N° d'ordre : 21 / IRS / TCO Année Universitaire : 2014 / 2015

UNIVERSITÉ D'ANTANANARIVO

ÉCOLE SUPÉRIEURE POLYTECHNIQUE

DÉPARTEMENT TÉLÉCOMMUNICATIONS

MÉMOIRE

en vue de l'obtention du GRADE de

LICENCE

Mention : TÉLÉCOMMUNICATIONS
Parcours : Ingénierie des Réseaux et Systèmes

par : **RAZAFIMAHALEO Kiady Herilala**

Titre :

« CONCEPTION D'UN RESEAU DE CAMPUS D'ENTREPRISE AVEC IMPLEMENTATION D'UNE ZONE DMZ»

Soutenu le 19 Avril 2016 devant la Commission d'Examen composée de :

Président :
MonsieurANDRIAMIASY Zidora

Examinateurs :
Monsieur RATSIMBAZAFY Andriamanga
MonsieurRATSIHOARANA Constant
MonsieurRANDRIAMANAMPY Samuel

Directeur de mémoire : MonsieurRANDRIARIJAONA Lucien Elino

REMERCIEMENTS

Tout d'abord, je rends grâce au Seigneur d'avoir donné la force, la santé et la sagesse, sans quoi je n'aurai pas pu achever le présent mémoire.

Je suis reconnaissant envers Monsieur ANDRIANAHARISON Yvon, Professeur Titulaire, Responsable de Domaine de l'École Supérieure Polytechnique d'Antananarivo, Monsieur RAKOTOMALALA Mamy Alain, Maître de Conférences, Responsable de la Mention Télécommunication, de m'avoir accueilli au sein de l'établissement.

Mes sincères remerciements pour Mr ANDRIAMIASY Zidora, Maître de Conférences, Enseignant au sein de la Mention Télécommunication, qui me fait l'honneur de présider le jury de ce mémoire ;

Je remercie aussi les membres du jury:

- Mr RATSIMBAZAFY Andriamanga, Maitre de Conférences, Enseignant au sein de la Mention Télécommunication ;
- Mr RATSIHOARANA Constant, Maitre de Conférences, Enseignant au sein de la Mention Télécommunication ;
- Mr RANDRIAMANAMPY Samuel, Assistant d'Enseignement et de recherche, Enseignant au sein de la Mention Télécommunication ;

Qui ont eu l'amabilité d'examiner ce mémoire malgré leurs nombreuses occupations.

Je remercie chaleureusement Mr RANDRIARIJAONA Lucien Elino, Assistant d'Enseignement et de recherche au sein de la mention Télécommunication, Directeur de ce mémoire, pour son inestimable conseil et son aide durant l'élaboration de ce mémoire.

Mes vifs remerciements s'adressent également à tous les Enseignants et les Personnels Administratifs de l'École Supérieure Polytechnique d'Antananarivo.

J'adresse enfin mes profonds et sincères remerciements à toute ma famille, à tous mes amis, à tous mes collègues de classe et toutes les personnes, qui, de près ou de loin, ont contribué à l'élaboration de ce mémoire pour leur amour, leurs encouragements et leur soutien constant durant mes études.

TABLE DES MATIÈRES

NOTATIONS ET ABRÉVIATIONS

ACK	Acknowledgement Number ou numéro d'acquittement
ADSL	Asymmetric Digital Subscriber Line
ARP	Address Resolution Protocol
ARPAnet	Advanced Research Projects Agency Network
ASA	Adaptive Security Appliances
ASN1	Abstract Syntax Notation One
ATM	Asynchronous Transfert Mode
BGP	Border Gateway Protocol
BLR	Boucle Local Radio
BSS(ID)	Basic Service Set (Identifier)
CERN	Conseil européen pour la recherche nucléaire
CIDR	Classless InterDomain Routing
CRC	Cyclic Redondancy Code
CSMA/CD	Carrier Sense Multiple Access With Collision Detection
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Service
DoD	Department of Defense
EGP	Exterior Gateway Protocol
ESS	Extended Service Set
FAI	Fournisseur d'Accès Internet
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HDLC	High level Data Link Control

HSRP	Hot Standby Routing Protocol
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfert Protocol
IANA	Internet Assigned Numbers Authority
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGP	Interior Gateway Protocol
IP	Internet Protocol
IRP	Interior Routing Protocol
ISO	International Organization for Standradization
ITU	International Telecommunication Union
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MAN	Metropolitian Area Networks
MID	Man In the Middle
NAT	Network Address Translation
ND	Neighbor Discovery
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
P.M.E	Petites et Moyennes Entreprises
PAN	Personnal Area Network
PAT	Port Address Translation
PDU	Protocol Data Unit
PPDIOO	Prepare Plan Design Implement Operate Optimize

RARP	Reverse Address Resolution Protocol
RIP	Routing Information Protocol
RSA	Rivest, Shamir et Adleman
RC4	Ron’s Code 4
RTPC	Réseau Téléphonique Public Commuté
SSH	the Secure SHell
STP	Spanning Tree Protocol
SYN	Synchronization
TCP	Transmission Control Protocol
Telnet	Telecommunication Network
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless-Fidelity
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitian Area Network
WWW	World Wide Web

INTRODUCTION GÉNÉRALE

Depuis le siècle dernier, maximum de production, de profit, de bénéfice deviennent les priorités de toutes organisations gouvernementales et non-gouvernementales, des entreprises et des industries de notre temps. L'arrivée des réseaux informatiques a encore plus mis en valeur ces principes. Partager les ressources et les informations à temps réel est devenu possible. Chacun a alors créé leur propre réseau, un réseau qui, au fil du temps, a été standardisé par quelques organisations internationales qui sont très connues de nos jours. L'accès au service internet devient fondamental pour assurer les activités quotidiennes. Actuellement, beaucoup de tâches ne peuvent être accomplies sans lui. Alors, posséder une infrastructure réseau fonctionnelle devient nécessaire.

Cependant, le réseau doit évoluer parallèlement à l'évolution de chaque entreprise pour assurer leurs besoins proprement dite. Ainsi, la productivité suit le rythme de l'évolution et les profits, de même. Un réseau doit être alors bien conçu minutieusement. Par ailleurs, les types de trafic, qu'il soit vidéo ou voix, qui circule au sein du réseau d'entreprise se multiplient progressivement, il est essentiel de les contrôler et de s'assurer qu'aucun de ces trafics ne se rentre en conflit. Les pannes sont à éviter, le moindre point de défaillance est à exclure. La transparence et la disponibilité prouvent une bonne conception, du point de vue des utilisateurs. Accompagnant toutes ces évolutions, la concurrence et la curiosité ont causé la naissance des hackers, spécialement ceux appelés « black hat ». Les vols d'informations et de données sensibles deviennent un travail très rémunéré. Le monde du réseau et de l'internet deviennent ainsi très exposé à divers attaques. Il est né alors le besoin de sécuriser les données. Plusieurs sont les techniques de sécurisation déjà conçues et créés. Nombreux ceux qui ont des failles, et nombreux ceux encore en cours de conception.

Ainsi, une question se pose: « comment créer un réseau sécurisé et efficace pour une entreprise tout en partageant des informations sur Internet ? ». C'est à cette question que le présent mémoire tient à répondre. Celui-ci se déclinera en trois parties : la première sera destinée aux généralités sur le réseau informatique, la deuxième sur la conception d'un réseau et le dernier sur sa création.

CHAPITRE 1

GENERALITE SUR LES RESEAUX INFORMATIQUES

1.1 Historique

En 1969, le département américain de la Défense (DoD ou Departement of Defense) décide de construire un réseau appelé ARPAnet (Advanced Research Projects Agency Network). Une dizaine de sites sont donc connectés par un réseau maillé, non hiérarchique, basé sur le protocole IP (Internet Protocol). Ce réseau était utilisé pour le courrier électronique et en 1972, Il ne comptait encore qu'une quarantaine d'ordinateurs, des ordinateurs militaires et universitaires.

Durant cette même année, les spécifications des protocoles TCP/IP (Transfert Control Protocol/IP) avec l'expérience de l'usage de X25 sur ARPAnet commencèrent. Le but était de concevoir un réseau qui résiste à des attaques militaires telles que des bombardements. Ainsi, il ne devait pas y avoir de point névralgique dans le réseau, dont l'arrêt aurait provoqué le blocage complet de celui-ci, et les données devaient pouvoir automatiquement prendre un chemin différent en cas de coupure de liaison. D'où l'absence de contrôle centralisé dans l'internet et un cheminement dynamique des données.

Mis dans le domaine public, il fut repris par les universitaires en 1979 (La Duke University à Durham Caroline du Nord), qui y virent le moyen d'échanger des informations. Durant ces temps-là, l'informatique était centralisée. De grosses machines travaillaient en temps partagé pour plusieurs utilisateurs. Après les militaires et les universitaires l'Internet devient aux États-Unis l'affaire des grandes entreprises privées, des P.M.E. (Petites et Moyennes Entreprises) et des particuliers. En 1983, c'est au tour de l'Europe et du reste du monde de se connecter à ce réseau de réseaux [1].

L'arrivée du web dans l'internet en 1992 a eu un grand impact dans le partage d'information. Le web, appelé encore World Wide Web (WWW) était développé par le CERN (Conseil Européen pour la Recherche Nucléaire) à Genève. Il constitue un moyen simple d'organiser l'information et la navigation sur Internet par des hyperliens, en utilisant le format de fichier HTML (Hyper Text Markup Language). En ce moment-là, les ordinateurs personnels étaient déjà inventés. L'internet connecte déjà plusieurs ordinateurs, facilitant ainsi la communication. C'est l'un des plus grandes inventions en télécommunication.

1.2 Réseau

Un réseau informatique est un ensemble de plusieurs ordinateurs reliés entre eux par un système de communication permanent.

Les réseaux sont nés d'un besoin d'échanger des informations de manière simple et rapide entre machines. Ils ont pour objectif de :

- Permettre le partage des ressources : un utilisateur peut changer de poste de travail sans pour autant devoir transporter ses fichiers sur des supports de stockage
- Accroître la résistance aux pannes,
- Économiser les ressources (argent et temps)

1.2.1 Catégories de réseau

Distinguer les réseaux se fait en plusieurs manières, mais le critère le plus standard est l'espace géographique occupé. Le critère se base alors sur la distance des équipements et terminaux à connecter [2]. On parle ici de réseau :

- **Personnels** : PAN "Personal Area Network " aux dimensions d'une pièce, qui permettent l'interconnexion de matériel informatique comme les souris et claviers sans fil : Bluetooth
- **Locaux** : LAN "Local Area Network » pouvant s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise.
- **Métropolitains** : MAN "Metropolitan Area Networks" aux dimensions d'une ville, ce sont typiquement les réseaux auxquels on se connecte de chez soi pour l'accès à Internet. (ADSL ou Asymmetric Digital Subscriber Line, Câble).
- **Étendus** : WAN "Wide Area Networks" aux dimensions d'un pays ou de la planète (l'Internet).

1.2.2 Les normalisations

La technique usuelle en informatique pour résoudre un problème complexe consiste à le découper en problèmes simples à traiter. L'interconnexion réseau étant un problème complexe, on a donc abouti à des traitements séparés par niveaux ou couches.

1.2.2.1 Le modèle OSI

Le modèle OSI (Open System Interconnection) est le premier modèle standard utilisé pour assurer la compatibilité ou l'interopérabilité entre les équipements réseaux hétérogènes. Ainsi tous

leséquipements, ou ensemble d'équipements à interconnecter deviennent un système ouvert s'il respecte les normes d'interconnexions. Le modèle OSI est une architecture abstraite de communication, décrit dans la norme X.200 de l'ITU (International Telecommunication Union). Il est composé de sept couches, chacune remplissant une partie bien définie des fonctions permettant l'interconnexion. [3]

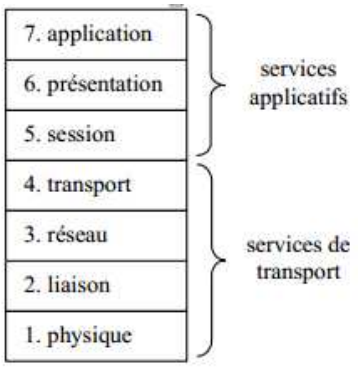

Figure 1.0 1 : *Sept couches de la modèle OSI.*

Les couches basses (1-4) gèrent le transfert de l'information par les différents services de transport. Les couches hautes (5-7) gèrent le traitement de l'information par les différents services applicatifs. [4]

a. Couche Physique

La couche physique fournit l'interface avec le support physique sur lequel elle transmet un train de bits en assurant, éventuellement, la transparence binaire. Elle se charge de la synchronisation entre les horloges source et destination. Elle ne prend pas en compte si c'est en mode connecté ou non-connecté. Cependant, elle prend en charge les transmissions synchrones ou asynchrones que ce soit en mode simplex ou semi-duplex ou duplex et que ce soit en mode point à point ou multipoint.[5]

Alors pour résumer, cette couche fournit :

- L'établissement et la libération de la connexion physique
- La transmission de bits
- L'identification des extrémités de la connexion physique qui peut être unique ou multiple
- Le maintien en séquence des bits émis
- La synchronisation d'horloge

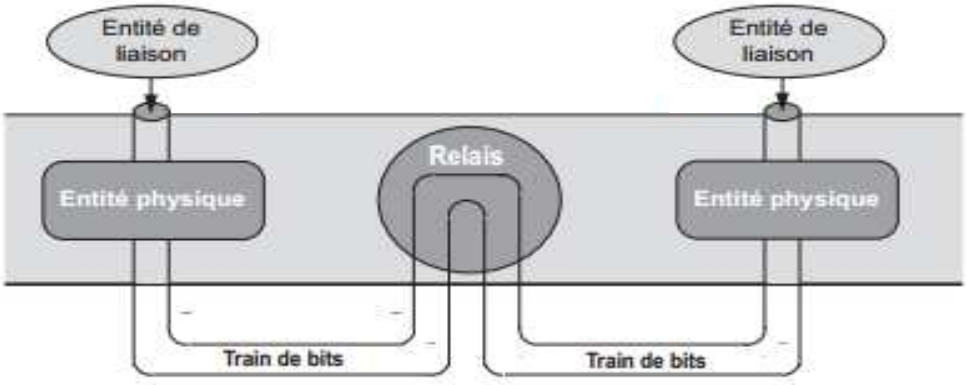

Figure 1.0 2 : *Principe de la couche physique.*

L'unité de données transportées par cette couche est le Bit. [6]

PDU (Protocol Data Unit) : bit

b. La couche liaison de données

Cette couche fournit les fonctions nécessaires pour transporter un bloc d'information, appelé trame, d'un nœud de transfert vers un autre nœud de transfert. Elle offre essentiellement les services suivante[5]:

- L'établissement, le maintien et a libération de la connexion logique établie entre deux points d'accès au service de liaison de données,
- La fourniture d'identificateur d'extrémité
- La délimitation et le transfert de données, en assurant
- Le maintien en séquence, c'est-à-dire :
  - ✓ La détection et la correction d'erreur
  - ✓ La notification d'erreur non corrigée
  - ✓ Le contrôle de flux

Cette couche est divisée en deux sous-couches :

- La sous-couche MAC (Media Access Control) où se trouve les protocoles de diffusion d'information tel que l'ATM, le Token Ring.
- La sous-couche LLC (Logical Link Control) ou HDLC (High Level Data Link Control) qui offre les services de base pour la transmission de données.

La qualité de service fournie s'exprime principalement par le taux d'erreurs résiduelles, ces erreurs pouvant provenir de données altérées, perdues, dupliquées ou du non-respect de l'ordonnancement des trames.

Pour résumer, elle fournit des outils de transmission de paquets de bits (trames) à la couche supérieure. Les transmissions sont garanties par des mécanismes de contrôle de validité.[6]

PDU : Trame

c. La couche réseau

Cette couche est dite de niveau paquet. Son rôle est de transporter les paquets, en formant un flot, d'un émetteur jusqu'à un récepteur connecté au même réseau. Elle permet alors d'acheminer correctement les paquets d'information jusqu'au récepteur en transitant par des nœuds de transfert intermédiaires.

En réalité, cette couche utilise des trames mais encapsulés, ce qui forme les paquets. Cette encapsulation permet la reconnaissance du début et de la fin de ce dernier.

Le niveau paquet comporte essentiellement trois principales fonctions : le contrôle de flux, le routage et l'adressage.[5]

- Le contrôle de flux évite les congestions dans le réseau
- Le routage permet d'acheminer les paquets d'informations vers leur destination, au travers du maillage des routeurs.
- L'adressage est la solution pour identifier le destinataire. Cela peut être une adresse complète ou une simple référence.

PDU : Datagramme/paquet

d. La couche transport

Cette couche est maintenant dite niveau message. C'est l'ultime niveau qui s'occupe l'acheminement de l'information. Son rôle est de compléter les fonctions des couches sous-jacentes qui sont insuffisant car son fonction de base est « le fragmentation-réassemblage » comme illustre la figure 1.0 3.

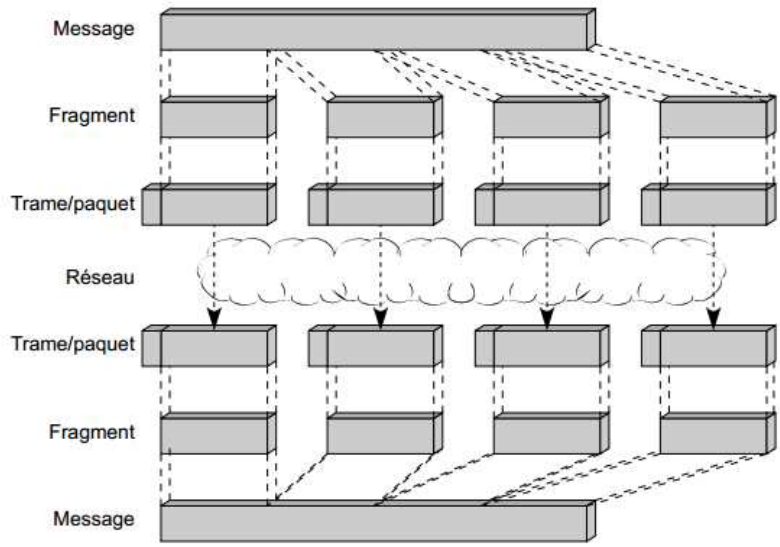

Figure 1.0 3 : *Principe de la couche transport.*

Les protocoles de niveau 4 vont de logiciels très simples, n'offrant que les fonctionnalités minimales de fragmentation et de réassemblage, à des logiciels de communication complexes, qui intègrent des fonctions de détection d'erreur et de reprise sur erreur, de contrôle de flux et de congestion, de resynchronisation,… [7]

Elle fournit alors aux couches supérieures un service de fiabilité au niveau du transport des données.

PDU : Message / segment/Fragment

e. La couche session

On le nomme maintenant « le niveau session ». Comme son nom l'indique, cette couche a pour but d'ouvrir et de fermer des sessions entre les utilisateurs. Ainsi elle fournit les moyens nécessaires à l'organisation et à la synchronisation du dialogue entre les clients en communication. Ces clients ou au moins leurs représentants (boîte aux lettres électroniques par exemple) doivent être présents lors du dialogue. [7]

La couche session possède alors les fonctionnalités nécessaires à l'ouverture, à la fermeture et au maintien de la connexion impliquant aussi la gestion des interruptions et les reprises de session.

f. Le niveau présentation

Cette couche met en forme les données transférées pour les rendre compréhensible par le destinataire. Elle se charge alors de la syntaxe des informations que les entités d'application se communiquent entre eux.

Cette couche joue un rôle important dans un environnement hétérogène. On l'a normalisé suivant des syntaxes de transfert, dont le plus courant est la syntaxe ASN 1 (Abstract Syntax Notation One) ou « la notation syntaxe abstraite N°1 (ISO 8824 Abstract Syntax Notation 1)(ISO pour International Organization for Standradization). Grâce à ASN 1, l'interopérabilité au niveau de la présentation des données est résolue. [7]

ASN1 fournit :

- une méthode pour décrire (syntaxe) les données échangées indépendamment des processeurs et systèmes d'exploitation ;
- un ensemble de types de données de base (types simples ou primitifs) pouvant être employés pour en construire d'autres (types construits) ;
- un ensemble de règles de construction de ces types et les opérateurs associés

g. Le niveau application

C'est la couche la plus abstraite du modèle de référence OSI. Elle s'occupe de la sémantique des données, contrairement au niveau présentation qui prend en charge la syntaxe.

En générale, elle est présentée par ce que voit l'usager. Elle fournit des éléments et services de base aux applications, c'est-à-dire les routines systèmes, la communication interprocessus, l'accès aux protocoles et aux services sur le réseau.

h. Transmission de donnée à travers le modèle OSI

La transmission des données dans le modèle OSI se fait par les encapsulations de décapsulation.

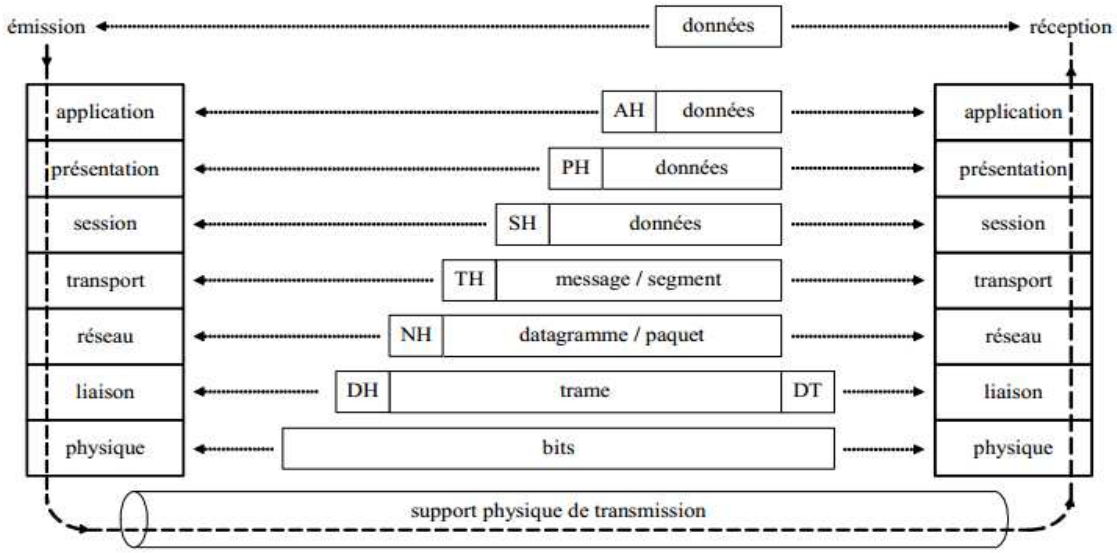

Figure 1.0 4 : *Transmission de données dans le modèle OSI.*

Il est important de noter que le modèle OSI, reste comme son nom l'indique, un simple modèle. Il n'est pas scrupuleusement respecté, mais vers lequel on tente généralement de se rapprocher. De plus, ce modèle a été historiquement établi après la mise en place de technologies ayant fait leurs preuves. Il ne peut pas toujours ainsi être rigoureusement suivi. C'est le cas pour le protocole TCP/IP.

1.2.2.2 Le modèle TCP/IP

Le modèle ou protocole TCP/IP est développée au départ par le ministère de la défense américain en 1981. Il est une évolution du réseau ARPAnet et est employé en très forte proportion sur le réseau internet. Au-delà de son aspect historique, TCP/IP doit aussi son succès à son indépendance vis-à-vis de tout constructeur informatique.

TCP/IP définit une suite de différentes protocolespour la communication sur un réseau informatique, notamment le protocole TCP et le protocole IP. Ce sont parmi les principaux protocoles de ce modèle.

Il est à noter que ce modèle est antérieur au modèle OSI, il ne respecte pas réellement celui-ci. Cependant, on peut considérer une correspondance des différents services utilisés et proposés par TCP/IP avec le modèle OSI. Ainsi, suivant cette correspondance, on peut dire que TCP/IP est un modèle en quatre couches.[*8*]

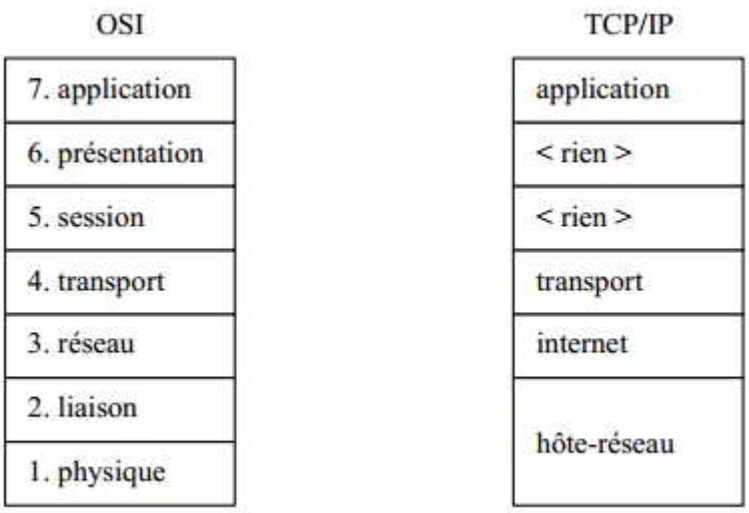

Figure 1.0 5 : *Correspondance entre le modèle OSI et TCP/IP avec les couches correspondantes.*

Les couches 1 et 2 du modèle OSI sont intégrées dans la couche hôte-réseau. Les couches 5 et 6 n'existent pas réellement dans le modèle TCP/IP mais leurs services sont réalisés par la couche application s'il y a le besoin.

a. Hôte-réseau ou Accès réseau

Cette couche intègre les services des couches physiques et liaison de donnée du modèle OSI. Elle a en charge la communication avec l'interface physique dans le but de transférer ou de récupérer les paquets qui lui sont transmis de la couche Internet. Cet interfaçage peut être assuré par divers protocoles. Mais cela dépend du réseau utilisé. (Ethernet en LAN, X25 en WAN, …).[8]

b. La couche Internet

La couche internet correspond à la couche réseau du modèle OSI. Elle s'occupe de l'acheminement, à bonne destination, des paquets de données. Cela intègre alors en lui la fonction de routage et de commutation de paquets à travers différents nœuds par rapport au trafic et à la congestion du réseau. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol). Ce protocole assure intégralement les services de cette couche..[8]

c. La couche transport

Cette couche, comme celle du modèle OSI, gèrent le fractionnement et le réassemblage en paquets du flux de données à transmettre. Ainsi, elle est chargée de l'ordonnancement des paquets à l'arrivée après la commutation. En plus elle prend aussi en charge les questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs..[8]

Les principaux protocoles qui assurent les services de cette couche sont le protocole TCP (Transfert Control Protocol) et l'UDP (Unit Datagram Protocol)

d. La couche application

La couche application gère les protocoles de haut niveau : représentation, codage et contrôle de dialogue. Elle correspond aux différentes applications utilisant les services réseaux pour communiquer à travers un réseau.

Un grand nombre de protocoles de haut niveau permettent d'assurer les services de cette couche, comme : Telnet (Telecommunication Network), FTP (File Transfer Protocol), HTTP (HyperText Transfert Protocole)

1.2.2.3 Les protocoles de communication des modèles OSI et TCP/IP

Pour que les paquets des données arrivent bien à destination dans le réseau, il est important que tous les équipements parlent la même langue ou protocole. Ces protocoles sont des règles qui déterminent le format et la transmission des données. Chaque couche des modèles de référence à leurs propres protocoles de communication.

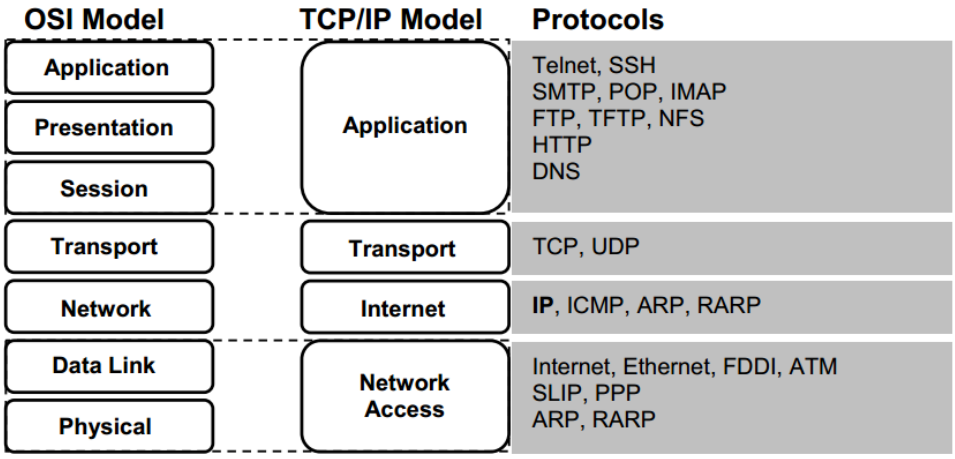

Figure 1.0 6 :*Protocoles de communication des modèles de référence.*

1.3 Les protocoles du modèle de référence TCP/IP

1.3.1 L'Ethernet

1.3.1.1 Historique

Robert Metcalfe, membre de la direction de recherche de la société Xerox, et son assistant David Boggs a conçu le premier LAN Ethernet au milieu des années 1970. L'entreprise Digital Equipment, Intel s'entraidaient ensuite ave Xerox pour promouvoir l'Ethernet comme un standard. Jusqu'à 1990, Ethernet ne s'est pas bien distinguer des autres technologies telles que le Token

Ring (IEEE 802.5), FDDI (Fiber Distributed Data Interface) (802.7), ATM (Asynchronous Transfert Mode). Mais petit à petit, il s'est propagé comme une norme pour les réseaux locaux bien que l'IEEE (Institute of Electrical and Electronics Engineers) s'est basée sur Ethernet pour définir une norme officiel qui est l'IEEE 802.3. Cependant cette nouvelle norme n'est pas complètement identique à celui de Xerox, ils se différencient par quelques détails. Depuis, peu de personne appelle l'Ethernet comme un protocole, mais il est maintenant considéré comme une norme, un standard.[9] [10]

1.3.1.2 Définition

L'Ethernet est un protocole, une norme de réseau local à commutation de paquets. Il est défini sur les deux premières couches du modèle OSI, à savoir la couche physique et la couche liaison de données. Il utilise une transmission en bande de base, et des trames pour la transmission au niveau liaison de données. Ce protocole se décline dans de nombreuses variantes. [9] [10]

1.3.1.3 Carrier Sense Multiple Access with Collision Detection

Dans la topologie Bus, les signaux électriques circulent sur le même câble. En plus, Ethernet considère les stations égaux, il n'y a pas de maître ni d'esclave. Toutes ses stations ont les mêmes priorités d'émission. Alors cela risque des collisions.

C'est la raison d'utilisation de la méthode CSMA/CD (Carrier Sense Multiple Access with Collision Detection). CSMA/CD est une technique d'accès au support de transmission et gère les collisions.[4]

Pour assurer la bonne transmission des données, les règles que chaque station doit suivre sont les suivants :

- Une station peut commencer à transmettre sur le support à n'importe quel moment. Mais, elle ne transmette pas quand il y a de l'activité sur le canal.
- La station interrompt sa transmission des qu'elle détecte une autre activité sur le canal.
- Avant de retransmettre, elle patiente pendant une durée aléatoire. Cela évite que deux stations ne décident de retransmettre en même temps.

1.3.1.4 Format des trames Ethernet

Une trame Ethernet est formée par le datagramme IP avec un ajout d'en-tête et d'en-queue.

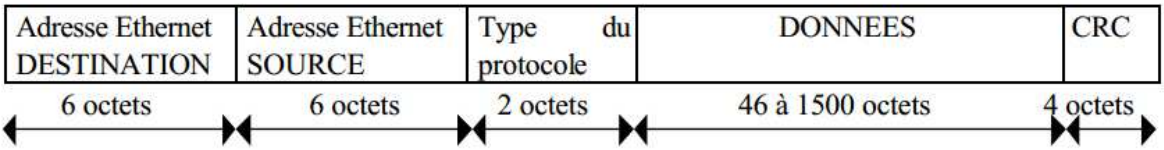

Figure 1.0 7 :*Trame Ethernet*

Les champs adresses Ethernet sont composés d'adresse MAC. L'adresse MAC est composée de deux parties : un identifiant de 24 bits assigné par l'IEEE, et un identifiant assigné par le fabricant matériel.

Valeur Ether Type	Protocole correspondant
0x0800	Datagramme IP
0x0806	ARP
0x0805	RARP
0x86DD	IPv6

Tableau 1.0 1

Ce tableau 1.01 représente des valeurs standards du champ « Type de protocole » ou **Ether Type**. Chaque valeur correspond à un protocole unique.

Le champ **CRC** (Cyclic Redondancy Code) est une valeur de 32 bits calculée par l'émetteur à partir des données à transmettre. La valeur CRC est utilisée par le récepteur pour vérifier qu'aucune erreur n'est faite lors de la transmission.

Cependant, la structure de la trame Ethernet a été normalisée par l'IEEE, après avoir été défini à l'origine par Xerox, Digital et Intel. Il existe donc deux types de trames Ethernet.

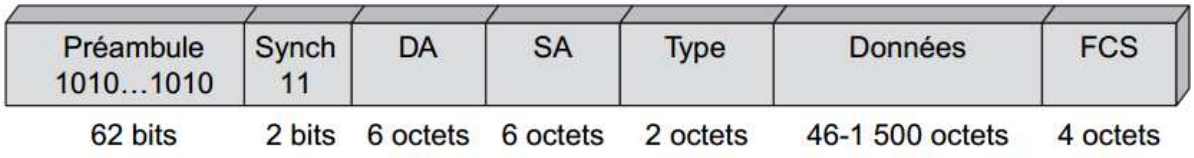

Figure 1.0 8 :*Format de trame Ethernet version Xerox.*

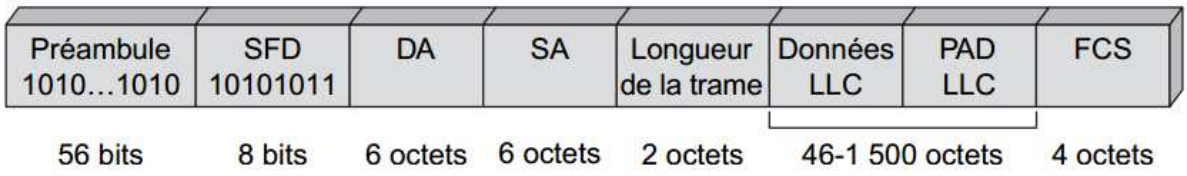

Figure 1.0 9 : *Format de trame Ethernet de l'IEEE.*

La trame Ethernet émise est toujours précédée d'un préambule. Ensuit il est suivit d'un champ **SFD** pour le cas de l'Ethernet normalisé et du champ **SYNCH** pour l'ancien trame Ethernet. Ils sont formés par une succession de 8 octets commençant par 1010 et ainsi de suite jusqu'à la fin du huitième coté qui se termine par 11. Il permet de synchroniser l'horloge de réception de toutes les stations. Les deux derniers bits 11 indiquent le début utile de la trame Ethernet.

Pour le cas de la trame Ethernet de l'IEEE, la zone Longueur de la trame (**Length**) indique la longueur du champ de données provenant de la couche supérieure. La trame encapsule ensuite le bloc de niveau trame proprement dit, ou trame LLC (Logic0al Link Control). Cette trame encapsulée contient une zone PAD, qui permet de remplir le champ de données de façon à atteindre la valeur de 46 octets, qui est la longueur minimale que doit atteindre cette zone pour que la trame totale fasse 64 octets en incluant les zones de préambule et de délimitation. [4]

1.3.2 Les protocoles IP, ICMP et ARP

1.3.2.1 Protocole IP

Le protocole IP est le protocole de base du réseau Internet. C'est un protocole pour l'interconnexion des réseaux, et sert à transporter les informations nécessaires à la réalisation de cette dernière.Ainsi, le moyen le plus simple pour interconnecter des réseaux est de leur demander de transporter un paquet commun, ayant le même format et une adresse commune, compréhensible par toutes les passerelles, comme les routeurs pour le cas de l'internet.[3][7]

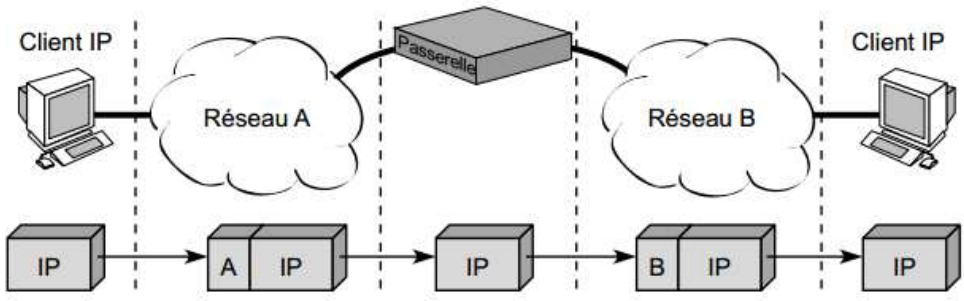

Figure 1.10 :*Interconnexion entre des réseaux IP.*

Ce protocole est utilisé par les protocoles de la couche transportet cherche constamment un chemin pour transférer les données (datagrammes) d'un équipement émetteur à un équipement destinataire.

Ainsi, il inclut un ensemble de règles, qui définissent comment traiter les paquets, gérer la fonction de routage.

En réalité, ce protocole ne fournit aucune garantie d'un acheminement correct des données et ne gère aucun dialogue avec le module IP d'une autre machine, c'est-à-dire qu'il propose un service sans connexion. Ce mode sans connexion explique les attentes assez longues lors de l'interrogation de serveurs très fréquentés. Même surchargés, ces derniers ne peuvent refuser l'arrivée de nouveaux paquets puisque l'émetteur ne demande aucune connexion, c'est-à-dire ne se préoccupe pas de savoir si le serveur accepte de les servir.[3]

Il existe une analogie entre le réseau physique et le réseau logique dans lequel s'inscrit IP. Dans un réseau physique, l'unité transférée est la trame, en réalité un paquet ou une trame du sous-réseau traversé. Cette trame comprend un en-tête et des données, données composées du paquet IP. L'en-tête contient les informations de supervision nécessaires pour acheminer la trame. Dans le réseau IP logique, l'unité de base à transférer est le paquet IP, que l'on appelle datagramme IP, Les datagrammes peuvent être d'une longueur quelconque. Comme ils doivent transiter de routeur en routeur, ils peuvent être fractionnés, de sorte à s'adapter à la structure de la trame sous-jacente. Ce concept est appelé l'encapsulation. Pour un sous-réseau, un datagramme est une donnée comme une autre. Dans le meilleur des cas, le datagramme est contenu dans une seule trame, ce qui rend la transmission plus performante. [7]

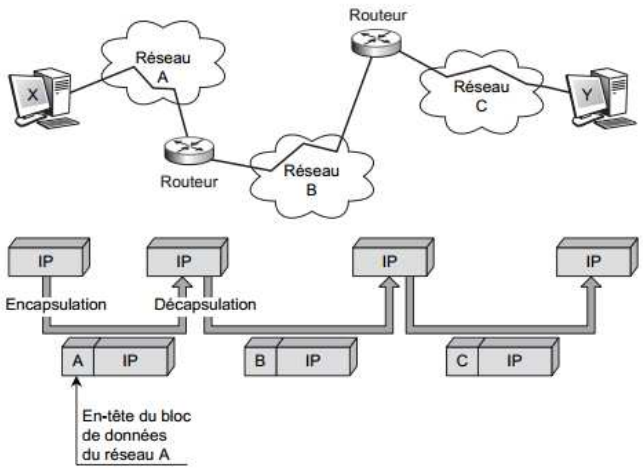

Figure 1.11 :*Transmission des données par le protocole IP.*

Jusqu'ici, ce protocole possède deux versions : IPv4 et IPv6

a. Le protocole IPv4

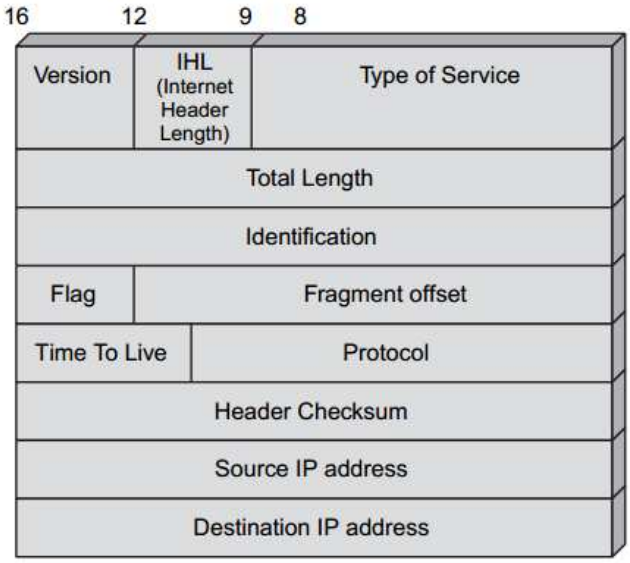

Figure 1.12 :*Datagramme IPv4.*

C'est la première version du protocole IP. Il est en ce moment le plus utilisé sur l'Internet. Le service rendu par ce protocole se fonde sur un système de remise de paquets non fiable. C'est ce qu'on appelle service « best effort » ou « au mieux » et sans connexion. La raison de ce non fiabilité est due à la remise non garantie d'un paquet. Un paquet peut être perdu, dupliqué ou remis hors séquence sans être détecter ni être connu par l'émetteur ou le récepteur.[4]

Sur la Figure 1.12, on trouve les champs suivants :

- Le champ **Version** indique le numéro de la version du protocole, donc c'est 4.
- Le champ **IHL** (Internet Header Length) indique la longueur de l'en-tête, cela permet de connaître l'emplacement du début des données du fragment IP.
- Le champ **ToS** (Type of Service) indique le type de service des informations transportées dans le corps du paquet
- Vient ensuite le champ « **longueur total** » du paquet.
- Le champ **Identification** identifie le message auquel appartient le paquet : le message a été découpé en paquets, il est alors nécessaire de faire connaître au récepteur à quel message appartient le paquet.
- Le champ **Flag** ou drapeau porte plusieurs notifications. S'il y a eu une segmentation, a place du segment est indiqué dans le champ **Offse**t (emplacement du Segment)

- Le champ **TTL** (Time To Live), ou temps de vie, indique le temps après lequel le paquet est détruit.
- Le champ **Protocol** indique le protocole encapsulé dans le paquet.
- **HeaderChecksum** est la zone de détection d'erreur permettant de déterminer si la transmission du paquet s'est faite correctement.
- Les deux derniers champs indiquent les adresses source et de destination.

Adresse IPv4 :

L'adresse IPv4 est représentée sur un entier de 32 bits soit 4 octets et écrite en notation décimale pointée : les octets sont séparés par des points. Ces octets sont représentés par des valeurs décimales soit entre 0 à 255. L'adresse est constituée de deux parties : un identificateur de réseau (Net ID) et un identificateur de machine (Host ID) pour ce réseau. Cependant, on catégorise ces adresses en cinq (5) classes :

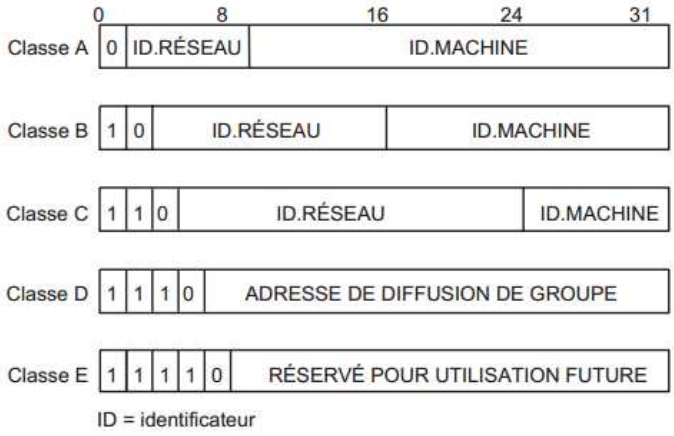

Figure 1. 13 : *Classes d'adresse IPv4.*

b. Notion de sous-réseau

Cette notion est introduite en 1984. L'adressage sur 32bits est encore conservé. Le but est de découpé un réseau en plusieurs sous-réseaux. Ce découpage n'est connu qu'à l'intérieur du réseau lui-même. C'est-à-dire qu'une adresse IP de réseau, vu de l'extérieur, reste une adresse sur 32 bits avec deux champs. Il est impossible de savoir si le réseau est subdivisé en plusieurs sous-réseaux. On parle ici de découpage de réseau avec Classe.

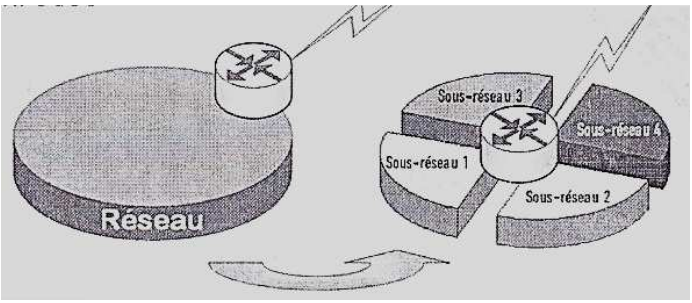

Figure 1. 14 : *Découpage de réseau.*

Le principe est d'emprunter un nombre de bits à définir dans l'adresse hôte afin d'en faire une adresse de sous réseau. Par exemple, 1 bit emprunté permet de définir deux sous-réseaux et donc de diviser l'espace de départ en deux parties égales. 2 bits empruntés permettent de définir 4 sous-réseaux et 3 bits 8 sous-réseaux.[12]

	B8	B7	B6	B5	B4	B3	B2	B1	Masque résultant du 4ème Octets	Nombre d'espace résultants	Taille de chaque espace	Adresses IP potentielles
Poids	128	64	32	16	8	4	2	1				
Exclu	1	0	0	0	0	0	0	0	128	2	128	126
Permis	1	1	0	0	0	0	0	0	192	4	64	62
Permis	1	1	1	0	0	0	0	0	224	8	32	30
Permis	1	1	1	1	0	0	0	0	240	16	16	14
Permis	1	1	1	1	1	0	0	0	248	32	8	6
Permis	1	1	1	1	1	1	0	0	252	64	4	2
Exclu	1	1	1	1	1	1	1	0	254	128	2	0

Tableau 1.0 2 : *Découpage d'une adresse IPv4 de classe C.*

c. Adressage sans classe CIDR

CIDR a pour acronyme Classless InterDomain Routing. C'est un concept proposé à partir de 1994. L'idée est d'organiser une adresse réseau indépendamment de sa classe. Le format de l'adresse IPv4 reste le même, mais le masque de sous-réseaux peut être fixé librement. On ne parle plus alors d'adresse de classe A ou B ou C. On peut noter le masque par « /n » ou n désigne ne nombre de bits 1 dans ce dernier et les « 32-n » bits seront réservés pour l'adresse machine. Le principe

découpage du réseau en sous-réseau reste le même. Mais on appelle le procédé VLSM ou Variable Length Subnet Mask.

CIDR affranchit les contraintes imposées par le format des classes d'adresse. Cependant, les seules restrictions concernent les adresses dévolues au réseau lui-même, à la diffusion dans le réseau et aux anciennes classes D et E de l'IPv4.[12]

d. Protocole IPv6 :

Parfois appelé IPng (IP next generation), IPv6 est un protocole entièrement repensé par rapport à IPv4. Il appartient au niveau paquet. On l'a créé vu la pénurie d'adresse IPv4 sur l'Internet.[4]

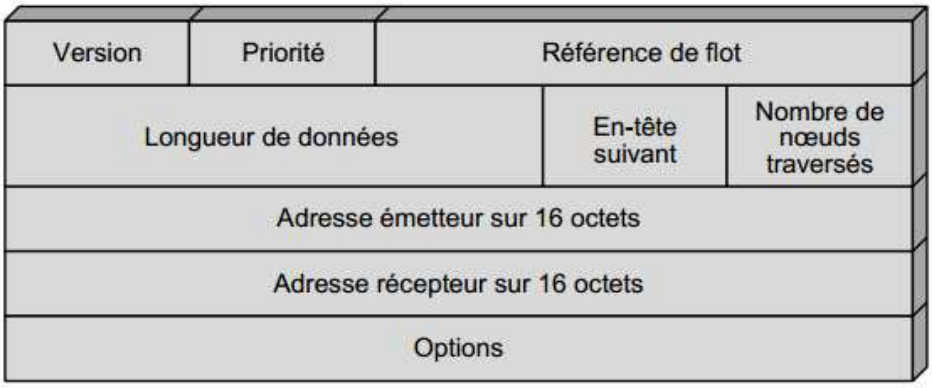

Figure 1. 15 : *Format paquet IPv6.*

- Le champ **version** porte le numéro 6
- Le champ **Priorité** montre un niveau de priorité dans le transfert du paquet :

  0: pas de priorité

  1: trafic de base (news)

  2: transfert de donnée sans contrainte temporelle (e-mail)

  3: réservé pour des développements futurs

  4: transfert en bloc avec attente du récepteur (transfert de fichiers)

  5 : réservé pour les développements futurs

  6 : trafic interactif (terminal virtuel ou rlogin)

  7 : trafic pour le contrôle (routage, contrôle de flux)

- Le champ **Référence de flot**, ou flow-label sert à transporter une référence (label) précisant le flot auquel le paquet appartient.
- Le champ **Longueur**, ou length, indique la longueur total du datagramme en octet.
- Le champ **En-têteSuivante**, ou **NextHeader**, indique le protocole encapsulé dans la zone de données paquet. Par exemple : 4 indique le protocole IP, 6 le TCP, 17 : UDP, 58 ICMP et 59 pour No Next Header
- Le champ **Nombre de nœuds traversés** (Hop Limit) indique le nombre de nœuds restants à traversés avant la destruction du paquet.
- Les deux derniers champs indiquent l'adresse IPv6 de la source et de la destination : Les adresses IPv6 sont représentés sur 128 bits soit 16 octets. La représentation se fait par groupe de 16 bits et se présente sous la forme 123:FCBA:1024:AB23:0:0:24:FEDC.
- Le champ **Option** : permet l'ajout de nouvelles fonctionnalités, en particulier concernant la sécurité.

1.3.2.2 Le protocole ARP et RARP

Ayant pour acronyme « Address Resolution Protocol », **ARP** offre un service d'établissement d'une correspondance dynamique entre adresses physiques et adresse logiques. Il permet alors à une machine de trouver l'adresse physique d'une autre machine dans le même réseau local.

Principe

Quand une machine A veut résoudre l'adresse IP d'une machine B, elle diffuse un message, en utilisant l'adresse MAC FF:FF:FF:FF:FF:FF comme adresse du destinataire et en envoyant aussi avec l'adresse IP de B. Quand la machine B reçoit message, B reconnaît son adresse IP et répond en voyant son adresse MAC. A reçoit cette réponse et connaît maintenant l'adresse MAC de la machine B.

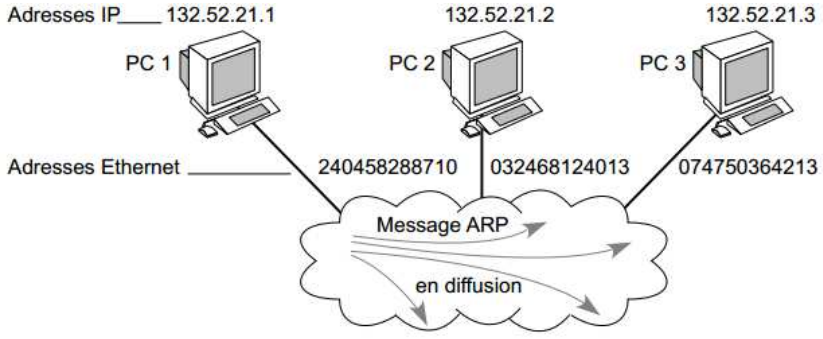

Figure 1. 16 : *Requête ARP.*

Le PC1 recherche l'adresse physique de la station ayan l'adresse IP 132.52.21.3, autrement dit l'adresse MAC de PC3.

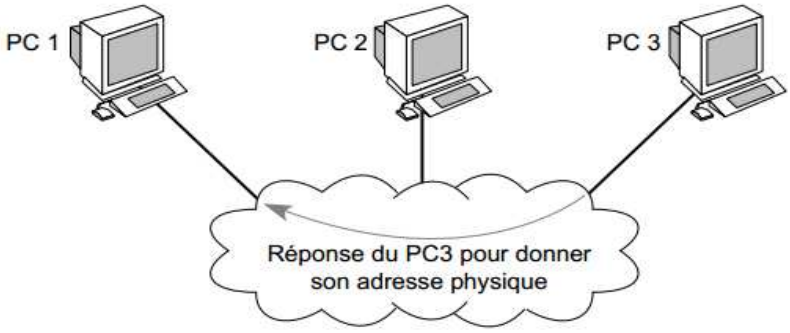

Figure 1. 17 : *Réponse de PC3.*

Voici les éléments dans une requête et une réponse ARP :

- L'adresse physique de l'émetteur. Dans le cas d'une requête ARP, l'émetteur place son adresse ; dans une réponse ARP, ce champ révèle l'adresse recherchée.
- L'adresse logique de l'émetteur (l'adresse IP de l'émetteur).
- L'adresse physique du récepteur. Dans le cas d'une requête ARP, ce champ est vide.
- L'adresse logique du récepteur (l'adresse IP du récepteur).

Il est à noter que la requête ARP n'est envoyer que si seulement si la correspondance de l'adresse MAC et IP de la machine à communiquer est absente dans la table de correspondance de la machine qui va émettre. [7]

RARP pour Reverse Address Resolution Protocol, est un protocole similaire à ARP. RARP permet à une machine de d'utiliser son adresse physique pour déterminer son adresse logique sur internet. Ainsi, c'est l'inverse d'ARP. Ce protocole est souvent utiliser entre une machine et un serveur d'adresse. Son fonctionnement ne diffère pas beaucoup de l'ARP sauf qu'au lieu d'envoyer son adresse IP dans le paquet de requête ARP, on envoie son adresse MAC. [3]

Pour le protocole IPv6, ARP et RARP sont remplacés par le protocole de découverte de voisins ND (Neighbor Discovery).

1.3.2.3 Le protocole ICMP

Dans un réseau, les pannes matérielles et logicielles, les déconnexions temporaire ou permanent d'une machine, l'expiration du datagramme et la congestion trop importante d'une passerelle peuvent s'intervenir à tout moment. Pour réagir correctement à ces défaillances en informant les

équipements de ces anomalies de fonctionnement, on ajouter un protocole de messages de contrôle qui est l'ICMP (Internet Control Message Protocol). On l'appelle aussi un protocole de diagnostic. Il s'occupe alors de la transmission des messages de contrôle.

ICMP est donc un mécanisme de contrôle des erreurs au niveau IP. Les messages ICMP traverse le réseau en tant que datagramme IP. Leur traitement se fait comme tout autre datagramme IP. Généralement, ces datagrammes se différencient des autres dans le champ protocole de l'en-tête du datagramme IP, on y met la valeur correspondant à ICMP. [3]

ICMP caractérise les problèmes en les classant par type. Par exemple, dans la pratique, l'utilitaire « ping » créé un message ICMP de type 8 (Echo Request) que la machine envoi à l'adresse IP destinataire. Le but est de tester ci cette machine destinataire est opérationnel. Si tel est le cas, la machine destinataire répond par des messages ICMP de type 0 (Echo Reply), en renvoyant avec les données contenues dans le message émis. Pour le cas d'un routeur, lorsqu'un datagramme ne peut être délivré, il envoie un message ICMP de type 3 (Destination unreachable) à l'émetteur. [7]

Le protocole ND est un sous-ensemble du protocole ICMP.

1.3.3 Les protocoles de transport TCP et UDP

Un protocole de transport offre aux applications sur une machine une interface, permettant à ces derniers, d'utiliser les services offerts par les couches inférieurs. Cette interface correspond au « port ». Le but est d'éviter l'erreur de transmission vers les applications. Ainsi un protocole de transport sait exactement à qui il travaille. Chaque application est alors associée à un « numéro de port» de 16 bits. L'adresse IP local couplé avec le numéro de port forme ce qu'on appelle « socket». C'est l'IANA (Internet Assigned Numbers Authority) qui affecte officiellement quel port est associé à quel application. [3]

1.3.3.1 Transmission Control Protocol (TCP)

TCP pour Transmission Control Protocol comble les services fournis par le protocole IP lorsque la demande de fiabilité est très élevée. C'est un protocole complexe qui met en œuvre la détection et la correction d'erreur, gère le contrôle de flux et négocie les conditions du transfert de données.

Pour assurer la fiabilité d'échange de données, TCP ouvre une connexion et gère un dialogue. Il est à noter que ce protocole n'est implanté que sur les machines des utilisateurs.

La différence entre TCP et IP, c'est qu'IP est responsable de la traversée du paquet et TCP est responsable de la gestion et de la fiabilité des échanges.

a. Mécanisme de transfert sur TCP

TCP gèrent des « fragments » ou « Segment ». Après la création des segments, le module TCP sollicite le module IP de la même machine pour le service de transmission. Le fragment est ensuite encapsulé et envoyé vers le module IP de la machine de destination. Le datagramme est ensuite décapsulé et le module IP signal le module TCP de l'arrivée d'un fragment. [7]

b. Format du segment TCP

Il est à noter qu'il n'y a qu'un seul format de fragment TCP.[4]

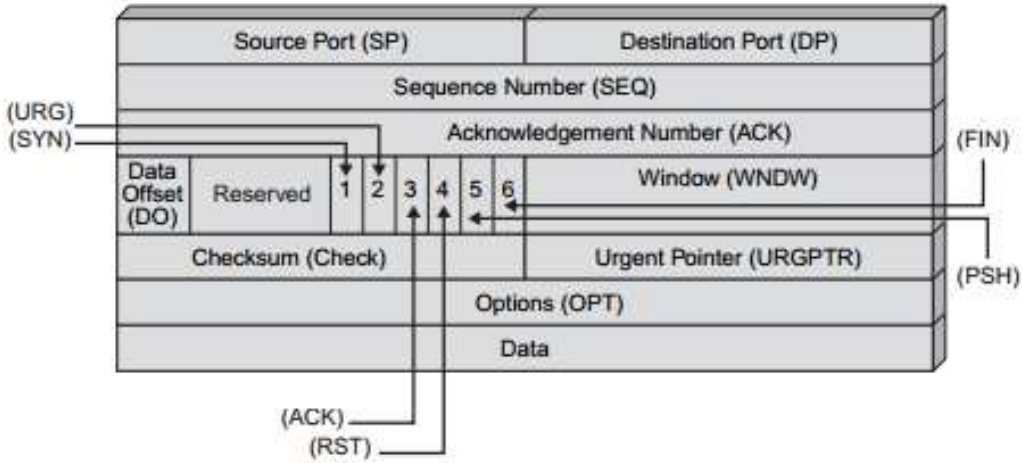

Figure 1. 18 : *Fragment TCP.*

- **Port Source** : Adresse du port d'entrée
- **DP (Destination Port)** ou Port de destination : Adresse du port d'entrée de la machine de destination
- **SEQ (Sequence Number)** ou Numéro de séquence : champ de 32 bits indiquant le numéro du premier octet porté par le fragment
- **ACK (Acknowledgement Number)**, ou numéro d'acquittement. Champ sur 32 bits indiquant le numéro SEQ du prochain fragment attendu et correspondant à l'acquittement de tous les octets reçus auparavant.
- **DO (Data Offset)**, ou longueur de l'en-tête: ou longueur de l'en-tête. Champ sur 4 bits indiquant la longueur de l'en-tête par un multiple de 32 bits.
- La zone suivant est réservée à une utilisation ultérieure. Et doit être égale à 0
- URG (Urgent Pointer) : Champ de 1 bit indiquant une urgence. Si ce bit a pour valeur « 1 », cela signifie que le champ Urgent Pointer situé dans la suite de l'en-tête comporte une valeur significative.

- **PSH (Push Function),** ou fonction de push : champ de 1 bit. Si PSH = 1, cela signifie que l'émetteur souhaite que les données de ce fragment soient délivrées le plus tôt possible au destinataire.
- **RST (Reset),** ou redémarrage : champ de 1 bit. Si RST=1, l'émetteur demande que la connexion TCP redémarre.
- **SYN (Synchronization),** ou synchronisation : Champ de 1 bit. SYN=1 désigne une demande d'ouverture de connexion. Dans ce cas, le numéro de séquence porte le numéro du premier octet du flot
- **FIN (Terminate),** ou fermeture : Champ sur 1 bit. FIN=1 signifie que l'émetteur souhaite fermer la connexion.
- **WNDW (Window),** ou fenêtre. Champ sur 16 bits indiquant le nombre d'octet que le récepteur accepte de recevoir.
- **CHECK (Checksum)**, Champ sur 16 bits permettant de détecter les erreurs dans l'entête et le corps du fragment.
- **URGPTR (Urgent Pointer),** ou pointeur d'urgence. Champ sur 16 bits spécifiant le dernier octet d'un message urgent.
- **OPT (Options),** ou options. Zone contenant les différentes options du protocole TCP.

1.3.3.2 User Datagram Protocol (UDP)

Contrairement à TCP, UDP est un protocole très simple. Ce protocole permet aussi aux applications d'échanger des datagrammes. Comme tous les protocoles de transport, il a besoin des numéros de port des applications pour fournir ses services.

C'est un protocole en mode sans connexion et sans reprise sur erreur. Il n'utilise aucun acquittement, ne ré-séquence pas les messages et ne met en place aucun contrôle de flux. Il est alors non fiable par rapport à TCP. Cependant, il est très rapide et très efficace pour les applications qui n'ont pas besoin d'une forte sécurité au niveau transmission. [3]

DNS (Domain Name System) et DHCP (Dynamic Host Configuration Protocol) sont les protocoles les plus en vogue qui utilisent le protocole de transport UDP.

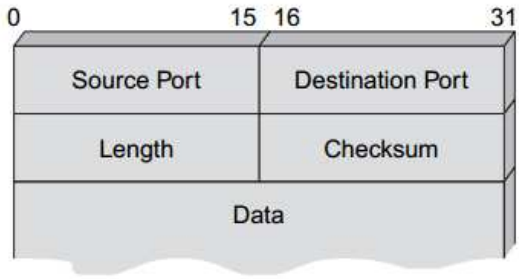

Figure 1. 19 : *Fragment UDP.*

1.3.4 Les protocoles de la couche application

On a déjà vu qu'il existe nombreux protocoles qui gère les services de cette couche application du modèle TCP/IP, mais on ne va citer que peu d'entre eux, peu qui est très utile dans ce présent mémoire.

1.3.4.1 File Transfer Protocol (FTP)

FTP est un protocole de transfert de fichiers entre deux hôtes d'extrémité, qui permet de garantir une qualité de service. Pour assurer cet garantis, il sollicite les services données par le protocole TCP. L'application FTP est de type client-serveur, avec un utilisateur, ou client, FTP et un serveur FTP. [4]

Dans le cas du FTP anonyme, il faut se connecter sous un compte spécial et donner par convention son adresse de messagerie électronique comme mot de passe. FTP met en place une session temporaire dans le but de transférer un ou plusieurs fichiers. Le transfert a lieu par l'intermédiaire du logiciel client, auquel on donne l'adresse de la machine FTP sur laquelle on souhaite récupérer les fichiers. Une fois le transport effectué, la session est fermée.

1.3.4.2 Telnet

Telnet ou « Telecommunication Network » est une application, qui permet de connecter un terminal à une machine distante. C'est l'application de terminal virtuel.

La connexion Telnet utilise le protocole TCP pour transporter les informations de contrôle nécessaires à l'émulation de la syntaxe du terminal. Dans la plupart des cas, Telnet est utilisé pour établir une connexion entre deux machines considérées comme des terminaux virtuels.[13]

1.3.4.3 Dynamic Host Configuration Protocol(DHCP)

Le service de configuration dynamique transmette des informations de configurations à des machines d'un réseau TCP/IP. Il leur communique leurs paramètres de configuration, comme l'adresse IP, l'adresse du DNS. [3]

Ce protocole utilise UDP au niveau transport. C'est suffisant pour des échanges simples. Ainsi, DHCP fonctionne en mode non connecté.

1.3.4.4 HyperText Transfer Protocol (HTTP)

HTTP est souvent appelé le protocole de l'Internet. Http a reçu cette désignation parce que presque tous les trafics sur Internet sont basés sur lui. C'est en réalité un protocole de communication qui est utilisé par le système de documentations hypermédias distribués WWW ou World-Wide Web, qu'on appelle aussi le web. [4]

1.3.4.5 Domain Name System (DNS)

C'est le système qui translate les adresses URL (Uniform Ressource Locator) en adresse IP.

1.3.4.6 Simple Mail Transfer Protocol (SMTP)

C'est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique.[4]

1.4 Conclusion

Ce chapitre commence par un petit historique du réseau,de l'internet et de ses évolutions. Les catégories de réseaux ont été développées commençant par le PAN et en terminant cela par le WAN. Les modèles de référence OSI et TCP/IP ont été longuement étudiés. Leurs différences ont été bien prouvées et rédigées dans ce chapitre. Et pas seulement cela, mais aussi les théories sur les protocoles de ces modèles qui sont utilisés partout où il y a de l'accès internet. Parmi ces protocoles, il y a l'IP et le TCP qu'on dit souvent les protocoles de bases de l'internet.

CHAPITRE 2

FONCTIONNALITES DANS LES RESEAUX INFORMATIQUES

2.1 Introduction

Nombreuses sont les techniques et les fonctions utiles à savoir dans un réseau. Ses connaissances aideront beaucoup lors de la simulation dans le chapitre 4. Ainsi, prenons en sérieux les études portées dans ce chapitre en commençant par le plus élémentaire qui est la commutation.

2.2 Commutation

La nécessité de mettre en relation un utilisateur avec n'importe quel autre utilisateur est l'origine du concept de réseau à commutation. En plus, il est impossible de créer autant de liaisons point à point qu'il y a de paires potentielles de communicants.[5]

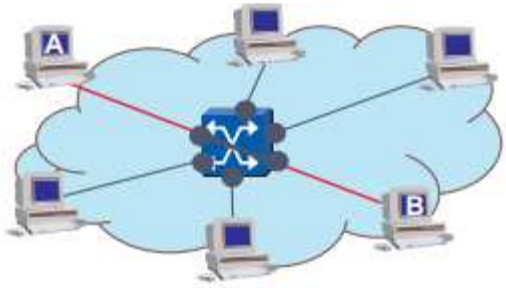

Figure 2.0 1 : *Unité de commutation.*

Un réseau à commutation assure une connectivité totale. Dans ses conditions, la topologie logique ou interconnexion totale, vue du côté des utilisateurs, est différente de la topologie physique réelle.

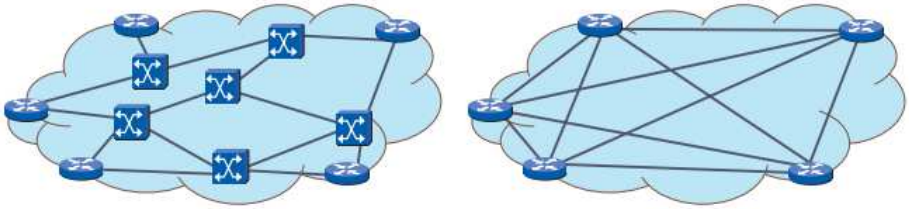

Figure 2.0 2 : *Vue physique du réseau à gauche et vue logique à droite.*

On dénombre cinq types de commutations :

2.2.1 Commutation de circuits

Dans la commutation de circuits, un lien physique est établi par juxtaposition de différents supports physiques afin de constituer une liaison de bout en bout entre une source et une destination. La mise en relation physique est réalisée par les commutateurs avant tout échange de

données et est maintenue tant que les entités communicantes ne la libèrent pas expressément. Le taux de connexion peut être important, alors que le taux d'activité peut être faible[4].

Après la constitution d'un chemin physique, les données sont transférées et l'ordonnancement des informations sont garanti. Cependant, les deux utilisateurs doivent être connectés tous au long de la connexion, sinon les données sont perdus. Il n'y a pas d'entité de stockage intermédiaire. En plus, l'émetteur et le destinateur doivent se fonctionner au même débit. Lors de la connexion, les ressources sont monopolisées.[5]

2.2.2 Commutation de message

Dans ce type de commutation, il n'y a pas de constitution de lien physique. Le message est transféré de nœud en nœud et mis en attente si le lien inter nœud est occupé. Le message est ainsi mémorisé et retransmis au nœud suivant dès qu'un lien se libère. Le transfert réalisé, le lien est libéré. Les lignes sont utilisé à bon escient, la commutation de messages autorise alors un dimensionnement de réseaux à commutation de messages inférieur à celui des réseaux à commutation de circuits. En cas de fort trafic, il n'y a pas blocage de réseau mais seulement un ralentissement. Cependant, la mémorisation intermédiaire nécessite des mémoires de masse importantes et augment le temps de transferts. Ainsi, cette commutation n'est pas adaptée aux applications interactives.[5]

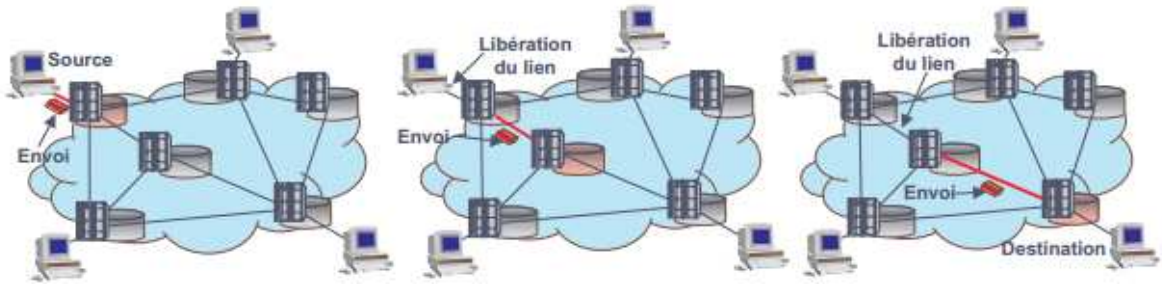

Figure 2.0 3 : *Principe d'une commutation de message.*

Les réseaux à commutation de messages assurent, par rapport à la commutation de circuits:

- le transfert, même si le correspondant distant est occupé ou non connecté ;
- la diffusion d'un même message à plusieurs correspondants ;
- le changement de format des messages ;
- l'adaptation des débits et éventuellement des protocoles.

2.2.3 Commutation de paquets

Dans ce type de communication, le message ou information est découpé en fragments ou paquets de petite taille. Chaque paquet est acheminé dans le réseau indépendamment du précédent. Contrairement à la commutation de messages, il n'y a pas de stockage d'information dans les nœuds intermédiaires. Chaque nœud, recevant un paquet, le réémet immédiatement sur la voie optimale. Ainsi, le séquencèrent des informations n'est plus garanti. De ce fait, le destinataire devra réordonnancer les paquets à l'arrivé avant de réassembler.[5]

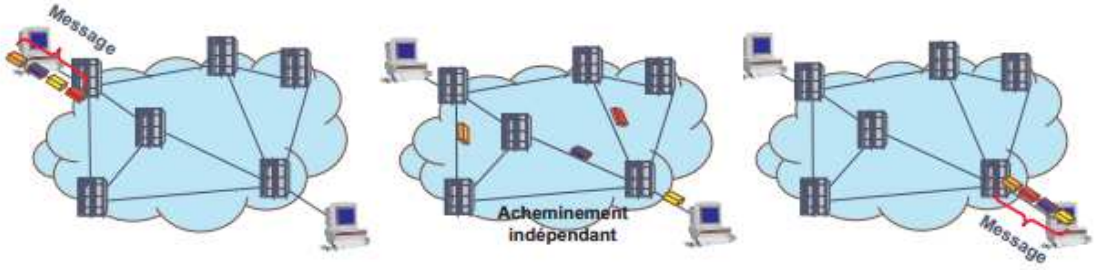

Figure 2.0 4 : *Principe d'une commutation paquets.*

2.2.4 Commutation de trame

Il a le même principe à la commutation de paquet. Les nœuds du réseau sont des commutateurs et traite des paquets aux trames niveau 2 de l'OSI.[11]

2.2.5 Commutation de cellule

Cette commutation combine la commutation des circuits et de paquets. Elle est adapté aux trafics à temps réelle et aux trafics sporadiques sans contrainte de temps. Un cellule est un paquet particulier de taille fixe de 53 octets.[11]

2.3 Routage

Le routage est un processus par lequel un paquet va être acheminé d'un endroit à un autre. Un élément faisant du routage doit connaître la destination, les itinéraires possibles, et les meilleurs itinéraires pour atteindre la destination et le moyen d'actualiser les itinéraires.

2.3.1 Principe du routage IP

Ce routage IP est basé uniquement sur l'adresse du destinataire. Chaque équipement du réseau sait atteindre un équipement d'un autre réseau, s'il existe au moins un équipement de routage pour acheminer les paquets à l'extérieur du réseau local. [14]

Les informations de routage sont mémorisées dans le table de routage des équipements qui est mis à jour soit manuellement, soit automatiquement.

2.3.2 Catégorie de routage IP

Le routage peut être catégorisé en deux parties, suivant la façon de mettre à jour les tables de routages. On peut lister le routage statique et le routage dynamique.

2.3.2.1 Routage statique

Les informations relatives à la route, ou le table de routage est mises à jour manuellement dans les routeurs avec ce catégorie de routage. Son principal avantage par rapport au routage IP dynamique, c'est au niveau de surcharge du routeur.La route par défaut est un des exemples de ce routage statique. Une route par défaut facilite fortement la circulation des données, spécialement sur un réseau de grande taille. En plus, on l'utilise au cas où la destination s'avère inconnue et que si le prochain saut ne figure pas explicitement dans la table de routage. [15]

2.3.2.2 Routage dynamique

Contrairement au routage statique, il est utilisé pour mettre à jour automatiquement, sans intervention manuelle, la table de routage d'un hôte ou d'un routeur. Pour ce faire, ils s'échangent des paquets « mise à jour de routage » contenant les informations destinées à remplir la table de routage. Ces échanges n'ont de sens qu'entre deux entités utilisant le même protocole de routage, c'est-à-dire que deux hôtes de différents protocoles ne peuvent se communiquer entre eux.

Il est à noter que les protocoles de routage ne doivent pas être confondus avec les protocoles routés comme IP. Un protocole de routage utilise une table de routage pour chaque protocole routé. [3][14]

2.3.3 Routage dans l'Internet

Plusieurs routeurs forment l'internet. On les groupe et cela forme des systèmes autonomes. Chaque système autonome est administré par une même organisation et s'échange des paquets par le biais d'un même protocole de routage. Ce protocole de routage est appelé IRP (Interior Routing Protocol). L'IRP n'a pas besoin d'être implémenté à l'extérieur d'un système autonome. De ce fait, on peut choisir son algorithme de routage de façon à optimiser le routage intérieur. On les appelle aussi IGP (Interior Gateway Protocol).

Les systèmes autonomes sont reliés entre eux à travers des protocoles de routage extérieur, ou ERP (Exterior Routing Protocol). Les protocoles ERP doivent avoir une connaissance des divers AS pour accomplir leur tâche. On les appelle aussi EGP (Exterior Gateway Protocol).

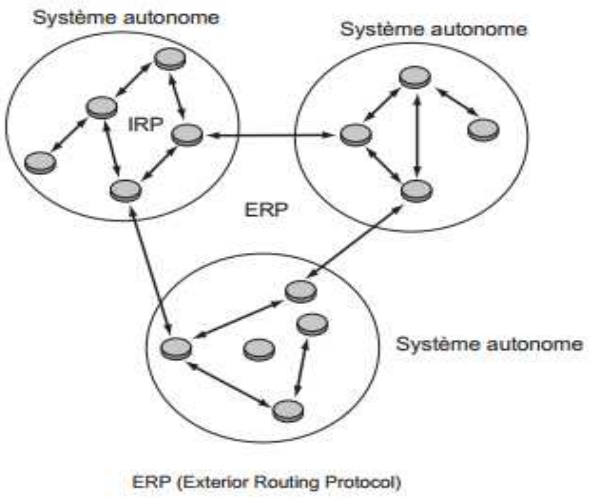

Figure 2.0 5 : *Routage dans le cœur de l'internet.*

Tous les protocoles de routage sont classés suivant ces deux protocoles, qui sont IGP et EGP. Et ces deux protocoles se caractérisent encore à travers l'algorithme de routage qui les gère. [4]

2.3.4 Algorithme de routage

Un algorithme de routage est un procédé permettant de déterminer le routage des paquets dans un nœud. Les boucles dans un routage est à éviter. Il ne faut pas qu'un nœud reçoit le même paquet. On distingue trois grandes catégories d'algorithme de routage :

- A vecteur de distance
- A état de liens
- A vecteur de chemin

2.3.4.1 Algorithme à vecteur de distance

Dans le routage vecteur distance ou routage de Bellman-Ford (distance vector routing), chaque nœud du réseau maintient une table de routage qui comporte une entrée par nœud du réseau et le coût pour joindre ce nœud. Périodiquement chaque nœud diffuse sa table de routage à ses voisins.

Le nœud destinataire apprend ainsi ce que son voisin est capable de joindre. Chaque routeur diffuse alors à ses voisins un vecteur listant chaque réseau qu'il peut atteindre avec la métrique associée, c'est-à-dire le nombre de sauts. Chaque routeur peut donc bâtir une table de routage avec les informations reçues de ses voisins mais n'a aucune idée de l'identité des routeurs qui se trouvent sur la route sélectionnée. [4]

À réception, le nœud compare les informations reçues à sa propre base de connaissance :

- La table reçue contient une entrée qui n'est pas déjà dans sa propre table, il incrémente le coût de cette entrée du coût affecté au lien par lequel il vient de recevoir cette table et met cette entrée dans sa table. Il a ainsi appris une nouvelle destination.
- La table contient une entrée qu'il connaît déjà. Si le coût calculé (coût reçu incrémenté du coût du lien) est supérieur à l'information qu'il possède, il l'ignore sinon il met sa table à jour de cette nouvelle entrée.

De proche en proche chaque nœud apprend la configuration du réseau et le coût des différents chemins. La convergence des différentes tables peut être assez longue. Le problème avec cet algorithme, c'est lorsque les nœuds augmentent, les tables deviennent trop lourdes. RIP (Routing Information Protocol) est un parfait exemple.[15]

2.3.4.2 Algorithme état de liens

Pour ce type d'algorithme, quand un routeur est initialisé, il doit définir le coût de chacun de ses liens connectés à un autre nœud. Le nœud diffuse ensuite l'information à l'ensemble des nœuds du système autonome, et donc pas seulement à ses voisins. À partir de l'ensemble de ces informations, les nœuds peuvent effectuer un calcul leur permettant d'obtenir une table de routage indiquant le coût nécessaire pour atteindre chaque destination. Lorsqu'un routeur reçoit des informations qui modifient sa table de routage, il en avertit tous les routeurs intervenant dans sa configuration. Comme chaque nœud possède la topologie du réseau et les coûts de chaque lien, le routage peut être vu comme centralisé dans chaque nœud.[4]

Ainsi, contrairement à l'algorithme à vecteur de distance, les protocoles à état des liens sont complètement informés de la topologie de la partie ou même de la totalité du réseau sur lequel ils opèrent. Le protocole OSPF (Open Shortest Path First) met en œuvre cette technique, qui correspond à la deuxième génération de protocoles Internet. [15]

2.3.4.3 Algorithme à vecteur de chemin

Cet algorithme se dispense des métriques et cherche à savoir quel réseau peut être atteint par quel nœud et quels systèmes autonomes doivent être traversés pour cela. Cette approche est très différente de celle par vecteur de distance puisque les vecteurs de chemin ne prennent pas en compte les distances ni les coûts. De plus, du fait que chaque information de routage liste tous les systèmes autonomes qui doivent être traversés pour arriver au routeur destinataire, l'approche par vecteur de chemin est beaucoup plus dirigée vers les systèmes de routage extérieurs. Le protocole BGP (Border Gateway Protocol) appartient à cette catégorie. [14]

2.3.5 Liste des protocoles de routage IP

Chaque protocole de routage IP est caractérisé par le mode d'adressage qu'il gère, c'est-à-dire adressage avec classe (classfull) ou sans class (classless) et le réseau où il s'applique, dans les systèmes autonomes ou dans les réseaux locaux.

	IGP				EGP
	Protocole de routage à vecteur de distance		Protocole de routage à état de liens		Vecteur de chemin
Avec classe	RIP	IGRP			EGP
Sans classe	RIPv2	EIGRP	OSPFv2	IS-IS	BGP
IPv6	RIPng	EIGRP pour IPv6	OSPFv3	IS-IS pour IPv6	BGPv4 pour IPv6

Tableau 2.0 1 : *Liste de protocole de routage IP*.

2.4 Network Address Translation

Le protocole IP version 4, massivement utilisé actuellement, offre un champ d'adressage limité et insuffisant pour tous les terminaux informatiques se connectant à un réseau. Il est à connaître qu'une adresse IPv4 est codée sur 32bits, soit 2^{32} adresses disponibles ou 4 294 967 296 terminaux accordables au même réseau.

Malheureusement, la croissance du nombre d'utilisateurs et de serveurs de l'internet conduit à l'épuisement de ces adresses. La quantité des adresses ipv4 publiques disponibles se sature progressivement. Cela menace l'évolution de l'internet.

C'est pour résoudre ce problème que le NAT (Network Address Translation) a été créé. Certes, l'adressage ipv6 est aussi créé, mais c'est le NAT qui est le plus utilisé, vu qu'on utilise encore des adresses IPv4. NAT consiste à établir des relations entre l'adressage privé dans un réseau et l'adressage public pour se connecter à Internet.

Ainsi, le NAT est un système servant de résoudre la pénurie de l'adresse IPv4.

Cela a amené à bien distinguer l'adresse publique à l'adresse privée qui est non-routable sur Internet.

Classe d'adresses	Plages d'adresses privées	Masque réseau	Espace adressable
A	10.0.0.0 à 10.255.255.255	255.0.0.0	Sur 24 bits, soit 16 777 16 terminaux
B	172.16.0.0 à 172.31.255.255	255.240.0.0	Sur 20 bits, soit 1 048 576 terminaux
C	192.168.0.0 à 192.168.255.255	255.255.0.0	Sur 18 bits, soit 65 536 terminaux

Tableau 2.0 2 : *Plage d'adresse IP privée.*

Il est à noter que les utilisateurs qui possèdent une adresse IP privée ne peuvent communiquer que sur leur réseau local, et non sur Internet, tandis qu'avec une adresse IP publique, ils peuvent communiquer sur n'importe quel réseau IP.[4]

L'adressage privé peut être utilisé librement par n'importe quel utilisateur du réseau. Par contre, l'adressage public est soumis à des restrictions de la déclaration et d'enregistrement de l'adresse IP auprès d'un organisme spécialisé, l'IANA ce que les FAI (Fournisseur d'Accès Internet) ou ISP (Internet Service Provider) effectuent globalement en acquérant une plage d'adresse IP pour leurs abonnée.

2.4.1 Principe du NAT

La translation d'adresse est assurée par une entité, un boîtier ayant au moins deux interfaces, l'une connecté au réseau privée et l'autre au réseau publique. Ce boîtier, généralement un routeur, un Switch multicouche, maintient en lui une table de correspondance des paquets de manière à savoir à qui distribuer les paquets reçus.

Dans l'exemple ci-dessous, un émetteur dont l'adresse IP est 10.0.0.3 envoie vers la passerelle NAT un paquet à partir de son port 12345, la passerelle NAT modifie le paquet en remplaçant l'adresse IP source par la sienne et le port source par un port quelconque qu'elle n'utilise pas, disons le port 23456. Elle note cette correspondance dans sa table de NAT. De cette manière, lorsqu'elle recevra un paquet à destination du port 23456, elle cherchera cette affectation de port dans sa table et retrouvera la source initiale.[4]

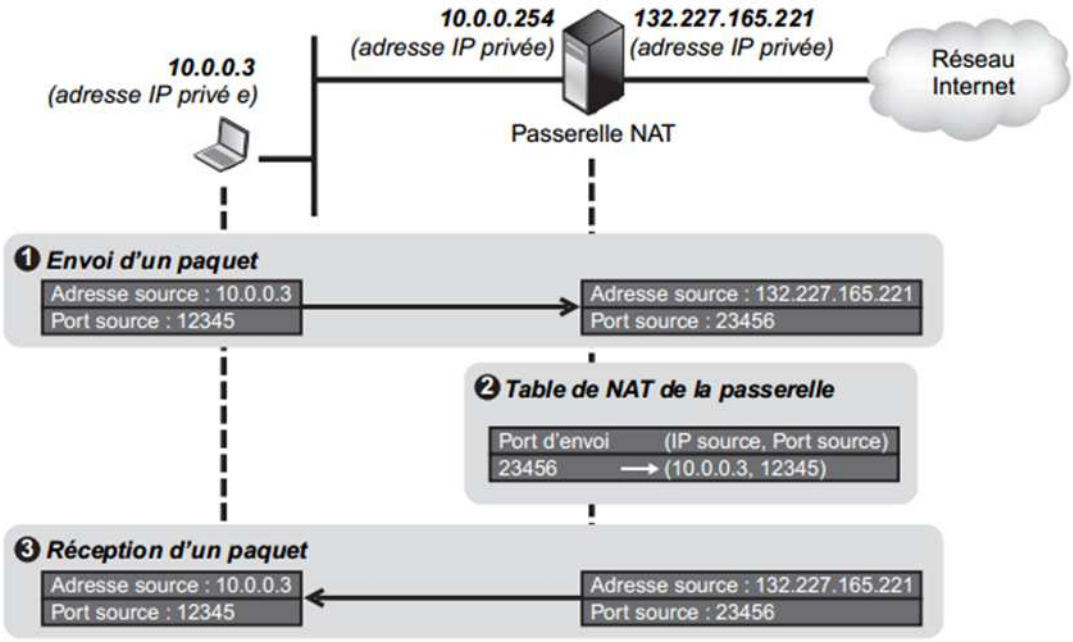

Figure 2.0 6 : *Modification de paquet lors d'un NAT.*

Ainsi, le réseau internet ne connaît pas la vraie adresse IP source du paquet. Il considère que la source initiale du paquet est l'adresse IP publique de la passerelle NAT qui est 132.227.165.221. Et il communiquera à 10.0.0.3 à travers cette adresse publique.

2.4.2 Catégorie NAT

Il existe trois catégories très courante de NAT, il en existe d'autre comme ceux lister dans RFC 3489, mais on se contentera de :

- Le NAT statique
- Le NAT dynamique
- Le NAPT

2.4.2.1 NAT statique

Dans le NAT statique, à toute adresse IP privée qui communique avec l'extérieur, une adresse IP publique fixe lui est affectée. Avec ce type de NAT, les utilisateurs du réseau local sont joignables de l'extérieur, car la passerelle réalise la correspondance d'une adresse IP locale en une adresse IP publique dans les deux sens [4] [16]

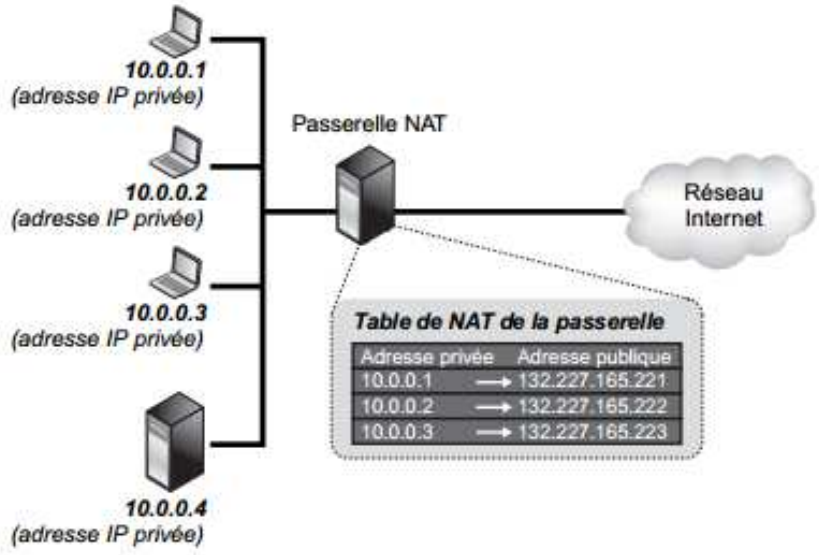

Figure 2.0 7 :*Table de routage dans une passerelle NAT.*

2.4.2.2 NAT dynamique

Avec le NAT dynamique, une plage d'adresses IP publiques est disponible et partagée par tous les utilisateurs du réseau local. Chaque fois qu'une demande d'un utilisateur local (avec une adresse privée) parvient à la passerelle NAT, celle-ci lui concède dynamiquement une adresse IP publique. Elle maintient cette correspondance pour une période fixe, mais renouvelable selon l'activité de l'utilisateur, qui assure le suivi des communications.

Les utilisateurs internes ne sont joignables de l'extérieur qu'à travers la passerelle NAT, sauf s'ils ont une entrée dans la table de la passerelle. Or tant que le correspondant interne n'a pas d'activité réseau, aucune entrée ne lui est attribuée dans cette table. En plus l'adresse IP publique qui lui est affecté n'est que temporaire et peut changer à la prochaine connexion. Cela restreint les possibilités d'être joignable de l'extérieur.

Cette forme de NAT a l'avantage d'être souple au niveau de l'utilisation par rapport au modèle statique. Tous devient dynamique, il n'est plus nécessaire de mentionné statiquement l'adresse publique correspondant à une adresse privée.[4][16]

2.4.2.3 NAPT (Network Address Port Translation)

C'est une variante du NAT dynamique. Il se nomme aussi dynamique PAT pour Port Address Translation, ou NAT dynamique avec surcharge. Le principe est d'attribuer une seule adresse IP publique à un groupe d'adresse. L'adresse réelle avec le numéro de port de l'utilisateur interne est translatée en l'adresse de la passerelle NAT. Si le numéro de port de l'utilisateur est disponible sur la passerelle NAT, le numéro de port après translation ne change pas. Par contre s'il est

indisponible, il y aura une translation de port, et le numéro à utiliser sera dans le même ranger que le numéro de ports réels, c'est-à-dire 0 à 511, 512 à 1023 et 1024 à 65535.

Ainsi le nombre maximal d'adresse IP du réseau interne qu'on peut translater sur une même adresse IP est de 65536. C'est alors l'affectation du port qui est dynamique, d'où le nom PAT.

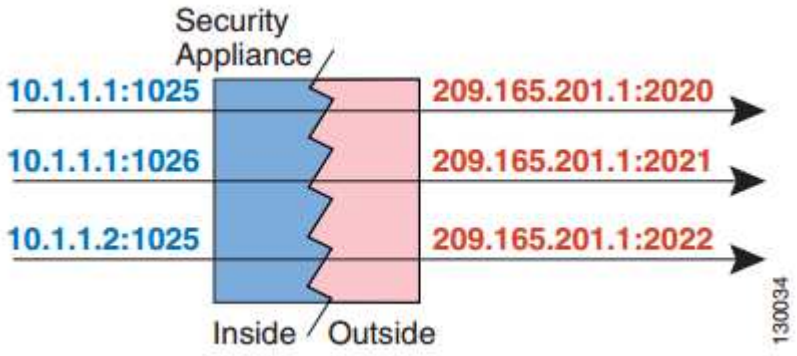

Figure 2.0 8 : *Principe du PAT.*

PAT a l'avantage de conserver les adresses IP routables. Cependant, il n'assure pas une bonne qualité de service pour certaines applications multimédia. [4][16]

2.5 VLAN

L'idée de base des VLAN (Virtual Local Area Network) est de découper un seul réseau local, c'est à dire un ensemble cohérent d'infrastructures de niveau 2, en des réseaux logiques totalement disjoints : c'est comme si on avait plusieurs réseaux physiques totalement disjoints, un par VLAN. L'avantage est de bien séparer les domaines de diffusion.[17][18]

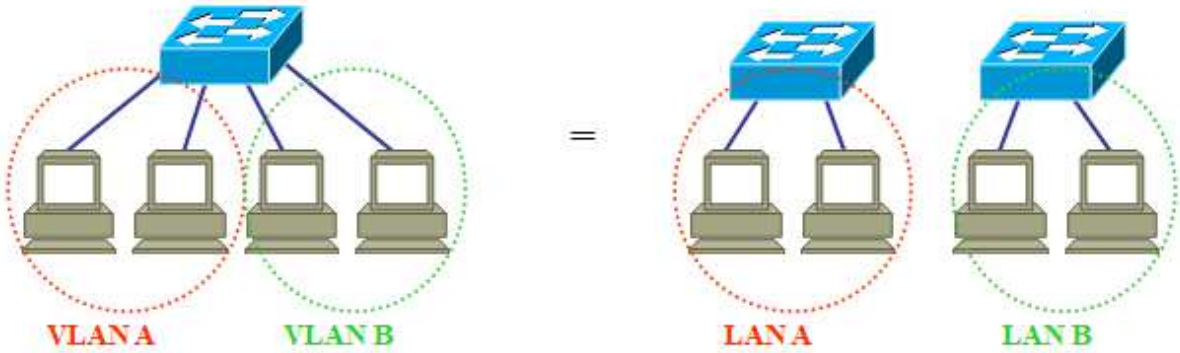

Figure 2.0 9 : *Principe du VLAN.*

Dans un réseau informatique, on dénombre en ce moment trois types de VLAN :

- VLAN par port

- VLAN par protocole
- VLAN par adresse

2.5.1 VLAN par port

Dans ce type de VLAN qu'on appelle aussi VLAN de niveau 1, chaque port physique d'un commutateur (en générale) est configuré pour appartenir à un VLAN, et toute machine qui se branche sur ce port fera partie de ce VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur. Ce port est affecté statiquement à ce VLAN. [18]

C'est le mode de fonctionnement de plus simple, celui où les défauts de logiciel sont le moins probable.

2.5.2 VLAN par adresse

2.5.2.1 Par adresse MAC au niveau trame

On l'appelle aussi VLAN de niveau 2. Comme principe, on affecte une adresse MAC au VLAN. L'appartenance d'un trame au VLAN est déterminée par son adresse MAC. Il s'agit donc, à partir de l'association MAC/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port.[18]

2.5.2.2 Par adresse de niveau 3

Aussi appelé VLAN de niveau paquet, ou VLAN de niveau 3, il correspond à des regroupements de stations suivant leur adresse de niveau 3. Cette adresse peut être une adresse IP ou un masque de sous-réseau. Il s'agit donc d'affecter dynamiquement suivant l'association d'adresse niveau3/VLAN des ports de commutateurs à chacun des VLAN

2.5.3 VLAN par protocole

Le critère d'appartenance à un VLAN n'est plus lié au port sur lequel la machine est connectée, mais à la nature du trafic généré par cette machine.[17]

2.6 Les réseaux sans fil et Wi-Fi

2.6.1 Les réseaux sans fils

Un réseau sans fils (Wireless network) est un réseau informatique qui connecte différents postes ou systèmes entre eux par ondes radio.

On catégorise les réseaux sans fil selon le périmètre géographique dans lequel ils offrent leurs sévices, c'est la zone de couverture. [5][19]

2.6.1.1 Réseaux personnels sans fils (WPAN)

Ces sont des réseaux PAN sans fils. WPAN (Wireless Personal Area Network) groupe les réseaux sans fil de faible portée (quelque dizaines de mètres). La plus célèbre technologie appartenant à ce type de réseau est le Bluetooth.

Le Bluetooth, ayant aussi pour nom IEEE 802.15.1, est une technologie lancée par Ericsson en 1994 proposant un débit théorique de 1Mbps ayant une portée maximal de trentaine de mètres.

2.6.1.2 Réseaux locaux sans fils (WLAN)

WLAN (Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise en ayant une portée d'environ une centaine de mètre. Le Wi-Fi (Wireless Fidelity) ou IEEE 802.11 en est la technologie la plus célèbre.

2.6.1.3 Réseaux métropolitains sans fils (WMAN)

C'est le réseau WAN mais sans fils. On l'appelle aussi le BLR (Boucle Local Radio). Ce BLR offre un débit de 1 à 10 Mbps allant une portée de 4 à 10 Km.

2.6.1.4 Réseaux étendus sans fils (WWAN)

WWAN (Wireless WAN) sont en ce moment les réseaux cellulaires mobiles. On dénombre le GSM (Global System for Mobile communication), GPRS (General Packet Radion Serviece) , UMTS (Universal Mobile Telecommunication System) ,…

2.6.2 Wi-Fi (Wireless-Fidelity)

Le Wi-Fi est donc une technologie des réseaux locaux sans fils normé IEEE 802.11.

Plusieurs variantes de la norme IEEE 802.11 existent actuellement. Chacun sont différencier par leurs débits maximaux qu'elles offrent et de sa fréquence porteurs. [20]

Le Wi-Fi possède deux modes opératoires :

- Le mode Infrastructure
- Le mode Ad-hoc

2.6.2.1 Mode Infrastructure

Chaque ordinateur est connecté à un point d'accès (AP). L'ensemble du point d'accès avec les stations sont appelé BSS (Basic Service Set). Cela forme une cellule. Un BSS est identifié par un BSSID (ID pour Identifier).

Plusieurs BSS peuvent être relié pour former un système de distribution noté DS (Distribution System) constituant ainsi un ensemble de services étendu ou ESS (Extended Service Set). Ce DS peut être une liaison filaire.

Chaque ESS est identifié par son ESSID. Un ESSID (ESS Identifier), souvent abrégé SSID, représente le nom du réseau. Cet identifiant est des suites de caractères de 32 bits au format ASCII.

2.6.2.2 Mode Ad-hoc

Un réseau en mode ad-hoc est un groupe de terminaux formant un IBSS (Independent Basic Service Set). Dans ce réseau, il n'y a pas d'utilisation d'un point d'accès. Cependant, ce réseau peut interconnecter des points d'accès entre eux. Ainsi, son rôle consiste à permettre aux stations de communiquer sans l'aide d'une quelconque infrastructure. [5][19]

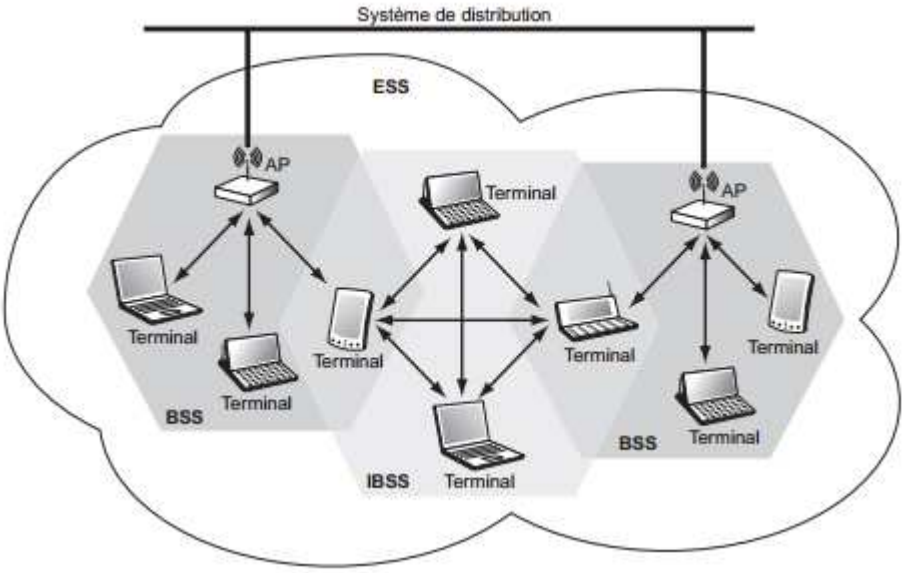

Figure 2. 10 : *Les services offertes par le mode Infrastructure et le mode ad-hoc.*

2.6.3 Sécurité

La façon la plus simple pour protéger un réseau Wi-Fi est de cacher le SSID. Cependant, il existe une autre méthode. Les spécifications 802.11 définissent plusieurs algorithmes de chiffrement, dont le WEP (Wired Equivalent Privacy) et le WPA (Wi-Fi Protected Access). [21]

2.6.3.1 WEP (Wired Equivalent Privacy)

Dans les réseaux sans fil, le support est partagé. Tout ce qui est transmis et envoyé peut donc être intercepté. Pour permettre aux réseaux sans fil d'avoir un trafic aussi sécurisé que dans les réseaux

fixes, le groupe de travail 802.11 a mis au point le protocole WEP, dont les mécanismes s'appuient sur le chiffrage des données et l'authentification des stations.

C'est RC4(Ron's Code 4) qui réalise le chiffrement des données en mode flux octets (stream cipher), à partir d'une clé de longueur comprise entre 8 et 2048 bits il génère (à l'aide d'un pseudo random generator PRNG) une suite d'octets pseudo aléatoire nommée KeyStream. Cette série d'octets (Ksi) est utilisée pour chiffrer un message en clair (Mi) à l'aide d'un classique protocole de Vernam, réalisant un « ou exclusif » (xor) entre Ksi et Mi (Ci = Ksi xor Mi). [4]

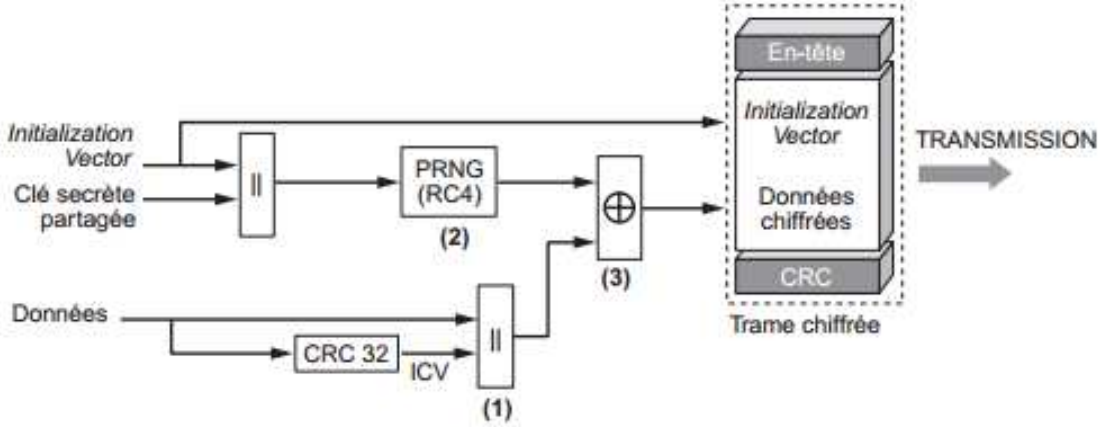

Figure 2. 11 : *Processus de Chiffrement WEP.*

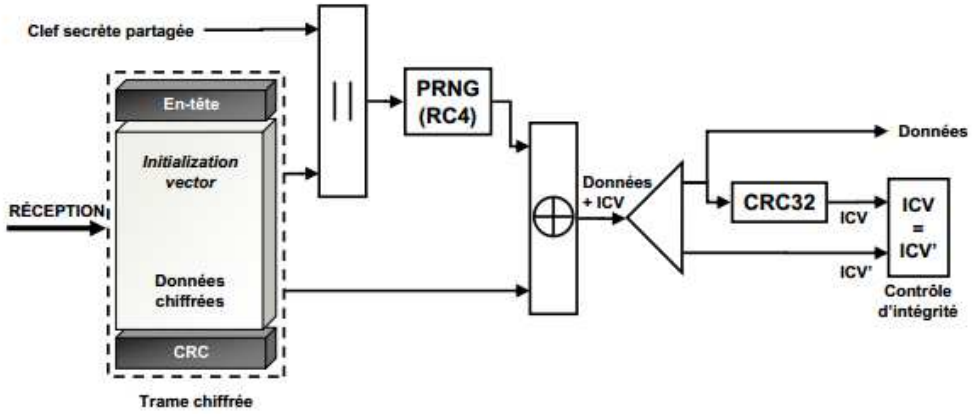

Figure 2. 12 : *Processus de déchiffrement WEP.*

2.6.3.2 WPA (Wi-Fi Protected Access)

La technique de chiffrement WEP possède déjà une faille bien connue des hackers. Ainsi, le groupe de travail IEEE 802.11i a finalisé en juin 2004 une architecture destinée à combler ces lacunes qui est le WPA (Wi-Fi Protected Access). [22]

2.7 Virtual Private Network

2.7.1 Définition

Un VPN (Virtual Private Network) est un tunnel de communication fournissant aux utilisateurs et administrateurs d'un système d'information des conditions d'exploitation, d'utilisation et de sécurité à travers un réseau public identiques à celles disponibles sur un réseau privée. [23][24]

2.7.2 Principe

Un VPN se base sur la création d'un tunnel crypté permettant la confidentialité des données transmises. On appelle cela la Tunneling.

Ce tunnel peut rendre des services différentes comme le chiffrement et déchiffrements de données, compression et décompression des données envoyées, ou même d'offrir l'impression à l'utilisateur de travailler en réseau local.[25]

Exemple: Tunnel SSH (The Secure Shell):

SSH est un protocole permettant d'établir une session interactive chiffré entre un client et un serveur. Il utilise l'algorithme RSA (Rivest, Shamir et Adleman) pour la négociation des clés. Après que les clés sontéchangées, la communication entre les deux machines se fait par un chiffrage symétrique tel que Blowfish. SSH possède maintenant une deuxième version moins vulnérable que la première. [26]

La création du tunnel est faite par l'IKE (Internet Key Exchange) et de le protocole IPSec (IP Security). IKE crée le tunnel et IPSec code les données.

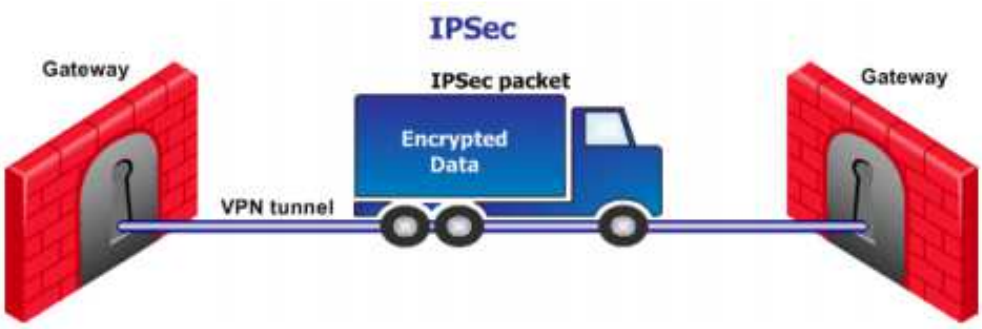

Figure 2. 13 : *Principe du tunneling.*

2.7.3 Type de VPN

En pratique, il existe trois types de VPN [25] [27] :

- VPN Host to Host
- VPN Host to LAN
- VPN LAN to LAN

2.7.3.1 VPN Host to Host

Le tunnel est directement entre deux machines. Les flux de données est crypté et transite sur les réseaux publics de manière codée.

2.7.3.2 VPN Host to LAN

On l'appelle aussi VPN d'accès. Il est utilisé pour permettre à des utilisateurs d'accéder au réseau privé de leur entreprise. Alors, c'est le VPN destiné pour les télétravailleurs.

2.7.3.3 VPN LAN to LAN

Comme son nom l'indique, ce type de VPN permet d'interconnecter deux réseaux privés. C'est ce type de VPN qu'on utilise pour interconnecter deux sites distants comme l'intranet VPN reliant deux intranets et l'extranet VPN reliant le réseau d'une entreprise à ses clients et partenaires.

2.8 Pare-feu et DMZ

2.8.1 Pare-feu ou Firewall

Le pare-feu est un programme, ou un matériel, chargé de vous protéger du monde extérieur en contrôlant tout ce qui passe, et surtout tout ce qui ne doit pas passer entre internet et le réseau local.

Le pare-feu joue un rôle essentiel dans la sécurisation d'un réseau. Tous les trafics doivent y passer et y être contrôler. Peu importe que ce soit un réseau d'entreprise ou réseau domestique, un pare-feu actif est nécessaire pour se protéger du réseau public. Les menaces sont nombreuses, on ressent actuellement nombreux menaces de virus, de vers, d'attaques par déni de Service (DoS Deny of Service), de hacking tel que les MID (man in the middle) l'homme au milieu, des attaques causés par des botnets. [28] [29]

2.8.1.1 Rôles

- Le pare-feu gère les connexions sortantes à partir du réseau local. (Rôle de contrôle)
- Il protège le réseau interne des intrusions venant de l'extérieur. (Rôle de sécurité)
- Il surveille et trace le trafic entre le réseau local et l'internet. (Rôle de vigilance)

2.8.1.2 Classe de Pare-feu

On peut classer les pare-feu comme suit :

- Les pare-feu de niveau réseau

Ils fonctionnent à un niveau bas de la pile TCP/IP. Il se base sur le filtrage des paquets et il est possible de filtrer les paquets suivant l'état de la connexion. Tout cela est transparent aux yeux des utilisateurs.

- Les pare-feu au niveau applicatif

Ils fonctionnent au niveau le plus haut de la pile TCP/IP et se base généralement sur des mécanismes de proxy. Avec ces pare-feu, il est possible d'interpréter le contenu du trafic.

- Les pare-feu des applications

Ce type de pare-feu donne simplement des restrictions au niveau des différentes applications.

2.8.1.3 Politique de sécurité

Un pare-feu doit être toujours régi par une politique de sécurité. Pour le définir, c'est le discipline que le pare feu doit suivre. Dans la vie quotidienne, elle représente les actes qui sont permis, les punitions pour ceux qui désobéissent la loi.

2.8.2 Demilitarized Zone

DMZ, « Demilitarized zone » ou zone démilitarisée, souvent appelé périmètre réseau, est un sous réseau physique ou logique qui contient et expose des services d'un entreprise destiné pour les réseaux externes.

Le concept de DMZ a été copié du conflit entre le Corée du Nord et du Corée du Sud lors de la guerre froide. En 1953, le terme d'armistice conclu entre ces deux Corée prévoit la création d'une zone neutre qui a reçu le nom de zone DMZ. Le DMZ était une portion géographique où les armes lourdes étaient non autorisées. L'intention était de prévenir un quelconque conflit jusqu'à ce que la résolution pour la paix soit atteinte. Ainsi, le but du DMZ est de garder les Nord-Coréens en Corée du Nord en dehors du territoire du Coré du Sud. Les Nord-Coréens ne sont acceptés que dans la zone DMZ. Par analogie au DMZ dans une infrastructure réseau, les utilisateurs non-internes sont interdits d'entrée dans le réseau interne ou privée. Ils ne sont autorisés qu'accéder dans le DMZ où il y a les serveurs. Et son but est de mieux sécuriser le réseau en ajoutant plus de politique de sécurité.

Initialement, le réseau est simplement protégé par un pare-feu, ce pare-feu sépare la partie interne et externe (Inside /Outside) du réseau. Si ce dernier possède une faille, ou s'il s'écroule, la sécurité du réseau interne tout entier s'écroule. À part cela, ce type de sécurisation ne permet que le NAT

et le filtrage de paquet. Le filtrage qui régissent le pare-feu a un grand défaut car il autorise ou bloque complètement un protocole pour tous les utilisateurs. Il n'y a pas de flexibilité et la disponibilité n'est pas ainsi assurée.

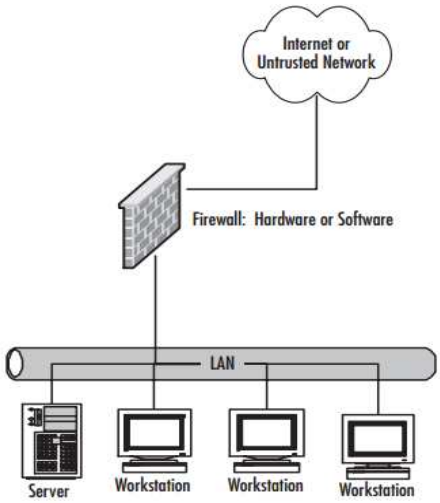

Figure 2. 14 :*Réseau interne protégé par un pare-feu.*

C'est à cause de ce grand défaut que le principe de DMZ a été implémenté dans un réseau. Un DMZ permet la division l'infrastructure réseau en trois partie : le réseau externe (Untrusted network), le réseau interne et le réseau neutre (zone DMZ).

Normalement, deux pare-feu doit séparer ces trois parties de réseau. La mise en place d'une bonne politique de sécurité devient ainsi plus flexible. Mais l'implémentation s'avère couteuse et complexe. Alors, il est préférable d'avoir une infrastructure de la figure 2.15. [30]

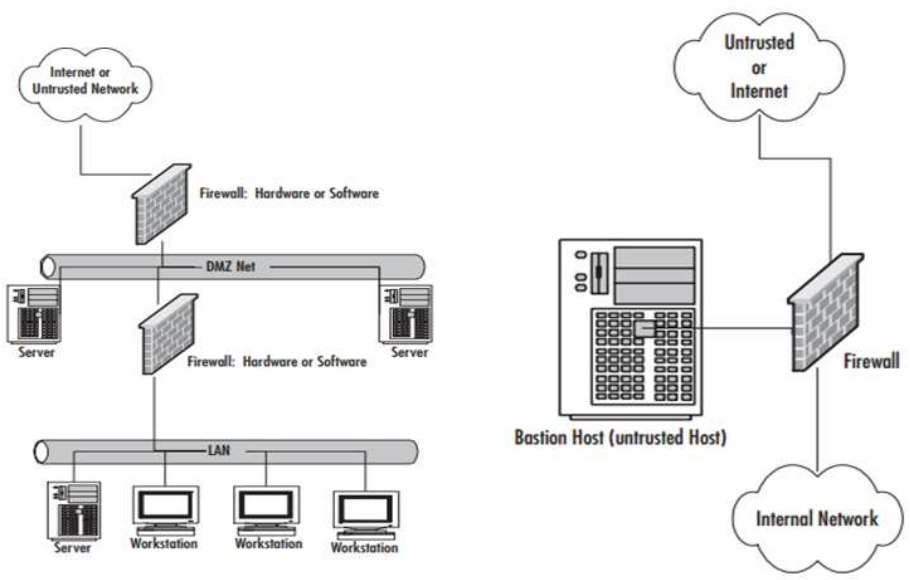

Figure 2. 15 :*Implémentation DMZ parfaite à gauche et DMZ basique à droite.*

2.9 Conclusion

Ce chapitre parle des fonctionnalités dans un réseau informatique. Touscommencent par le développement de la commutation et le routage. La technique NAT a été vu. On n'a pas oublié un des technologies le plus célèbre qui est le Wi-Fi. Et enfin, les études sur les bases essentielles pour une bonne sécurité et une bonne circulation de flux de réseau ont été faites, à travers le développement de VLAN, de VPN, de pare-feu et de la théorie de DMZ utile pour partager les ressources tels que l'information au monde entier à travers les réseaux.

CHAPITRE 3
ENVIRONNEMENT DE CONCEPTION DE RESEAU D'UNE ENTREPRISE

3.1 Objectifs de toutes les conceptions de réseaux

Concevoir un réseau requiert la prise en compte de son « extensibilité », de sa « disponibilité », de sa « facilité de gestion » et de sa « sécurité ».

Si le concepteur oublie un de ces paramètres, le réseau est mal créé, voire une conception à refaire. Ainsi, les objectifs sont ces quatre paramètres. [31]

3.1.1 Disponibilité

Le réseau doit être disponible et fonctionnel en permanence, même en cas de rupture de liaison, de panne matérielle ou de surcharge. La disponibilité est un des critères de QoS (Quality of Service) les plus importants, surtout du point de vue utilisateurs.

Généralement, ce critère sous-entend le pourcentage de temps durant lequel le réseau est opérationnel. Pour être toujours disponible, la redondance des matériels et alimentations utilisées est le plus simple à faire.

3.1.2 Extensibilité

Le réseau doit être facile à modifier. Son envergure et ses performances sont à tenir en compte au court du temps. Ses fonctions et ses services doivent tous être évolutifs. Ainsi il sera facile de s'adapter à sa croissance suivant les besoins de l'entreprise.

3.1.3 Sécurité

Toutes les données qui y circulent et qui y sont stockées doivent être protégées. La vulnérabilité d'une entreprise est souvent causée à partir d'une faille dans cette partie sécurité.

La fiabilité aux accès application doit aussi être assurée.

3.1.4 Facilité de gestion

Le réseau doit être facile à gérer. Cela facilite bien la tâche lors d'une extension ou modification de l'infrastructure. En plus, avoir un réseau facile à gérer permet un dépannage rapide et simple lors d'une panne. Le temps de réparation est réduit considérablement.

3.2 Modèles de conception réseau

Il est possible de concevoir un réseau de deux façons :

- Réseau linéaire
- Réseau hiérarchique

3.2.1 Réseau linéaire

C'est une topologie de réseau où les nœuds sont regroupés en plusieurs petites sections. Il est ainsi facile à gérer et de faible coût de déploiement. Cependant le trafic reste local. Seuls les trafics destinés aux autres réseaux sont acheminés vers une couche supérieure.

Le problème c'est que les périphériques de couche 2 offrent peu d'opportunités de contrôle de diffusion et de filtrage de trafic indésirable. Le domaine de diffusion reste aussi considérablement grand. L'ajout de nouveaux périphériques et application dégradera ainsi le temps de réponse.

De plus, tous les routeurs remplissent essentiellement les mêmes fonctions et leurs fonctions ne sont pas biens définies. L'expansion du réseau s'effectue au hasard et de façon arbitraire. Cette topologie est utilisée dans une structure de réseau maillé. [2][31]

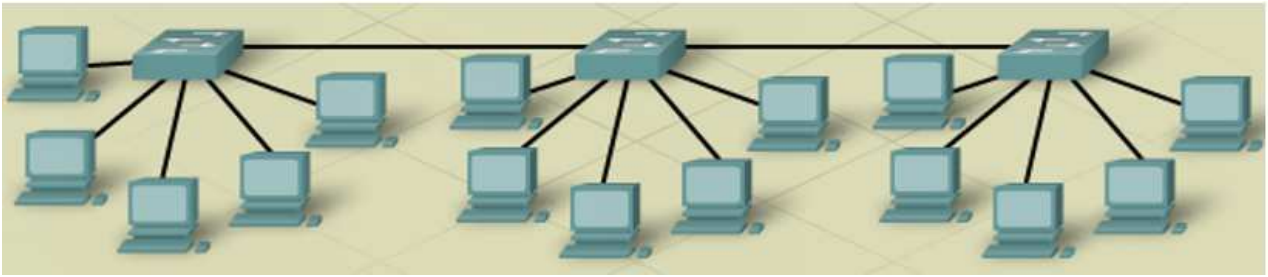

Figure 3.0 1 : *Un réseau linéaire.*

3.2.2 Réseau hiérarchique

Connu aussi sous le nom de « réseau en arbre », un réseau hiérarchique divise les périphériques en un certain nombre de réseaux distincts. Vu son infrastructure en arbre, on peut classifier chaque niveau en couche. Cette division est actuellement un modèle de référence d'une conception réseau. Cela permet d'obtenir un réseau simple, performant et facile à administrer.

Cette division permet aussi de créer un réseau modulaire. Cisco a créé un modèle d'approche de la conception d'un réseau, un modèle dit modulaire. [31]

Il existe essentiellement trois (3) couches de base :

- Couche cœur de réseau ou couche « centrale »
- Couche de distribution
- Couche d'accès

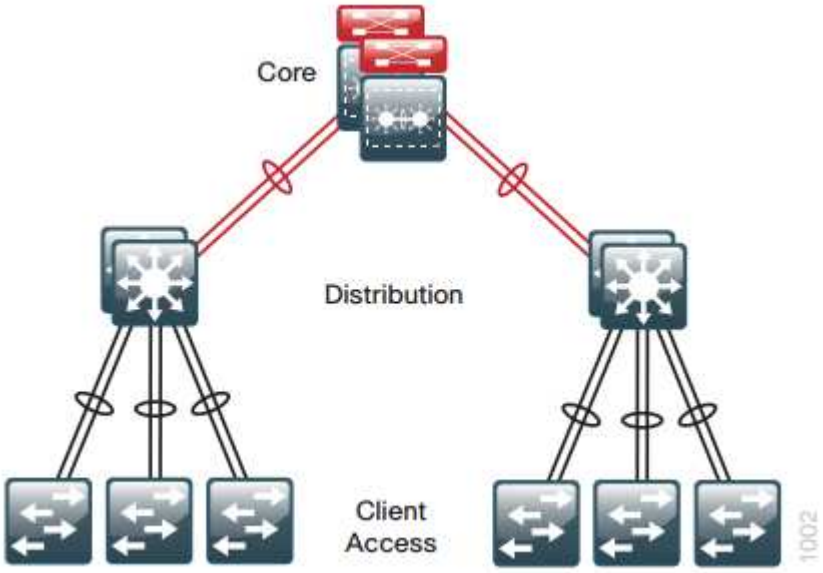

Figure 3.0 2 :*Réseau hiérarchique.*

3.2.2.1 Couche cœur de réseau :

La couche cœur offre un chemin rapide entre des sites distants. Elle permet aux deux couches distribution et accès de se connecter aux réseaux extérieurs. Cela peut être l'internet, réseaux VPN ou WAN, l'extranet.

Cette couche n'effectue pas des tâches liées au traitement de paquets, voire les filtrages, car cela réduira fortement la vitesse de commutation des paquets. Elle assure la redondance et la convergence rapide entre les autres modules ou couches du réseau. Elle est formée par des routeurs et des commutateurs œuvrant sur la couche 3 du modèle OSI. Ainsi, la connectivité haute vitesse du réseau est assurée. [31] [32]

Ses principaux rôles sont :

- Assurer la connexion de plusieurs bâtiment ou sites,
- Fournir une connectivité pour la batterie serveur ou ferme de serveur.

Ses objectifs sont :

- fournir un temps utile de 100 % ;
- optimiser le débit ;
- faciliter la croissance du réseau

Pour atteindre ces derniers, l'utilisation de certains technologies devient nécessaire, tel que :

- Routeur et commutateur multicouche,
- Redondance et équilibrage de la charge.

a. Routeur et commutateur multicouche

Il existe trois types de commutateurs. Ces trois sont différenciés suivant la couche du modèle OSI où ils opèrent. Ainsi, un commutateur de niveau 2 agit au niveau des couches physiques et liaison de données. Il n'opère que sur les trames MAC. Un commutateur de couche 3 ou de niveau 3 opère alors sur les paquets IP. Il est l'équivalent d'un routeur. Le dernier est le commutateur de niveau 4, traitant à la fois les paquets IP et les numéros de port. [31]

Un commutateur multicouche est la combinaison de ces trois types de commutateur. La règle qui le régit est : « route once, switch many » ou commuter plusieurs fois après un seul routage.

b. Redondance et équilibrage de la charge

La redondance de la liaison offre un chemin d'accès alternatif aux données en cas de pannes et un équilibrage de charge et sauvegarde.

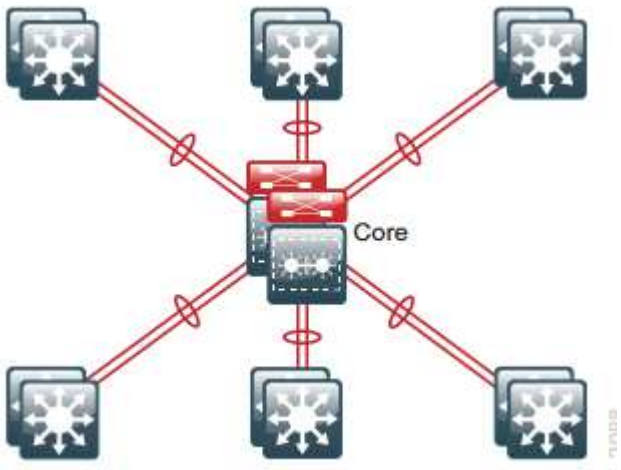

Figure 3.0 3 : *Couche cœur (core layer).*

La plupart des couches cœur de réseau sont câblées selon une topologie à maillage global ou à maillage partiel. Dans une topologie à maillage global, chaque périphérique dispose d'une

connexion avec tous les autres périphériques. Ce type de topologie offre l'avantage d'un réseau entièrement redondant, mais sa gestion et son câblage peuvent s'avérer difficiles et onéreux. Pour les installations de grande taille, on utilise plus couramment une topologie à maillage partiel modifié. Dans ce type de topologie, chaque périphérique est connecté à au moins deux autres, créant une redondance suffisante sans la complexité d'un maillage global.

En cas de panne d'un périphérique, la vitesse de reprise est un facteur essentiel. D'où la notion de « Convergence ». [31]

La convergence a lieu lorsque tous les routeurs de réseau possèdent toutes les informations nécessaires et précises à propos du réseau. Plus le délai de convergences est faible, plus le réseau réagira plus vite en cas de modification de la topologie. Ce délai affectera :

- la vitesse à laquelle les mises à jour de routage atteignent tous les routeurs du réseau ;
- le temps mis par chaque routeur pour effectuer le calcul nécessaire pour déterminer les meilleurs chemins d'accès.

Ce délai est en fonction du protocole de routage utilisé. [33]

3.2.2.2 Couche de distribution

Formé essentiellement par des périphéries de la couche 3 du modèle OSI, cette couche assure l'agrégation de ses liaisons avec les Switch de la couche d'accès. Elle relie la couche accès au cœur du réseau. [31][34]

Ses principales fonctions :

- Fournir un point de connexion pour les différents réseaux locaux distincts,
- Veiller à ce que le même réseau local reste local,
- Faire passer les trafics destinés à d'autres réseaux,
- Filtre les trafics entrants et sortants à des fins de gestion de la sécurité et de la circulation,
- Assure la connexion de l'accès au cœur, ainsi une connexion vers une connexion distante.

On y applique :

- le filtrage et la gestion des flux de trafic ;
- la mise en application des stratégies de contrôle d'accès ;
- le résumé des routes avant notification à la couche cœur de réseau ;

- l’isolation de la couche cœur de réseau par rapport aux pannes ou interruptions de service de la couche d’accès ;
- le routage entre les réseaux locaux virtuels de la couche d’accès.
- la gestion les files d’attente et la hiérarchisation du trafic, avant la transmission via le cœur du campus.

Vu la conception hiérarchique, cette couche évite qu’une panne au niveau du couche d’accès aura un effet au niveau du cœur du réseau.

Dans le cas d’utilisation des commutateurs de la couche 2, il est nécessaire d’appliquer le protocole STP (Spanning Tree Protocol).

3.2.2.3 Couche d’accès

C’est dans cette couche que les utilisateurs finaux se connectent à travers leurs équipements, appelés « périphériques finaux ». Cette connexion se fait avec et sans fil.

Elle fournit une connexion à haut débit pour les utilisateurs, et est souvent divisée en plusieurs sous-réseaux LAN grâce à la technologie VLAN.

Elle protège le réseau contre les erreurs humaines et les attaques malveillantes, en assurant qu’aucun périphérique ne fournit des services aux autres équipements des utilisateurs. Ainsi, prendre contrôle d’un autre équipement devient impossible. En plus de cela, cette couche vérifie que chaque dispositif a le droit de se connecter aux réseaux.

La découverte de nouvelles technologies sur la voix et les vidéos pousse maintenant les concepteurs à concevoir une couche d’accès apte à les supporter. Cela signifie que les trafics qui s’y rattachent doivent être séparés de ceux des donnés pour assurer une qualité des services élevée.

Figure 3.0 4 : *Exemple de couche d’accès.*

Un réseau n’a pas complètement besoin de ces trois couches pour fonctionner. Certes, c’est l’idéal. Cependant, un modèle à deux couches, n’ayant que les couches de distribution et d’accès, peut être utilisé dans le cas d’un réseau de petite taille.

3.2.2.4 Avantages

Les modèles de réseaux sont généralement conformes au modèle linéaire ou hiérarchique. Cependant, vu que chaque routeur du modèle linéaire ou mailléne possède pas une fonction bien précise, les concepteurs optent progressivement au modèle hiérarchique. De plus, ce dernier modèle possède beaucoup d’autres avantages par rapport à celui qui est linéaire. [31] [32] [33]

a. L’évolutivité

Les réseaux hiérarchiques sont conçus pour croître facilement. Cette croissance n’aura pas d’effet négatif sur le contrôle et la facilité de gestion. La modularité de la conception permet la reproduction simple des éléments de conception au fur et à mesure de l’évolution.

b. La redondance

La redondance au niveau des couches cœurs et de distribution garantit la disponibilité des chemins d’accès. Les routeurs et les Switch de niveau 3 seront doublés pour veiller à ce que le réseau soit disponible autant que possible et afin d’éviter des pannes nocifs pour le réseau.

c. La facilité de gestion

La tâche de gestion est fortement simplifiée vu que chaque couche a sa propre fonction spécifique. Avec le modèle hiérarchique, repérer une panne est facile. En plus si un réseau local tombe en panne, son dépannage n’aura pas d’impact sur le réseau tout entier.

d. La Performance

Dans ce modèle, les flux sont bien optimisés, différemment du modèle linéaire. Avec l’ajout des VLAN, on peut isoler les flux d’informations nécessitant une grande capacité de bande passante. On pourra alors profiter de toute la bande passante à la disposition.

e. La Sécurité

Grâce aux fonctionnalités de sécurité que les Switch et les routeurs possèdent, il est maintenant simple de configurer des pare-feu, des Access-List au niveau de la couche distribution. En plus, vu que la couche d’accès est divisé en plusieurs réseaux locaux, on peut les sécuriser un à un, de façon différente.

3.3 Entreprise Composite Network Model

Signifiant « architecture d'entreprise Cisco », ce modèle divise un réseau de grande taille en différentes zones modulaires. Il y alors une conception de réseau à la fois hiérarchique et modulaire. Chaque zone possède leur propre caractéristique au niveau de la connectivité physique ou logique. Cette modularité accroît la flexibilité, la facilité de mise en œuvre et de dépannage du réseau. On divise le réseau hiérarchique comme suit [34]:

- Entreprise campus ou Campus d'entreprise,
- Entreprise Edge ou périphérie d'entreprise,
- Service provider edge ou Réseau étendu et Internet.

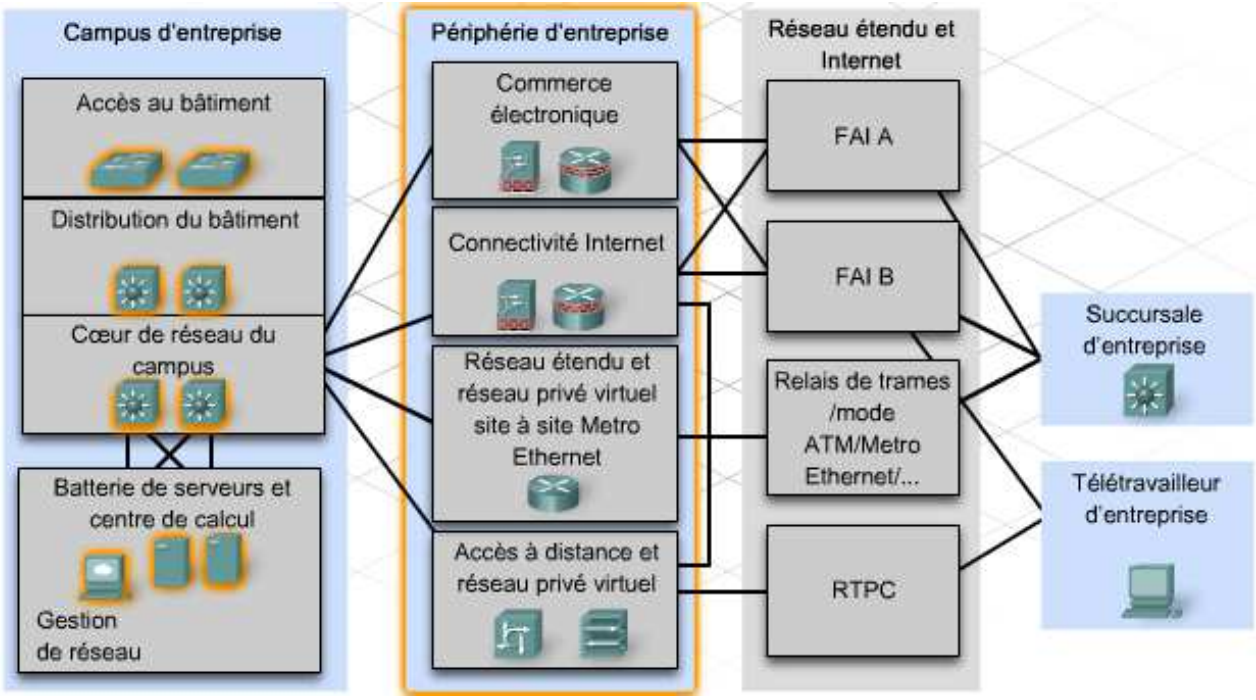

Figure 3.0 5 : *Réseau modulaire.*

3.3.1 Campus d'entreprise

Cette zone contient les éléments de réseau nécessaires à une exploitation indépendante, au sein d'un réseau de campus ou de filiale. Il est à noter que le réseau dans le campus suit encore le modèle hiérarchique. C'est pourquoi il est formé par les modules suivants:

3.3.1.1 Accès au bâtiment

Ce module couche d'accès comprend des commutateurs de couche 2 et de couche 3 pour fournir la densité de port requise. C'est là qu'a lieu l'implémentation de réseaux locaux virtuels et de

liaisons agrégées sur la couche de distribution du bâtiment. La redondance des commutateurs de la couche de distribution du bâtiment est importante.[31] [34]

3.3.1.2 Distribution du bâtiment

Ce module de couche de distribution agrège l'accès au bâtiment à l'aide de périphériques de couche 3. Le routage, le contrôle d'accès et la qualité de service s'effectuent sur cette couche. Il est essentiel de fournir une redondance dans cette zone.

3.3.1.3 Cœur de réseau du campus

Ce module de couche cœur de réseau fournit une inter-connectivité à haut débit entre les modules de couche de distribution, les batteries de serveurs de centre de calcul et la périphérie d'entreprise. La conception de cette zone est articulée autour de quatre éléments essentiels : redondance, convergence, rapidité et tolérance aux pannes.

3.3.1.4 Batterie de serveurs et centre de calcul

Ce module offre aux serveurs une connectivité à haut débit et une protection. Il est essentiel de fournir des fonctions de sécurité, de redondance et de tolérance aux pannes dans cette zone. La batterie de serveurs du centre de calcul protège les ressources de serveur. Il est bien surveillé aux niveaux de la performance en contrôlant la disponibilité du périphérique et du réseau.

3.3.2 Périphérie d'entreprise

Ce module étend les services de l'entreprise à des sites distants et permet à l'entreprise d'utiliser Internet et les ressources de partenaires. Il fournit la qualité de service, l'application des règles, des niveaux de service et la sécurité. Lorsque le trafic de données arrive au réseau campus, cette zone le filtre et le sépare des ressources extérieures, pour l'acheminer vers le réseau d'entreprise. Elle contient tous les composants nécessaires à une communication efficace et sécurisée entre le campus d'entreprise et les sites distants, les utilisateurs distants et Internet.

3.4 Méthodologie de conception de réseau

Être professionnel en conception réseau ne signifie pas qu'un réseau doit être très complexe. Plus la conception n'estsimple, plus sa maintenance, sa gestion et son extension deviennent fastidieuses.

Il est nécessaire de connaître les besoins de celui qui va utiliser le réseau, que ce soit un entreprise, une organisation, ou quelconque utilisateur. Analyser leurs besoins est nécessaire pour la conception et le choix des matériels utilisés.

L'utilisateur peut être des clients d'une entreprise, des simples visiteurs, des travailleurs. Cependant, en factorisant leur besoin, ce qu'ils veulent c'est une grande vitesse de connexion, de large bande passante, de la disponibilité 24h/24 et d'un faible temps de réponse.

Savoir les besoins des utilisateurs est alors primordial. Nombreux sont les concepteurs de réseau actuels qui se contentent du simple fonctionnement du réseau. Ils ne prennent pas en compte les vrais besoins des utilisateurs ; et ils oublient complètement l'évolution, l'extension, l'augmentation du nombre d'utilisateurs au futur. Ils se contentent seulement que le réseau fonctionne en temps voulu. La conséquence devient alors une nouvelle création, conception de réseau. Cela s'avère couteux.

La méthodologie de conception de réseau se divise généralement en trois étapes bien distinctes [31] [34] :

- Identification des besoins du réseau
- Analyser l'infrastructure déjà existant
- Conception de la topologie et des solutions de réseau

Le cycle de vie d'un réseau explique mieux cette méthodologie de conception.

3.4.1 Cycle de vie d'un réseau

Cisco a bien analysé une conception, il a ainsi bien distingué un cycle de vie d'une conception réseau. Ce cycle de vie accompagne l'évolution du réseau. Il s'agit d'une approche à six phases. Chacune de ces phases définit les activités requises pour déployer et faire fonctionner sans soucis tous les matériels informatiques. Ces phases indiquent également comment optimiser les performances d'un réseau tout au long de son cycle de vie [35]. Ces six phases sont :

- Phase de préparation (Prepare)
- Phase de planification (Plan)
- Phase de conception (Design)
- Phase d'implémentation (Implement)
- Phase d'exploitation (Operate)
- Phase d'optimisation (Optimize)

Souvent, l'ensemble de ces six phases est appelé méthode PPDIOO [31].

3.4.1.1 Phase de préparation

Dans cette phase, le but est de monter un dossier commercial à travers une envie d'améliorer l'expérience du client, de réduire les coûts, d'ajouter les services supplémentaires et de prendre en charge l'évolution de l'entreprise. Ce dossier justifiera l'investissement financier requis pour l'implémentation de la nouvelle infrastructure. Une fois ce dossier validé, l'entreprise émettra une demande de proposition ou une demande de devis qui définira les conditions requises pour le nouveau réseau.

Plusieurs actions sont définies dans cette phase. Tout commence tout d'abord sur le besoin de l'entreprise à renouveler ou à créer une nouvelle infrastructure réseau dans le but d'atteindre leurs objectifs commerciaux. Ensuite, il y a la phase d'appel d'offre où les fournisseurs répondront à la demande et proposeront leurs solutions et idées pour atteindre les objectifs mis en place. Cela implique déjà une partie technique de conception. À la fin, un personnel chargé de la clientèle du fournisseur prendra relation avec l'entreprise qui a émis l'appel d'offre. Bien sûr, les réponses de cet appel sera acceptées si et seulement si cela ne dépasse pas le deadline.

En tous, on y définit le but du projet, on y analyse les coûts et avantages, on y donne les options d'approvisionnements. C'est dans cette phase que la budgétisation et la gestion du projet sont faites. Donc on y détermine les exigences en matière de réseau.

3.4.1.2 Phase de planification

On y évalue le réseau existant. C'est le rôle de l'ingénieur en prévente. Il vérifie l'état actuel des infrastructures, de l'exploitation et de l'administration du réseau. Il doit maintenant identifier toutes les modifications à effectuer, qu'elles soient physiques, environnementales ou électriques (périphériques). Tous les changements apportés à l'infrastructure, au personnel, aux processus et aux outils doivent être terminés avant l'implémentation de la nouvelle solution.

Cette phase inclut aussi l'identification des utilisateurs qui utiliseront le réseau. Cela implique la connaissance des applications requises et à utiliser.

En tout, on y crée un document contenant tous les éléments requis en termes de conception, c'est-à-dire, le plan de projet avec la liste des tâches à réaliser, le calendrier et échéances clés, la liste des risques et des contraintes, la liste des responsabilités et les ressources requises.

3.4.1.3 Phase de conception

C'est là quand on fait le plan d'installation. C'est le rôle d'un ingénieur de conception de concevoir ce plan qui doit être créé suivant les objectifs fixés dans la première phase.

Ces plans contiennent :

- La configuration et le test de la connectivité ;
- L'implémentation du système proposé ;
- La démonstration de la fonctionnalité du réseau ;
- La migration des applications de réseau ;
- La validation du fonctionnement du réseau ;
- La formation des utilisateurs finaux et du personnel d'assistance.

Les étapes à suivre pour cette phase sont :

- Création d'un document de conception conforme aux deux premières phases en termes d'Extensibilité, de Disponibilité, de Sécurité et de Facilité de gestion,
- Création logique du réseau,
- Mise en place des plans pour guider l'installation,
- Garantit que les résultats finaux soit conforme aux exigences des clients.

3.4.1.4 Phase d'implémentation

Le réseau est construit conformément aux conceptions prédéfinies. Puis on le test. La vérification de la viabilité du réseau y est faite avec l'identification et la résolution d'éventuels problèmes.

Après une détection et une résolution de tous les problèmes, on fait un test d'acceptation. Ce test permettra de vérifier la conformité du nouveau réseau aux objectifs commerciaux et aux spécifications de conception demandées.

Les étapes suivant sont à suivre :

- On teste le nouveau réseau dans un environnement contrôlé pour identifier et résoudre des problèmes éventuels avant l'installation réelle
- On fait l'installation
- On fait un test d'acceptation du système

Parallèlement à ces étapes, des formations du personnel peuvent être envisagées si c'est nécessaire. Et cette phase est assurée par un ingénieur de services après-vente.

3.4.1.5 Phase d'exploitation

L'exploitation constitue le test final de l'adéquation de la conception. Elle correspond à l'utilisation quotidienne du réseau en mettant en service le réseau. On doit y définir des «

stratégies et des procédures ». La phase d'exploitation comprend la préservation de l'état de fonctionnement du réseau au moyen d'opérations quotidiennes, notamment le maintien d'une haute disponibilité et la réduction des dépenses. La détection des fautes, leur correction et la surveillance des performances au cours du fonctionnement, jour après jour, fournissent des données initiales pour la phase d'optimisation.

Donc, le butest de détecter les erreurs et problèmes qui se révèlent dans l'installation afin de les résoudre et d'assurer l'optimisation du réseau.

Il est primordial de vérifier si les spécifications de conception ont été respectées. Une administration complète inclut :

- Gestion des changements de configuration apportés au réseau
- Identification des pannes de réseau
- Contrôle des niveaux de performance
- Gestion comptable et de sécurité pour l'utilisation du réseau, en individuel ou en groupe

En plus, une architecture de gestion de réseau se compose essentiellement des éléments suivant :

- Système d'administration de réseaux (NMS : Network monitoring system) : application pour surveiller et contrôler les périphériques.
- Protocole de gestion de réseau : facilitant l'échange d'informations entre les périphériques et le NMS (ex : protocoles SNMPv3 -Simple Network Management Protocol version 3)
- Périphériques gérés

3.4.1.6 Phase d'Optimisation

Cette phase a pour objectif l'amélioration des performances et la fiabilité du réseau. On y compare l'expérience de l'utilisateur et le déploiement aux objectifs du projet.

3.4.2 Approche de conception

Il existe deux types d'approches pour concevoir un réseau. [31]

- L'approche ascendante
- L'approche descendante

3.4.2.1 L'approche ascendante

Cette approche est courante mais pourtant peu recommandée. Selon cette méthode, le concepteur choisit les périphériques et les technologies de réseau en fonction de l'expérience passée et non

sur la base d'une connaissance approfondie de l'organisation. Les objectifs commerciaux ne sont pas pris en compte et la conception de réseau proposée ne pourra peut-être pas prendre en charge les applications requises.

3.4.2.2 L'approche descendante

Cette approche adapte l'infrastructure du réseau en fonction des besoins de l'organisation. Elle clarifie les objectifs de conception et aborde celle-ci du point de vue des applications et des solutions de réseau requises par le client, par exemple la téléphonie IP, la mise en réseau du contenu et la vidéoconférence. Le modèle PPDIOO utilise une approche descendante.

.

3.4.2.3 Comparaison entre approche ascendante et approche descendante

	Approche ascendante	Approche descendante
Avantages	Permet une réponse rapide à une demande de conception Facilite la conception basée sur les expériences antérieures	Intègre les exigences organisationnelles Donne une vision globale à l'organisation et au concepteur
Inconvénients	Implémente une solution tenant peu ou pas du tout compte des exigences organisationnelles réelles Peut déboucher sur une conception de réseau inappropriée.	Nécessite plus de temps au préalable avant de créer une conception de réseau Approche peu familière à de nombreux concepteurs de réseau

Tableau 3.0 1 : *Comparaison entre approche ascendante et descendante.*

3.5 Conclusion

Une bonne conception de réseau, que ce soit un réseau de très grande taille ou de petite taille, ne se fait pas facilement. Il faut prendre en compte la disponibilité, l'extensibilité, la sécurité et la facilité de gestion du réseau. Afin d'assurer ces quatre objectifs d'une bonne conception, un bon concepteur a besoin de bien choisir le modèle de réseau à concevoir. En hiérarchisant le réseau, on le divise en plusieurs parties ou modules. Cela facilite grandement la partie extensibilité du réseau dans le futur. Ainsi, un concepteur peut se concentrer et concevoir un à un indépendamment chaque partie. À part cela, il est bon de concevoir un réseau complètement redondant, et même c'est l'idéale. Cependant, le coût d'implémentation sera très élevé et n'est pas à la portée de tous.

Il est alors nécessaire de savoir les besoins des entreprises à qui on va concevoir le réseau. Et pas seulement leur besoin mais aussi leur objectifs commerciaux. Une méthodologie de conception de réseau a déjà été conçue, c'est la méthodologie PPDIOO. En suivant cette méthodologie correspondant aussi au cycle de vie d'un réseau, ces besoins et ces objectifs commerciaux seront bien pris en compte.

Nombreux sont les logiciels de simulation déjà en vogue actuellement et nombreux sont ceux utiles pour une conception de réseau. Maintenant, toutes les théories d'une bonne conception ont été passées en revue. Entrons donc dans la partie pratique.

CHAPITRE 4

SIMULATION D'UN RESEAU CAMPUS AVEC IMPLEMENTATION DE DMZ

4.1 Présentation du logiciel Cisco Packet Tracer

Cisco Packet tracer est un logiciel de simulation de matériel réseau Cisco. C'est un outil développé par Cisco System. Elle permet de s'exercer à la conception ou à la maintenance d'un réseau. [35]

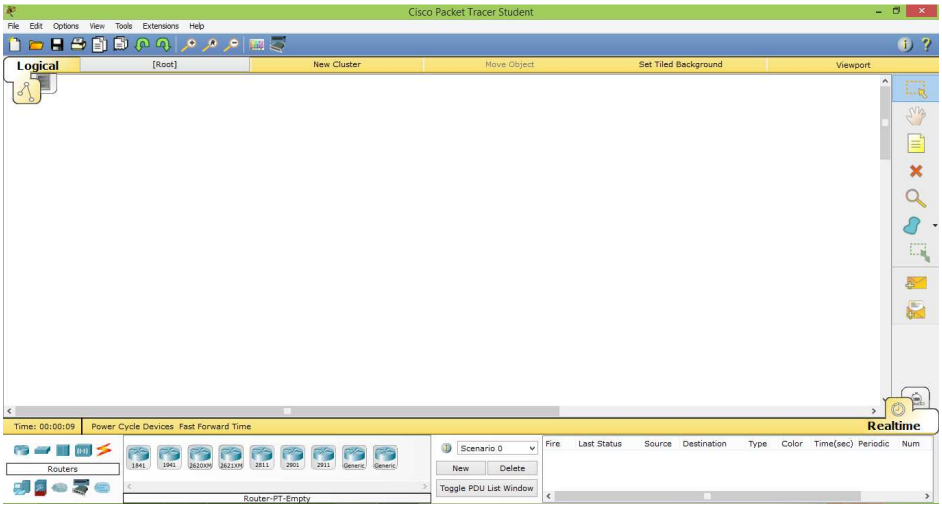

Figure 4.0 1 : *Fenêtre du logiciel Cisco Packet Tracer.*

Ce logiciel supporte presque tous les protocoles du modèle de référence TCP/IP.

Couches	Protocoles supporté par Cisco Packet Tracer
Application	FTP, SMTP, POP3, http, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP, AAA, ISR VOIP
Transport	TCP et UDP, RTP
Réseau	BGP, IPv4, ICMP, ARP, IPv6, IPSec, RIPv1/v2/ng, Muti-AreaOSPF, EIGRP, Routage Statique, NAT, GRE VPN, IPSec VPN,…
Accès Réseau	Ethernet (802.3), 802.11, HDLC, Frame Relay, STP, PPP, WPA, Simple WEP, EAP

Tableau 4.0 1 : *Protocoles supportés par Cisco Packet Tracer.*

Il est à préciser que Cisco System est une entreprise informatique américaine spécialisée dans les réseaux, les matériels réseaux et les serveurs.

Figure 4.0 2 : *Logo de Cisco System.*

La dernière version de Cisco Packet Tracer est 6.3.0 mais celui quiva être utilisée dans ce présent mémoire est la version 6.1.1.

4.2 Présentation du pare-feu ASA 5505

C'est le firewall qu'on va utiliser lors de cette simulation. Il fait partie de la gamme ASA (Adaptive Security Appliances) de la série 5500. Ce pare-feu supporte très bien l'implémentation d'un DMZ et même d'un Datacenter. Ce pare-feu est développé par Cisco Sytem . Dans Cisco Packet Tracer, ce matériel fonctionne déjà avec la License basique. Certes, cette licence limite beaucoup les fonctions du pare-feu, néanmoins, elle suffit à bien concevoir un réseau. [25]

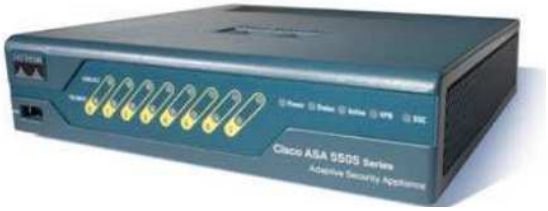

Figure 4.0 3 : *Pare-feu ASA 5505.*

4.3 La conception

Dans cette simulation, un modèle de réseau campus sera conçu pour une entreprise. Ce réseau sera hiérarchique et intégrera une zone neutre qui est le DMZ. Les quatre objectifs d'une bonne conception d'infrastructure de réseau seront à atteindre : la disponibilité, l'extensibilité, la sécurité et la facilité de gestion en suivant bien le modèle PPDIOO.

En réalité, la présente étude va s'arrêter à la phase de conception d'un modèle de réseau. Ce dernier ne va pas être implémenté physiquement.

4.3.1 Phase de préparation

Vu que le réseau à concevoir n'est qu'un modèle, les seuls objectifs posés ne concerneront que des objectifs techniques. Ceux-ci excluront les questions commerciales ainsi que financières. La faisabilité économique du projet ne sera donc pas ici considérée en abordant sa rentabilité et son coût.

Les objectifs sont de :

- Développer un réseau disponible 24h/24
- Développer un réseau facile à agrandir sans avoir à le reconcevoir.
- Sécuriser les informations, notamment celles de l'entreprise.
- Développer un réseau dont la maintenance et la gestion ne présente pas de difficultés pour l'administrateur
- Mettre en place des serveurs accessibles des réseaux publics
- Assurer un accès à distance aux télétravailleurs.

4.3.1 Planification

Il n'y a pas encore d'infrastructure de réseau à évaluer.

Les utilisateurs du réseau seront classés en trois: les employés internes de l'entreprise, les télétravailleurs et les visiteurs.

Les applications à intégrer seront l'application web via le protocole HTTP, une application de stockage de donnée via FTP, une application sur le protocole SMTP pour les services e-mail et une application d'accès VPN pour les télétravailleurs.

Les documents de gestion de projet ne seront pas ici mentionnés vu que le présent mémoire s'arrêtedans la phase de conception.

4.3.2 Phase de conception

Ce présent mémoire est destiné à la conception d'un modèle de réseau. Il faudra recourir aux trois dernièresphases si on veut vraiment créer physiquement le réseau.

4.3.2.1 Infrastructure du réseau

- Le réseau suivra le modèle à deux couches, c'est-à-dire qu'il ne sera formé que par deux couches : la couche fusionnant le rôle « de cœur et de distribution » et la couche d'accès.
- Le réseau est divisé en trois parties :
    - ✓ La partie interne (inside)
    - ✓ La partie Externe (outside)
    - ✓ La zone DMZ

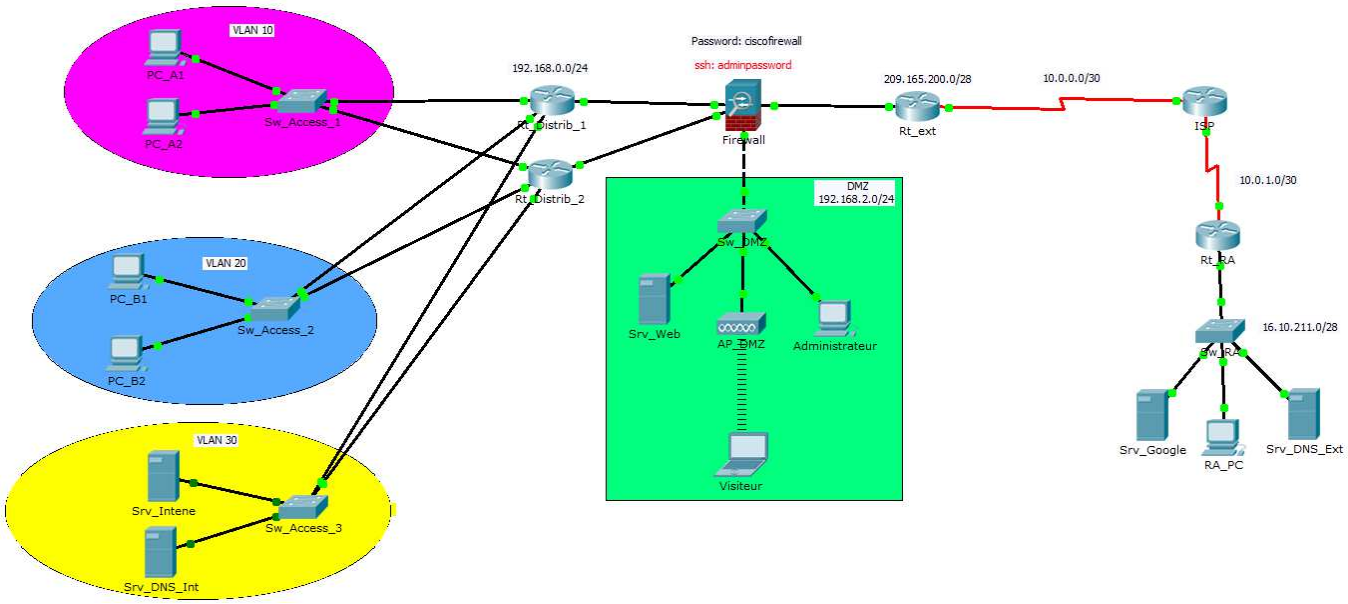

Figure 4.0 4 : *La partie interne à gauche, la zone DMZ en bas et la partie externe à droite (tous par rapport à la pare-feu.*

- Un Firewall ASA 5505 est utilisé pour avoir cette division et pour la sécurisation du réseau interne.

4.3.2.2 Caractéristiques de chaque partie du réseau

a. Partie interne

La couche de distribution est assurée par deux routeurs en redondance : Rt_Distrib_1 et Rt_Distrib_2

La couche d'accès est formée par trois (3) Switch.

Chaque Switch fait partie d'une VLAN configurée dans la couche distribution

b. Zone DMZ

Cette partie du réseau héberge en lui un serveur Svr_Web dont les services suivant sont activés : Service HTTP, Service FTP, Service DHCP et Service SMTP

Y sont mis le PC de l'administrateur et un point d'accès pour les visiteurs.

c. Partieexterne

Cette partie est formée par trois routeurs et un réseau local :

- Rt_ext : routeur se connectant à l'Internet
- ISP : routeur utilisé pour simuler une FAI (Fournisseur d'accès à Internet)
- Rt_RA : routeur avec quoi le réseau local peut se connecter à l'Internet
- Réseau local : réseau utilisé pour simuler « Google », les télétravailleurs RA_PC, et un DNS externe Srv_DNS_Ext

4.3.2.3 Configuration de chaque partie du réseau

Ici, sont citées simplement et globalement les configurations faites dans chaque partie du réseau. Les commandes sont développées à l'annexe.

a. Partie interne

Routeur de Distribution Rt_Distrib_1 et Rt_Distrib_2 :

- Configuration de 3 VLANs :
  - ✓ VLAN 10 / nom= «domaine_A » / adresse réseau: 192.168.0.0/27 : formé par 2 PC : PC_A1 et PC_A2
  - ✓ VLAN 20/ nom= « domaine_B »/adresse réseau : 192.168.0.32/27 : formé par 2 PC : PC_B1 et PC_B2
  - ✓ VLAN 30/nom= « domaine_intranet »/adresse réseau : 192.168.0.64/27 : formé par deux (2) serveurs : Serveur web Sv_Intranet et Serveur DNS Sv_DNS_INT
- Ajout d'une route par défaut
- Configuration du service DHCP pour les VLAN10 et VLAN 20 dont le DNS est Srv_DNS_Int
- Configuration d'un PAT pour accéder au pare-feu
- Configuration du protocole HSRP (Hot Standby Routing Protocol) pour avoir la redondance

HSRP est un protocole gérant la redondance entre les matériels Cisco, comme les routeurs,

b. ZoneDMZ

- Configuration des services Web, FTP et DHCP (pour les visiteurs) du serveur web du DMZ
- Configuration du point d'accès Internet
- Configuration du PC de l'administrateur, dont l'adressage est statique.

c. Partie externe

- Utilisation d'un routage statique pour l'interconnexion des trois routeurs Rt_ext, ISP et Rt_RA
- Activation du service web du serveur de google Svr_google, et du service DNS du serveur Svr_DNS_2.
- Affectation d'une adresse IP statique pour le PC RA_PC

4.3.2.4 Configuration du pare-feu ASA 5505

- Création de trois VLAN et leurs affectations aux ports respectifs:
  - ✓ VLAN 1/ nom = inside / adresse réseau : 192.168.1.0/29 / niveau de sécurité = 100 (le plus sécurisé)
  - ✓ VLAN2/ nom = outside / adresse réseau : 209.165.200.0/28 / niveau de sécurité = 0 (Pas du tout sécurisé et pas fiable)
  - ✓ VLAN3/ nom = DMZ / adresse réseau : 192.168.2.0/24 / niveau de sécurité = 50
- Ajout d'une route par défaut vers le réseau extérieur
- Configuration de deux PAT pour que les PC du réseau internet et DMZ aient accès au réseau externe
- Configuration d'une politique de sécurité pour autorisé les flux ICMP, FTP, TCP, DNS dans le pare-feu. Il est à noter qu'aucun de ces flux ne peut pénétrer dans le réseau interne sauf s'ils y ont été initiés.
- Configuration d'une NAT statique pour le serveur Svr_Web du DMZ. C'est là qu'une adresse IP publique est affectée à ce serveur.
- Configuration d'un accès SSH au pare-feu.
- Configuration de l'accès VPN Clientless des Télétravailleurs (simulé par le RA_PC) au serveur web interne Svr_Interne.

4.3.2.5 Tests de fonctionnement

a. Tests d'accès direct aux différents serveurs

L'accès au serveur Interne par les machines PC (PC_A1, PC du visiteur dans le DMZ et RA_PC) a été testé.

L'adresse IP de ce serveur est 192.168.0.66/27

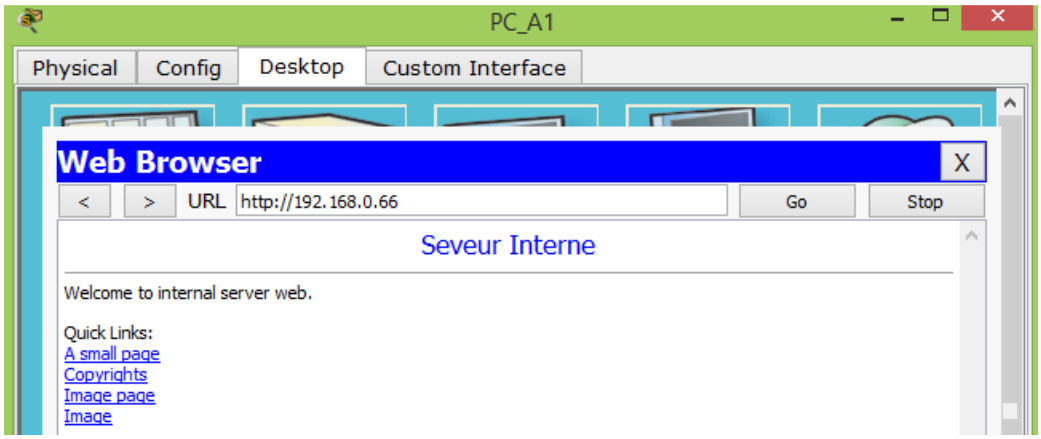

Figure 4.0 5 :*Accès via le réseau interne réussi.*

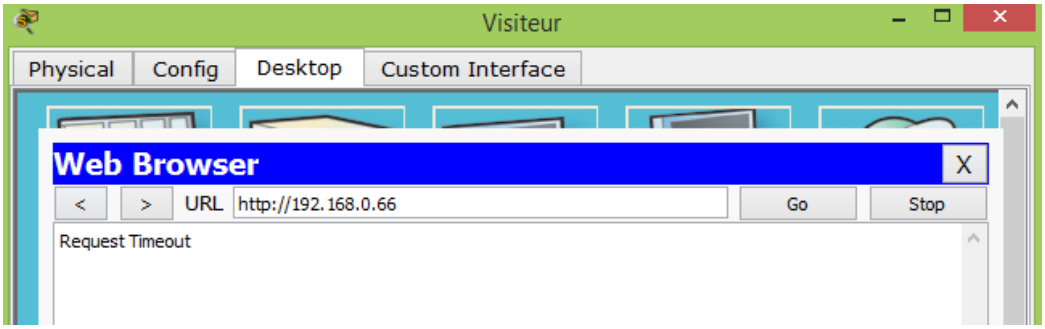

Figure 4.0 6 : *Accès via le réseau DMZ.*

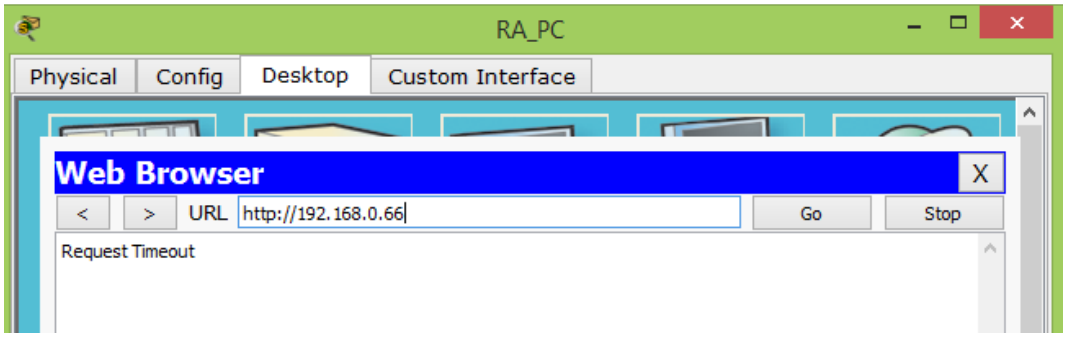

Figure 4.0 7 :*Accès via le réseau Externe impossible.*

En utilisant les mêmes machines, un test sur l'accès au serveur Web du DMZ Svr_Web a été également procédé.

Notons que l'adresse IP de ce serveur est 192.168.2.2 (adresse local) et 209.165.200.3 (adresse accessible du public).

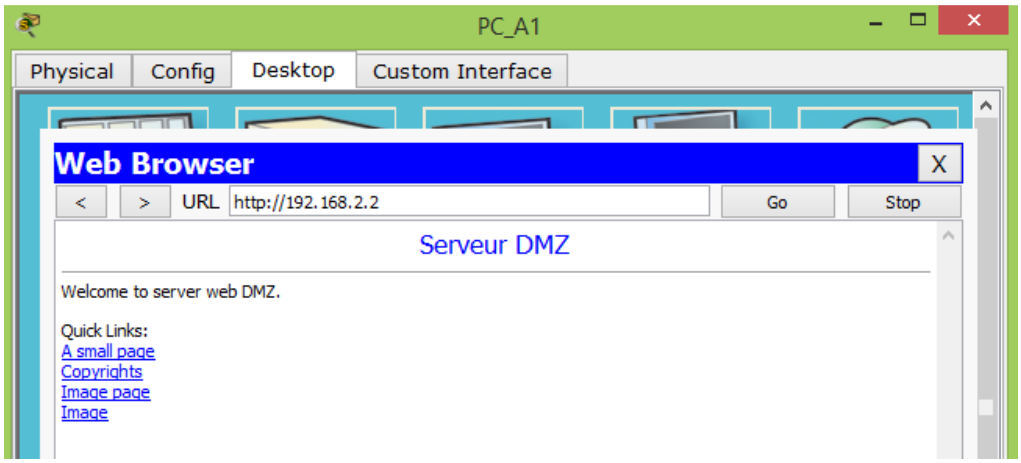

Figure 4.0 8 :*Accès possible via le réseau interne.*

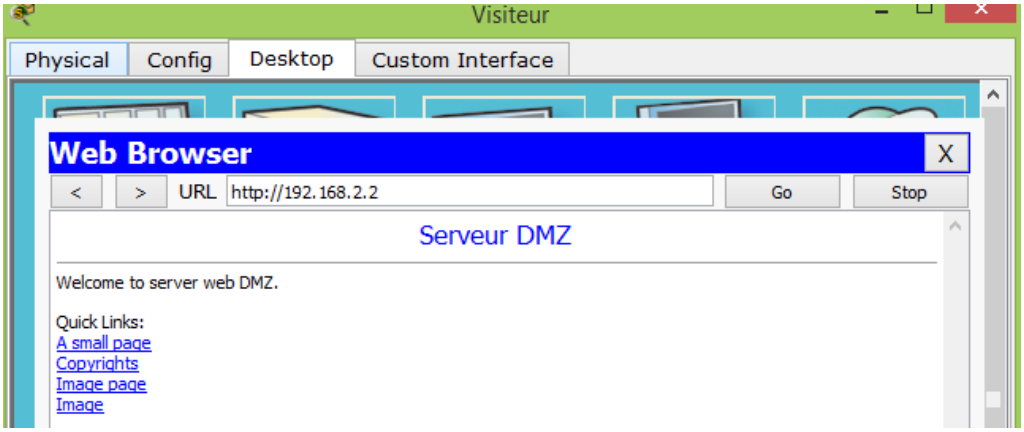

Figure 4.0 9 :*Accès possible via le réseau DMZ.*

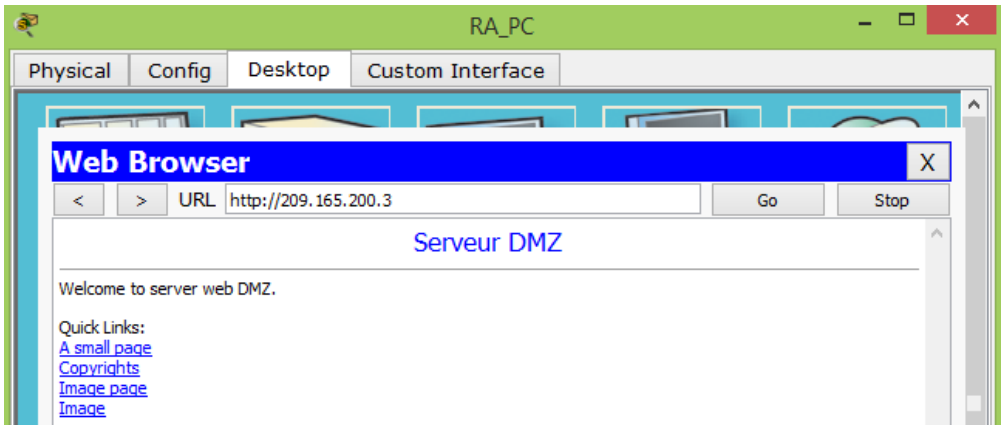

Figure 4. 10 :*Accès possible via le réseau externe.*

Testons en dernier lieu l'accès aux serveurs web de Google avec son nom de domaine via PC_A1 du réseau interne et du PC visiteur du réseau DMZ.

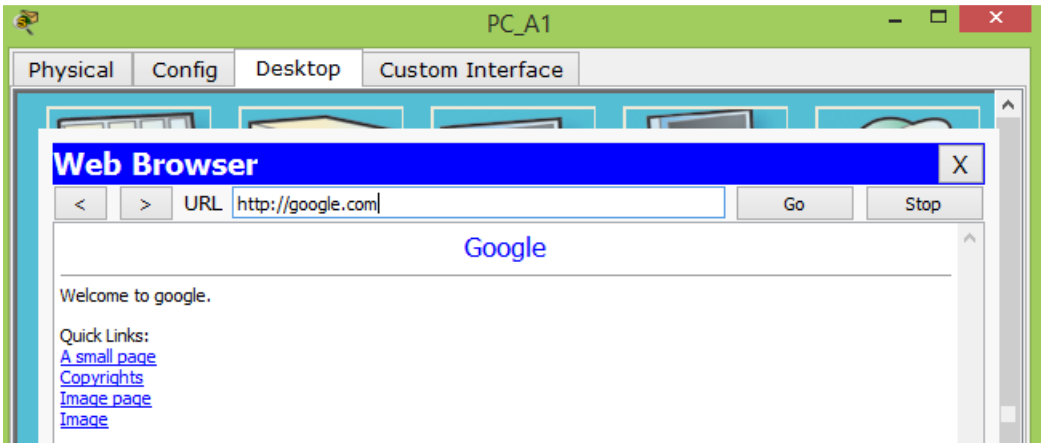

Figure 4. 11 :*Accès réussi via le réseau interne.*

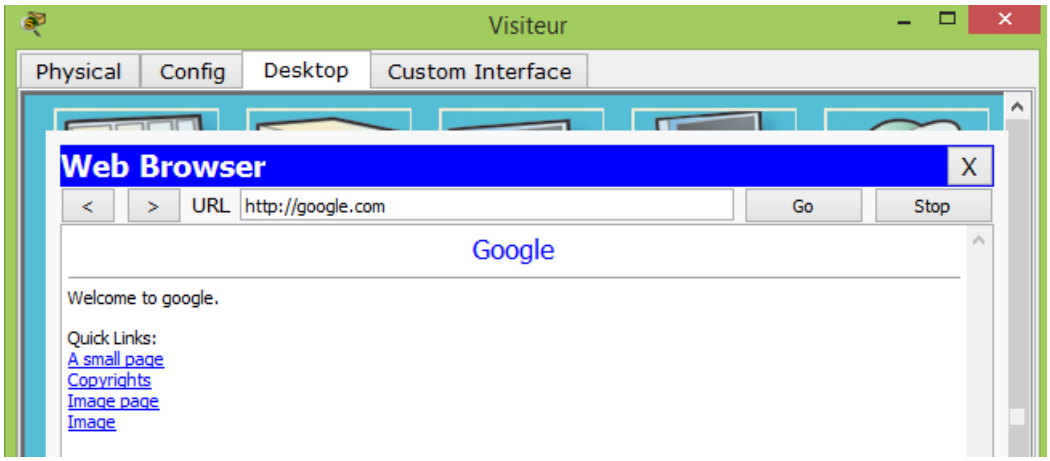

Figure 4. 12 :*Accès possible via le réseau DMZ.*

b. Test d'accès FTP

Le test d'accès au serveur FTP du réseau DMZ par le RA_PC est fait.

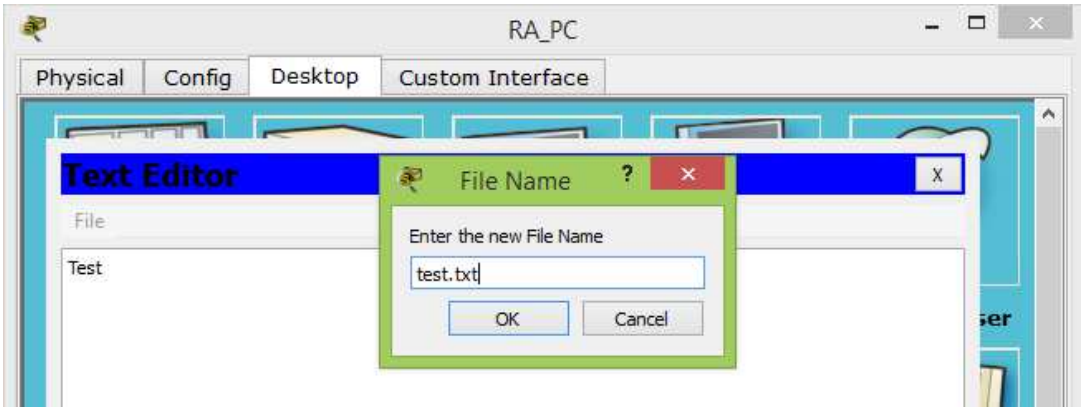

Figure 4. 13 : *Création d'un fichier test.txt dans RA_PC*

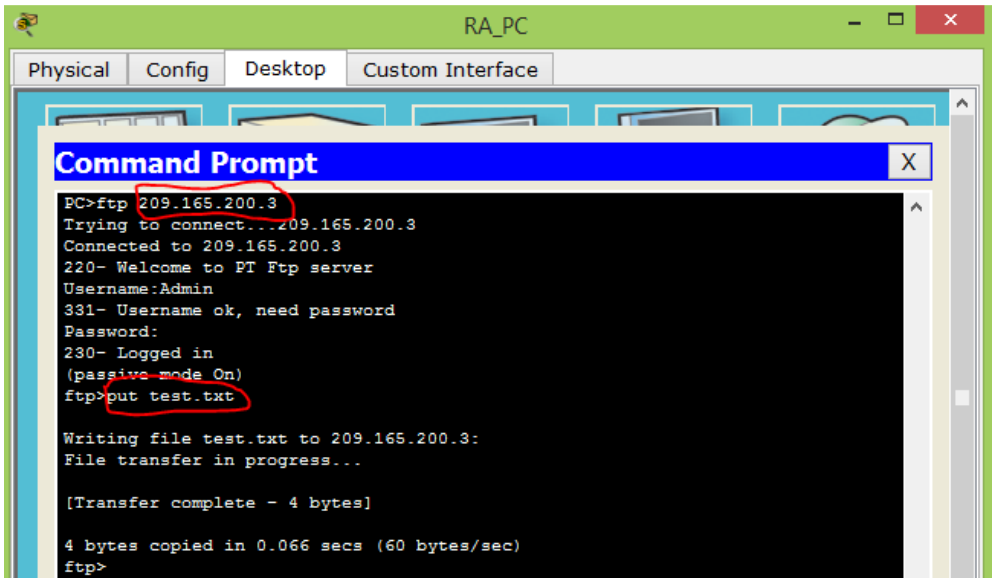

Figure 4. 14 : *Ajout du fichier test.txt réussi*

c. Test d'échange de mail

L'échange de mail fonctionne aussi. PC_A1 et RA_PC ont respectivement l'adresse mail pc_a1@test.com et ra_pc@test.com

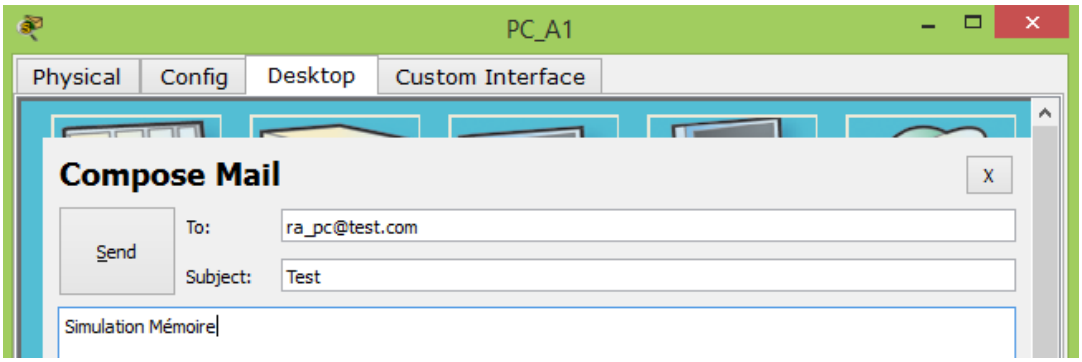

Figure 4. 15 : *Envoi d'un mail à RA_PC*

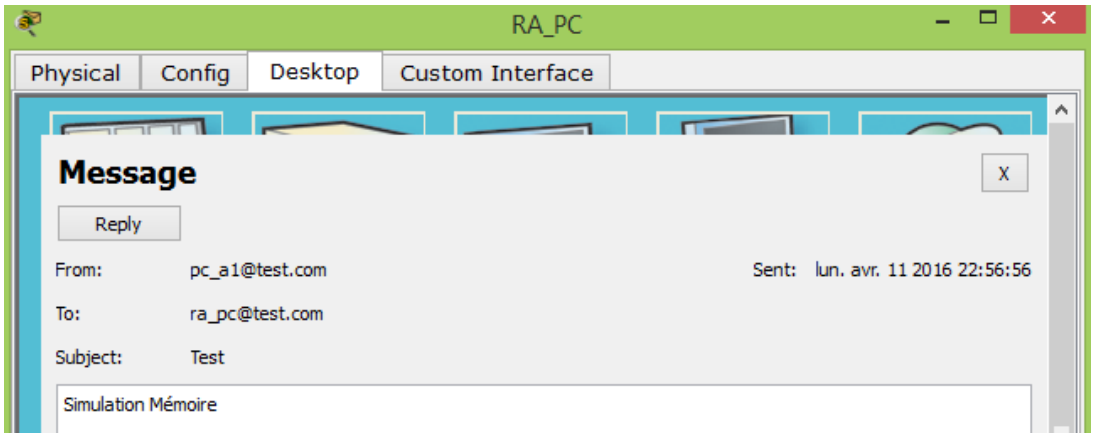

Figure 4. 16 : *Réception de RA_PC*

d. Test d'accès à distance du serveur web dans le réseau interne

L'accès au serveurweb dans le réseau interne par RA_PC est possible via le portail VPN de ASA 5505. C'est pour démontrer l'accès à distance des télétravailleurs.

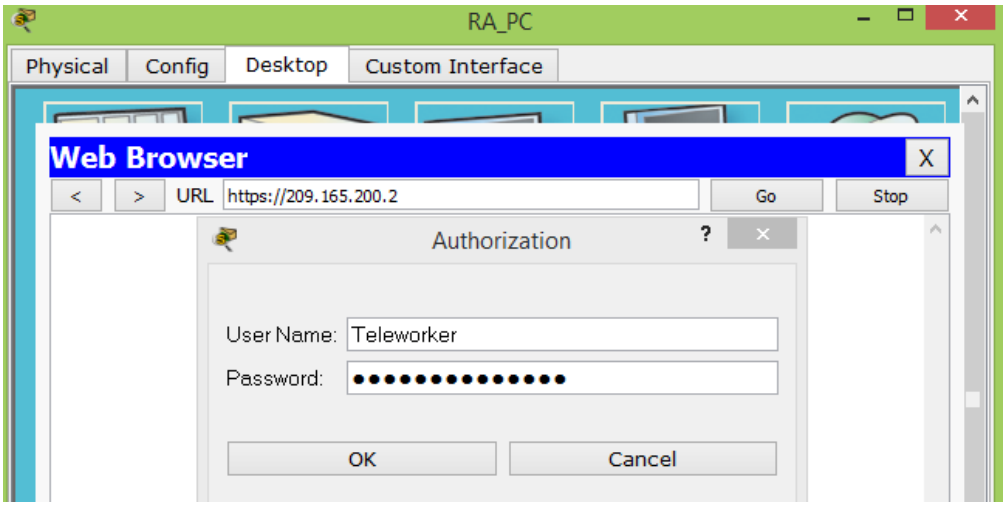

Figure 4. 17 : *Accès au portail VPN d'ASA 5505*

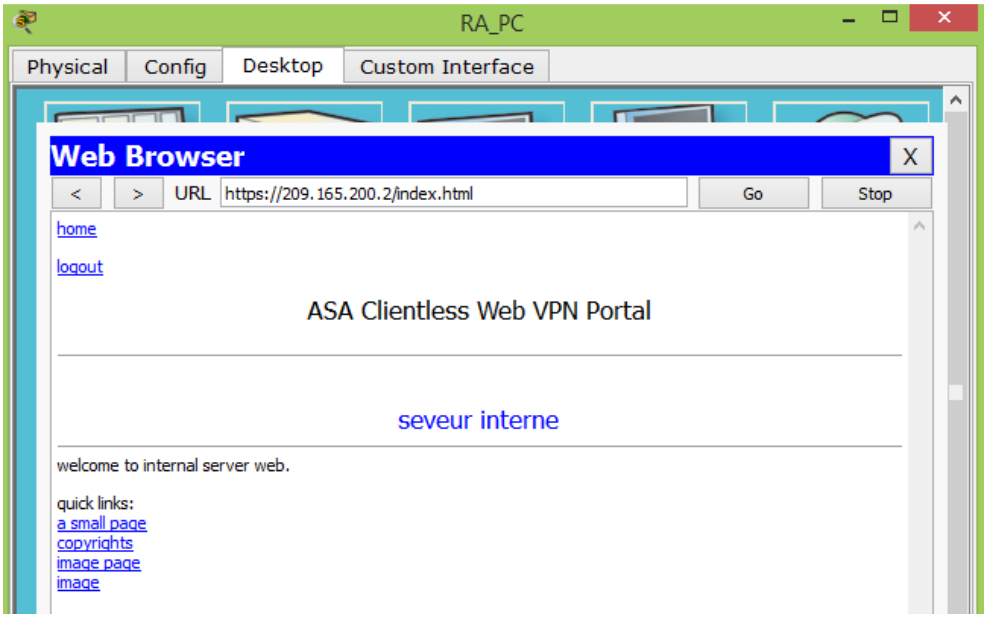

Figure 4. 18 : *Accès au serveur interne par RA_PC*

e. Test d'accès SSH à ASA 5505

L'accès à ASA 5505 par l'administrateur est possible.

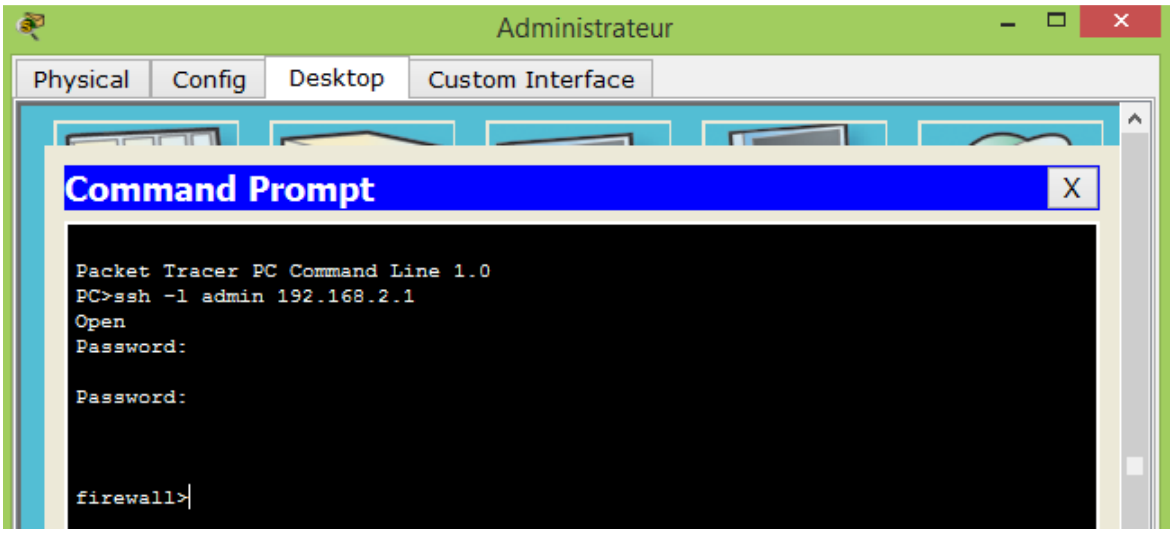

Figure 4. 19 : *Accès du PC administrateur à ASA 5505*

4.4 Conclusion partielle

Avant de concevoir un réseau, ou même une partie d'une infrastructure réseau, il est nécessaire de faire une analyse au préalable. Cette analyse est basée sur les besoins et les objectifs du futur propriétaire du réseau. Il est primordial de connaître les groupes d'utilisateurs du futur réseau et les applications qui vont être utilisées. La conception elle-même se basera sur ces données. Le réseau conçu dans ce chapitre essaye tant bien que mal à atteindre les six objectifs posés, à savoir la disponibilité, l'extensibilité, la facilité de gestion, la sécurité, l'accès à distance des télétravailleurs et le partage des données à travers l'implémentation de la zone DMZ. Les fonctionnalités incluses dans le réseau lui-même n'est pas complète, l'extensibilité et la facilité de gestion sont assurées par l'utilisation du modèle hiérarchique, la sécurité par les fonctionnalités du pare-feu et la division des parties de réseau en VLAN avec l'utilisation des NAT. Mais le réseau est moins disponible vu l'impossibilité d'implémenter la redondance du pare-feu sur le logiciel de simulation. C'est la limite de cette conception. Cependant, on a réussi à y implanter les applications web, FTP et SMTP en assurant la sécurité des données utilisées.

CONCLUSION GÉNÉRALE

Dans cet ouvrage, lethème s'est porté principalement sur la façon de concevoir un réseau informatique, spécialement pour les entreprises. L'objectif principal de l'étude a été de connaitre le moyen de créer un réseau type d'entreprise assurant l'extensibilité, la disponibilité, la facilité de gestion et la sécurité tout en partageant les données sur Internet. Il a été alors appris que le meilleur réseau pour une société est celui de modèle hiérarchique et que seule l'implémentation d'une zone DMZ permet de partager des données dans les réseaux publics. Dans le cadre du présent travail les théories de bases nécessaires des réseaux informatiques ont été d'abord étudiées. Les fonctionnalités et les technologies de réseau ont été analysées.Des modèles et des méthodes de conception de réseau ont été par la suitedéveloppés. Ce n'est qu'à la fin qu'une simulation d'un réseau a été effectuéesur le logiciel Packet Tracer.

Cisco Packet Tracer a été choisi du fait de sa simplicité et sa légèreté. En plus, tous les documentations et les cours publiés par Cisco system se base sur ce logiciel. Avec ce logiciel, l'implémentation du réseau modèle pour une entreprise est simple et le test de connectivité entre les équipements et l'étude des flux de donnée est facile. Le modèle de pare-feu ASA utilisé est à la portée de toutes les entreprises et les Sociétés que ce soit de grande taille ou de petite taille. Son utilisation a permis d'implémenter une zone DMZ assurant ainsi un niveau de sécurité élevée au réseau. La facilité de gestion et l'extensibilité du réseau, quant à eux, ont été assurées par la hiérarchisation de l'infrastructure du réseau. Cependant, la licence intégrée dans le pare-feu proposé par le logiciel a ses limites, rendant ainsi l'impossibilité de créer des redondances complètes dans la conception.

Ainsi, cette étude a permis demaitriser pratiquement la plupart des notions de réseau informatique, jusqu'ici étudiées en cours. Faisant suite à ce présent mémoire, il s'avère utile d'étudier l'implémentation d'un IDS (Intrusion Detection Service) et IPS (Intrusion Protection Service) dans l'infrastructure réseau. La sécurité déjà apportée par le pare-feu sera ainsi renforcé.

ANNEXES

ANNEXE 1

COMMANDE ET CONFIGURATION DANS LA SIMULATION

A1.1 Configuration Routeur de distribution Rt_Distrib_1

Il en est pareil pour Rt_Distrib_2, mais seule la priorité change de 110 à 90.

```
hostname Rt_Distrib_1
ip dhcp excluded-address 192.168.0.2 192.168.0.3
ip dhcp excluded-address 192.168.0.34 192.168.0.35
ip dhcp excluded-address 192.168.0.93 192.168.0.94
!
ip dhcp pool domaine_A
network 192.168.0.0 255.255.255.224
default-router 192.168.0.1
dns-server 192.168.0.67
ip dhcp pool domaine_B
network 192.168.0.32 255.255.255.224
default-router 192.168.0.33
dns-server 192.168.0.67
!
spanning-tree mode pvst
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
ip address 192.168.1.3 255.255.255.248
ip nat outside
duplex auto
speed auto
ipv6 ospf cost 1
standby version 2
standby 100 ip 192.168.1.2
standby 100 priority 110
standby 100 preempt
!
interface FastEthernet0/1/0
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/1/1
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/1/2
switchport access vlan 30
switchport mode access
!
interface FastEthernet0/1/3
switchport mode access
shutdown
!
interface Vlan1
no ip address
```

```
shutdown
!
interface Vlan10
ip address 192.168.0.2 255.255.255.224
ip nat inside
standby version 2
standby 100 ip 192.168.0.1
standby 100 priority 110
standby 100 preempt
!
interface Vlan20
ip address 192.168.0.34 255.255.255.224
ip nat inside
standby version 2
standby 100 ip 192.168.0.33
standby 100 priority 110
standby 100 preempt
!
interface Vlan30
ip address 192.168.0.93 255.255.255.224
ip nat inside
standby version 2
standby 100 ip 192.168.0.65
standby 100 priority 110
standby 1000 preempt
!
router rip
!
ip nat inside source list 4 interface FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
ip flow-export version 9
!
access-list 4 permit 192.168.0.0 0.0.0.255
```

A1.2 Configuration de l'ASA 5505

```
hostname firewall
domain-name ciscofirewall.com
enable password Y7SFjaK5ziHNKF1F encrypted
names
!
interface Ethernet0/0
switchport access vlan 2
!
interface Ethernet0/1
interface Ethernet0/2
switchport access vlan 3
interface Ethernet0/3
interface Ethernet0/4
interface Ethernet0/5
interface Ethernet0/6
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.248
!
```

```
interface Vlan2
nameif outside
security-level 0
ip address 209.165.200.2 255.255.255.240
!
interface Vlan3
no forward interface Vlan1
nameif dmz
security-level 50
ip address 192.168.2.1 255.255.255.0
!
webvpn
enable outside
object network dmz-subnet
subnet 192.168.2.0 255.255.255.0
object network inside-net
subnet 192.168.0.0 255.255.255.0
object network rt_distrib_1
subnet 192.168.1.3 255.255.255.255
object network rt_distrib_2
subnet 192.168.1.4 255.255.255.255
object network webserver
host 192.168.2.2
!
route outside 0.0.0.0 0.0.0.0 209.165.200.1 1
route inside 192.168.0.66 255.255.255.255 192.168.1.2 1
!
access-list 101 extended permit tcp any host 209.165.200.3
access-list 101 extended permit icmp any host 209.165.200.3
access-list 101 extended permit tcp any host 209.165.200.2
access-list 101 extended permit icmp any host 209.165.200.2
access-list 101 extended permit udp any host 209.165.200.2
!
access-group 101 in interface outside
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network inside-net
nat (inside,outside) dynamic interface
object network rt_distrib_1
nat (inside,outside) dynamic interface
object network rt_distrib_2
nat (inside,outside) dynamic interface
object network webserver
nat (dmz,outside) static 209.165.200.3
!
aaa authentication ssh console LOCAL
!
group-policy interne internal
group-policy interne attributes
vpn-tunnel-protocol ssl-clientless
webvpn
url-list value interne
username Teleworker password OKgAgVOOvUMuu8Fg encrypted
username Teleworker attributes
vpn-group-policy interne
username admin password JvOWEzhxYTAoEJya encrypted
!
class-map inspection_default
match default-inspection-traffic
!
```

```
policy-map global_policy
class inspection_default
inspect dns
inspect ftp
inspect http
inspect icmp
!
service-policy global_policy global
!
telnet timeout 5
ssh 192.168.2.0 255.255.255.0 dmz
ssh timeout 10
!
dhcpd enable inside
!
dhcpd auto_config outside
!
tunnel-group tunel type remote-access
tunnel-group tunel general-attributes
default-group-policy interne
!
```

ANNEXE 2

CONFIGURATIONS DE ROUTEUR ET FAILOVER SUR ASA 5505

A2.1 Configuration de routage statique d'un routeur

A2.1.1 Routage statique

Router# conf t

Router(config)# ip route adresseIPReseau Masque adrIPGateway

A2.1.2 Route par défaut

Router# conf t

Router(config)# ip route 0.0.0.0 0.0.0.0 (adresse du prochain routeur)

A2.1 Configuration d'un Failover sur ASA 5505

Configurer un failover entre deux ASA 5505 permet d'avoir une redondance au niveau du pare-feu.

Configuration du premier pare-feu en mode Active.

ASA1(config)# failover

ASA1(config)# failover lan unit primary

ASA1(config)# failover lan interface FAILOVER FastEthernet 0/7

INFO: Non-failover interface config is cleared on FastEthernet 0/7and its sub-interfaces

ASA1(config)# failover key fail0ver

ASA1(config)# failover replication http

ASA1(config)# failover link FAILOVER FastEthernet 0/7

ASA1(config)# failover interface ip FAILOVER 10.20.1.1 255.255.255.252 standby 10.20.1.1

ASA1(config)# exit

ASA1(config)# int fa0/3

ASA1 (config-if)# no shut

ASA1 (config-if)#exit

ASA1 (config)#exit

ASA1# copy run start

Configuration de la deuxième pare-feu en mode Standby.

ASA2(config)# failover

ASA2(config)# failover lan unit secondary

ASA2(config)# failover lan interface FAILOVER FastEthernet0/7

INFO: Non-failover interface config is cleared on FastEthernet0/7and its sub-interfaces

ASA2(config)# failover key fail0ver

ASA2(config)# failover replication http

ASA2(config)#exit

ASA2(config)# failover link FAILOVER FastEthernet0/7

ASA2(config)# failover interface ip FAILOVER 10.20.1.1 255.255.255.252 standby 10.20.1.2

ASA2(config)# int fa0/7

ASA2(config-if)# no shut

ASA2(config-if)#exit

ASA2# copy run start

BIBLIOGRAPHIE

[1] D.Gonzalez, «*SystèmesetRéseaux* »,http://www.grappa.univlille3.fr/polys/systreseaux/index.html,Mars 2016

[2] T. Randriamanalina, *« Contribution à l'étude au Dimensionnement d'un réseau d'entreprise »*, Antananarivo, 2006, Mémoire de fin d'études.

[3] O. Tharan, *« Architecture réseaux »,* 2004

[4] G. Pujolle, *« Les réseaux »*, Eyrolles, Paris, 2008

[5] C. Servine, *«Réseaux et télécoms »*,DUNOD, Paris, 2003

[6] C. Caleca, *« Les réseaux »*, 2007

[7] G.Pujolle, *« Initiation aux réseaux »*, Eyrolles, Paris, 2001

[8] Arquendra, *« Généralités, modèle OSI, protocole TCP/IP»*,http://info.arqendra.net/Files/_Rsx+OSI+TCPIP_cours.pdf, Février 2016

[9] S. Fontaine, *«En-tête Ethernet »*, http://www.frameip.com/entete-ethernet, Mars 2016

[10] O.Hoarau, *« Le protocole Ethernet »*,http://www.funix.org/fr/reseau/main-reseau.php?ref=lan/ethernet&page=menu, Mars 2016

[11] A. Ratsimbazafy, *« Téléinformatiques et Télématiques »*,Cours L3 – TCO, Dép. TCO.- E.S.P.A., A.U. : 2014-2015

[12] L. E. Randriarijaona, *« TCP/IP »*, Cours L2 – TCO, Dép. TCO.- E.S.P.A., A.U. : 2013-2014.

[13] COMPUTERNETWORKINGNOTES,«*NetworkTechnologies*»,http://computernetworkingnotes.com/comptia-n-plus-study-guide/network-technologies,Fevrier, 2016

[14] I. Rudenko, *« Configuration IP des routeurs Cisco »*,Eyrolles, Paris, 2001

[15] J. F. Rasolomanana, *« Routage »*,Cours L3 – TCO, Dép. TCO. - E.S.P.A., A.U.: 2014-2015

[16] Cisco System, *« Cisco ASA 5500 Series Configuration Guide using the CLI »*, San Jose, 2012

[17] C. Wolfhugel, « *Déploiement de VLAN 802.1Q/ISL dans un environnement hétérogène*», France, 2007

[18] R. Sanchez, *« Les réseaux locaux virtuels »*, 2006

[19] F. Di Gallo, *« WIFI L'essentiel qu'il faut savoir »*,2003

[20] A. Géron, *« WIFI Professionnel, La norme 802.11, Le déploiement, La sécurité »*, Dunod,2009

[21] J. Anzevui, *« Les réseaux sans fils »*, Université de Genève, 2007

[22] C. Diou, *« WLAN : les réseaux sans fils et Wi-Fi »*, Université de Metz, 2006

[23] OPENCLASSROMS, *« Les VPN, pour chiffrer vos communications »*, 18 Février 2016

[24] D. Reynal, J. Rorthais, S.S.Tan, *« Présentation sur les VPN »*, Université de Marne La Vallée, 2004

[25] B.Pascault, G.Rivoiras, *« VPN SSL sur ASA »*,2010

[26] L.Archimède, T.Chevalier, J.Herbin, S.Ledru, N.Pellegrin, *« Sécurité de l'information Tunnels et VPN »*, DESS ISYDIS, 2004

[27] I.Rachid, *« Virtual Private Network Études comparative et réalisation d'un VPN MPLS»*, École Marocaine des Sciences de l'Ingénieur, 2010

[28] C. Liorens, L. Levier, D. Valois, *« Tableaux de bord de la Sécurité réseaux »*, Eyrolles,2006

[29] Cisco System, *« Firewall and IPS Technology Design Guide »*, August 2014

[30] R.J. Shimonski, W.Schmied, T.W. Shinder, V. Chang, D. Simonis, D.Imperatore, *«Building DMZs for Entreprise Networks »*, Syngress, 2003

[31] Cisco System, *« CCNA Discovery 4.0 Conception et prise en charge des réseaux informatiques »*,2007

[32] V.Weber, *«Cisco Entreprise Composite Network Model »*,https://www.networklab.fr/cisco-entreprise-composit-network-model, Février, 2016

[33] P. Oppenheimer, *« Top-Down Network Design »*, Cisco Press, 2011

[34] Cisco System, *« Networking in the Entreprise »*, 2010

[35] Cisco System, *«CiscoPacket Tracer »*, 2010

PAGE DE RENSEIGNEMENTS

Nom : RAZAFIMAHALEO

Prénoms: Kiady Herilala

Adresse: Lot VT 1 ter UB Andohaniato Ambohipo

Antananarivo 101 Madagascar.

Tel: (+261) 33 46 166 19

E-mail: kiadyherilala.razafy@gmail.com

Titre du mémoire : « ***CONCEPTION D'UN RESEAU DE CAMPUS D'ENTREPRISE AVEC IMPLEMENTATIOND'UNE ZONE DMZ*** »

Nombre de pages : 84

Nombre de tableaux : 6

Nombre de figures : 58

Directeur de mémoire : Monsieur RANDRIARIJAONA Lucien Elino

Grade : Assistant d'Enseignement et de recherche

Adresse : E-mail :elrandri@gmail.com

Tel : (+261) 32 04 747 95

RÉSUMÉ

L'évolution rapide de la télécommunication a impacté durement le monde de l'entreprise. Informatiser et partager les informations à une vitesse phénoménale sont actuellement possibles. Avoir une infrastructure de réseau informatique pouvant automatiser les traitements des données en les partageant devient maintenant une nécessité incontournable chez les organisations et les sociétés. Ainsi, cet ouvrage se portera sur la façon de concevoir un réseau d'entreprise et le moyen de partager des informations dans le monde entier en étudiant la façon d'implémenter une zone DMZ (Demilitarized Zone) dans ce dernier. On a commencé à étudier les notions de base nécessaire pour a bonne compréhension des réseaux informatiques, puis, les fonctionnalités existantes ces réseaux. Ensuite, on a étudié les concepts de bases pour savoir le modèle et la méthode de conception de réseau les plus efficaces. Et en dernier lieu, le logiciel Cisco Packet Tracer a permis de simuler un modèle de réseau typique pour une entreprise avec l'implémentation d'une zone DMZ

Mots clés:DMZ, pare-feu, VLAN, PPCIEO, entreprise

ABSTRACT

The rapid evolution of telecommunications has severely impacted the business world. Computerize and share information at a phenomenal rate is currently available. Having a computer network infrastructure that can automate the processing of data is now an unavoidable necessityin organizations and companies. Thus, this book will focus on how to design a corporate network and the average sharing information around the world by studying how DMZ (Demilitarized Zone) is implemented. We started studying the basics of computer networks. Then, the existing features in networks. Afterwe studied the basic concepts to know the model and the most efficient-network design method. And finally, the Cisco Packet Tracer software allowed us to simulate a typical network model to a company with the implementation of a DMZ

Keys word:DMZ, Firewall, VLAN, PPDIOO, enterprise