le NAT (Network Address Translation) ou translation d'adresses permet alors de translater les adresses privées en adresse publique routable sur Internet. Cette translation se fait sur les routeurs de bordures d'une entreprise connectée à Internet.

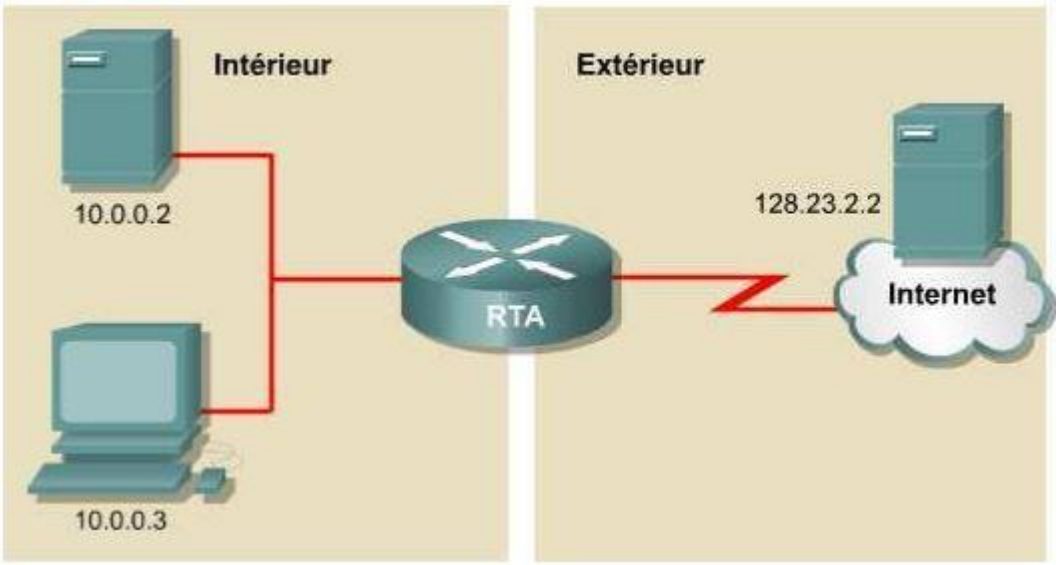


Figure 3.06 : *Communication d'un réseau interne et un réseau externe par le NAT*

On a alors une adresse locale interne (attribuée à un hôte du réseau interne), une adresse globale interne (adresse privée attribuée par l'InterNIC ou un FAI et qui représente le réseau pour l'extérieur), une adresse locale externe et une adresse globale externe (ces deux dernières reflètent la même chose qui est l'adresse attribuée à un hôte du réseau externe). [10]

La traduction NAT peut se faire de manière statique ou dynamique :

- Pour le NAT statique, chaque adresse privée est translatée en une même et unique adresse publique.
- Pour le NAT dynamique, on translate une adresse privée en une adresse publique appartenant à un pool d'adresses ; l'adresse IP publique utilisée n'est donc pas toujours la même.

Cependant, il existe aussi ce qu'on appelle PAT (Port Address Translation) qui permet de translater plusieurs adresses privées en une seule adresse publique. Chaque hôte est différencié à partir du numéro de port qui lui est attribué quand il veut se communiquer.

Le NAT et le PAT permettent alors la sécurisation du réseau car les données et les équipements qui s'y trouvent ne sont pas accessibles depuis l'extérieur.

3.2 Principes fondamentaux du routage

3.2.1 Routeur et routage

Dans le modèle OSI, c'est la couche réseau qui assure l'adressage et c'est le domaine de routage. Le routage aussi appelé commutation de paquet permet de sélectionner le meilleur chemin pour envoyer les paquets. Cette fonction est assurée par le routeur.

Le routeur est un ordinateur comme un autre possédant un système d'exploitation appelé IOS (Internetwork Operating System), un processeur, une mémoire vive RAM utilisant la configuration courante du routeur, une mémoire non volatile NVRAM, une mémoire morte ROM, un flash ou mémoire de stockage principale du routeur. Il possède aussi plusieurs types de connectiques tels que des interfaces LAN, des interfaces WAN, un port console, un port auxiliaire, des slots NM (Network module) et des slots WIC (WAN Interface Card).

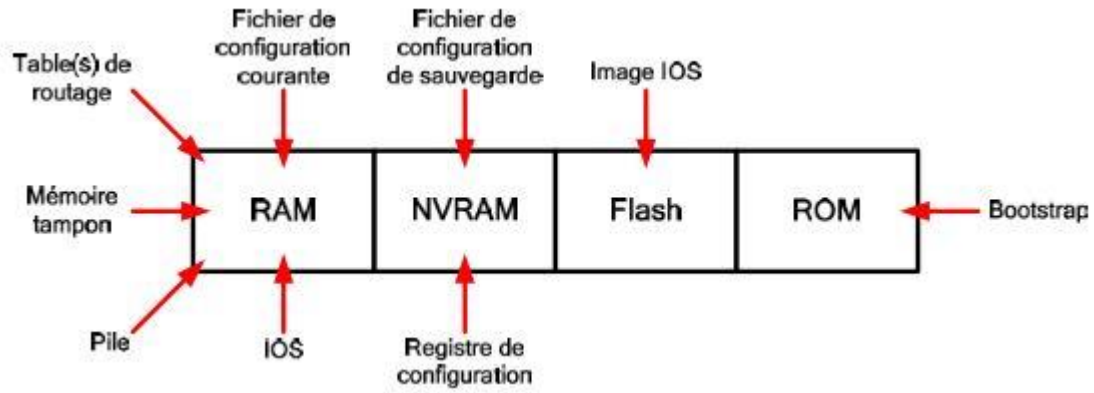


Figure 3.07 : *Les types de mémoire dans un routeur*

Pour permettre la transmission des paquets entre une source et un destinataire, le routeur utilise les adresses IP de ces derniers et assure les deux fonctions principales suivantes :

- La fonction de détermination de chemin
- La fonction de commutation

La fonction de détermination de chemin est le processus avec lequel le routeur trouve le meilleur chemin pour envoyer les paquets. Pour cela il consulte sa table de routage pour rechercher l'adresse réseau correspondant à l'adresse IP de destination. A la fin de cette fonction on peut avoir un réseau directement connecté à l'un des interfaces du routeur, un réseau distant, ou aucune route lorsque l'adresse de destination ne correspond à aucune entrée de la table de routage. Le routeur prend en compte des métriques pour qualifier un chemin par rapport un autre afin de décider le plus optimal. Ce sont le nombre de sauts (nombre de routeurs traversés par le paquet avant d'arriver à destination),

la bande passante (qui varie selon le média utilisé), le délai (le temps requis pour acheminer un paquet de la source à la destination), la charge (la quantité de trafic sur une ressource réseau : routeur ou liaison), le coût (basé sur une dépense monétaire attribuée à un lien par un administrateur réseau)…

La fonction de commutation est le processus pour lequel le routeur accepte un paquet à son interface d'entrée et le transfère à une autre interface, interface de sortie qu'il a déterminée par la détermination de chemin précédemment. Avant d'envoyer le paquet à sa destination, le routeur le ré-encapsule dans une trame de liaison de données appropriée à l'interface de sortie (qui peut être une interface FastEthernet ou une interface série).

Ces deux fonctions sont alors complémentaires. Le routeur agit au niveau des couches 1, 2 et 3 du modèle OSI jusqu'à ce que le paquet arrive à sa destination finale.

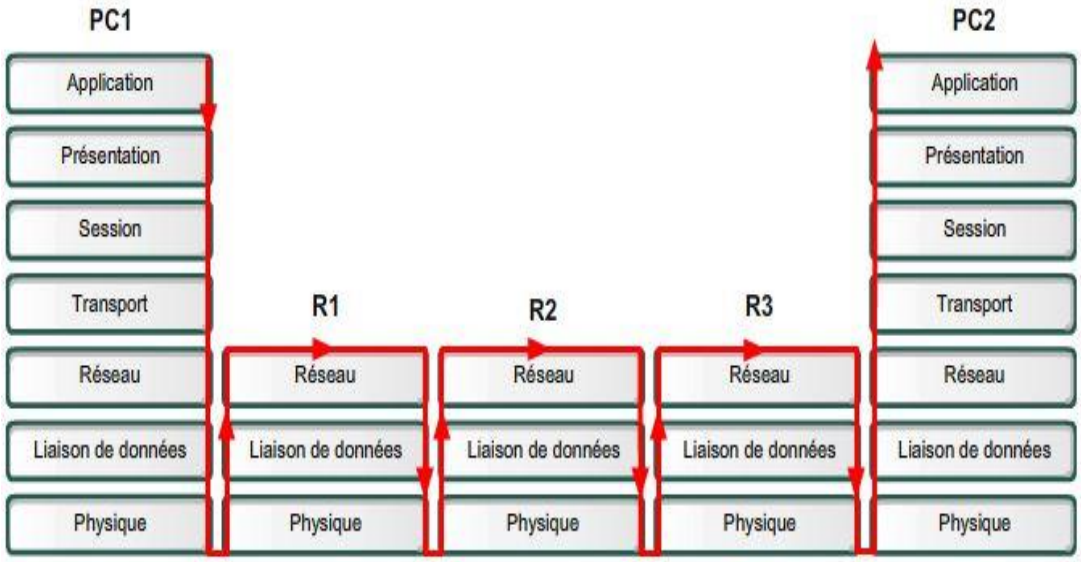


Figure 3.08 : *Commutation de paquets après détermination de chemin*

3.2.2 Table de routage

La table de routage est l'élément central du routeur. D'après ce qu'on a dit précédemment, il doit consulter sa table de routage pour déterminer le meilleur chemin ; de plus, les routeurs s'échangent les informations de leurs tables de routages pour assurer leur communication.

La table de routage est un fichier de données contenu dans la mémoire vive du routeur. Elle contient toutes les routes menant aux différents réseaux que ceux soient distants ou directement connectés au routeur. La table de routage peut être complétée manuellement ou dynamiquement. Les réseaux directement connectés sont entrés dans la table de routage en configurant les interfaces du routeur

par des adresses IP appartenant à différents réseaux. Le routeur ne peut accéder aux réseaux distants que si sa table de routage ne contienne d'abord des réseaux directement connectés.
La table de routage contient les champs suivants :

- La destination : adresse du réseau de destination associé à un prochain saut
- Le moyen d'apprentissage : qui identifie le type de protocole de routage qui a créé chaque entrée.
- Les associations du saut suivant : indiquent au routeur que la destination lui est directement connectée ou qu'elle peut être atteinte via un autre routeur (appelé saut ou tronçon suivant), il y a l'adresse IP du prochain routeur.
- L'interface de sortie : désigne l'interface par laquelle les données doivent être envoyées pour atteindre la destination finale
- La métrique de routage : dépend du protocole de routage utilisé ; plus la métrique est petite, plus le chemin est meilleur.
- La distance administrative : indique l'ordre de préférence entre les protocoles de routages attribués à une même entrée ; plus sa valeur est petite, plus le protocole est considéré comme prioritaire.

3.2.2.1 Protocole routé – Protocole de routage

Un protocole routé est un protocole de couche de niveau 3 (couche réseau) qui permet de transmettre des données entre les nœuds des différents réseaux par le biais d'un routeur. Un protocole routé est routable lorsqu'il permet d'attribuer un numéro de réseau et un numéro d'hôte à chaque machine. Exemple : IP (Internet Protocol), IPX (Internetwork Packet eXchange).
Un protocole de routage permet au routeur de choisir le meilleur chemin possible pour acheminer les données de la source vers la destination; il permet donc au routeur d'acheminer les protocoles routés. Exemple, pour le protocole routé IP on a les protocoles de routages RIP, IGRP, EIGRP, OSPF…

3.2.2.2 Routage statique – Routage dynamique

Les réseaux distants peuvent être introduits dans la table de routage soit par le routage statique soit par le routage dynamique.
Le routage statique définit une route permettant d'atteindre une destination. Il est effectué par l'administrateur de réseau. Le routage statique est surtout utilisé dans le cas où le nombre de routeurs

n’est pas considérable, ou lors d’un routage vers un réseau d’extrémité accessible par une seule route. On utilise la commande « ip route » pour la configuration d’une route statique. L’administrateur réseau doit alors mettre à jour manuellement la table de routage à chaque modification de topologie du réseau.

Le routage dynamique utilise les protocoles de routage pour faire connaître au routeur toutes les informations concernant les autres réseaux distants. Les protocoles utilisent les différentes métriques pour déterminer la meilleure route vers une destination donnée. Le routage dynamique présente un avantage dans sa mise à jour automatique à chaque modification de la topologie du réseau.

La plupart des tables de routage contiennent à la fois des routes statiques et des routes dynamiques.

3.2.2.3 Principes de la table de routage

Le fonctionnement de la table de routage se repose sur les trois principes suivants : [9]

- Chaque routeur prend, seul, sa décision en se basant sur les informations disponibles dans sa table de routage.
- Les informations dans la table de routage d’un routeur ne sont pas toutes informées aux autres routeurs
- L’information de routage liée à un chemin menant d’un réseau à un autre ne fournit pas d’information de routage pour le chemin inverse.

3.3 Familles de protocoles de routages dynamiques

Les protocoles de routage permettent aux routeurs de gérer et de mettre à jour automatiquement leurs tables de routage. Si plusieurs chemins existent pour atteindre une destination précise, ils choisissent le plus optimal tout en mettant en réserve un autre meilleur chemin en cas d’indisponibilité du premier.

Il existe deux familles de protocoles de routage dynamique :

- L’IGP ou Interior Gateway Protocol
- L’EGP ou Exterior Gateway Protocol

Un système autonome est un ensemble de réseaux gérés par un administrateur commun et qui suit les même règles de routage, c’est-à-dire qu’il y a partage d’une stratégie de routage commune. Un numéro d’identification est attribué à chaque système autonome par l’InterNIC afin de l’identifier

parmi le reste du monde. C'est un numéro de 16 bits que certains protocoles de routage utilisent pour fonctionner.

L'IGP permet d'acheminer les données à l'intérieur d'un système autonome tandis que l'EGP permet de router les données entre différents systèmes autonomes contrôlés par des administrateurs différents.

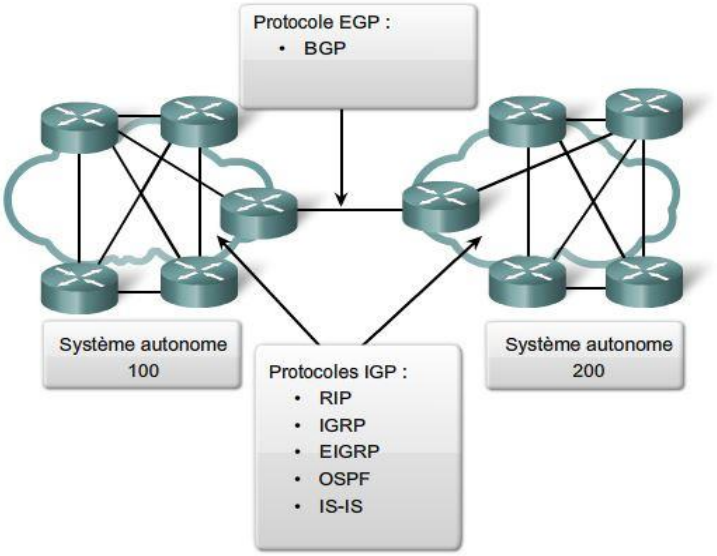


Figure 3.09 : *IGP et EGP*

3.3.1 IGP (Interior Gateway Protocol)

Les protocoles de routages intérieurs considèrent le système autonome comme un seul et unique protocole de routage, tout protocole différent qui s'y trouve est alors considéré comme externe. Cependant, l'IGP est aussi classé en :

- Protocole à vecteur de distance : qui détermine la direction et la distance vers n'importe quelle liaison de l'inter-réseau; il utilise l'algorithme de Bellman-Ford pour transmettre régulièrement les copies de tables de routage d'un routeur à l'autre. La mise à jour est de manière périodique.
- Protocole à état de lien (ou à état de liaison) : qui permet de refaire la topologie exacte du réseau et de trouver le chemin le plus court en utilisant l'algorithme de Dijkstra. Sa réponse est plus rapide car la mise à jour se fait seulement en cas de modification du réseau.

3.3.1.1 RIP

Le RIP ou Routing Information Protocol est un protocole de routage interne à vecteur de distance. La métrique utilisée pour déterminer le meilleur chemin est le nombre de sauts, c'est-à-dire le

nombre de routeurs que le paquet doit traverser avant d'arriver à la destination finale. Le nombre de sauts maximal avant que le paquet soit éliminer est 15. Les mises à jour de routage se font tous les 30 secondes. Il existe deux versions de RIP : le RIPv1 et RIPv2.

RIPv1	**RIPv2**
Facile à configurer	
Utilisation de protocole de routage par classe (classful)	Utilisation de protocole de routage CIDR (classless)
Les mises à jour se font par broadcast	Les mises à jour se font par multicast sur 224.0.0.9
Aucune information sur les sous-réseaux dans la mise à jour	Masques de sous-réseaux envoyés avec la mise à jour
Aucune authentification	Authentification des voisins dans les mises à jour
Utilisation d'un même masque de sous-réseau	Support du VLSM

Tableau 3.03: *Comparaison entre RIPv1 et RIPv2*

Malgré ses avantages, RIP présente un temps de convergence lent et l'utilisation du nombre de sauts comme métrique n'est pas très efficace pour choisir le meilleur chemin ; de plus ce nombre de sauts est limité à 15. Il faut noter que la distance administrative de RIP est de 120.

3.3.1.2 IGRP et EIGRP

L'IGRP (Interior Gateway Routing Protocol) et EIGRP (Enhanced IGRP) sont des protocoles de routage à vecteur de distance développés par Cisco. EIGRP est une version améliorée d'IGRP mais les deux protocoles sont compatibles.

	IGRP	**EIGRP**
Classe de Protocole	A vecteur de distance	A vecteur de distance mais à état de lien lors de la mise à jour
Nombre maximum de sauts	255	224

	IGRP	EIGRP
Métriques utilisées	Bande passante, fiabilité, délai, charge ; 24bits	Métriques composites ; 32 bits
Mise à jour	Toutes les 90s de façon multicast	Lors modification du réseau de façon multicast
Distance administrative	100	90
Bande passante	Consommation de la bande passante	Moins de bande passante utilisée
Spécificités		Support du CIDR et VLSM
		Découverte des voisins

Tableau 3.04: *IGRP et EIGRP*

3.3.1.3 OSPF

L'OSPF ou Open Shortest Path First est un protocole de routage à état de lien et c'est le plus répandu parmi les IGP. Il permet la connaissance exacte de la topologie du réseau avec découverte des voisins. La métrique utilisée pour la sélection de la meilleure route est la bande passante des liaisons. Plus la bande passante est grande plus le chemin est optimal. La mise à jour de routage ne se fait qu'à chaque modification topologique du réseau à partir d'une adresse multicast diminuant ainsi l'utilisation de la bande passante. C'est aussi un protocole de routage classless supportant le VLSM dont le domaine est dépourvu de boucle de routage. Sa distance administrative est de 110.

3.3.2 EGP (Exterior Gateway Protocol) et le BGP

La famille de protocole de routage externe ou BGP se résume à un seul protocole qui est le BGP ou Border Gateway Protocol. C'est un protocole qui permet alors d'acheminer des trafics Internet entre systèmes autonomes. Il est utilisé pour la connexion entre FAI (Fournisseur d'accès à Internet) ou entre un FAI et ses clients.

3.4 Conclusion

Le principe de routage se repose sur l'adressage IP. Ainsi, une bonne gestion et connaissance des adresses IP attribués aux stations du réseau devient indispensable. Les adresses avec classe sont délaissées à l'avenue des adresses sans classes qui réduisent le gaspillage d'adresses et améliorent

les fonctionnalités des routeurs. La table de routage est l'outil nécessaire pour assurer l'acheminement d'un paquet d'une source à l'autre. Ses informations sont obtenues de manière statique par l'intermédiaire direct de l'administrateur réseau ou dynamique par le biais des différents protocoles de routages.

Dans le quatrième chapitre, nous allons voir les technologies qu'on peut utiliser si on veut interconnecter les sites distants d'une même entreprise avec la notion de réseau de transport.

CHAPITRE 4
RESEAUX DE TRANSPORT

4.1 Introduction aux réseaux étendus

Dans le cadre professionnel, les réseaux LAN semblent ne pas satisfaire les besoins des entreprises ; ceci dû à leurs faibles portées, géographiquement parlant. En effet, les réseaux d'une entreprise peuvent s'étendre suivant le développement de son activité ; des implantations de succursales ou de filiales dans d'autres régions voire même dans d'autres pays sont possibles. C'est là qu'intervient le réseau étendu ou WAN. D'après ses caractéristiques, il permet d'interconnecter des réseaux LAN distants. Pour ce faire, le WAN utilise plusieurs technologies à l'instar des services d'opérateurs télécom : les fournisseurs de réseaux, les compagnies téléphoniques, les systèmes satellites ou des câbles.

Un réseau étendu est un réseau de communication de données dont les trafics sont de différents types : la voix, les images, les vidéos et les données. Il fonctionne au niveau de la couche physique et de la couche de liaison de données du modèle de référence OSI. Les fonctions de ces deux couches sont différentes pour un réseau LAN et pour un réseau WAN.

Pour le WAN, les protocoles de couche physique permettent de décrire les moyens de connexions électriques, mécaniques et fonctionnelles pour les services WAN ; les protocoles de la couche liaison de données décrivent la manière dont les trames sont encapsulées puis transmises à une destination distante.

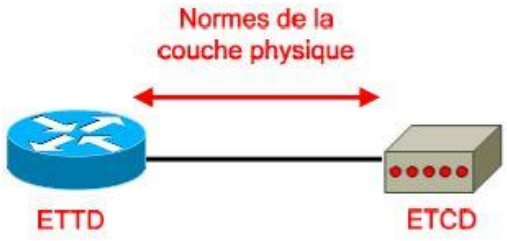


Figure 4.01 : *Norme de la couche physique WAN*

Figure 4.02 : *Norme de la couche liaison de données*

Les services d'opérateurs télécom permettent la communication bout à bout entre deux équipements en utilisant des différents types de services:

- Services à commutation de circuits
- Services à commutation de paquets
- Services à commutation de cellules
- Services dédiés

4.1.1 Equipements WAN

Les normes de la couche physique décrivent les équipements fournissant les données de l'utilisateur appelés ETTD (Equipement terminal de traitement de données) et les équipements ETCD (Equipement de terminaison de circuit de données) qui convertissent les données de l'utilisateur en un format adapté aux unités de service réseau WAN. L'ETCD sert donc d'interface entre l'ETTD et la liaison de communication WAN.

Les équipements WAN sont représentés par la figure suivante :

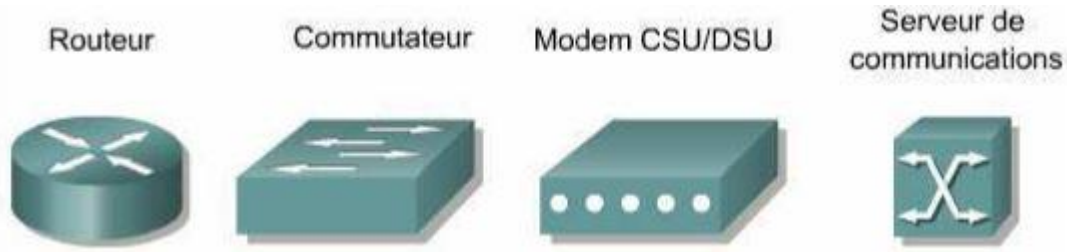


Figure 4.03 : *Les équipements WAN*

- Routeur : dispositif de routage possédant d'interfaces LAN et WAN permettent l'interconnexion de LAN avec les réseaux étendus ; il est utilisé en tant que ETTD.
- Commutateur WAN: dispositif de couche 2 multiports, présent au cœur du réseau WAN et assurant les commutations du trafic.
- Modem : dispositif de couche 1 permettant la conversion d'un signal numérique en un signal analogique par le principe de modulation/démodulation. Il adapte ainsi le signal au format désiré de chaque côté de la liaison WAN. Il est utilisé en tant qu'ETCD, on peut aussi trouver l'unité CSU/DSU (Circuit Service Unit/Data Service Unit).
- Serveur de communication : un concentrateur des communications des utilisateurs entrantes et sortantes.

4.1.2 Différentes technologies WAN

Les différents types de réseau WAN avec les différentes options de connexions de liaisons sont résumés ci-dessous :

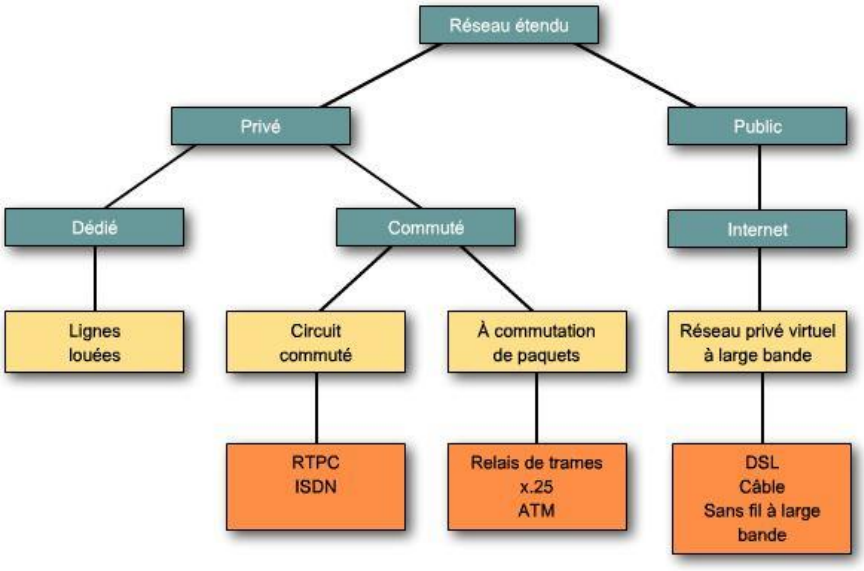


Figure 4.04 : *Les technoloogies WAN*

4.1.2.1 Commutation de circuits

C'est une commutation physique qui consiste à mettre bout à bout des tronçons de lignes de transmissions pour relier deux correspondants distants. C'est la commutation utilisée dans les réseaux téléphoniques.

Elle établit de façon dynamique une connexion virtuelle dédiée pour la voix ou les données et elle est effectuée dans les centraux téléphoniques. La liaison se fait de manière non permanente mais assure une bande passante maximale pendant la durée de la communication.

Le RTPC (Réseau Téléphonique Public Commuté) et le RNIS (Réseau Numérique à Intégration de Services) sont des exemples de commutation de circuits.

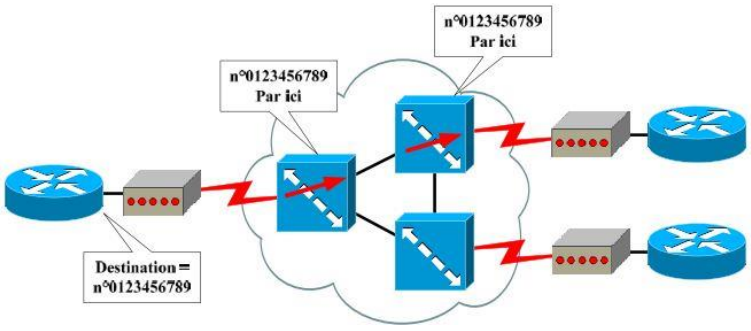


Figure 4.05 : *Exemple de commutation de circuits*

4.1.2.2 Commutation de paquets

C'est une commutation logique qui consiste à découper l'information initiale en plusieurs parties appelées paquets. Ces paquets vont ensuite transiter dans le réseau en empruntant des différents chemins selon la disponibilité des nœuds du réseau. Ces paquets sont libellés afin que le récepteur puisse les restituer. La taille des paquets dépend de la capacité d'acheminement des nœuds, cette capacité est appelée MTU (Maximum Transmission Unit) ou Unité de transfert maximal. C'est donc la taille maximale d'un paquet pouvant être transmis en une seule fois sur une interface. La bande passante est partagée entre les différents trafics de façon permanente.
Le Frame Relay ou relais de trame et le X.25 sont des exemples de ce type de commutation.

4.1.2.3 Commutation de cellules

C'est une commutation de paquets particulière. Le principe est le même que celui de la commutation de paquets, elle se diffère seulement de la taille de paquets qui reste fixe et porte le nom de cellules. L'ATM (Asynchronous Transfer Mode) est l'exemple de cette commutation. Dans le réseau ATM, la taille des cellules est de 53 octets permettant ainsi d'avoir des débits élevés.

4.1.2.4 Services dédiés

Ce type de service offre un lien physique dédié entre chaque source et destination. Le nombre de liens augmente donc en fonction du nombre d'utilisateurs à interconnecter. Les fournisseurs de services offrent ainsi à ses clients des lignes louées appelées aussi lignes spécialisées. On peut citer des exemples tels que les technologies xDSL (x désigne la famille et DSL Digital Subscriber Line), T1, T3, E1 et E3.
Notons qu'il existe aussi d'autres services qui font intervenir les systèmes satellites, le modem câble et le sans fil qui servent surtout à la connexion à Internet.

4.2 Réseaux de transport

Les services qu'on vient de citer ci-dessus permettant au réseau étendu d'interconnecter les réseaux LAN sont appelés réseaux de transport. Un réseau de transport correspond alors aux couches physique (niveau 1) et logique (niveau 2). On trouve les lignes spécialisées LS, l'ATM et le Frame Relay.

A l'inverse d'un LAN sur lequel nous pouvons réaliser des excès de vitesse gratuitement jusqu'au Gigabit, la vitesse est limitée à quelques dizaines de Mbps sur les réseaux WAN. Et plus nous allons vite et loin, plus c'est cher.

Le choix de l'une des trois technologies qui s'offrent à nous se fera en fonction de nos besoins, de l'offre du marché et du coût, que ce soit dans le cadre d'une solution privée ou opérateur.

Pour une interconnexion de réseaux locaux, la LS est la solution la plus adéquate ; sa limite est une distance allant jusqu'à 100 km au maximum.

A partir d'un certain nombre de sites (une dizaine) et au-delà d'une distance de 100km, la solution opérateur reposant sur un réseau Frame Relay ou ATM devient plus rentable. [12]

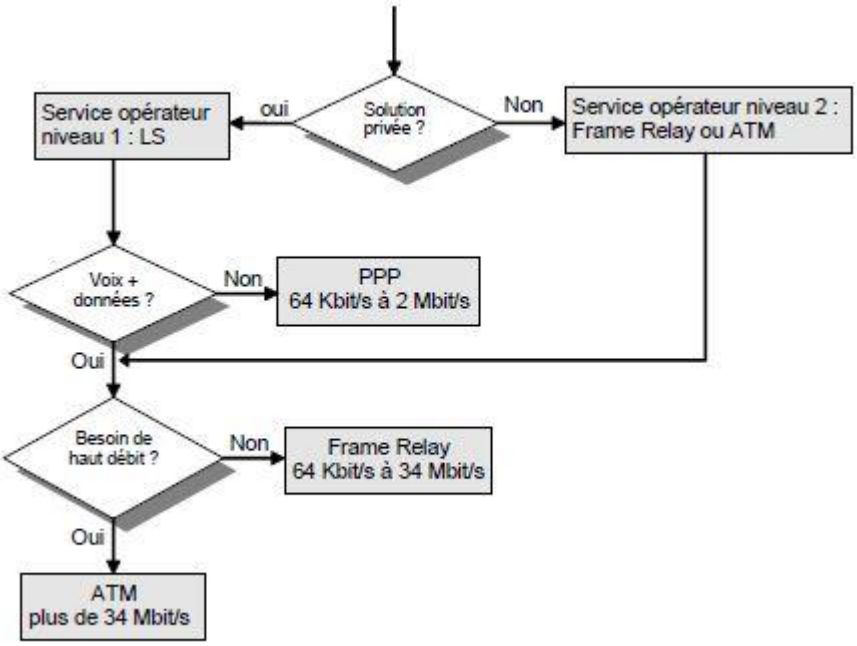


Figure 4.06 : *Choix de technlogie selon les besoins*

Un accès Frame Relay revient cependant moins cher par rapport à celui d'ATM. Les opérateurs réservent donc ce dernier pour des accès à haut débit (34Mbps et plus) et limitent les accès Frame Relay à 34Mbps (45Mbps au maximum).

Critère	Frame Relay	ATM
Débit	De 64 Kbps à 45 Mbps	A partir de 34 Mbps
Qualité de service	Gestion de congestion, débit garanti	Gestion de congestion, débit garanti, trafic synchrone, priorités

Critère	Frame Relay	ATM
Réseau	WAN	LAN, WAN
Application	Voix et données	Voix, données et vidéo
DSU	FRAD (Frame Relay Access Device)	DXI ou ATM
Overhead pour un MTU de 1500 octets	0.5 %	10.4 % au minimum
Adressage	Local (DLCI)	Local (VPI/VCI)

Tableau 4.01: *Comparaison entre Frame Relay et ATM*

Dans ce travail, nous allons nous intéresser au Frame Relay qui est un des services le plus utilisé des entreprises pour l'interconnexion de leurs sites.

4.2.1 Circuits virtuels

La transmission à travers les couches peut se faire par deux modes : le mode non connecté ou sans connexion et le mode connecté ou orienté connexion.

Dans le mode sans connexion, les paquets sont transmis à tout moment sans se soucier de l'état du destinataire : s'il est présent ou non. Tous les paquets doivent contenir l'adresse de destination.

Pour le mode connecté ou orienté connexion, trois procédures doivent être effectuées :

- D'abord, il y a l'établissement de la connexion ou ouverture de la connexion pour savoir à quelle destination on va dialoguer
- Il y a ensuite l'établissement d'un lien logique entre les deux équipements terminaux constituant le tube de dialogue appelé *circuit virtuel* assurant le transfert des données. La communication n'est active que si le destinataire accepte la communication. [6]
- Pour terminer la communication, il y a libération de la connexion par l'un des utilisateurs.

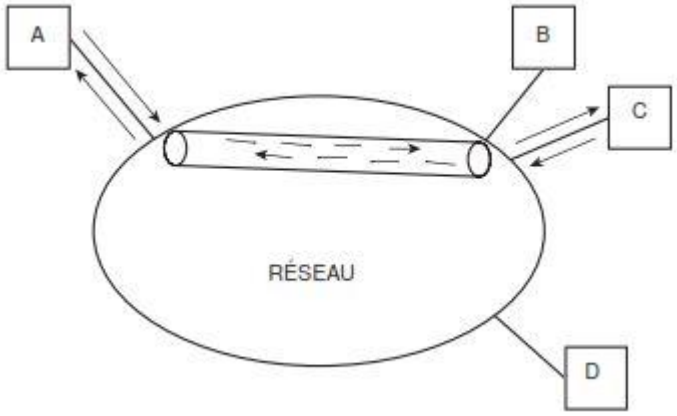


Figure 4.07 : *Transmission en mode connecté le long d'un circuit virtuel*

Le circuit est dit virtuel car le chemin n'est pas physique, c'est-à-dire qu'il n'y a pas de liaisons électriques directes entre les deux extrémités. Le chemin est défini à travers des équipements tels que les commutateurs et les routeurs. Le circuit virtuel permet une communication bidirectionnelle entre les terminaux.

Il existe deux types de circuit virtuel :

- Le circuit virtuel commuté CVC (SVC ou Switched Virtual Circuit) qui est établi dynamiquement sur demande et il est fermé après la transmission. Les trois phases de connexion précédentes sont établies grâce à des messages de signalisation au réseau, celles-ci consomment ainsi de la bande passante. Le coût dépend de la durée de la communication.
- Le circuit virtuel permanent CVP (PVC ou Permanent Virtual Circuit) qui est établi de façon permanente. La première et dernière étape de connexion n'existe plus, seule la phase de transfert de données est établie. La consommation en bande passante est moins élevée que celle de SVC mais le coût augmente à cause de la continuité de services. Le PVC est aussi appelé circuit virtuel privé.

4.2.2 Concept du Frame Relay

Le Frame Relay est un réseau de transport permettant d'interconnecter des réseaux locaux distants à partir des circuits virtuels, généralement, permanents. C'est aussi un protocole qui permet de combiner les fonctions des couches liaisons de données et réseau. En effet, en tant que protocole de couche 2, il permet l'encapsulation des trames avec détection d'erreur standard (le CRC ou Cyclic Redundancy Check); en tant que protocole de couche 3, il fournit plusieurs liaisons logiques sur un

même circuit physique et permet au réseau d'acheminer les données sur ces liaisons jusqu'à leurs destinations respectives. Ceci offre une efficacité en volume et en vitesse. [16]

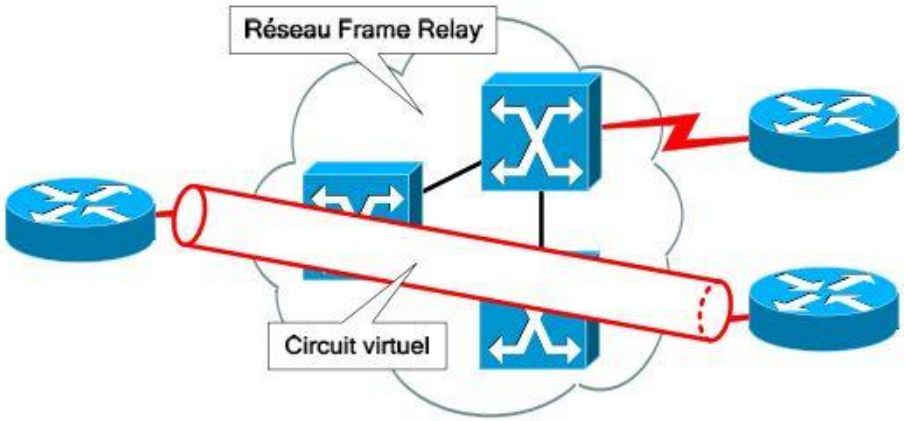


Figure 4.08 : *Réseau Frame Relay*

Le Frame Relay est une technologie similaire à X.25, mais contrairement à ce dernier il ne fournit pas de correction d'erreur et a un très faible contrôle de débit. On l'appelle aussi X.25 allégé. L'en-tête de la trame de Frame Relay est très faible. Il présente ainsi un meilleur temps de traitement car il y a moins de fonctionnalités.

Toute correction d'erreur, telle que la retransmission des données, est à la charge des composants d'extrémité. En cas d'erreur, le nœud Frame Relay abandonne tout simplement le paquet. Frame Relay n'envoie aucun avertissement à la source en cas d'abandon de trame.

4.2.2.1 Principe

Le Frame Relay est un service de télécom présentant plusieurs avantages comme son prix rentable, sa flexibilité, sa bande passante, sa fiabilité, sa facilité de mise en œuvre par rapport aux lignes privées ou louées. Il permet d'atteindre un débit allant de 64Kbps jusqu'à 34 Mbps voire même 45Mbps. [12]

Le terme circuit virtuel, ici un PVC, désigne alors la connexion entre deux ETTD par un réseau Frame Relay.

La bande passante est partagée entre les utilisateurs. Le circuit physique peut supporter plusieurs liaisons logiques pour atteindre une destination.

A chaque PVC correspond à un débit minimal de données garanti appelé CIR (Committed Information Rate) ; au-delà de ce débit, le bit DE (Discard Eligibility) contenu dans les trames en dépassement est positionné à «1 » ce qui signifie que ces trames seront détruites en cas de congestion

du réseau. Il existe aussi un débit maximal au-dessus duquel toute information est éliminée évitant ainsi la congestion du réseau. Ce débit maximal est l'EIR (Excess Information Rate).

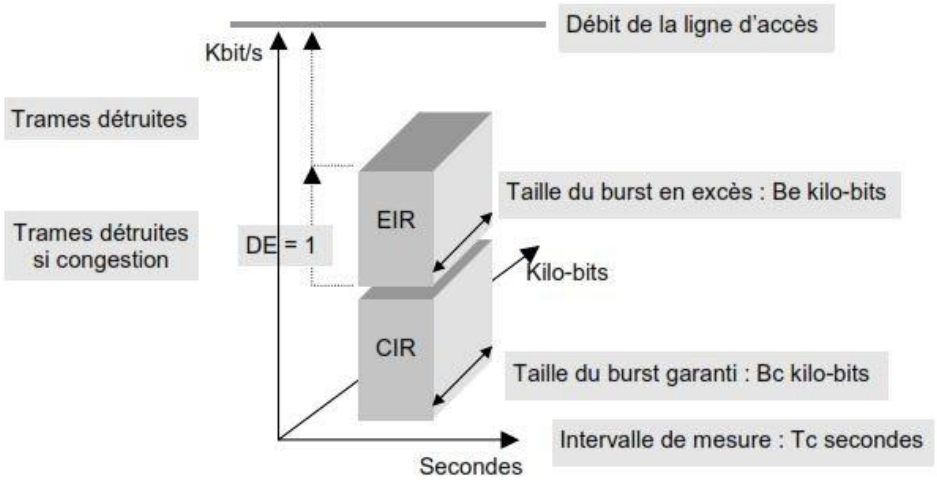


Figure 4.09 : *Qualité de service de Frame Relay*

L'AIR (ou Allowed Information Rate = CIR + EIR) ne dépasse pas le débit de la liaison de données. Le débit des liaisons internes au réseau peut être inférieur à la somme des AIR des clients.

Cependant, le débit de CIR associé à chaque PVC est déterminé en fonction des volumes d'informations échangées entre les sites ; il peut varier donc d'un circuit à l'autre. L'opérateur ne facturera ainsi que le débit garanti (CIR), l'EIR étant gratuit ou presque. [12]

Dans le protocole Frame Relay, l'extrémité de chaque liaison est identifiée par un numéro appelé DLCI (Data Link Connection Identifier) ou identificateur de connexion de liaison de données qui est fourni par le fournisseur de services Frame Relay. Le commutateur Frame Relay mappe alors deux DLCI (source et destination) pour créer un PVC.

Ces DLCI ont une valeur locale, autrement dit, ces valeurs ne sont pas uniques dans le réseau étendu Frame Relay. Deux équipements reliés par un circuit virtuel peuvent utiliser une valeur DLCI différente pour désigner la même connexion. Le routeur n'a besoin que d'une interface même pour plusieurs PVC.

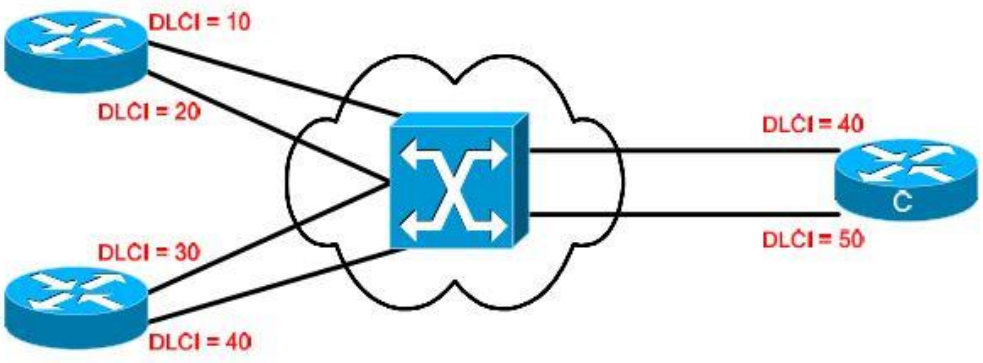


Figure 4.10 : *Une interface pour deux PVC*

Le DLCI est stocké dans le champ d'adresse de chaque trame. L'espace d'adressage DLCI est limitée à 10bits [16]. La plage d'adresse (0 à 1023) présente une partie utilisable pour adresser les extrémités de liaison (pour le transport des données utilisateur) mais le reste est réservé à des fins d'implémentation par le constructeur (Message LMI, adresse de multicast…). Voici un tableau résumant la plage d'adresse DLCI avec ses utilisations :

DLCI	Utilisation
0	Etablissement CV (Circuit Virtuel)
1 - 15	réservés
16 - 1007	PVC, SVC
1008 - 1018	réservés
1019 - 1022	Multicast
1023	Signalisation de congestion

Tableau 4.02: *Plage d'adresse DLCI*

Notons qu'un circuit virtuel commuté peut aussi être utilisé à partir d'un protocole de signalisation utilisant le DLCI 0. L'intérêt de celui-ci est d'assurer la qualité de service (CIR et EIR) par spécification à la demande. [12]

Il existe aussi un protocole appelé LMI (Local Management Interface) ou interface de supervision locale permettant la signalisation entre le point d'extrémité (l'utilisateur) et le commutateur de Frame Relay afin de connaitre l'état des PVC ou la modification de l'état du lien. Les fonctionnalités de base de LMI est de déterminer la fonctionnalité des PVC connus du routeur, transmettre des messages de veille pour éviter la fermeture de PVC à cause d'inactivité, indiquer au routeur les PVC

disponibles. L'interface LMI présente trois types : Cisco (extension LMI d'origine), Ansi (correspondant à la norme ANSI T1.617 annexe D) et q933a (correspondant à la norme ITU Q933 annexe A). Ces différents types sont réciproquement incompatibles. Il faut donc noter que le type de LMI utilisé par le routeur doit être le même que celui du commutateur Frame Relay (utilisé par le fournisseur).

La partie exploitable de la plage d'adresse DLCI est définie par le type de LMI utilisé :

LMI	**DLCI**
ansi	16 - 992
cisco	16 – 1007
Q933a	19 - 992

Tableau 4.03: *Correspondance entre LMI et DLCI*

4.2.2.2 Format de trame

L'unité de donnée utilisé par le protocole est appelé frame ou trame.

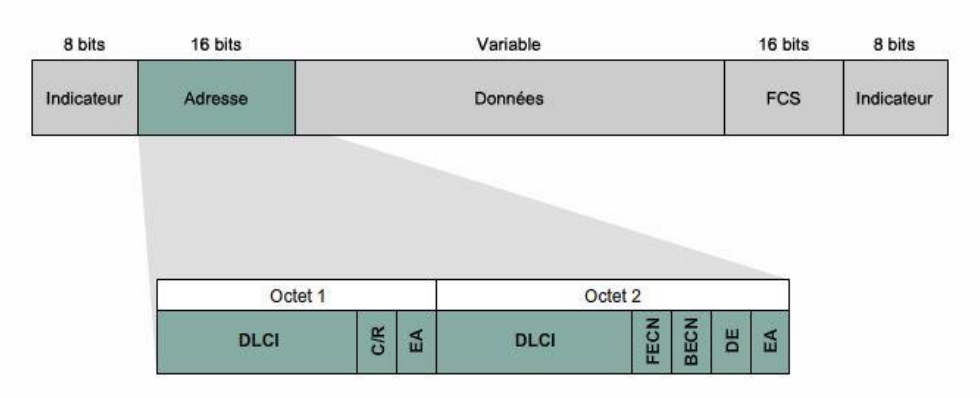


Figure 4.11 : *Format de la trame de Frame Relay*

- Indicateur (ou drapeau) : indique le début et la fin de la trame et permet de synchroniser l'émetteur et le récepteur. Il peut être présenté sous forme binaire par 01111110 ou hexadécimale par 7E.
- Adresse : contient l'adresse d'extrémité ou DLCI (10 premiers bits) et les mécanismes de notification de congestion (3 derniers bits)
  - DLCI

- C/R (Command/ Response) : indique si la trame est une commande ou une réponse
- FECN (Forward Explicit Congestion Notification) ou notification explicite de congestion au destinataire : c'est un bit défini dans une trame qui signale à l'unité réceptrice de lancer des procédures de prévention de congestion.
- BECN (Backward Explicit Congestion Notification) ou notification explicite de congestion de source : Idem que précédemment mais la notification est cette fois pour l'unité source. En recevant la notification, le routeur (l'utilisateur) doit réduire le débit de transmission de 25%.
- DE (Discard Eligibility) ou bit d'éligibilité à la suppression : c'est un bit qui marque qu'une trame peut être supprimée en priorité en cas de congestion.
- EA ou adresse étendue : indique si le champ adresse a une suite ou si c'est le dernier. C'est le huitième bit de chaque octet.

- Données : informations encapsulées de taille variable.
- FCS (Frame Check Sequence) ou séquence de contrôle de trame : indique si des erreurs se sont produites pendant la transmission ; elle est calculée par l'émetteur et le récepteur, les deux résultats doivent être le même pour indiquer que la trame n'est pas faussée.

4.2.3 Topologie et mise en place du Frame Relay

On peut concevoir un réseau Frame Relay selon trois types de topologie :

- La topologie en étoile : les terminaux sont connectés à un équipement central, la communication entre eux se font donc par intermédiaire de cet équipement central suivant les rayons. Dans un réseau Frame Relay en étoile, chaque site distant dispose d'une liaison d'accès au nuage Frame Relay avec un seul circuit virtuel tandis que le concentrateur a une liaison d'accès avec plusieurs circuits virtuels, un pour chaque site distant.
- La topologie à maillage globale : qui connecte un site à chacun des autres sites. Dans le cas de Frame Relay, celle-ci est réalisée en configurant des circuits virtuels entre tous les sites existants. Il n'y a pas d'ajouts d'équipements donc aucun coût supplémentaire de matériels mais seulement le coût de la bande passante supplémentaire. Cependant il existe une limite du nombre de circuits virtuels dans le réseau. De plus, l'opérateur facture à chaque circuit virtuel correspondant à chaque CIR.
- La topologie à maillage partielle : où le nombre d'interconnexion est plus élevé que dans une disposition en étoile mais moins élevé que dans un maillage total. Chaque extrémité n'est pas reliée à toutes les autres.

Pour la mise en place de la technologie, l'opérateur installe son modem numérique (le CSU) dans les locaux du client. Il va installer ensuite un commutateur appelé FRAD (Frame Relay Access Device) qu'il va connecter au modem. Le FRAD est un équipement de conversion entre des protocoles d'entrées et le protocole Frame Relay ; cet équipement, installé dans le cas où le routeur ne supporte pas le Frame Relay, prends les paquets IP issus d'un routeur ou les canaux issus d'un PABX (Private Automatic Branch eXchange) et les encapsule dans les trames Frame Relay. L'interface du routeur sera ensuite connectée à un des ports du FRAD et ce dernier est relié via la liaison d'accès au commutateur Frame Relay situé dans le POP (Point Of Presence) de l'opérateur. Plusieurs flux sont ainsi multiplexés sur une même liaison.

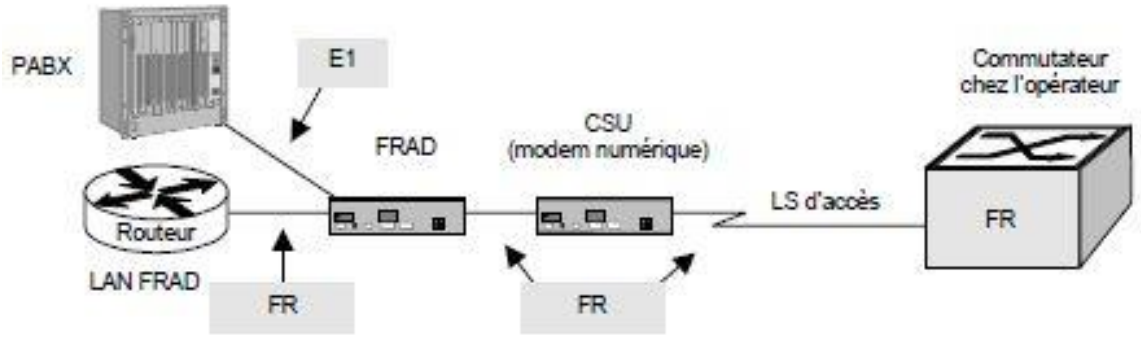


Figure 4.12 : *Connexion d'un routeur à un FRAD*

Dans le cas où le routeur supporte le Frame Relay, la solution la plus souple est de configurer le routeur en FRAD : les trames LAN (Ethernet dans notre cas) sont converties en trames Frame Relay. [12]

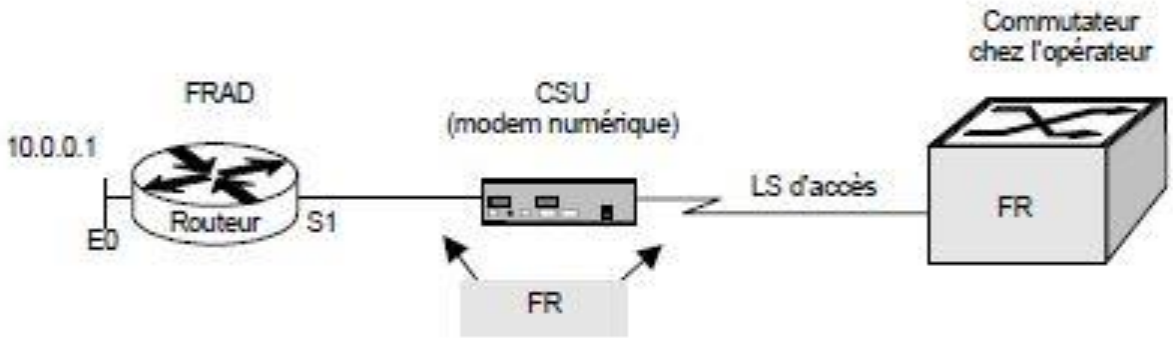


Figure 4.13 : *Connexion d'un routeur à un commutateur Frame Relay*

4.3 Différents protocoles utilisés

4.3.1 ARP, RARP, ARP- Inverse

4.3.1.1 ARP

ARP (Address Resolution Protocol) est un protocole de la couche réseau qui permet à une station IP de connaître l'adresse physique (adresse MAC ou autre) d'une autre station en sachant son adresse IP. La correspondance entre adresse IP et adresse physique se résume dans une table appelée table ARP stockée dans chaque station. [15]

4.3.1.2 RARP

RARP (Reverse Address Resolution Protocol) est un protocole de niveau 3 aussi et détermine l'adresse IP d'une station à partir de son adresse MAC et auprès d'un serveur d'adresses. [15]

4.3.1.3 InARP

InARP (Inverse ARP) est un protocole du réseau de transport Frame Relay ou ATM. C'est le mécanisme inverse d'ARP : il permet à un routeur de connaître l'adresse IP d'un autre routeur se trouvant à l'autre bout d'un circuit virtuel.

4.3.2 DHCP (Dynamic Host Configuration Protocol)

DHCP est un protocole qui fonctionne en mode client-serveur. Il sert à configurer dynamiquement les clients au niveau de la couche 3 comme l'attribution d'adresse IP. L'utilisation de ce protocole offre un gain de temps extrêmement précieux aux administrateurs réseau pour l'adressage des ordinateurs de bureau clients. Il faut noter que les équipements tels que les routeurs, les commutateurs et les serveurs sont attribués d'adresses IP statiques.

Le protocole DHCP s'appuie sur le protocole de transport UDP (User Datagram Protocol) et fonctionne sur un principe de location ou de bail. Le client envoie des messages au serveur sur le port 67 ; le serveur répond le client au port 68.

DHCP offre jusqu'à une trentaine de paramètres de configuration dont les principaux sont l'attribution d'adresse IP, le masque de sous-réseau, l'adresse IP passerelle par défaut, l'adresse IP de serveur DNS. Il assure ainsi la configuration automatique des paramètres IP d'une station: attribution automatique d'adresse IP et d'un masque de sous réseau. Il configure aussi l'adresse de

passerelle par défaut, des serveurs DNS, des serveurs de noms NBNS ou serveurs WINS (Windows Internet Naming Service pour les réseaux de la société de la société Microsoft).
Son fonctionnement est décrit par la figure suivante :

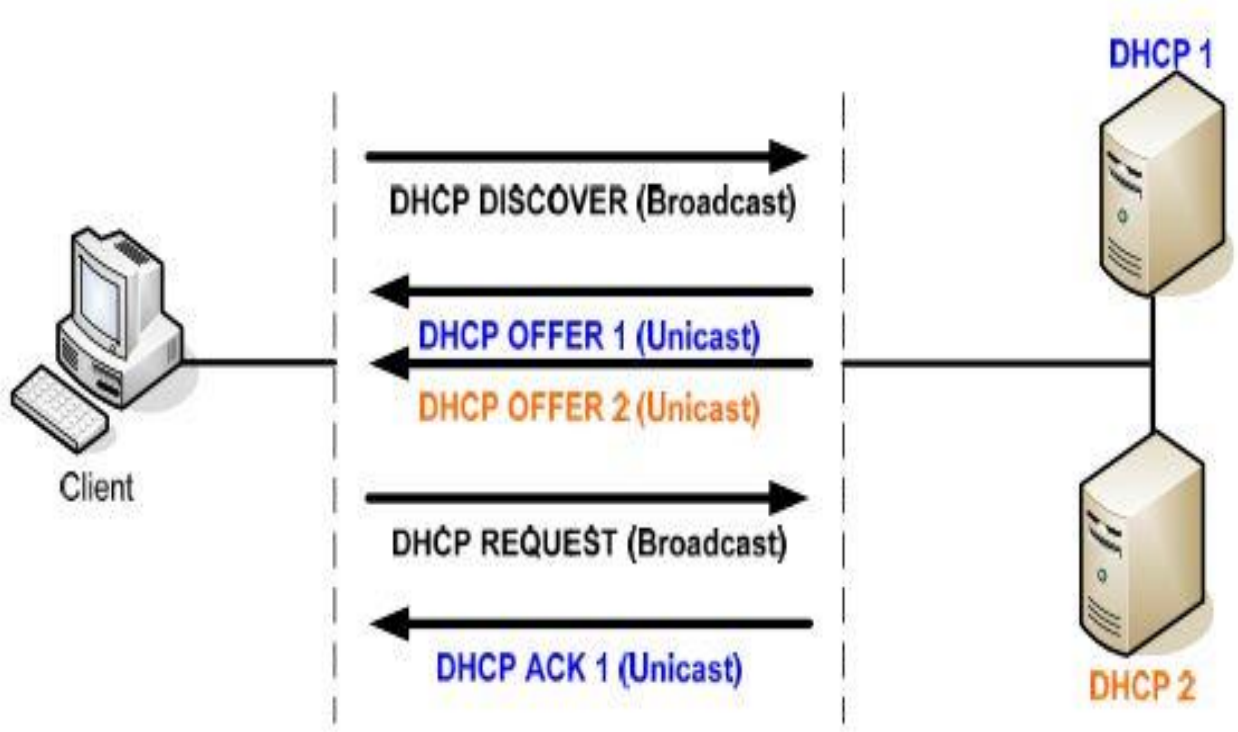


Figure 4.14 : *Fonctionnement de DHCP*

4.3.3 ICMP (Internet Control Message Protocol)

ICMP est un protocole qui fonctionne au niveau de la couche 3. Il offre des fonctions de messagerie et de contrôle pour IP lors de la transmission de paquets. Les messages du protocole ICMP peuvent être des messages d'erreurs ou des messages de contrôle. Il faut noter qu'ICMP ne signale l'état du paquet transmis qu'à l'équipement d'origine. Il ne corrige pas les erreurs, il sert juste à en faire part. [14]

L'utilisation principale de ce protocole est dans la commande *ping* qui permet de tester l'accessibilité et la disponibilité d'une destination et aussi de reporter les erreurs: après une demande echo, une réponse echo confirme l'accessibilité ou non de la destination.

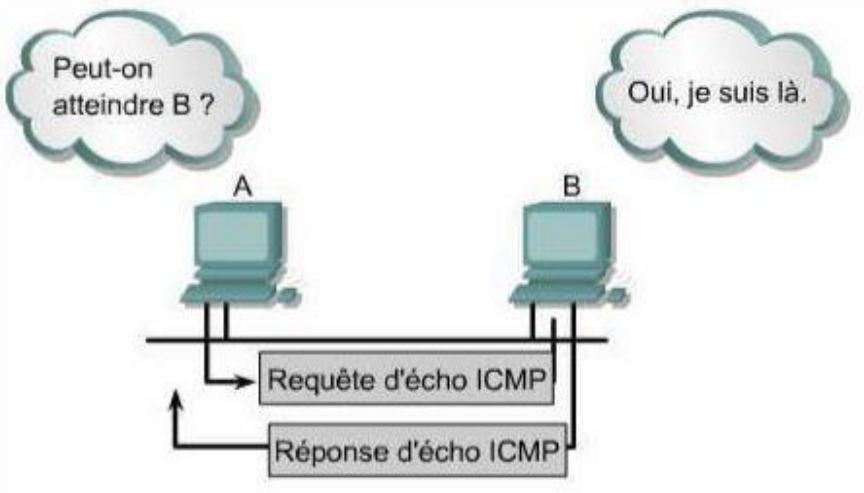


Figure 4.15 : *Echo Request/Reply ICMP lors d'un ping*

Après une commande ping effectuée, on obtient des informations telles que: le temps mis par le paquet pour atteindre une adresse, le problème de routage rencontré pour atteindre un hôte.

4.3.4 DNS (Domain Name System)

Pour une entreprise, il est difficile de retenir l'adresse IP d'un site car elle n'a aucun rapport apparent avec le contenu du site. Le protocole DNS permet alors d'associer des noms en langage courant aux adresses numériques. Pour ce faire, il y a mise en place d'un système de gestion de noms appelé Domain Name System ou Système de nom de domaine. Ce système consiste en une hiérarchie de noms permettant de garantir l'unicité d'un nom dans une structure arborescente.

On appelle FQDN (Full Qualified Domain) l'adresse qui permet de repérer de façon unique une machine. C'est l'ensemble d'un nom d'hôte, d'un point, et du nom de domaine. Le nom de domaine comporte deux composantes : le premier est le nom correspondant au nom de l'organisation ou de l'entreprise et le second est la classification de domaine (.fr, .com, .edu,… selon l'activité de l'entreprise). Le nom d'hôte est unique dans le domaine considéré, www est un exemple pour le serveur web.

Chaque ordinateur doit être configuré avec l'adresse d'une machine capable de transformer n'importe quel nom en une adresse IP. Cette machine est appelée Domain Name Server ou Serveur de nom de domaine.

4.4 Conclusion

Plusieurs LAN distants, géographiquement parlant, ne peuvent se communiquer ni s'interconnecter physiquement. C'est là qu'intervient alors le réseau de transport faisant partie du

réseau WAN. Divers services sont alors proposés tels que les services dédiés mettant en œuvre des liaisons physiques point-à-point ; des services commutés faisant intervenir des liaisons logiques ou circuits virtuels. Le choix de la technologie utilisée dépend des réseaux en questions. Cependant, Frame Relay semble l'une les plus utilisées des entreprises grâce à ses avantages par rapport aux autres. Dans le dernier chapitre, nous allons présenter les concepts de réalisation d'un réseau d'entreprise fictive pour aboutir à un prototype testé et viable pour une mise en œuvre réelle.

CHAPITRE 5
SIMULATION D'UN RESEAU D'ENTREPRISE

5.1 Outil de simulation Packet Tracer

Packet Tracer est un logiciel fourni par Cisco permettant à tout amateur ou non de réseau informatique de simuler des équipements propres Cisco. Il permet alors la mise en place d'une topologie de réseau, de visualiser le fonctionnement d'un inter-réseau et de simuler le comportement des protocoles réseaux. [11]

Packet Tracer offre un espace de travail avec plusieurs options facilitant sa manipulation, plusieurs possibilités concernant les différents équipements réseaux, les différents types de médias.

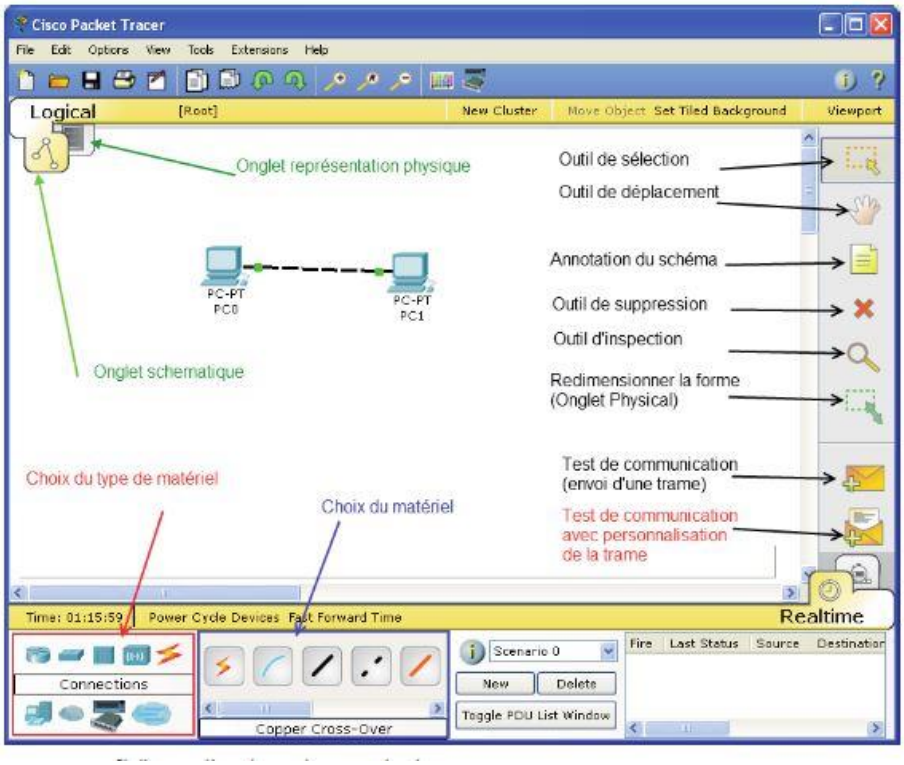


Figure 5.01 : *Fenêtre générale de Packet TracerPrésentation du réseau à simuler*

5.2 Description du réseau

Nous allons considérer une entreprise fictive portant le nom de « MADABANK » située dans la ville d'Antananarivo. MADABANK est une banque qui présente un siège et deux agences au cœur de la ville. Notre but est de concevoir un réseau informatique pour cette entreprise adapté selon ses besoins.

Le siège est constitué de deux branches : une branche regroupant la direction générale, la direction administrative et réseau, avec quinze employés disposant chacun d'un PC ; une autre branche regroupant la direction de crédit et la direction de recouvrement, avec 10 employés qui ont tous besoin de PC. Ces deux branches utilisent chacune un réseau local pour la communication et le partage des informations et d'équipement tel que l'imprimante. Le siège présente aussi au cœur de son réseau une batterie de serveurs composée de trois serveurs.

Les deux agences de MADABANK disposent chacune d'une vingtaine d'employés utilisant une quinzaine d'ordinateurs. Elles sont reliées au siège pour les échanges d'informations et pour avoir accès aux services des serveurs.

Par ailleurs, MADABANK veut implanter sa première agence dans la ville de Fianarantsoa pour étendre ses offres de services. Cette agence compte aussi 20 employés dont 15 nécessitent l'utilisation de PC. Pour offrir à cette agence la même fonctionnalité et les mêmes ressources que les agences locales, l'entreprise a opté pour la technologie de Frame Relay pour l'interconnecter au siège.

5.3 Besoins de l'entreprise en terme de réseau

MADABANK doit assurer une interconnexion sûre entre le siège et ses agences. Ses exigences sont surtout en termes de :

- disponibilité
- extensibilité
- fiabilité
- facilité de gestion du réseau.

Ainsi le plan de conception d'un prototype de réseau de cette entreprise doit répondre à ces demandes. Pour se faire, une étude préalable doit être établie à propos des équipements adéquats à utiliser, le plan d'adressage pour ces équipements, le choix du protocole de routage à utiliser, le choix de la technologie WAN convenable pour interconnecter l'agence distant au siège.

5.4 Simulation du réseau avec le logiciel Packet Tracer

5.4.1 Equipements utilisés

Pour simuler la mise en place du réseau de l'entreprise, nous avons besoin de quatre routeurs représentant chacun le siège et les trois agences, huit commutateurs, trois serveurs, cinq PC pour

représenter les machines hôtes de chaque réseau local, une imprimante pour figurer la présence de partage d'équipement.

Le routeur au cœur du siège est un routeur 2621XM dont nous avons ajouté trois cartes d'extension : deux modules WIC-2T et un module NM-2FE2W offrant respectivement quatre ports série et deux ports Fast Ethernet supplémentaires. Les routeurs des agences sont des routeurs 1841 avec un ajout d'une carte WIC-2T pour avoir deux ports série supplémentaires à leur disposition.

Les commutateurs sont repartis comme suit : quatre dans le réseau du siège, un pour chaque réseau local des agences et celui de la batterie de serveurs.

Dans la batterie de serveurs, parmi les trois serveurs on trouve un serveur DNS, un serveur Web et un serveur Email interne pour l'entreprise.

Nous avons utilisé un « cloud » configuré en tant que Frame Relay pour le réseau de transport.

Pour répondre à la disponibilité, la fiabilité et la facilité de gestion du réseau, nous avons appliqué un réseau hiérarchique qui présente une redondance au niveau des commutateurs reliés au routeur principal du siège. En cas de panne d'un équipement ou rupture d'une liaison, la redondance va assurer la continuité de service.

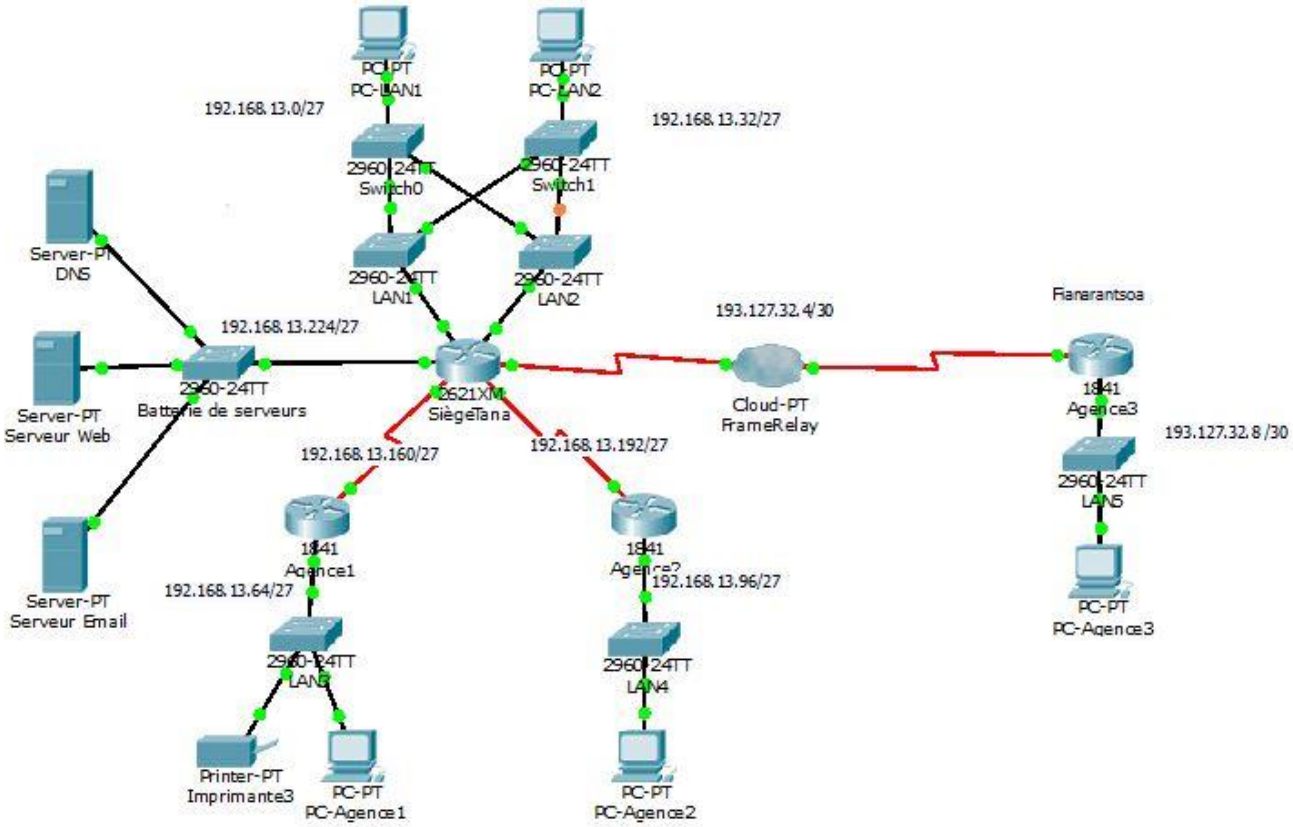


Figure 5.02 : *Topologie du réseau de MADABANK*

5.4.2 Tableau d'adressage, routage et réseau de transport

Pour répondre à l'extensibilité et aussi à la facilité de gestion de réseau, nous avons opté pour le plan hiérarchique d'adressage. Soient deux adresses de réseaux parents 192.168.13.0 /24 et 193.127.32.0 /24 utilisées respectivement pour les réseaux locaux situés à Antananarivo (le siège et les deux agences locales) et le réseau WAN incluant l'agence à Fianarantsoa.

- L'adresse réseau 192.168.13.0 /24 est divisée en 8 sous-réseaux pour permettre ainsi à chaque sous-réseau d'avoir une taille de 30 adresses utilisables. On obtient alors un nouveau masque de sous-réseau 255.255.255.224 ou /27. Ces sous-réseaux sont repartis comme suit :

Adresse de sous-réseau	**Réseau local**
192.168.13.0 /27	LAN1
192.168.13.32 /27	LAN2
192.168.13.64 /27	LAN3
192.168.13.96 /27	LAN4
192.168.13.128 /27	aucun
192.168.13.160 /27	Siège-Agence1
192.168.13.192 /27	Siège-Agence2
192.168.13.224 /27	Batterie de Serveurs

Tableau 5.01: *Distribution des huit sous-réseaux*

- L'adresse 193.127.32.0 /24 est divisée en 64 sous-réseaux puisqu'on a besoin de deux adresses seulement. Le nouveau masque de sous-réseau est alors 255.255.255.252 ou /30

Adresse de sous-réseau attribuée	**Réseau local**
193.127.32.4 /30	Siège-Frame Relay-Agence3
193.127.32.8 /30	Agence3

Tableau 5.02: *Adresses de sous-réseau utilisées*

Les équipements de réseau tels que les routeurs, les serveurs et les imprimantes doivent être adressés de manière statique. Quant aux PC, nous avons configuré chaque routeur comme étant un serveur DHCP capable ainsi de gérer et de distribuer les adresses IP de chaque hôte faisant partie de son réseau local.

Voici le tableau résumant l'adressage statique :

Périphérique	**Interface**	**Adresse IP**	**Masque de sous-réseau**
Siège	FastEthernet 0/0	192.168.13.1	/27
	FastEthernet 0/1	192.168.13.33	/27
	FastEthernet 1/0	192.168.13.225	/27
	FastEthernet 1/1		
	Serial 0/0	192.168.13.161	/27
	Serial 0/1	192.168.13.193	/27
	Serial 1/0	193.127.32.5	/30
	Serial 1/1		
Agence1	FastEthernet 0/0	192.168.13.65	/27
	FastEthernet 0/1		
	Serial 0/1/0	192.168.13.190	/27
	Serial 0/1/1		
Agence2	FastEthernet 0/0	192.168.13.97	/27
	FastEthernet 0/1		
	Serial 0/1/0	192.168.13.222	/27
	Serial 0/1/1		
Agence3	FastEthernet 0/0	193.127.32.9	/30
	FastEthernet 0/1		
	Serial 0/1/0	193.127.32.6	/30
	Serial 0/1/1		
Imprimante3	FastEhernet	192.168.13.66	/27
Serveur DNS	FastEhernet	192.168.13.226	/27
Serveur Web	FastEhernet	192.168.13.227	/27
Serveur Email	FastEhernet	192.168.13.228	/27

Tableau 5.03: *Tableau d'adressage statique*

Notre réseau présente alors un adressage hiérarchique pouvant introduire la notion d'agrégation de route ou résumé de routage facilitant et réduisant le temps de la recherche dans la table de routage. Ce fait nous amène alors de choisir le protocole de routage EIGRP capable de supporter le VLSM et le routage CIDR. Le choix de ce protocole est justifié grâce à ses caractéristiques :

- Un routage sans classe prenant en charge le masquage de sous-réseau de longueur variable (VLSM)
- Des mises à jour de la table de routage rapides et peu fréquentes réduisant le trafic
- Une convergence rapide en cas de défaillance.
- Une implémentation facile

De plus, Le protocole EIGRP comporte une fonction de résumé de routage automatique.
En ce qui concerne le réseau de transport, nous avons choisi la technologie de Frame Relay puisque les échanges entre clients se résument par des échanges de fichiers, des échanges d'e-mail et l'accès au serveur web. Un débit de 128 Kbps est alors suffisant pour assurer ces demandes. Le critère de Frame Relay répond aussi ce débit.

5.4.3 Observations et interprétations

5.4.3.1 Tables de routages des différents routeurs

La consultation de la table de routage se fait par la commande « show ip route ».

```
Siege#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.13.0/24 is variably subnetted, 8 subnets, 2 masks
D       192.168.13.0/24 is a summary, 01:01:01, Null0
C       192.168.13.0/27 is directly connected, FastEthernet0/0
C       192.168.13.32/27 is directly connected, FastEthernet0/1
D       192.168.13.64/27 [90/2172416] via 192.168.13.190, 01:00:52, Serial0/0
D       192.168.13.96/27 [90/2172416] via 192.168.13.222, 01:00:54, Serial0/1
C       192.168.13.160/27 is directly connected, Serial0/0
C       192.168.13.192/27 is directly connected, Serial0/1
C       192.168.13.224/27 is directly connected, FastEthernet1/0
     193.127.32.0/24 is variably subnetted, 3 subnets, 2 masks
D       193.127.32.0/24 is a summary, 01:01:01, Null0
C       193.127.32.4/30 is directly connected, Serial0/2
D       193.127.32.8/30 [90/2172416] via 193.127.32.6, 01:00:29, Serial0/2
```

Figure 5.03 : *Table de routage du routeur du siège*

```
Agence1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.13.0/27 is subnetted, 7 subnets
D       192.168.13.0 [90/2172416] via 192.168.13.161, 01:04:22, Serial0/1/0
D       192.168.13.32 [90/2172416] via 192.168.13.161, 01:04:22, Serial0/1/0
C       192.168.13.64 is directly connected, FastEthernet0/0
D       192.168.13.96 [90/2684416] via 192.168.13.161, 01:04:22, Serial0/1/0
C       192.168.13.160 is directly connected, Serial0/1/0
D       192.168.13.192 [90/2681856] via 192.168.13.161, 01:04:22, Serial0/1/0
D       192.168.13.224 [90/2172416] via 192.168.13.161, 01:04:22, Serial0/1/0
D    193.127.32.0/24 [90/2681856] via 192.168.13.161, 01:04:22, Serial0/1/0
```

Figure 5.04 : *Table de routage du routeur de l'agence1*

```
Agence2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.13.0/27 is subnetted, 7 subnets
D       192.168.13.0 [90/2172416] via 192.168.13.193, 01:05:30, Serial0/1/0
D       192.168.13.32 [90/2172416] via 192.168.13.193, 01:05:30, Serial0/1/0
D       192.168.13.64 [90/2684416] via 192.168.13.193, 01:05:28, Serial0/1/0
C       192.168.13.96 is directly connected, FastEthernet0/0
D       192.168.13.160 [90/2681856] via 192.168.13.193, 01:05:30, Serial0/1/0
C       192.168.13.192 is directly connected, Serial0/1/0
D       192.168.13.224 [90/2172416] via 192.168.13.193, 01:05:30, Serial0/1/0
D    193.127.32.0/24 [90/2681856] via 192.168.13.193, 01:05:30, Serial0/1/0
```

Figure 5.05 : *Table de routage du routeur de l'agence2*

```
Agence3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.13.0/24 is variably subnetted, 4 subnets, 2 masks
D       192.168.13.0/24 [90/2172416] via 193.127.32.5, 01:05:59, Serial0/1/0
S       192.168.13.0/27 [1/0] via 193.127.32.5
S       192.168.13.32/27 [1/0] via 193.127.32.5
S       192.168.13.224/27 [1/0] via 193.127.32.5
     193.127.32.0/30 is subnetted, 2 subnets
C       193.127.32.4 is directly connected, Serial0/1/0
C       193.127.32.8 is directly connected, FastEthernet0/0
```

Figure 5.06 : *Table de routage du routeur de l'agence3*

La table de routage contient toutes les routes menant d'un réseau à l'autre. En étudiant ces quatre tables de routage :

- Nous voyons que le protocole de routage utilisé par chaque routeur est l'EIGRP
- Nous remarquons que celle du routeur du siège présente toutes les routes pouvant atteindre les réseaux des trois agences.
- Les tables de routage de l'Agence1 et l'Agence2 montrent les chemins pour accéder aux réseaux locaux internes du Siège et aux serveurs
- La table de routage de l'Agence 3 présente une route agrégée automatiquement par EIGRP menant au Siège, trois routes statiques menant chacune aux deux réseaux locaux du Siège et au réseau local contenant les serveurs.

D'après ces résultats, nous pouvons dire que chaque routeur peut communiquer avec un autre routeur en disposant d'un chemin à emprunter. Afin de montrer cela, nous allons faire des tests d'interconnexion.

5.4.3.2 Test d'interconnexion du réseau global

Ce test peut se faire soit en mode ligne de commande (CLI) en utilisant la commande « ping » soit en mode simulation à partir du bouton « Add Simple PDU ».Nous allons voir ces deux types de test.

- ❖ Le PC du premier LAN du siège tente de se communiquer avec les PC de l'Agence1, de l'Agence2 et de l'Agence3 qui ont successivement les adresses IP suivantes : 192.168.13.67,

192.168.13.98 et 193.127.32.10. Nous faisons de même avec le PC du second LAN mais en mode simulation pour le LAN1.

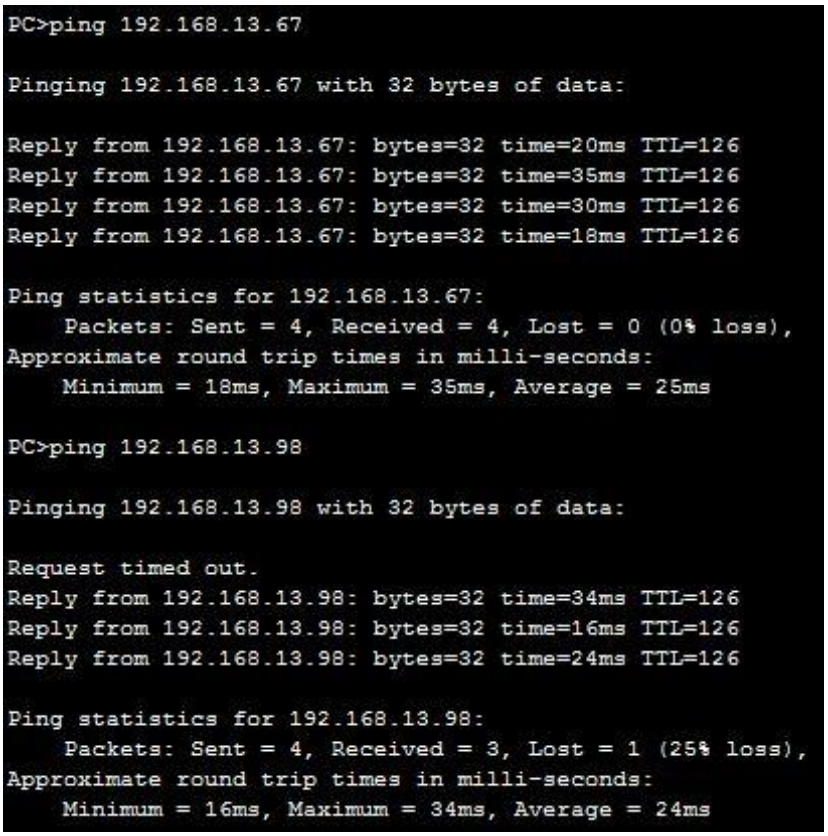


Figure 5.07 : *Test entre LAN1 et les Agences 1 et 2 avec ping*

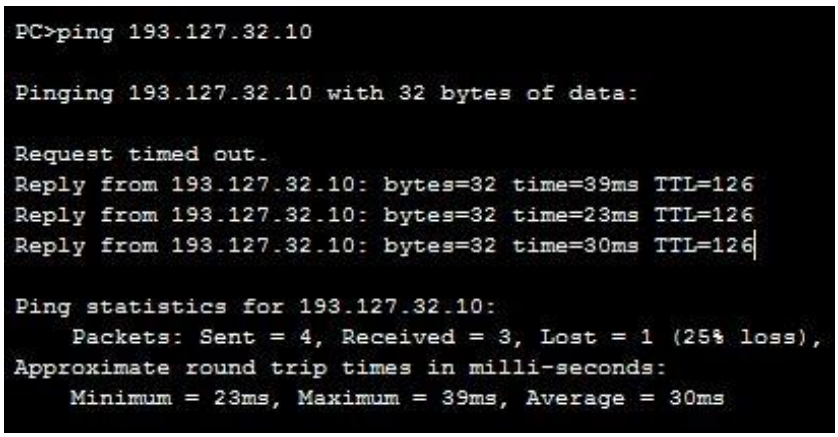


Figure 5.08 : *Test entre LAN1 et l'Agence 3 avec ping*

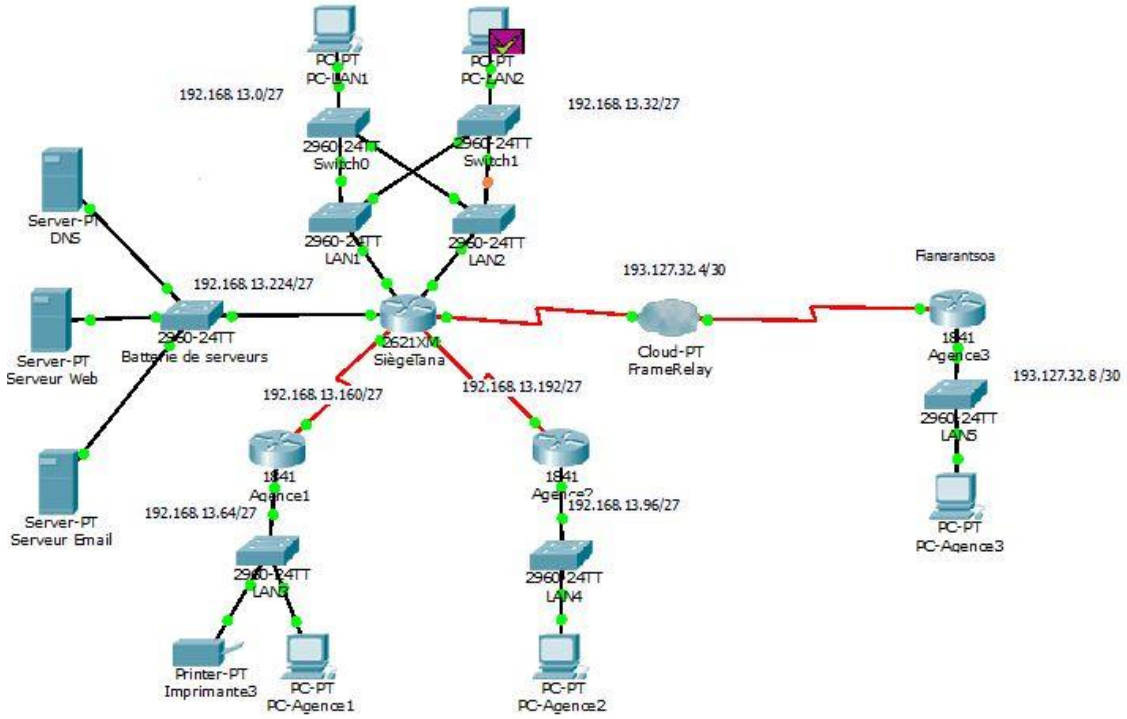


Figure 5.09 : *Test entre le LAN2 et l'Agence1*

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.13.98

Pinging 192.168.13.98 with 32 bytes of data:

Request timed out.
Reply from 192.168.13.98: bytes=32 time=36ms TTL=126
Reply from 192.168.13.98: bytes=32 time=35ms TTL=126
Reply from 192.168.13.98: bytes=32 time=24ms TTL=126

Ping statistics for 192.168.13.98:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 36ms, Average = 31ms

PC>ping 193.127.32.10

Pinging 193.127.32.10 with 32 bytes of data:

Reply from 193.127.32.10: bytes=32 time=50ms TTL=126
Reply from 193.127.32.10: bytes=32 time=35ms TTL=126
Reply from 193.127.32.10: bytes=32 time=42ms TTL=126
Reply from 193.127.32.10: bytes=32 time=37ms TTL=126

Ping statistics for 193.127.32.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 50ms, Average = 41ms
```

Figure 5.10 : *Test entre LAN2 et les Agences 2 et 3*

- Les trois agences testent leur connexion avec le siège. Les PC des deux LAN du siège ont respectivement comme adresses IP 192.168.13.2 et 192.168.13.34

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.13.2

Pinging 192.168.13.2 with 32 bytes of data:

Reply from 192.168.13.2: bytes=32 time=32ms TTL=126
Reply from 192.168.13.2: bytes=32 time=39ms TTL=126
Reply from 192.168.13.2: bytes=32 time=29ms TTL=126
Reply from 192.168.13.2: bytes=32 time=73ms TTL=126

Ping statistics for 192.168.13.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 73ms, Average = 43ms

PC>ping 192.168.13.34

Pinging 192.168.13.34 with 32 bytes of data:

Reply from 192.168.13.34: bytes=32 time=54ms TTL=126
Reply from 192.168.13.34: bytes=32 time=27ms TTL=126
Reply from 192.168.13.34: bytes=32 time=48ms TTL=126
Reply from 192.168.13.34: bytes=32 time=27ms TTL=126

Ping statistics for 192.168.13.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 54ms, Average = 39ms
```

Figure 5.11 : *Même résultat pour les trois agences*

Ces différents tests prouvent que le Siège est bien connecté à ses trois agences et vice-versa.

5.4.3.3 Analyse de paquets

- Paquet transitant entre le siège et les agences locales.

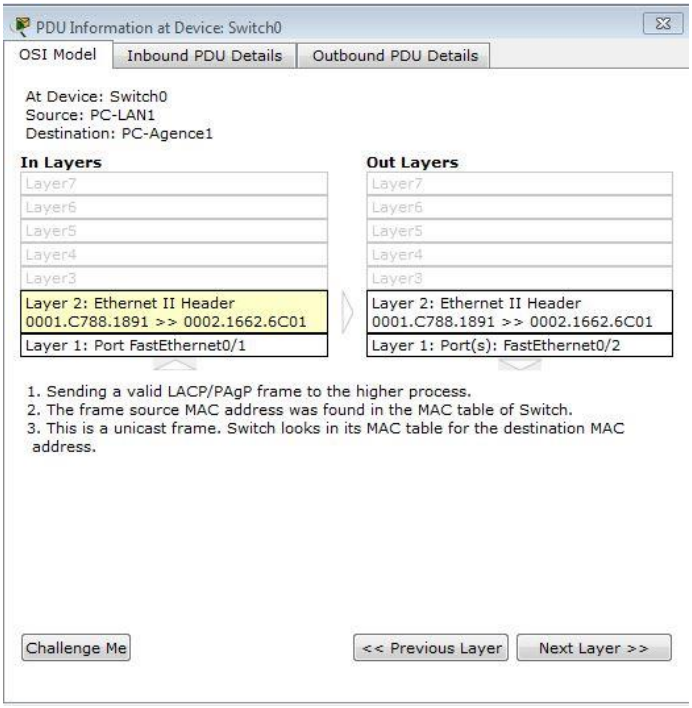


Figure 5.12 : *Paquet entre PC et commutateur*

La figure 5.12 nous montre que l'unité de donnée est une trame puisqu'elle affecte les couches 1 et 2 du modèle OSI et elle est de type Ethernet. La couche 2 nous informe l'adresse MAC source (celle du PC source) et l'adresse MAC de destination (celle du routeur du réseau local qui est la passerelle). La couche physique montre le port par lequel la trame va entrer puis sortir.

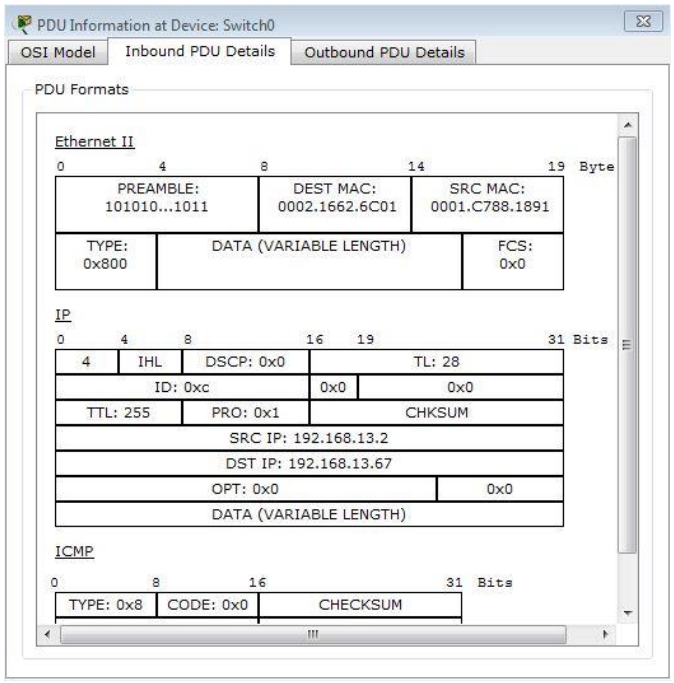


Figure 5.13 : *Détails de la trame à l'entrée*

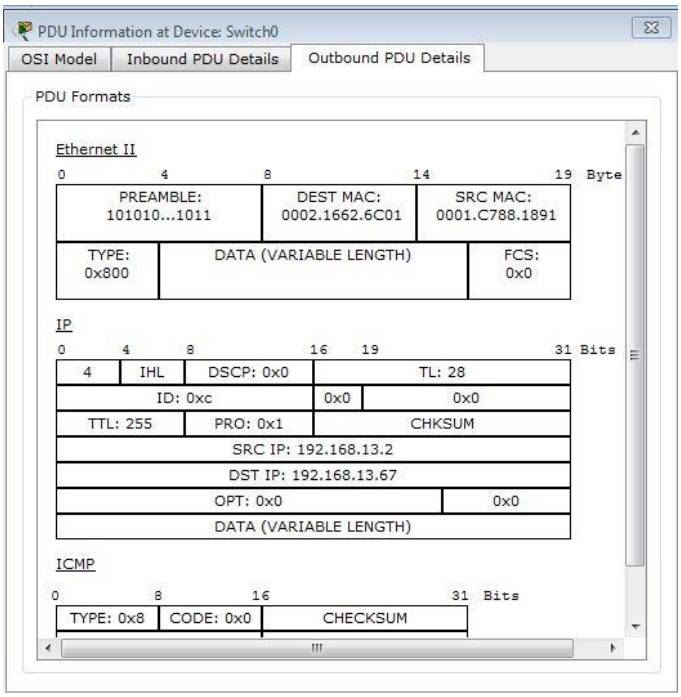


Figure 5.14 : *Détails de la trame à la sortie*

Ces deux figures 5.13 et 5.14 nous montrent que la trame est une trame Ethernet dont le champ type égal à 0x800 désigne que le protocole de niveau 3 est le protocole IP ; que le paquet IP présente l'adresse IP du PC source et l'adresse IP du PC de destination et il nous renseigne que la couche 3 utilise le protocole ICMP grâce à la valeur du champ protocole 0x1.

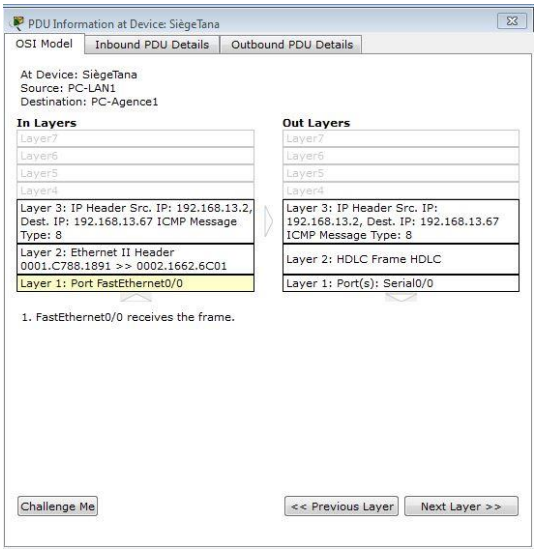
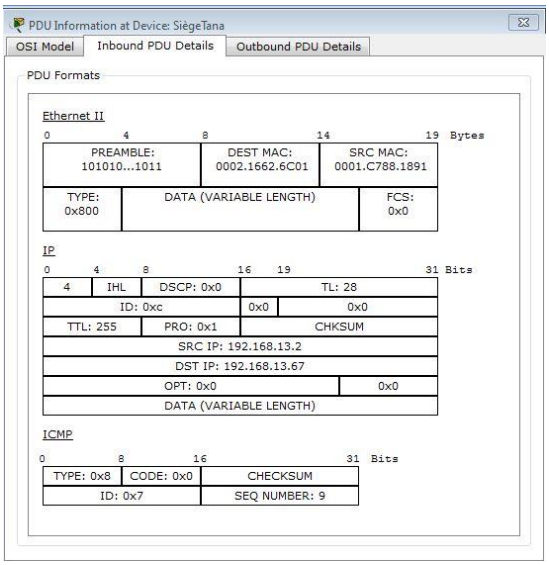


Figure 5.15 : *Paquet entre commutateur et routeur*

Cette figure 5.15 nous informe que la trame Ethernet à l'entrée du port Fast Ethernet0/0 présente les mêmes adresses MAC précédentes. Les couches 1, 2 et 3 du modèle OSI sont concernées car le paquet est analysé par le routeur pour y trouver l'adresse IP de destination. Le paquet IP présente les mêmes adresses IP que précédentes. A la sortie du routeur, le paquet est encapsulé en une trame HDLC et sort par le port série S0/0.



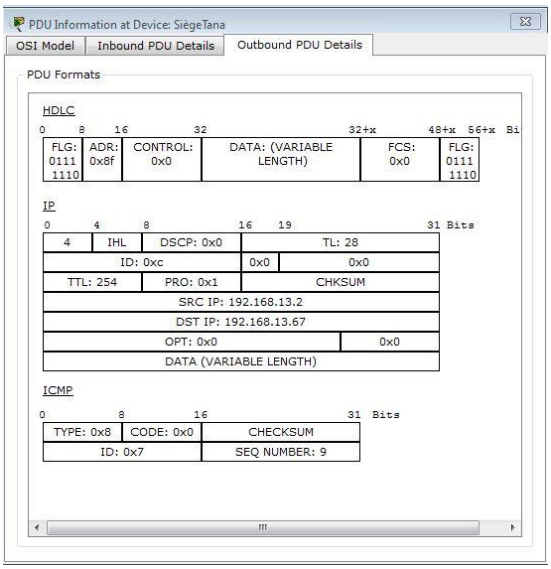


Figure 5.16 : *Détails du paquet à l'entrée et à la sortie du routeur*

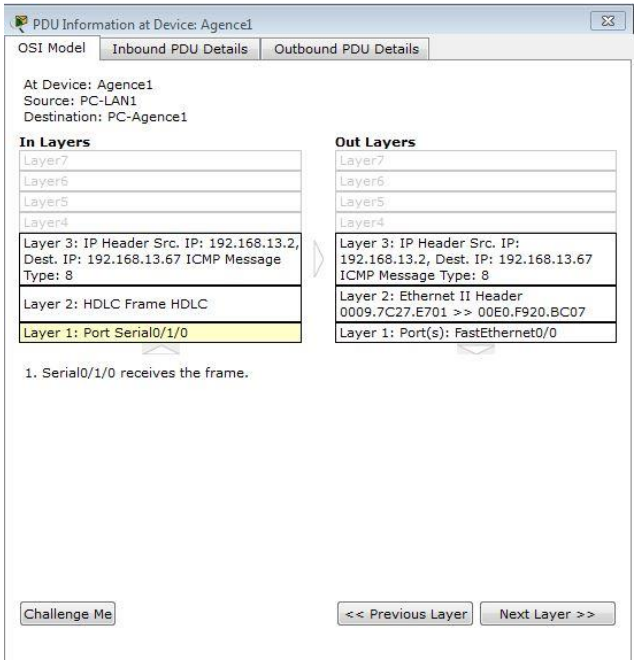


Figure 5.17 : *Paquet entre deux routeurs voisins*

La trame à l'entrée du port série 0/0 est une trame HDLC, tandis qu'avant d'être transmis au port Fast Ethernet du routeur suivant, le paquet reçu doit être encapsulé en une trame Ethernet avec l'adresse MAC source (celle du routeur du réseau local destinataire) et l'adresse MAC de destination (celle du PC destinataire). Les adresses IP source et destinataire restent inchangées.

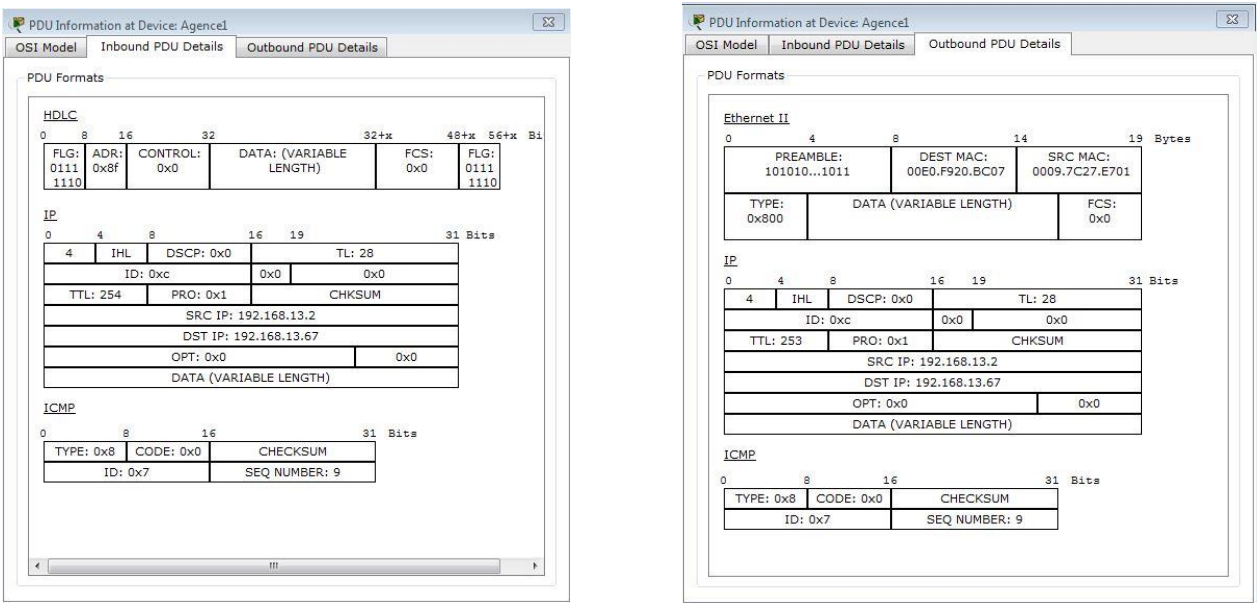


Figure 5.18 : *Détails du paquet à l'entrée et à la sortie du routeur*

❖ Paquet transitant entre le siège et l'agence distante

On retrouve les mêmes paquets que précédemment durant les transferts PC-Routeur et Routeur-PC. Sauf qu'à la sortie du routeur du siège, au lieu d'être encapsulé dans une trame HDLC, le paquet est encapsulé dans une trame Frame Relay. Cependant, il y a quelques changements lors de la transmission Routeur-Frame Relay et la transmission entre Frame Relay-Routeur.

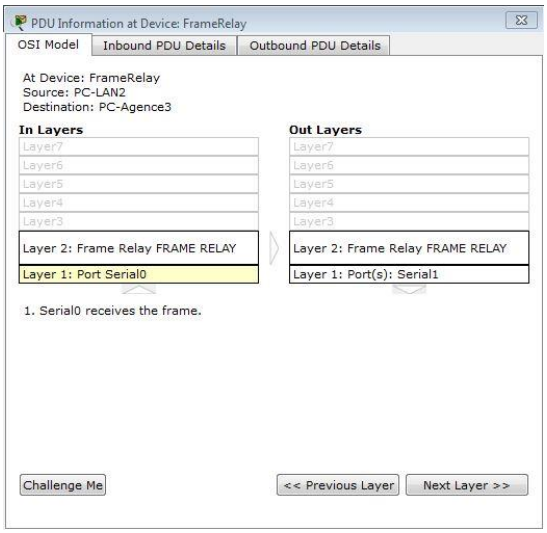


Figure 5.19 : *Paquet transitant dans le nuage de Frame Relay*

D'après cette figure 5.19, Frame Relay est une technologie de réseau étendu, ce qui explique qu'elle n'affecte que la couche liaison de données et la couche physique. La trame à l'entrée et à la sortie des ports séries est une trame Frame Relay. Le paquet IP encapsulé par cette trame contient les adresses IP source et destinataire.

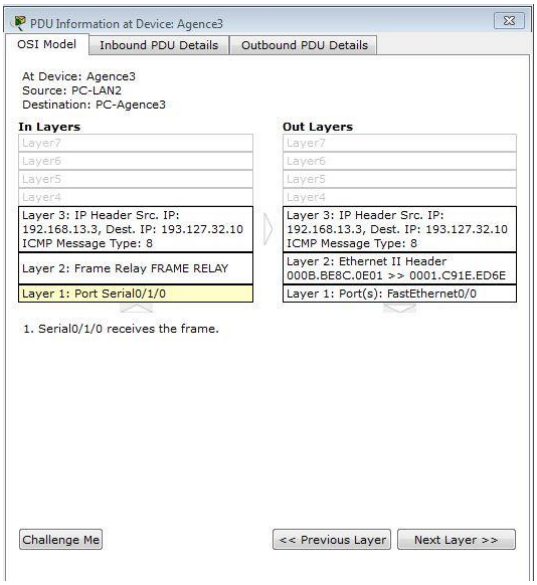


Figure 5.20 : *Paquet allant vers le routeur distant*

La figure 5.20 montre que la trame à l'entrée du routeur au port série 0/1/0 est encore une trame Frame Relay, le routeur y trouve l'adresse IP de destination mais pour l'acheminer à sa sortie au port Fast Ethernet0/0 le paquet IP est encapsulé dans une trame Ethernet avec son adresse MAC et celui du PC destinataire de l'agence 3.

5.4.3.4 Connexion au serveur Email de l'entreprise

Les employés de l'entreprise disposant du réseau informatique peuvent s'échanger des e-mails du fait qu'il y a accès au serveur Email. Les adresses e-mails de ces employés sont constituées du nom de domaine du serveur Email qui est « madabank.com ».

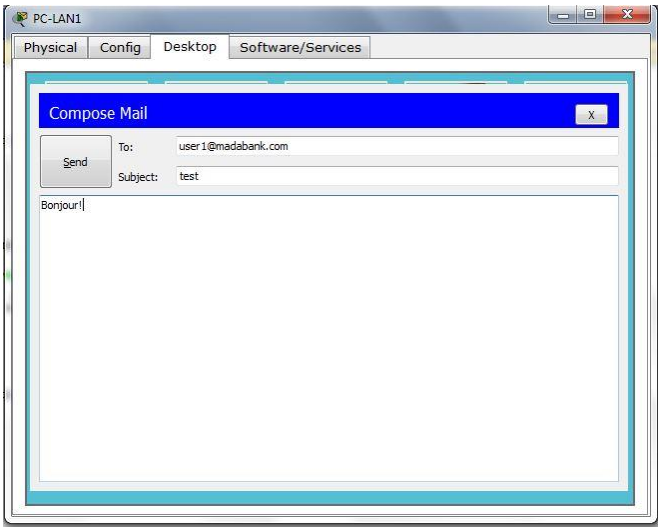


Figure 5.21 : *Envoi de message d'un client du Siège vers un autre de l'agence 1*

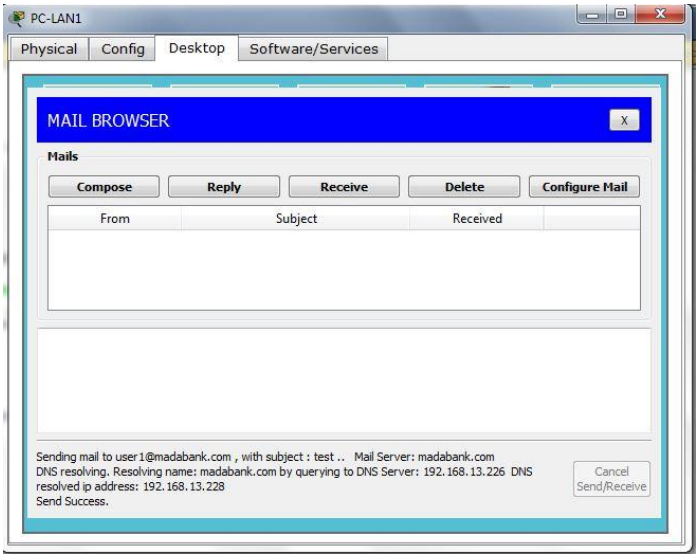


Figure 5.22 : *Envoi du message réussi*

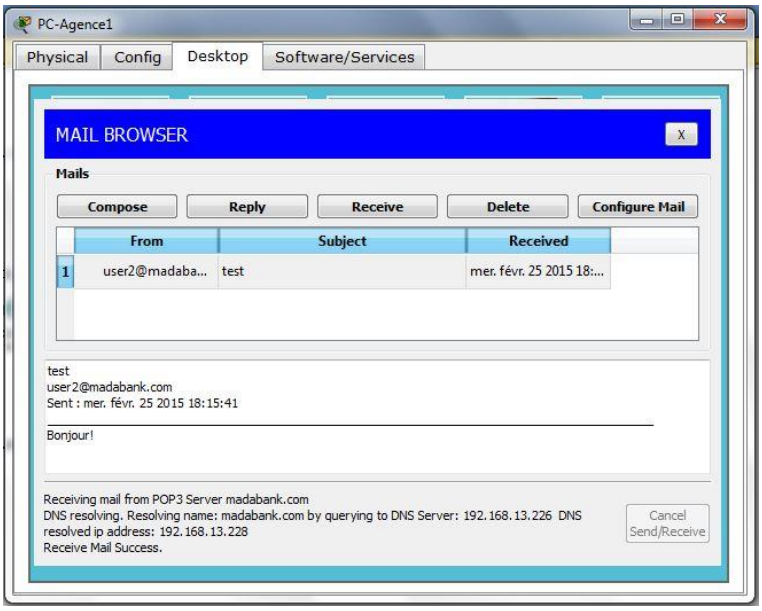


Figure 5.23 : *Boîte de réception du destinatire de l'agence 1*

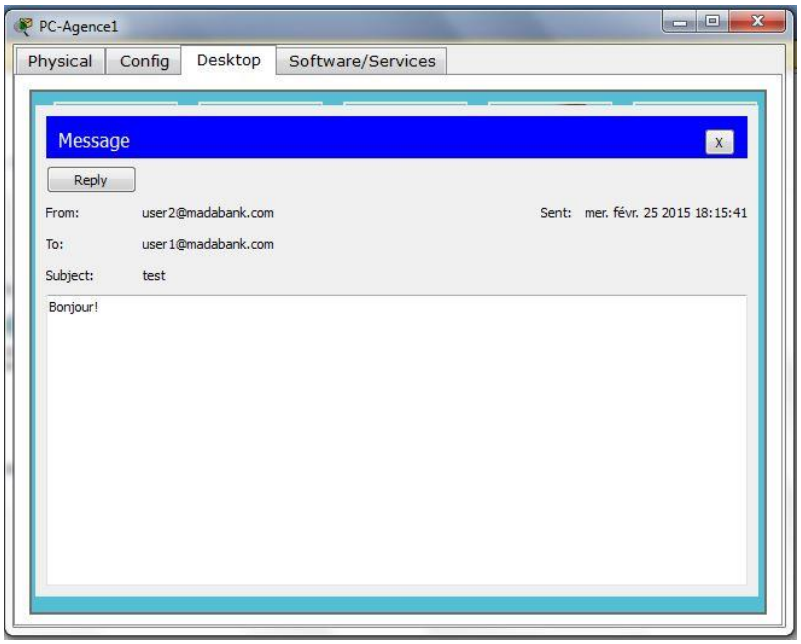


Figure 5.24 : *Message reçu venant du siège*

5.4.3.5 Connexion au serveur Web

Le siège de l'entreprise et ses trois agences dispose d'un serveur Web interne. Ainsi, tous les employés y accèdent en utilisant un navigateur et en indiquant le nom de domaine du serveur qui est « madabank.mg ».

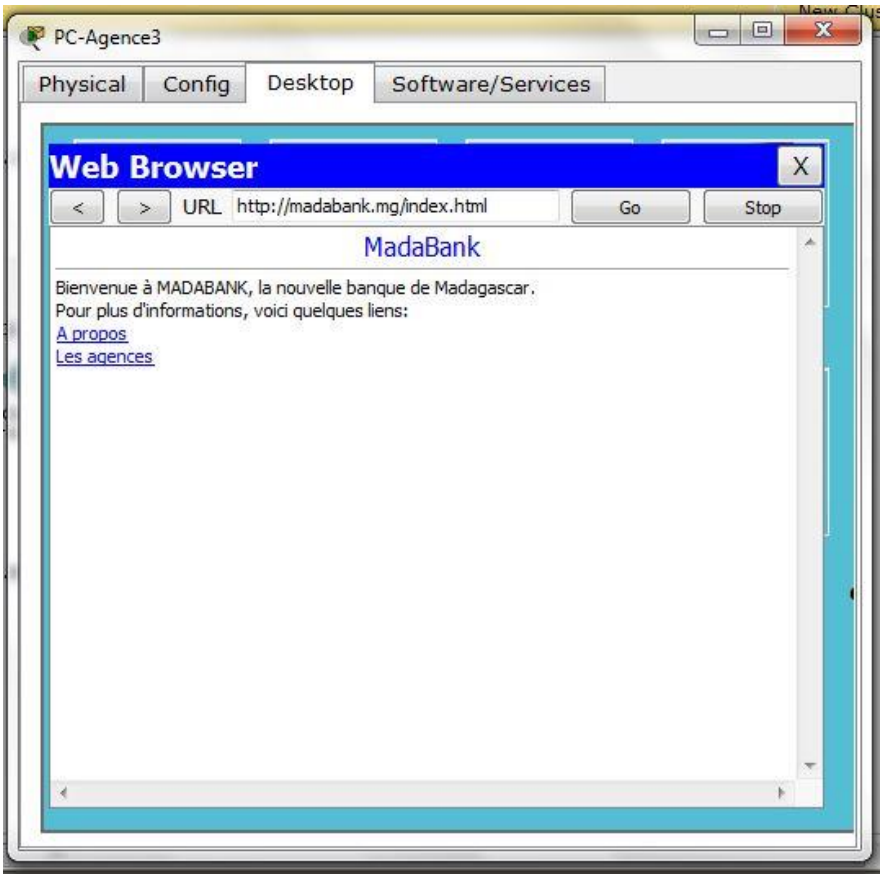


Figure 5.25 : *Un employé de l'agence 3 accèdant à la page web d'accueil de l'entreprise*

Dans la page d'accueil du site web de l'entreprise, nous avons deux liens « A propos » et « Les Agences » qui présentent successivement une petite historique de l'entreprise et ses différentes agences. Ce site illustre seulement l'accès des clients du réseau au serveur web.

5.5 Conclusion

Après avoir mis en place la topologie du réseau de l'entreprise MADABANK et configuré tous les équipements pour son bon fonctionnement sous le logiciel de simulation Packet Tracer, plusieurs tests et vérifications sont effectués tels que la vérification de toutes les tables de routage des routeurs, le test d'interconnexion entre les périphériques du Siège de l'entreprise et ceux des différentes agences, le test de connexion avec le serveur Email à partir d'un échange de message entre deux hôtes et enfin l'accès au site web de l'entreprise.

Tous ces tests s'avèrent tous vérifiés. Toutes les configurations ont donc été justes, le réseau de l'informatique est en marche. On a alors aboutit à un prototype qui peut être réalisé avec des équipements physiques réels.

CONCLUSION GENERALE

Pour mettre en place un réseau informatique, il est d'abord nécessaire de connaître le principe de fonctionnement du réseau en prenant compte des fonctions des différentes couches du modèle de référence ainsi que les protocoles utilisés. Ensuite, nous devons avoir quelques connaissances concernant tous les dispositifs à utiliser tels que les équipements de réseau (routeur, serveur,…) et les différents types de médias avec leurs caractéristiques respectives afin de les choisir pour les conditions adéquates.

Les différents types de réseaux sont associés. En effet, le réseau étendu WAN sert à interconnecter les réseaux locaux. On parle ainsi d'un réseau intersites. C'est le cas concret d'une entreprise présentant un siège et plusieurs succursales distantes. Une des technologies que nous avons utilisée, permettant cette interconnexion, est le Frame Relay. Ce réseau de transport est le plus utilisé par les entreprises du fait de sa facilité de mise en œuvre, de son coût abordable et de sa qualité de service satisfaisante. Nous avons créé l'entreprise fictive MADABANK pour illustrer les méthodologies nécessaires pour la conception d'un réseau.

Ce mémoire nous a aussi montré l'intérêt d'un outil de simulation de réseau comme le Packet Tracer pour vérifier les configurations des équipements et tester leurs interconnexions. En effet, dans le cas réel, il est plus lent, plus difficile et surtout plus cher de faire des modifications de configurations et des topologies ; les risques d'erreurs augmentent aussi. Le logiciel de simulation permet alors au concepteur réseau de posséder un total contrôle du fonctionnement du réseau dans son ensemble.

ANNEXES

ANNEXE 1 : CONFIGURATIONS DU RESEAU

A1.1 Configurations des différents routeurs

A1.1.1 Configuration du routeur du siège

- *Configuration de base*

```
Router#configure terminal
Router(config)#hostname SiègeTana
SiègeTana(config)#enable password tco
SiègeTana(config)#enable secret licence
SiègeTana(config)#line console 0
SiègeTana(config-line)#password tco
SiègeTana(config-line)#login
SiègeTana(config-line)#exit
SiègeTana(config)#line vty 0 4
SiègeTana(config-line)#password tco
SiègeTana(config-line)#login
SiègeTana(config-line)#exit
SiègeTana(config)#interface Fa0/0
SiègeTana(config-if)#ip address 192.168.13.1 255.255.255.224
SiègeTana(config-if)#no shutdown
SiègeTana(config-if)#exit
SiègeTana(config)#interface Fa0/1
SiègeTana(config-if)#ip address 192.168.13.33 255.255.255.224
SiègeTana(config-if)#no shutdown
SiègeTana(config-if)#exit
SiègeTana(config)#interface Fa1/0
SiègeTana(config-if)#ip address 192.168.13.225 255.255.255.224
SiègeTana(config-if)#no shutdown
SiègeTana(config-if)#exit
SiègeTana(config)#interface S0/0
SiègeTana(config-if)#ip address 192.168.13.161 255.255.255.224
SiègeTana(config-if)#no shutdown
SiègeTana(config-if)#exit
SiègeTana(config)#interface S0/1
SiègeTana(config-if)#ip address 192.168.13.193 255.255.255.224
SiègeTana(config-if)#no shutdown
SiègeTana(config-if)#exit
SiègeTana(config)#interface S0/2
SiègeTana(config-if)#ip address 193.127.32.161 255.255.255.252
SiègeTana(config-if)#no shutdown
SiègeTana(config-if)#exit
SiègeTana(config)#router eigrp 1
```

```
SiègeTana(config-router)#network 192.168.13.0 0.0.0.31
SiègeTana(config-router)#network 192.168.13.0 0.0.0.31
SiègeTana(config-router)#network 192.168.13.32 0.0.0.31
SiègeTana(config-router)#network 192.168.13.224 0.0.0.31
SiègeTana(config-router)#network 192.168.13.160 0.0.0.31
SiègeTana(config-router)#network 192.168.13.192 0.0.0.31
SiègeTana(config-router)#network 193.127.32.4 0.0.0.3
SiègeTana(config-router)#^Z
```

- *Configuration du routeur en tant que serveur DHCP*

```
SiègeTana#configure terminal
SiègeTana(config)#ip dhcp excluded-address 192.168.13.1
SiègeTana(config)#ip dhcp pool LAN1
SiègeTana(dhcp-config)#network 192.168.13.0 255.255.255.224
SiègeTana(dhcp-config)#default-router 192.168.13.1
SiègeTana(dhcp-config)#dns-server 192.168.13.226
SiègeTana(dhcp-config)#exit
SiègeTana(config)#ip dhcp excluded-address 192.168.13.33
SiègeTana(config)#ip dhcp pool LAN2
SiègeTana(dhcp-config)#network 192.168.13.32 255.255.255.224
SiègeTana(dhcp-config)#default-router 192.168.13.33
SiègeTana(dhcp-config)#dns-server 192.168.13.226
SiègeTana(dhcp-config)#exit
```

- *Configuration du Frame Relay*

```
SiègeTana(config)#interface S0/2
SiègeTana(config-if)#encapsulation frame-relay
SiègeTana(config-if)#frame-relay map ip 193.127.32.9 103 broadcast
SiègeTana(config-if)#exit
```

A1.1.2 Configuration du routeur de l'agence 1

- *Configuration de base*

```
Router#configure terminal
Router(config)#hostname Agence1
Agence1(config)#enable password tco
Agence1(config)#enable secret licence
Agence1(config)#line console 0
Agence1(config-line)#password tco
Agence1(config-line)#login
Agence1(config-line)#exit
Agence1(config)#line vty 0 4
Agence1(config-line)#password tco
Agence1(config-line)#login
Agence1(config-line)#exit
Agence1(config)#interface Fa0/0
Agence1(config-if)#ip address 192.168.13.65 255.255.255.224
```

```
Agence1(config-if)#no shutdown
Agence1(config-if)#exit
Agence1(config)#interface S0/1/0
Agence1(config-if)#ip address 192.168.13.190 255.255.255.224
Agence1(config-if)#no shutdown
Agence1(config-if)#exit
Agence1(config)#router eigrp 1
Agence1(config-router)#network 192.168.13.64 0.0.0.31
Agence1(config-router)#network 192.168.13.160 0.0.0.31
Agence1(config-router)#^Z
```

- *Configuration du routeur en tant que serveur DHCP*

```
Agence1#configure terminal
Agence1(config)#ip dhcp excluded-address 192.168.13.65 192.168.13.66
Agence1(config)#ip dhcp pool LAN3
Agence1(dhcp-config)#network 192.168.13.64 255.255.255.224
Agence1(dhcp-config)#default-router 192.168.13.65
Agence1(dhcp-config)#dns-server 192.168.13.226
Agence1(dhcp-config)#exit
```

A1.1.3 Configuration du routeur de l'agence 2

- *Configuration de base*

```
Router#configure terminal
Router(config)#hostname Agence2
Agence2(config)#enable password tco
Agence2(config)#enable secret licence
Agence2(config)#line console 0
Agence2(config-line)#password tco
Agence2(config-line)#login
Agence2(config-line)#exit
Agence2(config)#line vty 0 4
Agence2(config-line)#password tco
Agence2(config-line)#login
Agence2(config-line)#exit
Agence2(config)#interface Fa0/0
Agence2(config-if)#ip address 192.168.13.97 255.255.255.224
Agence2 (config-if)#no shutdown
Agence2(config-if)#exit
Agence2(config)#interface S0/1/0
Agence2(config-if)#ip address 192.168.13.222 255.255.255.224
Agence2(config-if)#no shutdown
Agence2(config-if)#exit
Agence2(config)#router eigrp 1
Agence2(config-router)#network 192.168.13.96 0.0.0.31
Agence2(config-router)#network 192.168.13.192 0.0.0.31
Agence2(config-router)#^Z
```

- *Configuration du routeur en tant que serveur DHCP*

```
Agence2#configure terminal
Agence2(config)#ip dhcp excluded-address 192.168.13.97
Agence2(config)#ip dhcp pool LAN4
Agence2(dhcp-config)#network 192.168.13.96 255.255.255.224
Agence2(dhcp-config)#default-router 192.168.13.67
Agence2(dhcp-config)#dns-server 192.168.13.226
Agence2(dhcp-config)#exit
```

A1.1.4 Configuration du routeur de l'agence 3

- *Configuration de base*

```
Router#configure terminal
 Router(config)#hostname Agence3
Agence3(config)#enable password tco
Agence3(config)#enable secret licence
Agence3(config)#line console 0
Agence3(config-line)#password tco
Agence3(config-line)#login
Agence3(config-line)#exit
Agence3(config)#line vty 0 4
Agence3(config-line)#password tco
Agence3(config-line)#login
Agence3(config-line)#exit
Agence3(config)#interface Fa0/0
Agence3(config-if)#ip address 193.127.32.9 255.255.255.252
Agence3(config-if)#no shutdown
Agence3(config-if)#exit
Agence3(config)#interface S0/1/0
Agence3(config-if)#ip address 192.168.13.6 255.255.255.252
Agence3(config-if)#no shutdown
Agence3(config-if)#exit
Agence3(config)#router eigrp 1
Agence3(config-router)#network 193.127.32.4 0.0.0.3
Agence3(config-router)#network 193.127.32.8 0.0.0.3
Agence3(config-router)#^Z
Agence3(config)#ip route 192.168.13.0 255.255.255.224 192.168.13.1
Agence3(config)#ip route 192.168.13.32 255.255.255.224 192.168.13.33
Agence3(config)#ip route 192.168.13.224 255.255.255.224 192.168.13.225
Agence3(config-router)#^Z
```

- *Configuration du routeur en tant que serveur DHCP*

```
Agence3#configure terminal
Agence3(config)#ip dhcp excluded-address 193.127.32.9
Agence3(config)#ip dhcp pool LAN5
Agence3(dhcp-config)#network 193.127.32.8 255.255.255.252
```

```
Agence3(dhcp-config)#default-router 193.127.32.9
Agence3(dhcp-config)#dns-server 192.168.13.226
Agence3(dhcp-config)#exit
```

- *Configuration du Frame Relay*

```
Agence3(config)#interface S0/1/0
Agence3(config-if)#encapsulation frame-relay
Agence3(config-if)#frame-relay map ip 193.127.32.5 301 broadcast
Agence3(config-if)#exit
```

A1.2 Configurations des serveurs et du Nuage de Frame Relay

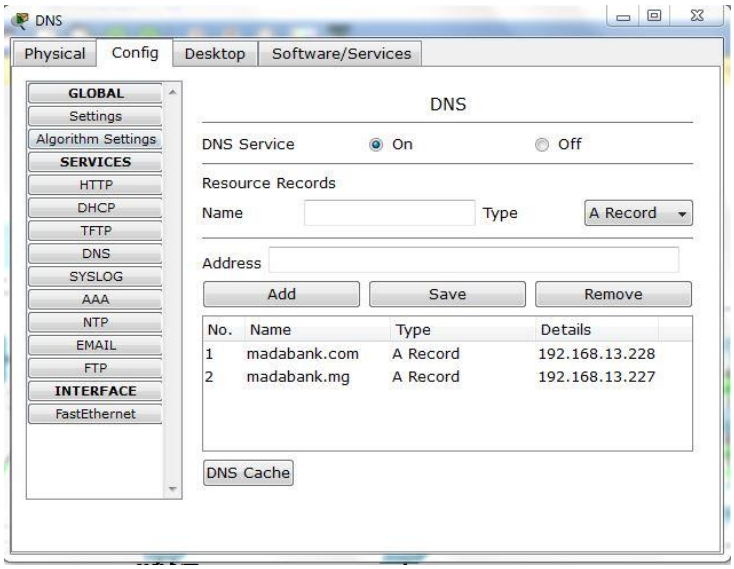


Figure 5.26 : *Serveur DNS*

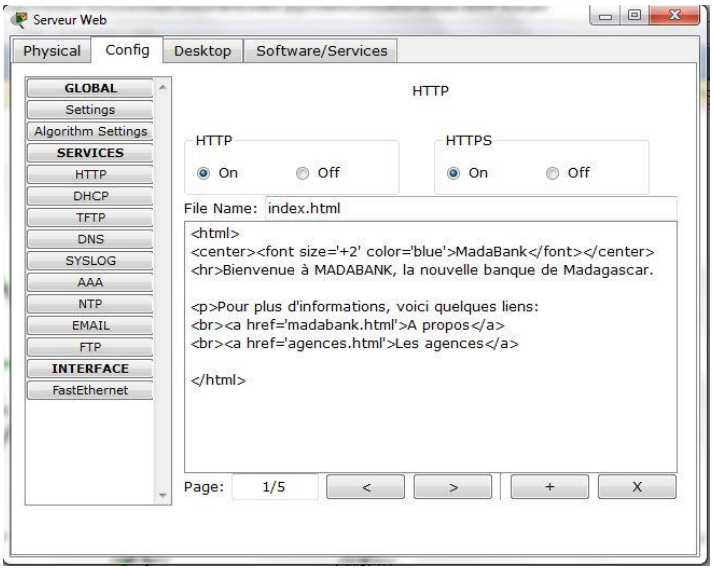


Figure 5.27 : *Serveur Web*

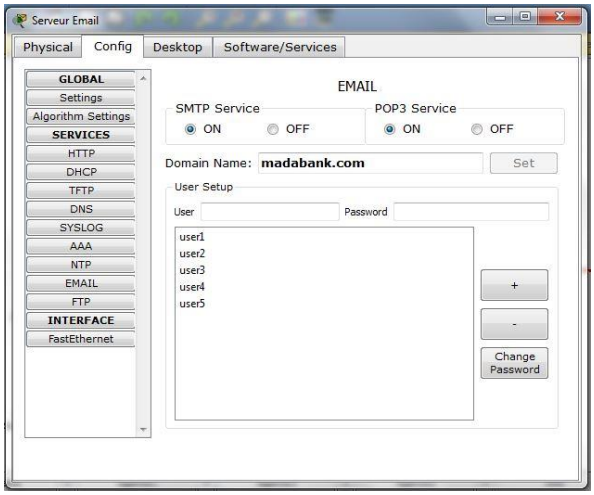


Figure 5.28 : *Serveur Email*

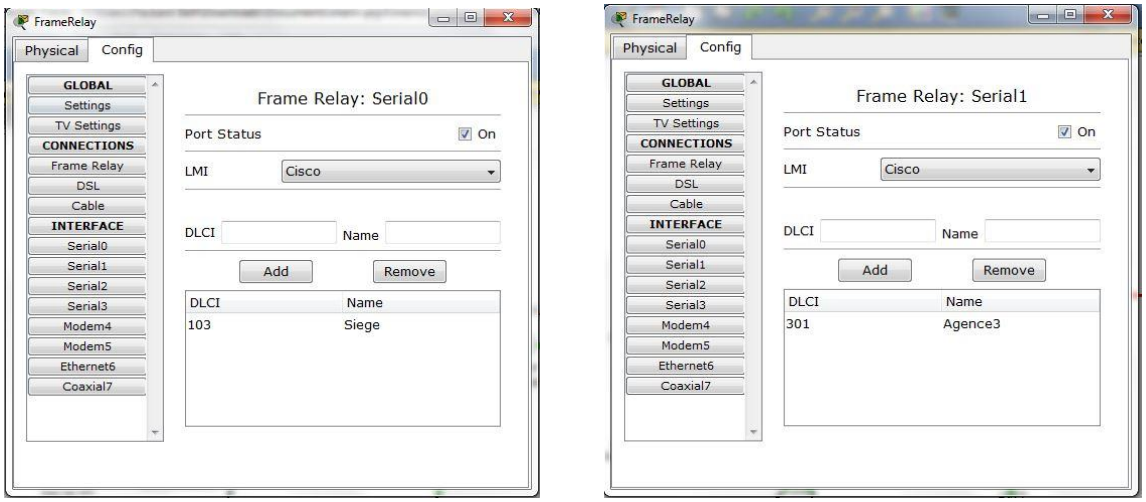


Figure 5.29 : *Configuration des DLCI sur les interfaces*

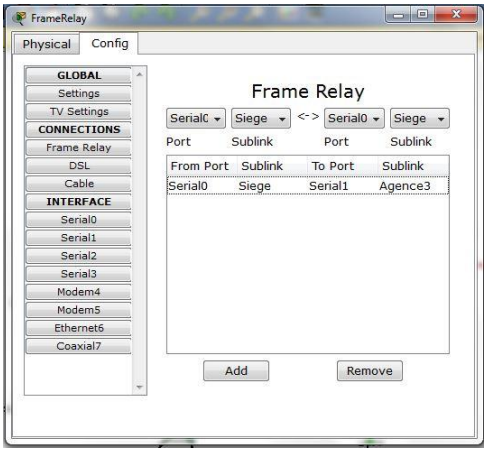


Figure 5.30 : *Configuration du Frame Relay*

ANNEXE 2 : PACKET TRACER

A2.1 Différents équipements

Packet Tracer propose les principaux équipements réseaux composant nos réseaux actuels. 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 via CLI.

On peut trouver un routeur, un commutateur, des terminaux (ordinateur, portable, serveur, imprimante et téléphone IP), un point d'accès Modem, un concentrateur.

Sachant que chaque équipement se voit attribuer un certain nombre de modules, permettant d'ajouter soit des ports supplémentaires, soit des nouveaux types de port. Les équipements propriétaires Cisco ont la possibilité de se voir attribuer les nouveaux IOS disponibles sur le site Cisco, si ceux-ci sont compatibles. Ces IOS peuvent ajouter de nouvelles fonctionnalités ou options de configuration.

Périphérique	**Symbole**
PC	
Serveur	
Imprimante	
Téléphone IP	
Switch	
Pont	
Répéteur	
Hub	

Périphérique	Symbole
Commutateur de niveau 3	
Routeur	
Routeur Wifi	
Modem cable	
Modem DSL	
Point d'accès Wifi	

Tableau 5.04: *Les équipements de Packet Tracer*

A2.2 Principaux protocoles

Couche	Protocoles
Physique	Pas d'objet
Liaison de données	Ethernet (802.3), 802.11, HDLC, Frame Relay, PPP STP, RSTP, VTP, DTP, CDP, 802.1q, PAgP, LACP L2 QoS, SLARP, Auto Secure Wifi: Simple WEP, WPA, EAP
Réseau	IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, GRE, ISAKMP Routage: RIPv1/v2/ng, Multi-Area OSPF, EIGRP, Static Routing Sécurité: Context Based Access Lists , Zone-based policy firewall et Intrusion Protection System (sur certain routeur) Multilayer Switching, L3 QoS, NAT
Transport	TCP and UDP, TCP Nagle Algorithm & IP Fragmentation
Session	Pas d'objet
Présentation	Pas d'objet

Couche	Protocoles
Application	HTTP, HTTPS, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, Radius, TACACS, Syslog

Tableau 5.05: *Les principaux protocoles utilisés*

A2.3 Principales connexions possibles

Média	Description
Câble Console 	les connexions console peuvent être établies entre PC 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 sérials se font entre 2 ports séries. Elles sont souvent utilisées pour simuler des liens WAN. Le 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.

Tableau 5.06: *Les principales connexions possibles*

BIBLIOGRAPHIE

[1] L. E. Randriarijaona, *« Réseau TCP/IP »*, Cours L3 – TCO, Dép. TCO.- E.S.P.A., A.U. : 2012-2013.

[2] D. Tilloy, *« Introduction aux réseaux TCP/IP »*, Support de cours, Institut Universitaire de Technologie d'Amiens, A.U : 1998-1999

[3] Cisco Networking Academy, *« CCNA 2.1.2 »*, Cisco Systems, 2000

[4] J. L. Montagnier, *« Construire son réseau d'entreprise »*, Eyrolles, 2001

[5] Cisco Networking Academy, « CCNA Discovery 4.0 », Cisco Systems, 2007-2008

[6] D. Dromard, D. Seret, « *Architecture des réseaux* », Pearson Education : France, 2009

[7] T. Vaira, « *Cours Réseaux – Adressage IP »*, BTS IRIS, 2012

[8] E. Robin, L. Boudin, G. Tourres, *« Essentiel CCNA 3»*, Laboratoire SUPINFO des Technologies Cisco, 2005

[9] Cisco Networking Academy, « CCNA Exploration 4.0 », Cisco Systems, 2007-2008

[10] E. Robin, L. Boudin, G. Tourres, M. Vernerie, *« Essentiel CCNA 4»*, Laboratoire SUPINFO des Technologies Cisco, 2005

[11] Cisco Networking Academy, *« Packet Tracer 4.11 »*, http://www.labo-cisco.com

[12] J. L. Montagnier, *« Réseau d'entreprise par la pratique »*, Eyrolles 2004

[13] E. Robin, L. Boudin, G. Tourres, *« Essentiel CCNA 1»*, Laboratoire SUPINFO des Technologies Cisco, 2005

[14] E. Robin, L. Boudin, G. Tourres, *« Essentiel CCNA 2»*, Laboratoire SUPINFO des Technologies Cisco, 2005

[15] G. Pujolle, « *Cours Réseaux et Télécoms»*, Eyrolles 3è Edition, 2008

[16] G. Pujolle, *« Les réseaux, Annexes »*, Eyrolles, Edition 2011