

الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

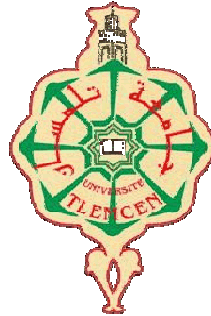
وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد – تلمسان

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE



MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

En : Télécommunications

Spécialité : Réseaux et Télécommunications

Par :

ABDALLAH BERREHAIL Nardjess

BENDEDDOUCHE Nassima

Sujet

Développement d'une application de segmentation VLSM (CIDR) des réseaux d'adressage IPv4

Soutenu publiquement, le 23/ 09 /2020, devant le jury composé de :

Mr. MERZOUGUI. R	Professeur	Univ. Tlemcen	Président
Mr. ZERROUKI. H	Maitre de Conférences	Univ. Tlemcen	Directeur de mémoire
Mr. MOUSSAOUI. D	Maitre de Conférences	Univ. Tlemcen	Examineur

Dédicace

Tous les mots ne sauraient exprimer la gratitude, l'amour, le respect, la reconnaissance, c'est tous simplement que : Je dédie ce mémoire à :

A Ma tendre Mère Dalila

Tu représente pour moi la source de tendresse et l'exemple de dévouement qui n'a pas cessé de m'encourager. Tu as fait plus qu'une mère puisse faire pour que ses enfants suivent le bon chemin dans leur vie et leurs études.

A Mon très cher Père Ghouti

Aucune dédicace ne saurait exprimer l'amour, l'estime, le dévouement et le respect que j'ai toujours pour vous. Rien au monde ne vaut les efforts fournis jour et nuit pour mon éducation et mon bien être. Ce travail est le fruit de tes sacrifices que tu as consentis pour mon éducation et ma formation le long de ces années.

A mon très cher mari Mohamed

Aucun mot ne saurait t'exprimer mon profond attachement et ma reconnaissance pour l'amour, la tendresse et la gentillesse dont tu m'as toujours entouré. Cher mari j'aimerai bien que tu trouve dans ce travail l'expression de mes sentiments de reconnaissance les plus sincères car grâce à ton aide et à ta patience avec moi que ce travail a pu voir le jour.

A ma chère sœur Manel.

A mon petit cher frère Nassreddine.

A mes chers beaux parents.

A mes chère belle sœurs, mes chers beaux frères.

A mes très chère amies : Nardjess, Rania, Miriam, Fitna, Fadia, Houda, Nezha et asma

A monsieur Zerrouki Hadj: Cette humble dédicace ne saurait exprimer mon grand respect et ma profond estime, que dieu vous procure bonne santé et long vie.

A tous les membres de ma promotion.

A tous mes enseignants depuis mes premières années d'études.

A tous ceux qui me sens chers et que j'ai omis de citer.

M.BENDEDDOUCHE Nassima

Je dédie ce mémoire

A ma très chère mère et mon cher Père

Grâce à leurs tendres encouragements et leurs grands sacrifices, ils ont pu créer le climat affectueux et propice à la poursuite de mes études. Aucune dédicace ne pourrait exprimer mon respect, ma considération et mes profonds sentiments envers eux. Je prie le bon Dieu de les bénir, de veiller sur eux, en espérant qu'ils seront toujours fiers de moi.

A mes chères sœurs

*Merci mes adorables pour votre présence, votre amour et votre tendresse, pour donner du goût et du sens à ma vie.
Veuillez trouver dans ce modeste travail l'expression de mon affection*

A mon cher mari

Merci d'être toujours à mes côtés, par ta présence, par ton amour, merci pour l'encouragement que tu m'as donné, merci pour tout ce que tu as fait pour moi.

A tous mes professeurs

Leur générosité et leur soutien m'oblige de leurs témoigner mon profond respect et ma loyale considération.

*A tous les membres de ma famille, petits et grands
A tous mes amis et mes collègues*

ABDALLAH BERREHAIL Nardjess

Remerciements

Nous tenons particulièrement à remercier Allah le tout puissant, qui nous a donné la force et le courage de mener à bien ce modeste travail, qui n'aurait jamais été réalisé sans sa bénédiction

La première personne que nous tenons à remercier est notre encadrant Mr. ZERROUKI Hadj, maître de conférences à l'université Abou-Bekr Belkaid - Tlemcen, pour l'orientation, la confiance, la patience qui ont constitué un apport considérable, sans lequel ce travail n'aurait pas pu être mené au bon port. Qu'il trouve dans ce travail un hommage vivant à sa haute personnalité, Nous saisissons cette occasion pour vous exprimer notre profonde gratitude, tout en vous témoignant notre respect.

Nous tenons à exprimer nos sincères remerciements à Mr. MERZOUGUI Rachid, Professeur à l'université Abou-Bekr Belkaid - Tlemcen, en étant président du jury, et Mr. MOUSSAOUI Djillali Maître de conférences à l'université Abou-Bekr Belkaid - Tlemcen, pour leur présence, pour leur lecture attentive de notre mémoire, ainsi que pour les remarques qu'ils m'adresseront lors de cette soutenance afin d'améliorer notre travail.,

Nous tenons à exprimer ainsi nos sincères remerciements à tous les professeurs qui nous ont enseigné et qui par leurs compétences nous ont soutenu dans la poursuite de nos études.

Résumé :

L'adressage sans classes (ou adressage CIDR) est le système de gestion et d'allocation d'adresses IP le plus utilisé aujourd'hui. Ce système a été conçu pour remplacer l'adressage par classes pour les raisons de pourcentage assez élevé de perte et la pénurie d'adresses IPv4. Le but de ce nouveau système s'articule autour de deux points essentiels ; économiser les adresses IP et faciliter le routage.

Le masque de sous-réseaux à longueur variable (VLSM) est une technique utilisée dans le but de mieux gérer les adresses IP, tout comme le CIDR. Le VLSM permet l'utilisation de masques différents pour chaque sous-réseau. Une fois qu'une adresse réseau est divisée en sous-réseaux, toute autre division de ces sous-réseaux entraîne la création de « sous-sous-réseaux ».

L'objectif de ce projet de fin d'études est le développement d'une application d'aide à la segmentation des réseaux IPv4 par l'utilisation des deux techniques VLSM et CIDR. Cette application est un outil pratique pour trouver le nombre de sous-réseaux possibles pour tout bloc d'adresse réseau donné. Vous pouvez choisir la combinaison de sous-réseaux et le nombre d'hôtes par sous-réseau qui convient à votre réseau et obtenir la plage d'adresses des hôtes et l'adresse de diffusion pour tout masque de sous-réseau donné.

Mots clés : *Réseaux informatiques, découpage, VLSM, CIDR, adressage IPv4, sous-réseaux, routage, segmentation.*

Abstract :

Classless Inter-Domain Routing (CIDR) is the most widely used IP address allocation and management system today. This system was designed to replace class addressing due to the relatively high percentage loss and the shortage of IPv4 addresses. The aim of this new system revolves around two essential points; economize IP addresses and routing facilitate.

Variable Length Subnet Mask (VLSM) is a technique used to better manage IP addresses, as the CIDR. VLSM allows the use of different masks for each subnet. Once a network address is divided into subnets, any further division of those subnets results in the creation of "sub-subnets".

The objective of this graduation project is the development of an application to help in the segmentation of IPv4 networks using the two techniques VLSM and CIDR. This application is a practical tool for finding the number of possible subnets for any given network address block. You can choose the combination of subnets and number of hosts per subnet that suits your network, and get the host address range and broadcast address for any given subnet mask.

Keywords: *Computer networks, subnetting, VLSM, CIDR, IPv4 addressing, subnets, routing, segmentation.*

Table des matières

Dédicaces	i
Remerciments	iii
Résumé et Abstract	iv
Table des matières	v
Liste des figures	viii
Liste des tableaux	x
Liste des abriviations	xi
Introduction générale	1

CHAPITRE I : Généralité sur les réseaux informatiques

I.1	Introduction	3
I.2	Définition d'un réseau informatique	3
I.2.1	Que signifie un réseau ?	3
I.2.2	Pourquoi les réseaux ?	4
I.2.3	Les réseaux informatiques	4
I.3	Les types des réseaux informatiques	5
I.3.1	Réseau personnel (PAN)	6
I.3.2	Réseau Local (LAN)	6
I.3.3	Réseau Métropolitain (MAN)	7
I.3.4	Réseau Etendu (WAN)	8
I.4	La structure physique d'un réseau informatique	8
I.4.1	Topologie des mailles	8
I.4.2	Topologie en étoile	9
I.4.3	Topologie en bus	10
I.4.4	Topologie en anneau	10
I.4.5	Topologie de l'arbre	11
I.5	La structure logique d'un réseau informatique	11
I.5.1	Le modèle OSI	11
I.5.1.1	Les couches de modèle OSI	13
I.5.1.2	Transmission de données au travers du modèle OSI	15
I.5.2	Le modèle TCP/IP	16
I.5.2.1	Les couches du modèle TCP/IP	17
I.5.3	Comparaison du modèle TCP/IP avec le modèle OSI	19
I.6	Conclusion	19

CHAPITRE II : Le protocole IP et l'adressage IPv4

II.1	Introduction	20
II.2	Historique et définition	20
II.2.1	Définition	20
II.3	Le protocole IP	21
II.3.1	Le protocole IPv4	22
II.3.1.1	Caractéristiques de base de protocole IPv4	22
II.3.1.2	Le niveau paquet	22
II.3.1.3	Paquet IPv4	23
II.4	L'adressage IP	25
II.4.1	L'adressage IPv4	25
II.4.1.1	Classe d'adressage IP	26
II.4.1.2	Espace d'adressage IP	29
II.4.1.3	Les adresses particulières	30
II.4.1.4	L'utilisation d'un masque	30
II.4.1.5	Méthode par calcul binaire	31
II.5	Le routage IP	32
II.5.1	Principes de routage IP.....	32
II.5.2	Routage statique	32
II.5.3	Routage dynamique.....	33
II.5.4	La différence entre le routage statique et dynamique	35
II.6	Conclusion	35

CHAPITRE III : Découpage en des sous-réseaux, CIDR et VLSM

III.1	Introduction	37
III.2	Découpage en sous-réseaux avec classe	37
III.2.1	Construction de sous-réseaux	37
III.2.2	Méthode de calcul	38
III.3	Découpage en sous-réseaux de base.....	40
III.3.1	Détermination du masque de sous-réseau	40
III.3.2	Découpage selon le nombre d'hôtes	41
III.3.3	Selon le nombre de sous-réseaux	43
III.4	Découpage en des sous-réseaux sans classe	44
III.4.1	Le CIDR	44
III.4.1.1	La notion CIDR	44

III.4.1.2	Principe de CIDR.....	46
III.4.2	Le VLSM	47
III.4.2.1	Les différentes méthodes de VLSM	48
III.4.2.1.1	Méthode de boîte	48
III.4.2.1.2	La méthode numérique	50
III.4.2.1.3	La méthode graphique	51
III.4.2.2	Découpage VLSM d'un réseau	53
III.5	Conclusion	54

CHAPITRE IV : Conception et réalisation de l'application de segmentation VLSM

IV.1	Introduction	55
IV.2	Outils de conception	55
IV.2.1	Choix de langages de conception	55
IV.2.1.1	Langage HTML	56
IV.2.1.2	Langage CSS	58
IV.2.1.3	Langage JavaScript	59
IV.2.2	Tableau récapitulatif	60
IV.3	Le site Web et l'application Web	60
IV.3.1	Le site Web.....	60
IV.3.1.1	Quelle est l'utilité d'un site Web ?	60
IV.3.2	L'application Web	61
IV.3.2.1	Les types d'applications Web	62
IV.4	La structure de l'application VSC	64
IV.4.1	Présentation de l'application	64
IV.4.2	Présentation des interfaces graphiques	64
IV.4.2.1	Interface Subnetting (Host)	65
IV.4.2.2	Interface Subnetting (Subnet)	67
IV.4.2.3	Interface Subnetting (VLSM)	68
IV.4.2.4	Interface About	70
IV.5	Conclusion	71
	Conclusion générale.....	72
	Bibliographie	73

Liste des figures

Figure I.1 : Exemple d'un réseau informatique	5
Figure I.2 : La couverture de différent types de réseau.....	6
Figure I.3 : Exemple d'un réseau personnel (PAN).....	6
Figure I.4 : Exemple d'un réseau local (LAN)	7
Figure I.5 : Exemple d'un réseau métropolitain (MAN)	7
Figure I.6 : Exemple d'un Réseau étendu (WAN)	8
Figure I.7 : Topologie des mailles.....	9
Figure I.8 : Topologie en étoile	10
Figure I.9 : Topologie en bus.....	10
Figure I.10 : Topologie en anneau.....	11
Figure I.11 : Illustration du modèle OSI	12
Figure I.12 : La démarche de la transmission des données.....	16
Figure I.13 : Le modèle TCP/IP	17

Figure II.1 : L'entête de paquet IPv4.....	23
Figure II.2 : Identifiants de réseau et machine dans une adresse IPv4	25
Figure II.3 : Adresse IPv4 de classe A.....	27
Figure II.4 : Adresse IPv4 de classe B.....	27
Figure II.5 : Adresse IPv4 de classe C.....	28
Figure II.6 : Adresse IPv4 de classe D.....	29
Figure II.7 : Adresse IPv4 de classe E.....	29
Figure II.8 : Fonctionnement de routage statique.....	33
Figure II.9 : Internet : interconnexion de systèmes autonomes	34

Figure III.1 : Position des identifiants de sous-réseau et d'hôte dans une adresse IPv4.	38
Figure III.2 : Calcul du masque de sous-réseau.....	39
Figure III.3 : Découpage en sous-réseaux par la méthode de boîte	49
Figure III.4 : Exemple de découpage par le la méthode de boit.	50
Figure III.5 : Résultat de calcul de découpage par le la méthode de boit.	50
Figure III.6 : Graphique VLSM des adresses de classe C 24-30 bits (4ème octet).	52
Figure III.7 : Exemple de découpage VLSM d'un réseau.	53

Figure IV.1 : Interface de l'outil Notepad++.....	56
Figure IV.2 : Structure de base d'un document HTML.	58
Figure IV.3 : Site web statique.....	61
Figure IV.4 : Site web dynamique.	61
Figure IV.5 : Logo de l'application Web (VSC).....	64
Figure IV.6 : Interface Subnetting (Host).....	65
Figure IV.7 : Résultat de calcul des sous-réseaux en Subnetting (Host).....	66
Figure IV.8 : Quelques fenêtres "Alert !" du programme défensif.	66
Figure IV.9 : Interface Subnetting (Subnet).....	67
Figure IV.10 : Résultats de calcul des sous-réseaux en Subnetting (Subnet)	68
Figure IV.11 : L'interfec Subnetting (VLSM).....	69
Figure IV.12 : Résultats de calcul des sous-réseaux en Subnetting (VLSM).....	69
Figure IV.13 : L'interface de la page "About"..	70

Liste des tableaux

Tableau II.1 : Les différents espaces d'adressage pour chaque classe	29
Tableau III.1 : Résultat de calcul des sous-réseaux.....	42
Tableau III.2 : Options de découpage en sous-réseaux possibles	43
Tableau III.3 : Le nombre d'adresses hôtes disponibles pour chaque type de notation CIDR..	46
Tableau III.4 : Découpage du réseau 198.51.100.0/25 avec VLSM	53
Tableau IV.1 : Différences entre les langages HTML, CSS et JS.....	60

Liste des abréviations

A

ARPANET : Advanced Research Projects Agency NETwork.

B

BGP : Border Gateway Protocol.

BSD : Berkeley Software Distribution.

C

CIDR : Classless Inter Domain Routing.

CMS : Content Management System.

CSS : Cascading Style Sheets.

D

DHCP : Dynamic Host Configuration Protocol.

E

EGP : Exterior Gateway Protocol.

EIGRP : Enhanced Interior Gateway Routing Protocol.

F

FDDI : Fiber Distributed Data Interface.

FTP : File Transfer Protocol.

H

HTML : Hyper Text Markup Language.

HTTP : Hyper Text Transfer Protocol.

I

IBM : International Business Machines.

IEEE : Institute of Electrical and Electronics Engineers.

IETF : Internet Engineering Task Force.

IGP : Interior Gateway Protocol.

IPv4 : Internet Protocol version 4.

IPv6 : Internet Protocol version 6.

J

JS : JavaScript.

L

LAN : Local Area Network.

M

MAN : Metropolitan Area Network.
MTU : Maximum transmission unit.
MySQL : My Structured Query Language.

N

NetBEUI : Net Bios Extended User Interface.
NTIC : Nouvelles Technologie d'Information et de Communication.

O

OSI : Open Systems Interconnection.
OSPF : Open Shortest Path First.

P

PAN : Personal Area Network.
PHP : Hypertext Preprocessor.

R

RIP : Routing Information Protocol.

S

SMTP : Simple Mail Transfer Protocol.

T

TCP/IP : Transmission Control Protocol / Internet Protocol.
Telnet : Terminal network ou Telecommunication network.
TFTP : Trivial File Transfer Protocol.

U

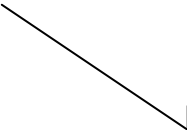
UDP : User Datagram Protocol.
URL : Uniform Resource Locator.

V

VLSM : Variable Length Subnet Mask.
VSC : VLSM Subnet Calculator.

W

WAN : Wide Area Network.
WWW : World Wide Web.



Introduction générale

Introduction générale

Si vous côtoyez des développeurs web ou courtisez les firmes de développement ou de marketing web, vous avez sûrement déjà entendu ces deux termes. Vous n'y avez peut-être jamais porté attention, ou au contraire, c'est une question qui vous tenaille jour et nuit. Quand doit-on parler de site web et quand doit-on parler d'application web ?

Un site web est ce que l'on retrouve lorsqu'on entre une adresse et qu'on atterrit sur une page. Le site correspond à cette page et toute page reliée qui est gérée par la même entité (souvent sous le même nom de domaine). Le rôle principal d'un site web est de fournir et présenter de l'information aux visiteurs. Un blogue, un site de nouvelles ou un site d'information sur un produit ou une compagnie sont de bons exemples de sites web.

Une application web est tout site web qui permet à ses utilisateurs d'accomplir des tâches spécifiques. Une application gère donc généralement des utilisateurs et toutes sortes de données selon les requis spécifiques au projet.

Depuis 1981, Internet fonctionne sur la base du protocole Internet (IP) : un protocole réseau qui régule les circuits de distribution des utilisateurs. Pour envoyer un paquet de données dans un réseau, l'expéditeur doit connaître l'adresse IP du destinataire. Dans un réseau comportant un grand nombre de machines, il devient nécessaire de subdiviser l'ensemble pour optimiser les échanges entre les machines. Avec les numéros de réseau IP devenant rapidement une espèce en voie de disparition, l'utilisation efficace de ces ressources de plus en plus rares est importante

Une définition simple du *subnetting* est le fait de diviser un réseau en plusieurs sous-réseaux. Le *subnetting* permet aux administrateurs réseau, par exemple, de diviser leur propre réseau d'entreprise en sous-réseaux sans le faire connaître sur Internet. En d'autres termes, le routeur qui relie finalement le réseau à Internet est toujours spécifié comme une adresse simple. Cependant, de nombreux hôtes peuvent se cacher derrière. Les possibles hôtes qui sont à la disposition de l'administrateur sont très étendus.

Les administrateurs réseau sont régulièrement confrontés à un autre problème : l'adresse réseau et le nombre d'hôte qui doivent être logés dans le sous-réseau donné. L'administrateur doit calculer un masque de sous-réseau qui autorise suffisamment d'hôtes, et pour ce faire il est besoin d'une application qui facilite cette tâche.

L'application Web VSC est un outil de segmentation en sous réseaux avec un masque de longueur fixe et variable. VSC est une application moderne qui fait la gestion de l'espace d'adressage IP. L'utilisation de notre application aidera convenablement les administrateurs à gagner le temps et éviter les erreurs coûteuses, même à résoudre le problème de l'espace d'adressage par la segmentation de même réseau ou par le découpage de même adresse. L'application web VSC représente plusieurs interfaces chacune effectue des calculs pour un bloc d'adressage données

Dans ce cadre, se réalise notre projet de fin d'étude. Au cours de notre rapport, nous avons quatre chapitres à mettre en œuvre :

Le premier chapitre donnera un aperçu général sur les réseaux informatiques, ses types, sa structure physique et logique,.

Le deuxième chapitre est une étude profonde sur le protocole IP et l'adressage IPv4, ses caractéristiques de base, le paquet IPv4, les classes d'adressage, le routage IP et ses principes.

Le troisième chapitre sera consacré pour détailler le découpage en des sous réseaux, CIDR et VLSM, dans lequel nous expliquons en détails la méthode de calcul selon le nombre d'hôtes et le nombre de sous réseaux, et nous allons étudier la notion CIDR et son principe, aussi la technique VLSM et ses différentes méthodes.

Dans le quatrième et dernier chapitre, nous présentons la conception de l'application de segmentation VLSM, sa structure et les différentes interfaces graphiques constituant notre application VSC. Nous élaborons la conception et la réalisation par l'exposition des différentes interfaces de l'application accompagnée d'une description précise.

A la fin, nous terminerons avec une conclusion qui récapitule notre travail et qui présente les connaissances acquises suite à ce projet de fin d'étude.

CHAPITRE I :

*Généralité sur les réseaux
informatiques*

I.1 Introduction :

La connexion entre les différents éléments constitutifs d'un réseau, peut s'effectuer à l'aide de liens permanents comme des câbles, mais aussi au travers des réseaux de télécommunications publics. Les dimensions de ces réseaux sont très variées, depuis les réseaux locaux, reliant quelques éléments dans un même bâtiment, jusqu'aux ensembles d'ordinateurs installés sur une zone géographique importante.

Les réseaux informatiques permettent aux utilisateurs de communiquer entre eux et de transférer des informations. Ces transmissions de données peuvent concerner l'échange de messages entre utilisateurs, l'accès à distance à des bases de données ou encore le partage de fichiers [1].

Le transport des données informatiques sur les réseaux, transparent pour les utilisateurs, est le fruit de technologies complexes. Elles offrent des services nombreux et variés. Les nouvelles technologies de l'information et de la communication (NTIC) permettent une souplesse de raccordement aux réseaux, à laquelle l'internet n'est pas étranger [2].

Nous avons divisé ce premier chapitre en deux grandes parties. Dans la première, nous allons aborder les concepts des réseaux informatiques, en l'occurrence la classification, les topologies et les caractéristiques des réseaux informatiques, puis dans la deuxième partie nous passerons à la description du modèle OSI et la pile de protocole TCP/IP.

I.2 Définition d'un réseau informatique :

I.2.1 Que signifie un réseau ?

Un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre ces objets selon des règles bien définies [3]. Un réseau en général est le résultat de la connexion de plusieurs machines entre elles, afin que les utilisateurs et les applications qui fonctionnent sur ces dernières puissent échanger des informations. Le terme réseau en fonction de son contexte peut désigner plusieurs choses.

Il peut désigner l'ensemble des machines, ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés, ce qui 'est le cas lorsque l'on parle de Internet. Le terme réseau peut également être utilisé pour décrire la façon dont les machines d'un site sont interconnectées. C'est le cas lorsque l'on dit que les machines d'un site (sur un réseau local) sont sur un réseau Ethernet, Token Ring, réseau en étoile, réseau en bus,... Le terme réseau peut également être utilisé pour spécifier le protocole qui est utilisé pour que les machines communiquent. On peut parler de réseau TCP/IP, NetBeui (protocole Microsoft) DecNet (protocole DEC), IPX/SPX,... [4]. Lorsque l'on parle de réseau, il faut bien comprendre le sens du mot.

I.2.2 Pourquoi les réseaux ?

Les réseaux sont nés d'un besoin d'échanger des informations de manière simple et rapide entre des machines. Lorsque l'on travaillait sur une même machine, toutes les informations nécessaires au travail étaient centralisées sur la même machine. Presque tous les utilisateurs et les programmes avaient accès à ces informations. Pour des raisons de coûts ou de performances, on est venu à multiplier le nombre de machines. Les informations devaient alors être dupliquées sur les différentes machines du même site. Cette duplication était plus ou moins facile et ne permettait pas toujours d'avoir des informations cohérentes sur les machines. On est donc arrivé à relier d'abord ces machines entre elles; ce fût l'apparition des réseaux locaux. Ces réseaux étaient souvent des réseaux "maisons" ou propriétaires. Plus tard on a éprouvé le besoin d'échanger des informations entre des sites distants. Les réseaux moyenne et longue distance commencèrent à voir le jour. Ces réseaux étaient souvent propriétaires [4].

Aujourd'hui, les réseaux se retrouvent à l'échelle planétaire. Le besoin d'échange de l'information est en pleine évolution. Pour se rendre compte de ce problème il suffit de regarder comment fonctionnent des grandes sociétés. Comment pourrait-on réserver une place de train dans n'importe quelle gare ? Sans échange informatique, ceci serait très difficile.

I.2.3 Les réseaux informatiques :

La technologie des réseaux informatiques constitue l'ensemble des outils qui permettent à des ordinateurs de partager des informations et des ressources [2]. Un réseau informatique, est un ensemble d'équipements matériels et logiciels interconnectés les uns avec les autres dans le but de partager des données. Ces équipements peuvent être éloignés ou rapprochés [3]. En outre, est un ensemble mis en œuvre pour assurer les communications entre ordinateurs, stations de travail et terminaux informatiques.

Il s'agit d'une structure présentant un schéma caractéristique. L'infrastructure d'un réseau informatique est connue comme étant un réseau de données dont la conception permet la transmission d'informations par l'échange de données. Chacun de ces réseaux a été spécifiquement conçu pour répondre à des objectifs, avec une architecture spécifique pour faciliter le transfert de contenu.

Cependant, un réseau informatique est également mis en service avec deux autres objectifs principaux : partager à la fois le logiciel et le matériel et fournir un soutien et une centralisation à l'administration concernée [5]. La figure suivante schématise un exemple d'un réseau informatique.

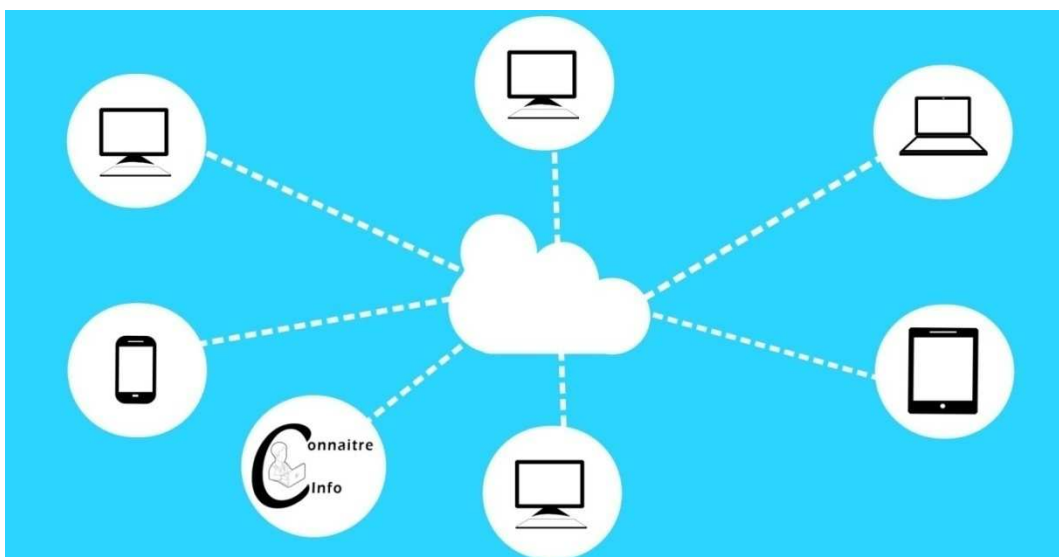


Figure I.1 : Exemple d'un réseau informatique.

Un réseau informatique dispose de nombreux avantages [5] :

- Il est possible d'améliorer sensiblement la rapidité et la fiabilité de l'échange d'informations et de réduire les coûts dans l'entreprise ou l'entité qui décide de le créer.
- Lorsque nous parlons d'un réseau informatique, nous devons garder à l'esprit qu'il doit comporter une série d'éléments fondamentaux pour qu'il puisse fonctionner sans problème :
- Les serveurs, qui en viennent à être comme les administrateurs de l'information et de l'ensemble du processus lui-même.
- Les panneaux de brassage, qui sont les systèmes responsables de l'organisation de tout le câblage nécessaire.

I.3 Les types des réseaux informatiques:

Le réseau informatique, système mis en œuvre pour permettre l'échange de données entre les différents périphériques de ce réseau informatique. Il existe différents types de réseaux informatiques selon les critères suivants : **la taille de zone de couverture, le nombre d'utilisateur connecté, le nombre et les types des services disponibles, et le domaine de responsabilité.**

Voici ci-dessous les principales catégories :

- Personal Area Network (PAN) : Réseau Personnel
- Local Area Network (LAN) : Réseau Local
- Metropolitan Area Network (MAN) : Réseau Métropolitain
- Wide Area Network (WAN): Réseau Etendu

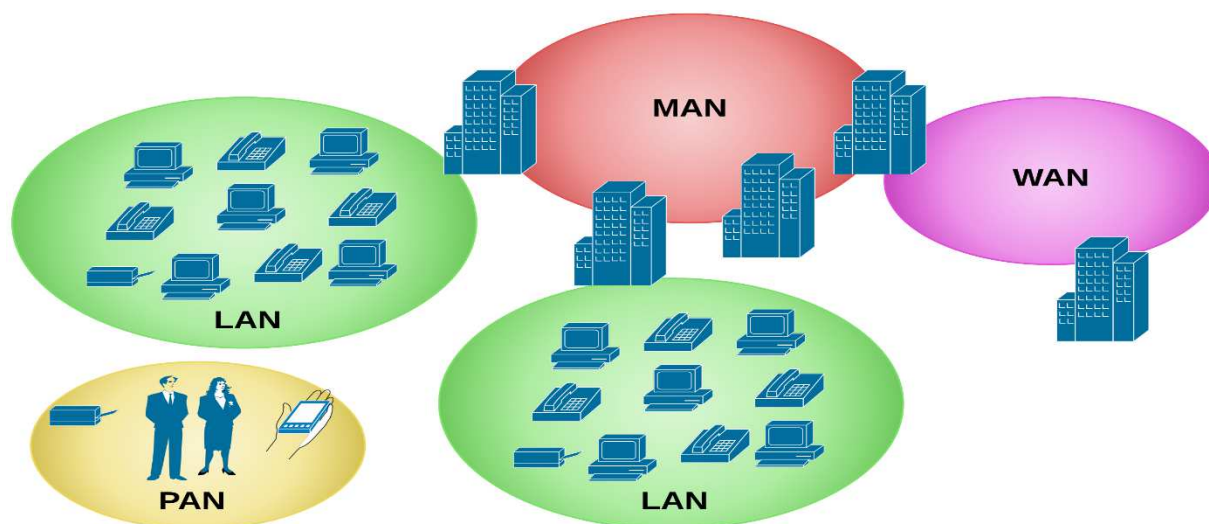


Figure I.2: La couverture de différent types de réseau.

I.3.1 Réseau personnel (PAN) :

Un réseau personnel relie des périphériques tels que des souris, des claviers, des imprimantes, des Smartphones et des tablettes sur une portée très limitée pour une seule personne. Tous ces périphériques sont dédiés à un seul hôte et utilisent généralement une connexion Bluetooth qui est une technologie sans fil permet aux périphériques de communiquer sur des distances courtes (Figure I.3). Un périphérique Bluetooth peut se connecter à sept autres périphériques Bluetooth au maximum. Décrits dans la norme IEEE 802.15.1, ces périphériques sont capables de gérer de la voix et des données [7].

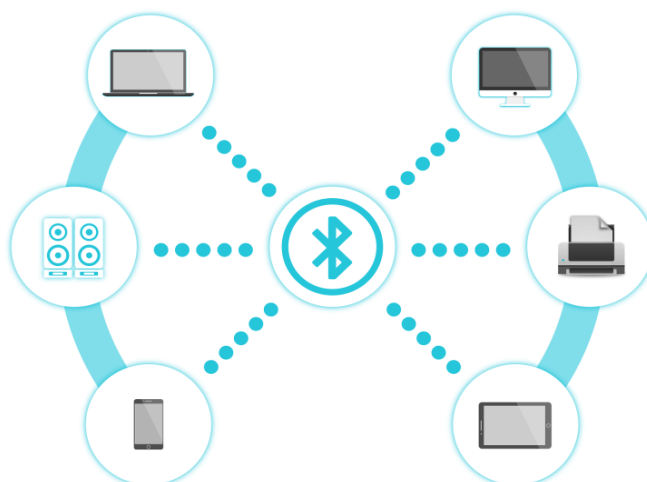


Figure I.3 : Exemple d'un réseau personnel (PAN).

I.3.2 Réseau Local (LAN) :

Les réseaux LAN (Figure I.4) englobent généralement une petite zone géographique de petite taille. Toutefois, leur principale caractéristique actuellement est d'appartenir à une entité, comme un travailleur à domicile ou une petite entreprise, ou d'être entièrement gérés par un

service informatique, comme dans une école ou une grande entreprise. Cet individu ou groupe garantit le respect des politiques de sécurité et de contrôle d'accès sur le réseau [7].

Des LAN peuvent être interconnectés pour former des réseaux plus grands (WAN, MAN,...). On dit alors que le LAN est un sous-réseau du réseau auquel il est connecté [4].

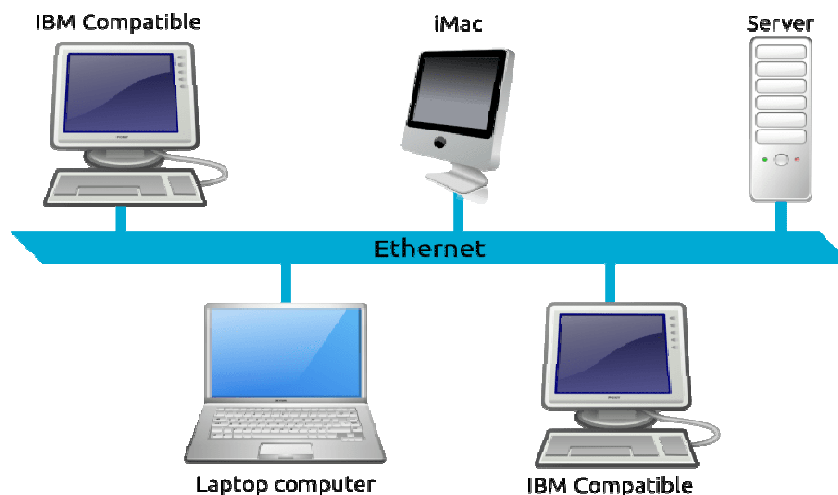


Figure I.4 : Exemple d'un réseau local (LAN).

I.3.3 Réseau Métropolitain (MAN) :

Ce type de réseaux est récent et garde les avantages des LAN sur de plus longues distances de l'ordre de la ville. Un réseau métropolitain est un réseau qui couvre une vaste zone (comme une ville). Il comprend plusieurs bâtiments interconnectés en réseaux fédérateurs sans fil ou à fibres optiques (Figure I.5). Dans ce cas, les lignes et équipements de communication appartiennent généralement à un consortium d'utilisateurs ou à un fournisseur d'accès, qui vend ce service aux utilisateurs. Un réseau métropolitain peut être un réseau à haut débit permettant le partage de ressources locales [7].

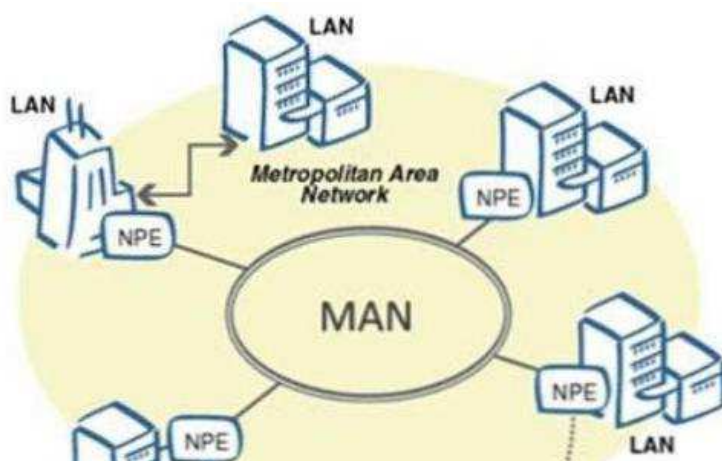


Figure I.5 : Exemple d'un réseau métropolitain (MAN).

I.3.4 Réseau Étendu (WAN) :

Un réseau étendu (WAN) permet de connecter plusieurs réseaux situés dans des zones géographiques distinctes, couvre une très grande échelle (pays, continents, monde). Il appartient à un opérateur télécoms. Les particuliers et les entreprises s'abonnent aux services WAN [7]. L'exemple le plus courant de réseau étendu est Internet (Figure I.6). Internet est un vaste réseau étendu composé de millions de réseaux interconnectés.

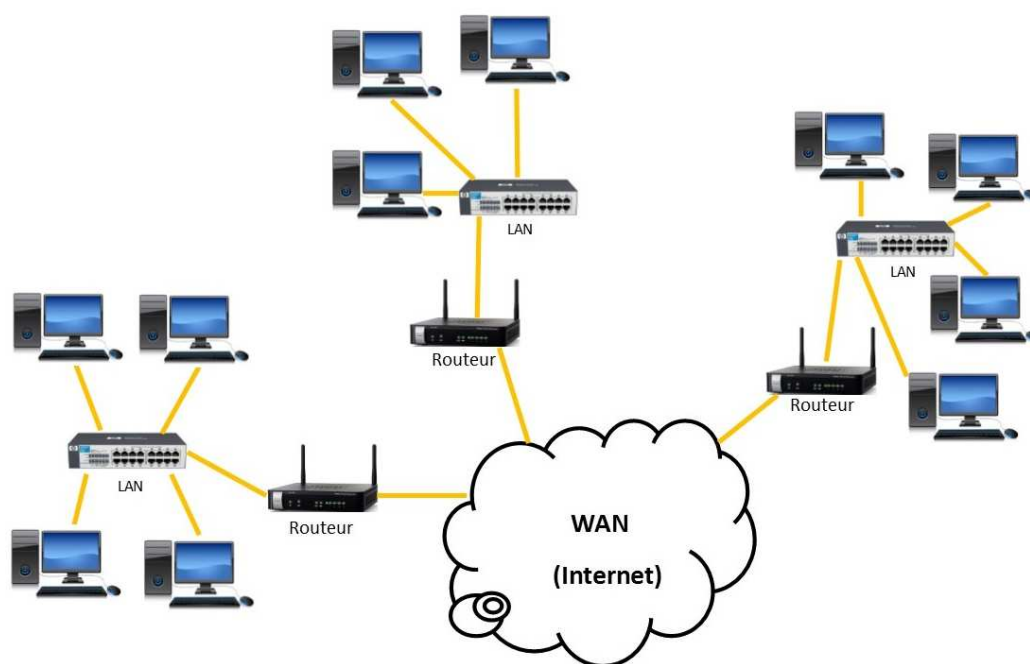


Figure I.6 : Exemple d'un Réseau étendu (WAN).

I.4 La structure physique d'un réseau informatique :

La topologie d'un réseau représente la disposition de celui-ci. La façon dont les différents nœuds au sein d'un réseau sont connectés, les uns aux autres et communiquent, est déterminée par cette même topologie du réseau. nous allons ici évoquer les cinq principales topologies réseau.

I.4.1 Topologie des mailles

Dans un réseau maillé (figure I.7), les dispositifs sont connectés avec de nombreuses interconnexions redondantes entre les nœuds du réseau. Dans une véritable topologie de maillage, chaque nœud a une connexion avec tous les autres nœuds du réseau. Il existe deux types de topologie maillé :

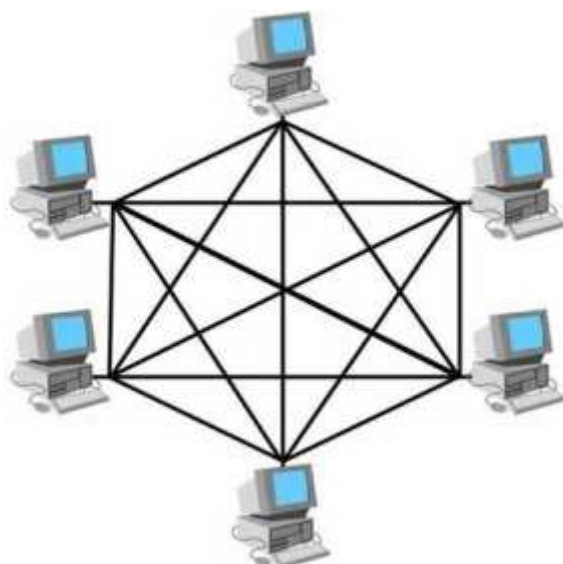


Figure I.7 : Topologie des mailles.

- a) **Topologie maillée complète** : Dans ce cas de figure, chaque nœud a un circuit qui le relie à tous les autres nœuds du réseau. Le maillage complet est assez coûteux à mettre en œuvre, mais c'est lui qui offre la plus grande quantité de redondance. Ainsi en cas de défaillance de l'un de ces nœuds, le trafic réseau peut être dirigé vers n'importe lequel des autres nœuds. Le maillage complet est généralement utilisé aux réseaux de longue distance.
- b) **Topologie maillée partielle** : Solution moins coûteuse à mettre en œuvre mais qui produira moins de redondance que la topologie maillée complète. Avec un maillage partiel, certains nœuds sont organisés selon un schéma de maillage complet, mais d'autres ne sont connectés qu'à un ou deux nœuds du réseau. La topologie maillée partielle se retrouve couramment dans les réseaux qu'on pourrait appeler périphériques aux réseaux longue distance évoqués au-dessus.

I.4.2 Topologie en étoile

Dans un réseau en étoile (Figure I.8), les périphériques sont connectés à un ordinateur central appelé "Hub". Les nœuds communiquent sur le réseau en faisant passer simplement les données par ce hub.

L'avantage principal, dans un réseau en étoile, est qu'un nœud qui se verrait être défectueux n'affectera pas le reste du réseau. Inconvénient est si l'ordinateur central qui fait office de hub tombe en panne, c'est l'ensemble du réseau qui deviendra inutilisable.

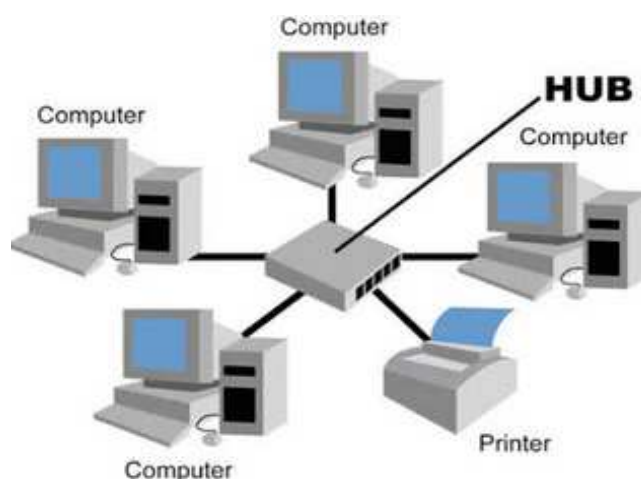


Figure I.8 : *Topologie en étoile.*

I.4.3 Topologie en bus :

Ici il existe un câble central appelé bus qui relie entre eux tous les appareils sur le réseau. Il est un peu la colonne vertébrale de ce réseau (Figure I.9). Les réseaux de bus sont relativement peu coûteux ainsi que faciles à installer dans le cadre d'un petit réseau. Les systèmes Ethernet utilisent aujourd'hui une topologie en bus.

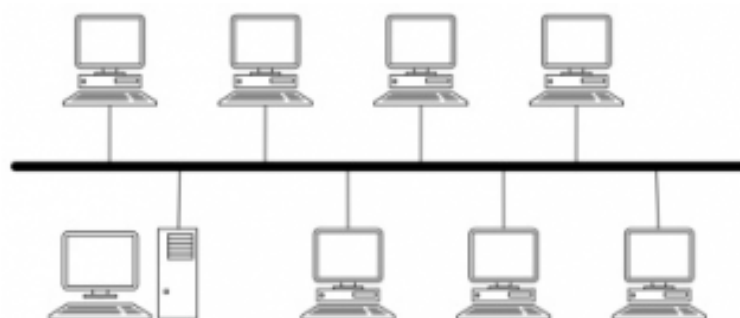


Figure I.9 : *Topologie en bus.*

Avantage principal : Il est facile de connecter un nouvel ordinateur ou appareil à ce type de réseau et généralement moins de câbles qu'une topologie en étoile seront utilisés.

Inconvénient principal : L'ensemble du réseau s'arrête s'il y a un soucis avec le câble faisant office de bus et il peut être difficile d'identifier le problème en cas de soucis.

I.4.4 Topologie en anneau :

Ici notre réseau local aura une topologie physiquement similaire à un anneau. C'est-à-dire que tous les nœuds de ce réseau sont connectés en boucle fermée (figure I.10). Les informations transitent autour de l'anneau à travers tous ces nœuds. Si le message transféré concerne le nœud par lequel il transite, il sera tout simplement intercepté.

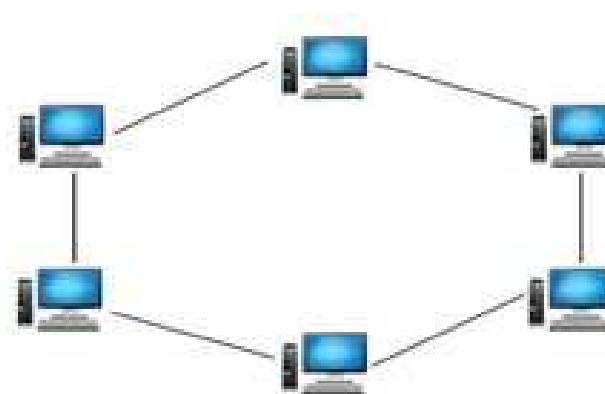


Figure I.10 : *Topologie en anneau.*

Avantage principal : L'avantage principal d'un réseau en anneau est qu'il est plus facile avec celui-ci de couvrir de plus grandes distances en comparaison avec les autres topologies. En effet chaque nœud régénère les messages au fur et à mesure que ceux-ci transitent.

Inconvénient principal : Un message peut transiter par beaucoup de nœuds.

I.4.5 Topologie de l'arbre :

Il s'agit d'une topologie qu'on pourrait qualifier "d'hybride". Elle combine les caractéristiques des topologies en bus et en étoile. Ici, des groupes de réseaux configurés en étoile sont connectés à un câble faisant office de bus [8].

Avantage principal : Une topologie en arbre est un bon choix pour les grands réseaux informatiques car l'ensemble du réseau est divisé en parties et est donc plus facile à gérer.

Inconvénient principal : L'ensemble du réseau est dépendant d'éléments centraux et une défaillance de ces éléments peut paralyser l'ensemble du réseau.

I.5 La structure logique d'un réseau informatique :

La topologie logique la façon dont les signaux agissent sur le support réseau, ou la façon dont les données passent d'un appareil à l'autre à travers le réseau [8]. La structure logique d'un réseau informatique se base sur les modèles (OSI et TCP/IP).

I.5.1 Le modèle OSI :

Pour faire circuler l'information sur un réseau on peut utiliser principalement deux stratégies ; l'information est envoyée de façon complète et l'information est fragmentée en petits morceaux (paquets), chaque paquet est envoyé séparément sur le réseau, les paquets sont ensuite réassemblés sur la machine destinataire.

La première stratégie n'est pas utilisée car les risques d'erreurs et les problèmes sous-jacents sont trop complexes à résoudre. Dans la seconde stratégie, on parle d'un réseau à commutations de paquets.

Le modèle OSI est un modèle à 7 couches qui décrit le fonctionnement d'un réseau à commutations de paquets, comme montre la figure suivante. Chacune des couches de ce modèle représente une catégorie de problème que l'on rencontre dans un réseau. Découper les problèmes en couche présente des avantages. Lorsque l'on met en place un réseau, il suffit de trouver une solution pour chacune des couches.

L'utilisation de couches permet également de changer de solution technique pour une couche sans pour autant être obligé de tout repenser. Chaque couche garantit à la couche qui lui est supérieure que le travail qui lui a été confié a été réalisé sans erreur [4].

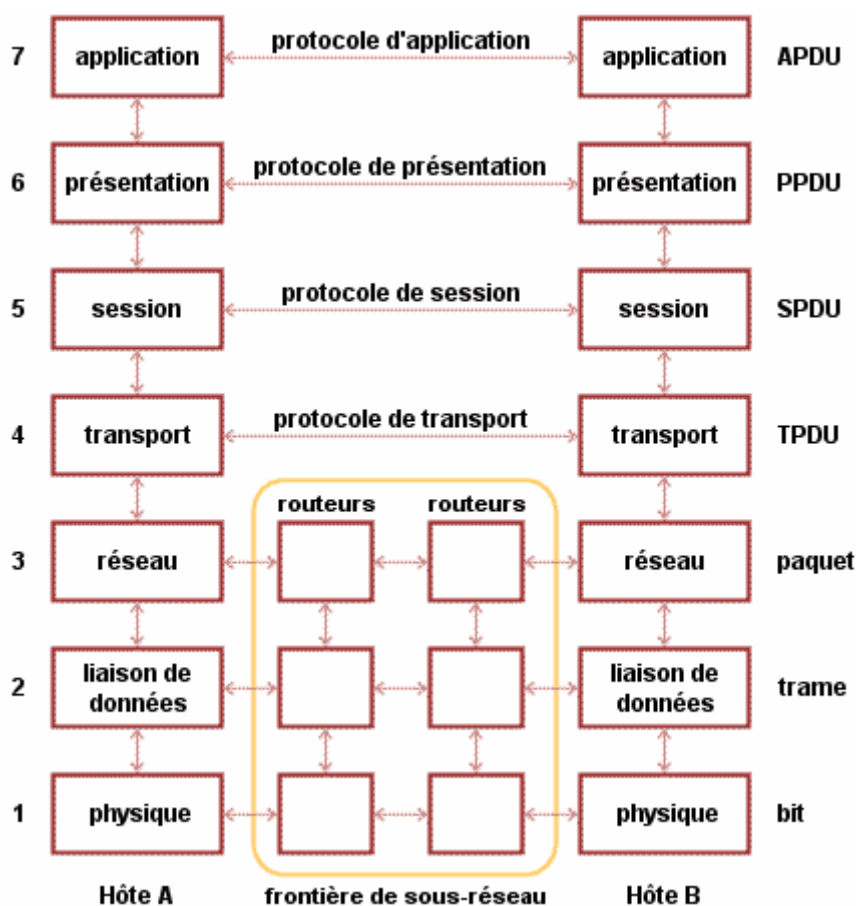


Figure I.11 : Illustration du modèle OSI.

Les principes qui ont conduit à ces 7 couches sont les suivants :

une couche doit être créée lorsqu'un nouveau niveau d'abstraction est nécessaire, chaque couche a des fonctions bien définies, les fonctions de chaque couche doivent être choisies dans l'objectif de la normalisation internationale des protocoles, les frontières entre couches doivent être choisies de manière à minimiser le flux d'information aux interfaces, le

nombre de couches doit être tel qu'il n'y ait pas cohabitation de fonctions très différentes au sein d'une même couche et que l'architecture ne soit pas trop difficile à maîtriser.

Les couches basses (1, 2, 3 et 4) sont nécessaires à l'acheminement des informations entre les extrémités concernées et dépendent du support physique. Les couches hautes (5, 6 et 7) sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques. Par ailleurs, les couches 1 à 3 interviennent entre machines voisines, et non entre les machines d'extrémité qui peuvent être séparées par plusieurs routeurs. Les couches 4 à 7 sont au contraire des couches qui n'interviennent qu'entre hôtes distants.

I.5.1.1 Les couches de modèle OSI [9] :

➤ *La couche 1 : Couche physique*

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1). Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie...), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données. L'unité d'information typique de cette couche est le bit, représenté par une certaine différence de potentiel.

➤ *La couche 2 : Couche liaison de données*

Son rôle est un rôle de « liant » : elle va transformer la couche physique en une liaison a priori exempte d'erreurs de transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquiescement renvoyées par le récepteur. Rappelons que pour la couche physique, les données n'ont aucune signification particulière. La couche liaison de données doit donc être capable de reconnaître les frontières des trames. Cela peut poser quelques problèmes, puisque les séquences de bits utilisées pour cette reconnaissance peuvent apparaître dans les données.

La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission. De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.

L'unité d'information de la couche liaison de données est la trame qui est composée de quelques centaines à quelques milliers d'octets maximum.

➤ ***La couche 3 : Couche réseau***

C'est la couche qui permet de gérer le sous-réseau, i.e. le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux. Au moment de sa conception, il faut bien déterminer le mécanisme de routage et de calcul des tables de routage (tables statiques ou dynamiques...).

La couche réseau contrôle également l'engorgement du sous-réseau. On peut également y intégrer des fonctions de comptabilité pour la facturation au volume, mais cela peut être délicat. L'unité d'information de la couche réseau est le paquet.

➤ ***La couche 4 : Couche transport***

Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.

Cette couche est également responsable de l'optimisation des ressources du réseau : en toute rigueur, la couche transport crée une connexion réseau par connexion de transport requise par la couche session, mais cette couche est capable de créer plusieurs connexions réseau par processus de la couche session pour répartir les données, par exemple pour améliorer le débit. A l'inverse, cette couche est capable d'utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage. Dans tous les cas, tout ceci doit être transparent pour la couche session.

Cette couche est également responsable du type de service à fournir à la couche session, et finalement aux utilisateurs du réseau : service en mode connecté ou non, avec ou sans garantie d'ordre de délivrance, diffusion du message à plusieurs destinataires à la fois... Cette couche est donc également responsable de l'établissement et du relâchement des connexions sur le réseau. Un des tout derniers rôles à évoquer est le contrôle de flux.

C'est l'une des couches les plus importantes, car c'est elle qui fournit le service de base à l'utilisateur, et c'est par ailleurs elle qui gère l'ensemble du processus de connexion, avec toutes les contraintes qui y sont liées. L'unité d'information de la couche transport est le message.

➤ ***La couche 5 : Couche session***

Cette couche organise et synchronise les échanges entre tâches distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle établit

également une liaison entre deux programmes d'application devant coopérer et commande leur dialogue (qui doit parler, qui parle...). Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. La couche session permet aussi d'insérer des points de reprise dans le flot de données de manière à pouvoir reprendre le dialogue après une panne.

➤ ***La couche 6 : couche présentation***

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information. Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

➤ ***La couche 7 : couche d'application***

Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie.

1.5.1.2 Transmission de données au travers du modèle OSI :

Le processus émetteur remet les données à envoyer au processus récepteur à la couche application qui leur ajoute un entête application AH: *Application Header* (éventuellement nul). Le résultat est alors transmis à la couche présentation.

La couche présentation transforme alors ce message et lui ajoute (ou non) un nouvel entête (éventuellement nul). La couche présentation ne connaît et ne doit pas connaître l'existence éventuelle de AH ; pour la couche présentation, AH fait en fait partie des données utilisateur. Une fois le traitement terminé, la couche présentation envoie le nouveau « message » à la couche session et le même processus recommence.

Les données atteignent alors la couche physique qui va effectivement transmettre les données au destinataire. A la réception, le message va remonter les couches et les entêtes sont progressivement retirés jusqu'à atteindre le processus récepteur. cette démarche est représentée sur la figure I.12.

Le concept important est le suivant : il faut considérer que chaque couche est programmée comme si elle était vraiment horizontale, c'est à dire qu'elle dialoguait directement avec sa couche paire réceptrice. Au moment de dialoguer avec sa couche paire, chaque couche rajoute un entête et l'envoie (virtuellement, grâce à la couche sous-jacente) à sa couche paire [9].

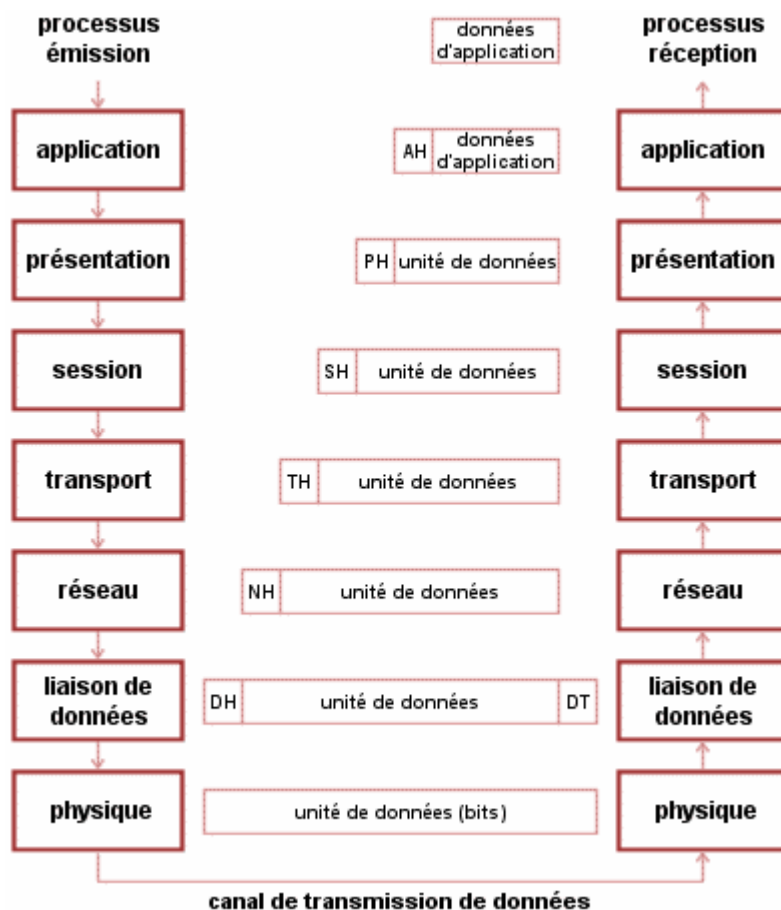


Figure I.12 : La démarche de la transmission des données.

I.5.2 Le modèle TCP/IP :

TCP/IP (*Transmission Control Protocol/Internet Protocol*) est un ensemble de protocoles qui définit une forme d'adressage, une théorie de routage et des méthodes de contrôle du bon transport des données [4].

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (*Transmission Control Protocol*) qu'on utilise « par-dessus » un protocole réseau, IP (*Internet Protocol*). Ce qu'on entend par « modèle TCP/IP », c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP [9].

Le modèle est apparu pratiquement en même temps que le modèle OSI. Il est devenu un standard de fait car c'est celui utilisé sur Internet. Il fonctionne sensiblement de la même manière que le modèle OSI. Ses couches sont au nombre de quatre : couche réseau, couche Internet, couche transport et couche application. Elles ont le même rôle que celles du modèle OSI (Figure I.13) [4].

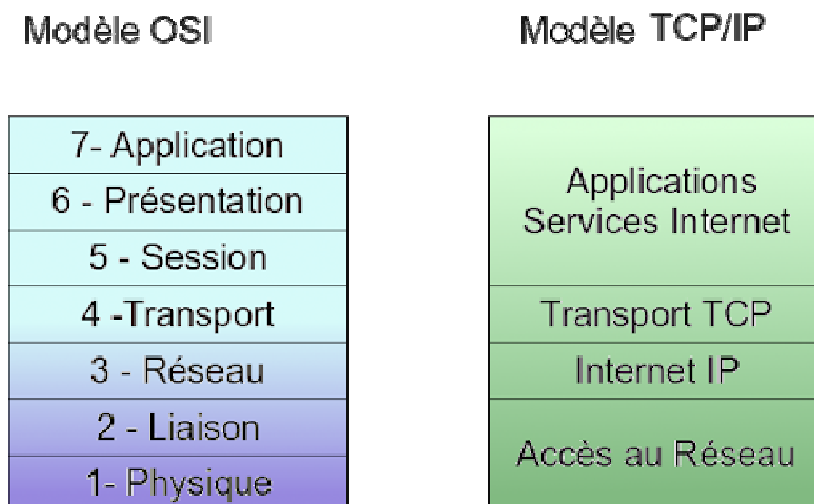


Figure I.13 : Le modèle TCP/IP.

I.5.2.1 Les couches du modèle TCP/IP [9] :

➤ *La couche 1 : Couche accès au réseau*

Cette couche est assez « étrange ». En effet, elle semble « regrouper » les couches physique et liaison de données du modèle OSI. En fait, cette couche n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre une hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche accès-réseau.

➤ *La couche 2 : Couche internet IP*

Cette couche est la clé de voûte de l'architecture, réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage. C'est en ce sens que l'on peut se permettre de comparer cette couche avec la couche réseau du modèle OSI. La couche internet possède une implémentation officielle : le protocole IP (*Internet Protocol*).

➤ *La couche 3 : Couche transport*

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation.

Officiellement, cette couche n'a que deux implémentations : le protocole TCP (*Transmission Control Protocol*) et le protocole UDP (*User Datagram Protocol*). TCP est un protocole fiable, orienté connexion, qui permet l'acheminement sans erreur de paquets issus d'une machine d'un internet à une autre machine du même internet. Son rôle est de fragmenter le message à transmettre de manière à pouvoir le faire passer sur la couche internet. A l'inverse, sur la machine destination, TCP replace dans l'ordre les fragments transmis sur la couche internet pour reconstruire le message initial. TCP s'occupe également du contrôle de flux de la connexion.

UDP est en revanche un protocole plus simple que TCP : il est non fiable et sans connexion. Son utilisation présuppose que l'on n'a pas besoin ni du contrôle de flux, ni de la conservation de l'ordre de remise des paquets. Par exemple, on l'utilise lorsque la couche application se charge de la remise en ordre des messages. On se souvient que dans le modèle OSI, plusieurs couches ont à charge la vérification de l'ordre de remise des messages. C'est là un avantage du modèle TCP/IP sur le modèle OSI, mais nous y reviendrons plus tard. Une autre utilisation d'UDP : la transmission de la voix. En effet, l'inversion de 2 phonèmes ne gêne en rien la compréhension du message final.

➤ *La couche 4 : Couche application*

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches.

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée. Ce choix rend TFTP plus rapide que le protocole FTP qui utilise TCP. A l'inverse, SMTP utilise TCP, car pour la remise du courrier électronique, on veut que tous les messages parviennent intégralement et sans erreurs.

I.5.3 Comparaison du modèle TCP/IP avec le modèle OSI :

Les modèles OSI et TCP/IP sont tous les deux fondés sur le concept de pile de protocoles indépendants. Ensuite, les fonctionnalités des couches sont globalement les mêmes.

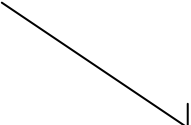
Au niveau des différences, on peut remarquer la chose suivante : le modèle OSI faisait clairement la différence entre 3 concepts principaux, alors que ce n'est plus tout à fait le cas pour le modèle TCP/IP. Ces 3 concepts sont les concepts de services, interfaces et protocoles. En effet, TCP/IP fait peu la distinction entre ces concepts, et ce malgré les efforts des concepteurs pour se rapprocher de l'OSI. Cela est dû au fait que pour le modèle TCP/IP, ce sont les protocoles qui sont d'abord apparus. Le modèle ne fait finalement que donner une justification théorique aux protocoles, sans les rendre véritablement indépendants les uns des autres.

Enfin, la dernière grande différence est liée au mode de connexion. Certes, les modes orienté connexion et sans connexion sont disponibles dans les deux modèles mais pas à la même couche : pour le modèle OSI, ils ne sont disponibles qu'au niveau de la couche réseau (au niveau de la couche transport, seul le mode orienté connexion n'est disponible), alors qu'ils ne sont disponibles qu'au niveau de la couche transport pour le modèle TCP/IP (la couche internet n'offre que le mode sans connexion). Le modèle TCP/IP a donc cet avantage par rapport au modèle OSI : les applications (qui utilisent directement la couche transport) ont véritablement le choix entre les deux modes de connexion [9].

I.6 Conclusion :

Ce chapitre nous a permis en premier lieu de découvrir et de mieux comprendre les notions et les aspects élémentaires des réseaux informatiques, où nous avons décrit les notions de base et les différents types des réseaux informatiques, leurs topologies, et en deuxième lieu de comprendre les deux principaux modèles et leurs couches, et plus particulièrement le modèle OSI et le modèle TCP/IP. Le chapitre qui suit sera dédié au protocole IP, les principes de base de l'adressage IP et le routage.

CHAPITRE II :



*Le protocole IP et
l'adressage IPv4*

II.1 Introduction :

Les réseaux IP deviennent non seulement un moyen de communication, mais aussi un moyen de commerce global de développement et de distribution. TCP/IP est très connu dans le domaine des réseaux, il correspond à toute une architecture. Il ne correspond pas à un seul protocole, mais bien à un ensemble de petits protocoles spécialisés appelés sous protocoles (TCP, IP, UDP, ARP, ICMP) [10]. La plus part des administrateurs réseaux désignent ce groupe par TCP/IP.

Pour pouvoir envoyer des données via des réseaux numériques, vous avez besoin d'une adresse correcte, dans ce cas présent, il s'agit d'une adresse IP. Les paquets de données obtiennent une adresse IP, tout comme les lettres possèdent une adresse postale pour s'assurer qu'elles arrivent bien au bon destinataire. Toutefois, leurs homologues numériques ne sont pas liés à un emplacement spécifique, en effet les adresses IP sont automatiquement ou bien manuellement affectées au périphérique réseau lors de la configuration de la connexion. Dans ce processus, l'Internet Protocol, en français protocole Internet (mais appelé plus communément protocole IP) joue un rôle important.

Nous nous proposons dans ce chapitre, d'étudier les définitions théoriques nécessaires à la compréhension des notions fondamentales de protocole IP, ces caractéristiques de base et le détail de l'entête du paquet IP. Nous nous attacherons ensuite à l'adressage IPv4, les classes et les adresses particuliers, puis à la notion de routage et nous rappellerons simplement leur types.

II.2 Historique et définition :

En 1974, l'*Institute of Electrical and Electronics Engineers* (IEEE) a publié un document de recherche des informaticiens américains Robert Kahn et Vint Cerf qui décrivait un modèle de protocole pour une connexion mutuelle de paquets de réseau basé sur ARPANET, le prédécesseur d'Internet. En plus du protocole de contrôle de transmission TCP, le composant principal de ce modèle était le protocole IP, qui, en plus d'une couche d'abstraction spéciale, permettait la communication à travers différents réseaux physiques. Au cours des années suivantes, de plus en plus de réseaux de recherche ont été consolidés sur la base de cette combinaison de protocoles « TCP/IP », qui a finalement été spécifiée en 1981 comme standard dans le RFC 791 [11].

II.2.1 Définition :

Internet Protocol (IP) est un protocole sans connexion, en tant qu'élément central de la famille des protocoles Internet (un ensemble d'environ 500 protocoles réseau), est responsable de l'adressage et de la fragmentation des paquets de données dans les réseaux numériques.

Avec le protocole de transport TCP (*Transmission Control Protocol*), l'IP constitue la base de l'Internet. Pour envoyer un paquet de l'expéditeur au destinataire, le protocole IP définit une structure de paquets qui résume les informations envoyées. Le protocole détermine la manière dont les informations sur la source et la destination des données sont décrites et sépare ces informations des données informatives dans l'en-tête IP. Ce type de format de paquet est également connu sous le nom de datagramme IP [11].

Ce protocole permet de gérer l'acheminement des paquets d'une machine à une autre, ainsi que l'adressage. Au plus bas niveau (physique), on dispose alors d'interfaces pour communiquer d'un point à un autre. Grâce à trois champs du paquet, on peut facilement déterminer le destinataire d'un message :

- Le champ adresse IP
- Le champ masque sous-réseau
- Le champ passerelle

Les données circulent sur le réseau Internet sous forme de datagrammes (c'est pour cela que l'on parle alors de commutation de paquets). Les datagrammes sont des ensembles de données encapsulées, auxquelles on a ajouté des entêtes, correspondant aux informations liées à leur transport : adresse IP, destination, type de service...

La taille maximale d'un datagramme est de 65536 octets. Mais, cette valeur est rarement atteinte, car les réseaux ont une capacité moindre par rapport à une telle dimension. De plus, les réseaux utilisés pour propager de l'information sur Internet, sont adossés à différentes technologies, si bien que la taille maximale d'un datagramme peut également varier selon le type de réseau sous-jacent [12].

II.3 Le protocole IP :

Le protocole IP est conçu pour interconnecter les machines dans un réseau à commutation de paquets. Il traite chaque datagramme comme une entité indépendante de tout autre datagramme. Il n'y a pas de notion de connexions ni de circuits logiques. Il existe deux versions du protocole IP : IPv4 et IPv6.

➤ **IP Version 4 :**

L'Internet Protocol version 4 est la première version d'IP à avoir été largement déployée, et forme encore la base de l'Internet. Ce protocole utilise une adresse IP sur **32 bits**, ce qui est un facteur limitant à l'expansion d'Internet puisque seulement 4294967296 adresses sont possibles. Cette limitation conduit à la transition d'IPv4 vers IPv6.

➤ **IP Version 6 :**

C'est une nouvelle version du protocole IP qui dispose d'un espace d'adressage bien plus important qu'IPv4. Les différences avec IPv4 peuvent être résumées en ce qui suit [13] :

- Espace d'adressage plus large grâce à la longueur plus élevée des champs d'adresse.
- Format simplifié de l'en-tête.
- Possibilité d'identification des flux à l'aide d'étiquette.

II.3.1 Le protocole IPv4 :

La version 4 est actuellement la plus utilisée : elle est généralement représentée en notation décimale avec **quatre nombres** compris entre **0** et **255**, séparés par des points, ce qui donne par exemple: **212.85.150.134**. Les plages d'adresses Pv4 sont proches de la saturation, les opérateurs incitent donc à la transmission d'IPv4 vers IPv6 [12].

II.3.1.1 Caractéristiques de base de protocole IPv4 :

Les principaux caractéristiques de base de protocole IPv4 sont [14] :

- **Sans connexion** : aucune connexion n'est établie avant l'envoi de paquets de données.
- **Au mieux (peu faible)** : aucune surcharge n'est utilisée pour garantir la transmission des paquets.
- **Indépendant des médias** : fonctionne indépendamment du média transportant les données.

II.3.1.2 Le niveau paquet :

Le rôle du niveau paquet est de transporter d'une extrémité à l'autre du réseau des blocs de données provenant d'une fragmentation des messages du niveau supérieur, le niveau transport. Le paquet est l'entité de la couche 3 qui possède l'adresse du destinataire ou la référence nécessaire à son acheminement dans le réseau. Le niveau paquet est en outre responsable du contrôle de flux, qui, s'il est bien conçu, évite la congestion dans les nœuds du réseau.

Les fonctionnalités du niveau paquet peuvent se trouver au niveau trame. Un paquet ne peut être transmis directement sur un support physique, car le récepteur serait incapable de reconnaître les débuts et fins de paquet.

L'ensemble des paquets allant d'un même émetteur vers un même destinataire s'appelle un flot. Celui-ci être long ou court, suivant la nature du service qui l'a créé, si un gros fichier donne naissance à un flot important, une transaction ne produit qu'un flot très court, d'un à quelque paquets [15].

II.3.1.3 Paquet IPv4 :

Les données circulent sur Internet sous forme de datagrammes IP (paquets). Les datagrammes sont des données encapsulées, c'est-à-dire des données auxquelles on a ajouté des en-têtes renfermant des informations sur leur transport (telles que l'adresse IP de destination, la qualité de services exigée, le nombre de réseaux pouvant être atteints, etc.). Les données contenues dans les datagrammes sont analysées (et éventuellement modifiées) par les routeurs permettant leur transit [10].

L'IPv4 encapsule, ou empaquette le datagramme ou segment de la couche transport pour que le réseau puisse le délivrer à l'hôte de destination. L'encapsulation IPv4 reste en place du moment où le paquet quitte la couche réseau de l'hôte émetteur jusqu'à son arrivée dans la couche réseau de l'hôte de destination.

Le processus d'encapsulation de données par couche permet aux services des différentes couches de se développer et d'évoluer sans affecter d'autres couches. Ceci signifie que des segments de couche transport peuvent être facilement encapsulés par les protocoles de couche réseau existants, comme IPv4 et IPv6.

Les routeurs peuvent mettre en œuvre ces différents protocoles de couche réseaux pour fonctionner simultanément sur le réseau vers et depuis les mêmes hôtes ou des hôtes différents. Le routage effectué par ces périphériques intermédiaires tient compte uniquement du contenu de l'entête de paquet qui encapsule le segment. Dans tous les cas, la partie donnée du paquet reste inchangée durant les processus de couche réseau.

Comme l'illustre la figure suivante, un protocole IPv4 définit de nombreux champs différents dans l'entête de paquet IPv4. Ces champs contiennent des valeurs binaires que les services IPv4 référencent lors de la transmission de paquets sur le réseau [16].

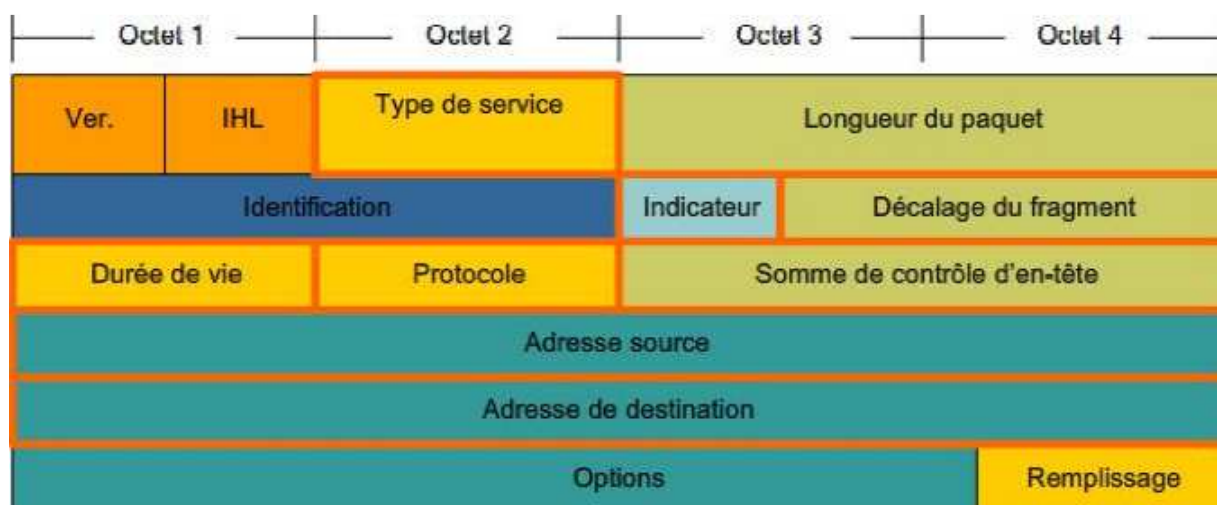


Figure II.1 : L'entête de paquet IPv4.

Un paquet IP permet de transmettre un message d'une machine à une autre sur un réseau. Celui-ci est découpé en plusieurs morceaux et transmis séparément. Ce paquet est inclus dans une entête, qu'on retrouve souvent sous le nom de « Header ». Cet entête du paquet comprend les informations nécessaires pour acheminer et reconstituer le message. On va examiner par la suite les principaux champs d'entête du paquet IPv4 [15], [16].

Ver. = 4 ; Contient le numéro de version IP(4).

IHL = 5 ; Spécifie la taille de l'entête en mots de 32 bits (4 octets).

Type de service ; Le champ de type de service contient une valeur binaire de 8 bits permettant de déterminer la priorité de chaque paquet. Cette valeur permet d'appliquer un mécanisme de qualité de service (QoS) aux paquets de priorité élevée, tel que ceux transportant des données vocales de téléphonie. Le routeur traitant les paquets peut être configuré pour déterminer le paquet à transmettre en premier en fonction de la valeur de type de service.

Longueur du paquet : Ce champ donne la taille du paquet entier, entête et données compris, en octets. (valeur maximale 472 octets).

Identification = 111 ; indicateur de paquet d'origine (obligatoire en cas de fragmentation ultérieure).

Indicateur = 0 ; indique que le paquet peut être fragmenté en cas de nécessité.

Décalage de fragment = 0 ; indique que ce paquet n'est actuellement pas fragmenté (il n'y a aucun décalage).

Durée de vie (TTL: *Time To Live*) ; indique la durée de traitement de couche 3, en seconde, qui doit s'écouler avant que le paquet ne soit supprimé.

Protocole ; Cette valeur binaire de 8 bits indique le type de données utiles transportées par le paquet. Le champ de protocole permet à la couche réseau de transmettre les données au protocole de couche supérieure approprié. (**01** ICMP, **06** TCP, **17** UDP).

Somme de contrôle d'entête ; Le champ de somme de contrôle est utilisé pour vérifier l'absence d'erreurs dans l'en-tête de paquet.

Adresse IP de destination ; le champ adresse IP de destination contient une valeur binaire de 32 bits qui représente l'adresse de l'hôte de couche réseau de destination du paquet.

Adresse IP source ; Le champ adresse IP source contient une valeur binaire de 32 bits qui représente l'adresse hôte de couche réseau source du paquet.

Options ; Des champs supplémentaires sont prévus dans l'en-tête IPv4 afin de fournir d'autres services, mais ils sont rarement utilisés.

II.4 L'adressage IP :

Le rôle fondamental de la couche réseau est de déterminer la route que doivent emprunter les paquets. Cette fonction de recherche de chemin nécessite une identification de tous les hôtes connectés au réseau. On identifie un hôte réseau par une adresse qui englobe les mêmes informations. Le modèle TCP/IP utilise un système particulier d'adressage qui porte le nom de la couche réseau de ce modèle ; l'adressage IPv4 [17].

Le protocole IP propose donc un format d'adresse standardisé qui permet d'identifier de manière unique une machine au sein d'un réseau. Un datagramme IP véhiculera simultanément deux adresses :

- **l'adresse source** qui est l'adresse IP de la machine qui a formaté et qui émet le paquet IP
- **l'adresse destination**, qui est inscrite par la machine émettrice, et qui correspond à l'adresse de la machine pour qui est destiné le paquet IP.

En conséquence, et à l'instar de beaucoup de protocoles de niveau 3, une hiérarchie est définie dans le format d'adresse IP. Une adresse IP est scindée en deux parties :

- **l'adresse réseau** : elle identifie un groupe de machine, généralement regroupées sur un même sous réseau physique (Ethernet, Token Ring, X25, etc.)
- **l'adresse machine** : elle identifie la machine dans le sous-réseau considéré.

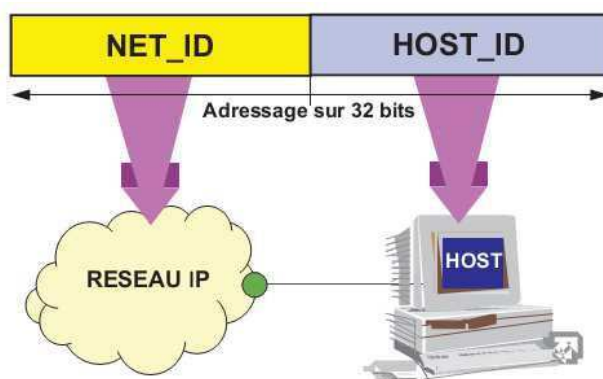


Figure II.2 : Identifiants de réseau et machine dans une adresse IPv4.

II.4.1 L'adressage IPv4 :

Une adresse IPv4 (*Internet Protocol version 4*) est une identification unique pour un hôte sur un réseau IP. L'adresse IPv4 est codée sur 4 octets. Elle est représentée en notation décimale pointée, est un nombre d'une valeur de 32 bits représentée par 4 valeurs décimales

séparés par points, Chaque octet peut prendre une valeur comprise entre 0 (8 bits à zéro) et 255 (8 bits à un). Le point matérialise la frontière d'octet [18].

Exemple :

10001010 00110000 00011010 00000001 ➡ 138.48.26.1

- **L'adresse unicast** : est une adresse unique attribuée à chaque interface d'un hôte du réseau ou d'un routeur. Elle apparaît toujours dans le champ *Source Address* de l'entête IPv4. Le champ *Destination Address* de l'entête IPv4 peut également contenir une adresse si le paquet IPv4 est transmis à un seul destinataire. Dans ce cas le paquet unicast est transféré par le routeur sur l'interface de sortie, indiqué par la table de routage.
- **L'adresse broadcast** : est une adresse de diffusion. Elle n'apparaît que dans le champ *Destination Address* de l'entête IPv4. Dans ce cas, le paquet *broadcast* n'est diffusé qu'à l'intérieur du réseau et ne traverse pas le routeur qui interconnecte les réseaux. Un hôte recevant un paquet *broadcast* va traiter le paquet pour vérifier si l'application est active ou non.
- **L'adresse multicast** : est une adresse attribuée à une application multicast, permettant d'établir une communication multipoints entre les nœuds proposant la même adresse IP multicast. Elle n'apparaît que dans le champ *Destination Address* de l'entête IPv4. Comme le paquet broadcast, le paquet multicast est diffusé à l'intérieur du réseau. A la différence du paquet broadcast, le paquet multicast est également diffusé par le routeur.

II.4.1.1 Classe d'adressage IP :

On définit les classes d'adresses IPv4 qui correspond au tout premier mode de découpage de l'espace d'adressage. Un plan d'adressage à classe définit une frontière fixe entre le préfixe et le suffixe.

Les différentes classes ont chacune leurs spécificités en termes de répartition du nombre d'octet servant à identifier le réseau ou les ordinateurs connectés à ce réseau. Il existe 5 classes d'adresses IP. Chaque classe est identifiée par une lettre allant de A à E, les Trois premiers classe A, B et C sont définies pour les adresses *unicast*, la classe D est une classe d'adresse *multicast* et la classe E est réservée pour la recherche.

➤ Classe A

Le bit de poids fort du premier octet est à zéro. Le premier octet peut prendre la valeur comprise entre 0 et 127. Le premier octet est affecté au réseau et les trois octets suivants aux utilisateurs du réseau (figure II.3). Les réseaux disponibles en classe A sont donc les réseaux allant de **1.0.0.0** à **126.0.0.0**. Un réseau de classe A peut raccorder ($2^{24}-2$) utilisateurs [18].

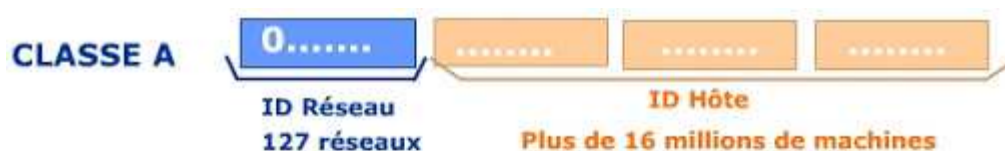


Figure II.3 : Adresse IPv4 de classe A.

- Les adresses de type **0.X.X.X** sont réservées. L'adresse **0.0.0.0** est utilisée par une station, dans le champ *Source Address* de l'entête IPv4, lorsqu'elle se configure dynamiquement. Ce paquet n'est pas transféré par un routeur et reste cantonné au réseau de l'utilisateur émetteur.
- Les adresses de type **127.X.X.X** sont réservées. Tout paquet émis vers l'adresse **127.0.0.1** (adresse de blocage) est retourné vers l'émetteur, sans être transmis sur le réseau. Elle permet d'effectuer un test interne à la machine.
- Les adresses de type **10.X.X.X** sont des adresses privées. Les paquets contenant ce type d'adresse ne doivent pas transiter dans le réseau public Internet.

Classe	Plage	Réseau	Adresse IP	Capacité
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8	10.X.X.X – 10.X.X.X	2 ⁰ réseaux, 2 ²⁴ hôtes

➤ Classe B

Le bit de poids fort du premier octet est à un et le bit suivant à zéro. Le premier octet peut prendre la valeur comprise entre 128 et 191 (Figure II.4). Les deux premiers octets sont affectés au réseau et les deux octets suivant aux utilisateurs du réseau. Les réseaux disponibles en classe B sont donc les réseaux allant de **128.0.0.0** à **191.255.0.0**. Un réseau de classe B peut raccorder ($2^{16}-2$) utilisateurs [18].



Figure II.4 : Adresse IPv4 de classe B.

- Les adresses de type **169.254.X.X** sont des adresses de type lien local (*Link-local*). Elles permettent à un utilisateur de se configurer automatiquement et de trafiquer dans un réseau lorsqu'un serveur DHCP ne peut être atteint. Les paquets contenant ce type d'adresse ne sont pas transférés par le routeur.
- Les adresses de type **172.16.X.X** à **172.31.X.X** sont des adresses privées. Les paquets contenant ce type d'adresse ne doivent pas transiter dans le réseau public Internet.

Classe	Plage	Réseau	Adresse IP	Capacité
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12	172.16.X.X - 172.31.X.X	24 réseaux, 2 ¹⁶ hôtes

➤ **Classe C :**

Les deux bits de poids fort du premier octet est à un et le bit suivant à zéro. Le premier octet peut prendre la valeur comprise entre 192 et 223 (Figure II.5). Les trois premiers octets sont affectés au réseau et l'octet suivant aux utilisateurs du réseau. Les réseaux disponibles en classe C sont donc les réseaux allant de **192.0.0.0** à **223.255.255.0**. Un réseau de classe C peut raccorder (2⁸-2) utilisateurs.



Figure II.5 : Adresse IPv4 de classe C.

- Les adresses de type **192.0.0.X** sont réservées.
- Les adresses de type **192.0.2.X**, **198.51.100.X** et **203.0.113.X** sont utilisées uniquement comme description dans une documentation. Elles ne sont pas routables dans un réseau public Internet.
- Les adresses de type **192.168.X.X** sont des adresses privées. Les paquets contenant ce type d'adresse ne doivent pas transiter dans le réseau public Internet.

Classe	Plage	Réseau	Adresse IP	Capacité
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16	192.168.0.X - 192.168.255.X	2 ⁸ réseaux, 2 ⁸ hôtes

- Les adresses de type **198.18.X.X** et **198.19.X.X** sont des adresses dédiées pour les tests d'évaluation des dispositifs d'interconnexion de réseaux.

➤ **Classe D**

Il s'agit d'une classe d'adressage spéciale, est prévue pour faire du "Multicast", ou multipoint contrairement aux trois premières classes qui sont dédiées à l' "unicast" ou point à point [19].

Les trois bits de poids fort du premier octet est à un et le bit suivant à zéro (Figure II.6). Le premier octet peut prendre la valeur comprise entre 224 et 239 [18].



Figure II.6 : Adresse IPv4 de classe D.

- Les adresses comprises entre **224.0.0.0** et **238.255.255.255** sont des adresses publiques.
- Les « adresses de type **224.0.0.X** sont réservées à des applications de contrôle non routables. Les adresses de type **224.0.1.X** sont réservées à des applications de contrôle routables (par exemple la distribution de l'heure).
- Les adresses de type **239.X.X.X** sont des adresses temporaires.

➤ Classe E

Il s'agit d'une classe expérimentale, la classe E. La norme précise "*Class E addresses are reserved for future use*" mais n'indique pas de quel futur il s'agit [19]. Les quatre bits de poids fort du premier octet est à un (Figure II.7). Le premier octet peut prendre la valeur comprise entre 240 et 255.



Figure II.7 : Adresse IPv4 de classe E.

- L'adresse **255.255.255.255** (tous les bits à un) est une adresse broadcast dont la diffusion est limitée au réseau. Un paquet broadcast ne traverse en aucun cas un routeur.

II.4.1.2 Espace d'adressage IP :

Classe	Masque réseau	Adresses réseau	Nombre de réseaux	Nombre d'hôtes
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0 - 239.255.255.255	Adresses uniques	Adresses uniques
E	Non défini	240.0.0.0 - 255.255.255.255	Adresses uniques	Adresses uniques

Tableau II.1 : Les différents espaces d'adressage pour chaque classe.

Le tableau précédent indique la décomposition d'une adresse IPv4 standard en espaces d'adressage hôte et réseau. Pour chaque classe, la plage de valeurs décimales du premier octet du numéro de réseau est indiquée en gras dans la colonne "Adresses réseau".

II.4.1.3 Les adresses particulières :

Lorsqu'on annule la partie *Host-id*, c'est-à-dire lorsqu'on remplace les bits réservés aux machines du réseau par des zéros, on obtient ce que l'on appelle l'adresse réseau. Cette adresse ne peut être attribuée à aucun des ordinateurs du réseau.

Lorsque la partie *Net-id* est annulée, c'est-à-dire lorsque les bits réservés au réseau sont remplacés par des zéros, on obtient l'adresse machine. Cette adresse représente la machine spécifiée par le host-ID qui se trouve sur le réseau courant.

Chaque réseau possède une adresse particulière dite de diffusion. Tous les paquets avec cette adresse de destination sont traités par tous les hôtes du réseau local. Lorsque tous les bits de la partie host-id sont à 1, l'adresse obtenue est appelée l'adresse de diffusion (en anglais *broadcast*). Il s'agit d'une adresse spécifique, permettant d'envoyer un message à toutes les machines situées sur le réseau spécifié par le *Net-ID*.

L'adresse **127.0.0.1** est appelée adresse de bouclage (en anglais *Loopback*), car elle désigne la machine locale (en anglais *Localhost*) [20]. On n'évite au maximum l'usage d'une telle adresse IP sur les réseaux.

Quelques exemples d'adresses avec une signification particulière :

0.0.0.0 : Hôte inconnu, sur ce réseau

0.0.0.1 : L'hôte 1 de ce réseau

255.255.255.255 : Tous les hôtes

138.195.52.1 : L'hôte **52.1** du réseau **138.195.0.0**

138.195.0.0 : Cet hôte sur le **138.195.0.0**

193.104.1.255 : Tous les hôtes du **193.104.1.0**

127.0.0.1 : Cet hôte (boucle locale).

II.4.1.4 L'utilisation d'un masque :

Un masque va préciser de manière certaine dans quel réseau se trouve une adresse IP et en conséquence :

- 1) L'adresse du réseau (appelée aussi numéro de réseau, non assignable)
- 2) L'adresse de Broadcast (adresse visant toutes les destinations, non assignable)

- 3) La plage d'adresses utilisables (de la première à la dernière en dehors des adresses précitées)

Un masque sera une suite de 32 bits divisée en 4 octets pointés composée uniquement d'abord d'une suite de 1 et, après, d'une suite de 0. La notation est aussi décimale pointée. Toutefois, on trouvera une autre notation dite CIDR (*Classless Inter-Domain Routing*) qui représente le nombre de bits pris par la partie réseau du masque [21].

Le nombre d'hôtes possibles obtenus ci-dessus correspond à l'application d'un masque par défaut sur un type de classe d'adresse :

- Le masque par défaut des adresses de Classe A est 255.0.0.0 ou /8
- Le masque par défaut des adresses de Classe B est 255.255.0.0 ou /16
- Le masque par défaut des adresses de Classe C est 255.255.255.0 ou /24

II.4.1.5 Méthode par calcul binaire :

L'adresse du réseau, l'adresse de Broadcast et la plage d'adresses utilisables peuvent être obtenues à partir d'un calcul booléen de type ET ou la conjonction logique (une proposition est vraie lorsque les deux termes sont tous les deux vrais) :

➤ Obtenir l'adresse du réseau :

Pour l'adresse IP 140.159.125.25, adresse de classe B à laquelle on applique un masque par défaut de 255.255.0.0 :

10001100.	10011111.	01111101.	00011001	140.159.125.25
11111111.	11111111.	00000000.	00000000	255.255. 0 . 0

10001100.	10011111.	00000000.	00000000	140.159. 0 . 0

L'adresse du réseau est donc 140.159.0.0. Elle est la première adresse de la plage.

➤ Obtenir l'adresse de Broadcast :

On va remplacer les bits de valeur 0 de la partie hôte du résultat obtenu pour l'adresse de réseau par des bits de valeur 1, soit les deux derniers octets maximisés :

10001100.	10011111.	00000000.	00000000	140.159. 0 . 0
-----------	-----------	-----------	----------	----------------

par

10001100.	10011111.	11111111.	11111111	140.159.255.255
-----------	-----------	-----------	----------	-----------------

:

➤ **Obtenir la plage d'adresses de ce réseau :**

La plage d'adresse du réseau sera comprise entre la première adresse utilisable et la dernière utilisable, autrement dit, celle qui suit l'adresse du réseau et celle qui précède l'adresse de Broadcast :

De : 10001100. 10011111. 00000000. 00000001 140.159. 0 . 1

à : 10001100. 10011111. 11111111. 11111110 140.159.255.254

II.5 Le routage IP :

Le routage IP fait partie intégrante de la couche IP de la suite TCP/IP. Le routage consiste à assurer l'acheminement d'un datagramme IP à travers un réseau en empruntant le chemin le plus court. Ce rôle est assuré par des machines appelées routeurs, c'est-à-dire des machines reliées (reliant) au moins deux réseaux si l'hôte récepteur se trouve dans un autre réseau: c'est le routeur indirect. Dans le cas contraire, l'expéditeur délivre le datagramme en effectuant un routage direct [10].

La route est représentée par la liste ordonnée des différentes machines intermédiaires et successives par lesquelles la communication s'effectue, ce choix de route s'appuie généralement sur le trafic et l'état de congestion du réseau au moment de l'envoi du message afin d'acheminer les paquets le plus rapidement possible, mais il peut aussi se baser sur des critères comme la fiabilité ou le coût de transmission.

Comme l'IP fonctionne selon un système de commutation par paquets, l'émetteur ne détermine donc pas l'intégralité de la route optimale et des routes optionnelles avant l'envoi, mais fonctionne suivant un système de routage par sauts successifs, en déterminant uniquement le premier routeur dans la direction de la destination. Lequel réalise la même opération, et ainsi de suite jusqu'à atteindre le réseau du destinataire. Ceci a aussi l'avantage d'éviter de maintenir une liste de routes exhaustive et complexe, et de laisser le choix du segment de route à l'appréciation de chaque routeur [19].

II.5.1 Principes de routage IP [22] :

- Routage IP 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.
- Les informations de routage sont mémorisées dans la table de routage des équipements (routeurs).
- Cette table doit être périodiquement mise à jour :
 - Manuellement : Routage Statique.

- Automatiquement : Routage Dynamique.
- Le routage s'effectue sur deux opérations: La sélection de la meilleure voie, La commutation du paquet sur l'interface appropriée.
- Faire la distinction entre protocole routable (IP, IPX) : comment les informations sont organisées pour être transportées sur le réseau.
- protocole de routage (RIP, OSPF, BGP, etc.):comment est réalisé l'acheminement des paquets.
- Routage Statique – Stations – Routeurs.
- Routage Dynamique – Échange périodique des tables de routage – Mise à jour automatique des tables de routage.

II.5.2 Routage statique :

Dans le **routage statique**, les administrateurs vont configurer les routeurs un à un au sein du réseau afin d'y saisir les routes (par l'intermédiaire de port de sortie ou d'IP de destination) à emprunter pour aller sur tel ou tel réseau. et le routeur d'après sera un autre pont entre deux autres réseaux (Figure II.8) :



Figure II.8 : *Fonctionnement de routage statique.*

Ici, l'administrateur a indiqué au qu'il connaît puisqu'il se situe sur le même réseau (B) que lui. Le routage statique permet donc à l'administrateur de saisir manuellement les routes sur les routeurs et ainsi de choisir lui-même le chemin qui lui semble le meilleur pour aller d'un réseau A à un réseau B. Si un no se créer sur le routeur 1 par exemple, il faudra indiquer au routeur le routeur 1 pour aller sur le réseau D [19].

II.5.3 Routage dynamique

Afin d'assurer la bonne transmission des datagrammes, tout comme nécessaire de maintenir régulièrement à jour les tables de routage de l'ensemble des routeurs d'un réseau.

Sur les gros réseaux, cette tâche devient rapidement irréalisable. Il faut alors mettre en place une solution de routage dynamique.

Le **routage dynamique** est un mécanisme par lequel les routeurs communiquent entre eux et peuvent alors se configurer les uns les autres de manière totalement automatique. Ainsi, on s'assure que les tables de routage sont à jour en reflétant multiples : optimisation du trafic, baisse des erreurs de transmission, gestion des surcharges,...

Le routage dynamique est implémenté par l'utilisation d'un protocole de routage. Divers protocoles existent que l'on peut regrouper en 2 catégories (Figure II.9) [19] :

- **IGP (Interior Gateway Protocol)** : Protocole de routage dynamique entre routeurs d'un même système autonome, c'est-à-dire dont la gestion dépend d'une administration unique (routeur vers internet d'un petit réseau local, ensemble des réseaux d'une multinationale, etc.) ; ce type de protocole privilégie la fiabilité et les plus courts chemins pour la rapidité de transmission ;
 - **RIP (Routing Information Protocol)** : Routage basé sur le nombre de routeurs intermédiaires entre deux réseaux ;
 - **OSPF (Open Shortest Path First)** : Routage basé sur l'état des liens entre deux réseaux.
- **EGP (Exterior Gateway Protocol)** : Protocole de routage dynamique entre routeurs de différents systèmes autonomes ; les règles de routage sont établies en fonction d'accords commerciaux, de considérations politiques ou de sécurité, etc.
 - **BGP (Border Gateway Protocol)** : Protocole utilisé pour l'internet afin de mettre à jour les informations de routage des quelques 20000 systèmes autonomes déployés dans le monde.

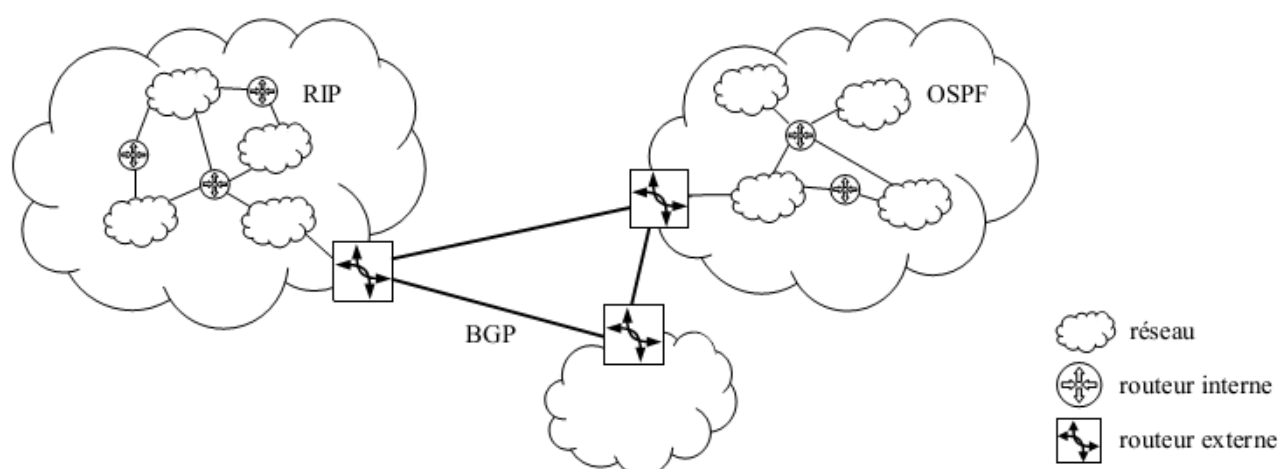


Figure II.9 : Internet : interconnexion de systèmes autonomes.

II.5.4 La différence entre le routage statique et dynamique :

Le routage est l'une des opérations les plus importantes du réseau informatique dans lequel le paquet de données est déplacé de la source à la destination en utilisant un chemin optimisé avec un délai faible; le chemin est élu à l'aide de techniques de routage.

La différence entre routage statique et dynamique réside dans la mise à jour des entrées de table. Dans le routage statique, les informations de routage sont mises à jour manuellement tandis que dans le routage dynamique, les informations sont automatiquement mises à jour à l'aide de protocoles. Les points suivants décrivent les principales différences [23] :

- Les routeurs sont configurés manuellement et la table est également créée manuellement dans le routage statique, tandis que dans le routage dynamique, la configuration et la création de table sont automatiques et pilotées par le routeur.
- Dans le routage statique, les itinéraires sont définis par l'utilisateur tandis que dans le routage dynamique, les itinéraires sont mis à jour en tant que modifications de topologie.
- Le routage statique n'utilise pas d'algorithmes complexes. Par contre, le routage dynamique utilise l'algorithme complexe pour calculer le chemin ou l'itinéraire le plus court.
- Le routage dynamique convient aux grands réseaux où le nombre d'hôtes est élevé. Inversement, le routage statique peut être implémenté dans un petit réseau.
- Lorsqu'un lien échoue dans le routage statique, le routage est interrompu et nécessite une intervention manuelle pour acheminer le trafic. En revanche, l'échec de liaison dans le routage dynamique ne perturbe pas le routage.
- Le message diffusé et la multidiffusion dans le routage dynamique le rend moins sécurisé. Tandis que, le routage statique n'implique pas de publicité qui le rend plus sûr.
- Le routage dynamique implique des protocoles tels que RIP, EIGRP, BGP, etc. Inversement, le routage statique ne nécessite pas de tels protocoles.
- Le routage statique n'a pas besoin de ressources supplémentaires alors que le routage dynamique nécessite des ressources supplémentaires telles que la mémoire, la bande passante, etc..

II.6 Conclusion :

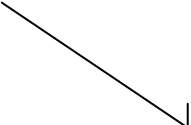
Le protocole IP, implanté dans tous les équipements du réseau (machines et routeurs), assure un service de remise des données non fiable et sans connexion. Il comprend la définition du plan d'adressage, la structure des informations transférées (le datagramme ou paquet IP) et les règles de routage.

Une adresse IP est un numéro d'identification qui est attribué de façon permanente ou provisoire à chaque périphérique relié à un réseau informatique qui utilise l'*Internet Protocol*.

L'adresse IP est à la base du système d'acheminement (le routage) des paquets de données sur Internet.

Pour compenser les problèmes de distribution de l'espace d'adressage IPv4, la première solution utilisée a consisté à découper une classe d'adresses IPv4 A, B ou C en sous-réseaux. Cette technique appelée *subnetting* et sera l'objectif de notre prochain chapitre, dans lequel nous nous intéresserons aux calculs des adresses IPv4, la notation CIDR et les masques de sous-réseaux de longueur fixe et variable, plus particulièrement le VLSM.

CHAPITRE III :



Découpage en des sous-réseaux, CIDR et VLSM

III.1 Introduction :

Le développement initial de l'adressage par classe a résolu temporairement le problème de la limitation à 256 réseaux. Dix ans plus tard, les plages d'adresses se faisaient de plus en plus rares. En réponse, le groupe de travail IETF a mis au point le routage inter domaine sans classe (CIDR), qui utilise la technique du masque de sous réseau de longueur variable (VLSM) afin d'optimiser l'espace d'adressage.

Avec l'utilisation du CIDR et du VLSM, les fournisseurs de service internet peuvent désormais attribuer un sous réseau à un client et un sous réseau différent à un autre client. Cette affectation d'adresses discontinues par les fournisseurs de service internet s'est accompagnée du développement de protocole de routage sans classe. A titre de comparaison : les protocoles de routage par classe effectuent toujours le regroupement par classe et n'incluent le masque de sous réseau dans les mises à jour de routage et ne nécessitent pas d'effectuer de regroupement de sous réseaux.

L'introduction de VLSM et de CIDR a obligé les administrateurs réseau à acquérir de nouvelles compétences en matière de découpage en sous réseaux. La technique VLSM découpe habituellement un réseau (ou sous réseau) en d'autre sous réseau. Les sous réseaux peuvent être eux même découpés en sous réseaux plus petits [24].

Ce chapitre a pour but d'une part décrire l'importance de découpage en des sous-réseaux, pour compenser les problèmes de distribution de l'espace d'adressage IPv4. D'autre part, l'exposition des solutions apportées pour tenter de compenser les problèmes de distribution de l'espace d'adressage. La première solution utilisée a consisté à découper une classe en utilisant un masque fixe, la deuxième permet l'exploitation de la notation CIDR et la technique VLSM, tout en optimisant l'attribution des adresses IP et offrir davantage de souplesse dans l'affectation du nombre adéquat d'hôtes et de sous-réseaux à l'aide de masques de longueurs différentes.

III.2 Découpage en sous-réseaux avec classe :

III.2.1 Construction de sous-réseaux :

La construction de sous-réseaux (*subnetting*) consiste à segmenter un même réseau, en plusieurs sous-réseaux de taille non nécessairement identiques, en utilisant des masques de sous-réseaux (*subnet mask*) différents.

Les intérêts de construire plusieurs sous-réseaux au sein d'un réseau sont divers :

- Organisation et gestion plus efficace des adresses IP par segment.
- Utilisation de technologies différentes sur chaque sous-réseau (Ethernet, Token Ring, FDDI, ATM, etc.).

- Services et applications dédiés par segment.
- Réduction de la charge globale du réseau avec amélioration du trafic dans chaque segment.
- Sécurisation de segments à l'intérieur du réseau.
- Nécessités liées à l'infrastructure (sites géographiques distants).

Le découpage de l'ensemble des nœuds d'un réseau en segments distincts est local, c'est-à-dire que l'identifiant du sous-réseau est obtenu en utilisant des bits de l'identifiant d'hôte de départ (Figure III.1). Le découpage en sous-réseau est donc invisible de l'extérieur du réseau considéré [19].

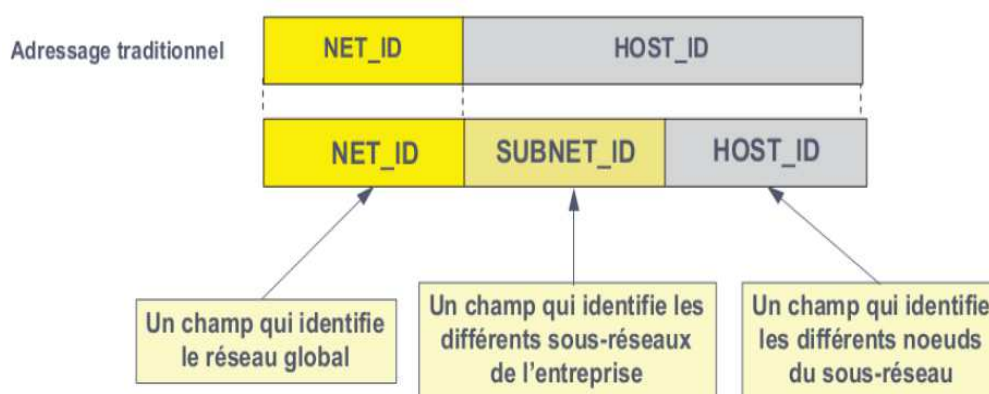


Figure III.1 : Position des identifiants de sous-réseau et d'hôte dans une adresse IPv4.

Pour calculer la partie sous-réseau d'une adresse IP, on effectue une opération ET logique (bit à bit) entre l'adresse et le masque. Pour trouver l'ensemble des sous-réseaux disponibles, on peut appliquer la formule $256 - X$ où X est le chiffre du dernier octet du masque

Pour calculer l'adresse de l'hôte, on effectue une opération ET (bit à bit) entre le complément à un du masque et l'adresse.

III.2.2 Méthode de calcul :

Pour illustrer le fonctionnement du découpage en sous-réseaux, on utilise un exemple pratique. On reprend l'exemple de la classe C **192.168.1.0** dont le masque réseau est par définition **255.255.255.0**. Sans découpage, le nombre d'hôtes maximum de ce réseau est de **254**. Considérant qu'un domaine de diffusion unique pour **254 hôtes** est trop important, on choisit de diviser l'espace d'adressage de cette adresse de classe C en **2 sous-réseaux**.

➤ Calcul de nombre de sous-réseaux

Si l'on utilise **1 bit** de la partie la plus significatif d'hôtes ➡ $2^1 = 2$ sous-réseaux. Donc on réserve **1 bit supplémentaire** du 4^{ème} octet en complétant le masque réseau. De cette façon on augmente la partie réseau de l'adresse IPv4 et on diminue la partie hôtes. cette dernière devienne $2^7 - 2 = 126$ machines par sous-réseau.

➤ Calcul du masque de sous-réseaux

Le masque de chaque sous-réseau est obtenu en rajoutant **1 bits** à **1** au masque initial (Figure III.2). Le masque de réseau par défaut est **255.255.255.0**,

Soit en binaire : **11111111 11111111 11111111 00000000**.

En ajoutant **1 bits** on obtient : **11111111 11111111 11111111 10000000**.

En fin, on a le masque de sous-réseau : **255.255.255.128**

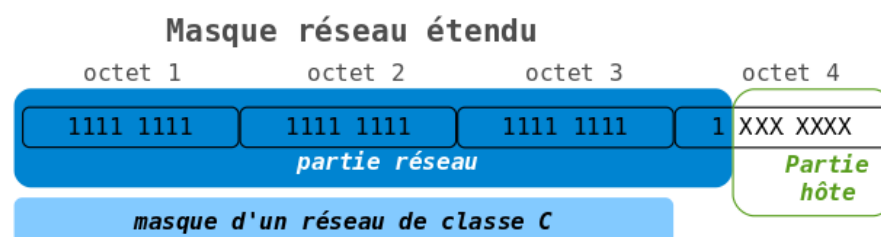


Figure III.2 : Calcul du masque de sous-réseau.

L'adresse du réseau 192.168.1.0, avec le masque (255.255.255.0) peut être considérée comme l'adresse réseau de 2 sous-réseaux différents, avec le masque complet après découpage en sous-réseaux (255.255.255.128).

➤ Calcul de l'adresse de chaque sous-réseaux

L'adresse du sous-réseau est la première adresse d'une plage d'adresse. Pour la trouver, rien de plus simple, vu que c'est la première, c'est l'adresse la plus basse, donc c'est l'adresse qui ne contient que des 0 dans la partie hôtes. Dans notre exemple, l'adresse de chaque sous-réseau sera constituée de 25 bits. (11111111 11111111 11111111 10000000), les 24 premiers bits seront ceux de l'écriture en binaire de **192.168.1**. Le bit suivant sera constitué du numéro du sous-réseau **0** (1^{er} sous-réseau) et **1** (2^{ème} sous-réseau). Donc 2 numéros de sous-réseau utilisables.

192.168.1.0xxx xxxx ➡ 192.168.1.0.

192.168.1.1xxx xxxx ➡ 192.168.1.128.

➤ Calcul de la plage d'adresses utilisables de sous-réseaux

La plage d'adresse du sous-réseau sera comprise entre la première adresse utilisable et la dernière utilisable, autrement dit, celle qui suit l'adresse du réseau et celle qui précède l'adresse de Broadcast. Le nombre d'hôtes pour chaque sous-réseau est calculé de la manière suivante ; **Nbr. de hôtes = $2^n - 2$** , ou **n** est le nombre de bits pour la nouvelle partie d'hôtes et **(-2)** pour écarter l'adresse de sous-réseau (tout les bits de la partie hôtes à 0) et l'adresse de diffusion de sous-réseau (tout les bits de la partie hôtes à 1).

Prenons le cas de l'adresse IP de premier sous-réseau : **192.168.1.0**. La plage d'adresses utilisables sera :

de **192.168.1.0000001** => **192.168.1.1** à **192.168.1.01111110** => **192.168.1.126**

Le nombre de machines dans ce sous-réseau est : $2^7 - 2 = 126$ machines.

Les mêmes démarches pour le deuxième sous-réseau : **192.168.1.128**. La plage d'adresses utilisables sera :

de **192.168.1.10000001** => **192.168.1.129** à **192.168.1.11111110** => **192.168.1.254**

Le nombre de machines dans ce sous-réseau sera le même que le premier sous-réseau.

➤ Calcul de l'adresse de diffusion (*Broadcast*)

Une adresse de diffusion est une adresse réseau à laquelle tous les machines connectées à un réseau de communication à accès multiple sont autorisés à recevoir des datagrammes [25]. Pour obtenir l'adresse de diffusion dans chaque sous-réseau; on met à **1** tous les bits de la partie d'hôtes.

L'adresse de diffusion de 1^{er} sous-réseau est **192.168.1.01111111**, soit **192.168.1.127**. et l'adresse de diffusion de 2^{ème} sous-réseau est **192.168.1.11111111**, soit **192.168.1.255**.

III.3 Découpage en sous-réseaux de base

Pour compenser les problèmes de distribution de l'espace d'adressage IP, la première solution utilisée a consisté à découper une classe d'adresses IP A, B ou C en sous-réseaux. Cette technique appelée "*subnetting*" a été formalisée en 1985. Si cette technique est ancienne, elle n'en est pas moins efficace face aux problèmes d'exploitation des réseaux actuels. Il ne faut jamais oublier que le découpage en réseaux ou sous-réseaux permet de séparer les domaines de diffusion. Les avantages de ce séparation de la diffusion réseau sont multiples.

III.3.1 Détermination du masque de sous-réseau :

Le masque de sous-réseau apporte au routeur l'information dont il a besoin pour déterminer le réseau et le sous-réseau. Le masque de sous-réseau permet de savoir quelle partie d'une adresse IP correspond à la partie numéro de réseau et laquelle correspond à la partie numéro de l'hôte. Un masque a la même longueur qu'une adresse IP. Il est constitué d'une suite de chiffres 1 terminée par (éventuellement) des chiffres 0 ; Autrement dit : il suffit de conserver les bits de l'adresse là où les bits du masque sont à 1 (un certain nombre de bits en partant de la gauche de l'adresse). La partie numéro d'hôte est contenue dans les bits qui restent (les plus à droite).

Les critères à prendre en considération pour la détermination d'un masque de sous-réseau sont [19] :

- L'espace de numérotation des hosts, c'est-à-dire le nombre de machines à numéroté et l'évolution probable de ce nombre (nombre de bits du champ "Host_ID") ;
- L'espace de numérotation des sous-réseaux, c'est-à-dire le nombre de sous-réseaux à distinguer et l'évolution probable de ce nombre (nombre de bits du champ "SubNet_ID") ;
- La lisibilité, c'est-à-dire permettre par simple lecture d'identifier facilement le sous-réseau concerné.

On fabrique un masque contenant des 1 aux emplacements des bits que l'on désire conserver, et des 0 pour ceux que l'on veut rendre égaux à zéro. Une fois ce masque créé, il suffit de faire un ET logique entre la valeur que l'on désire masquer et le masque afin de garder intacte la partie que l'on désire et annuler le reste.

III.3.2 Découpage selon le nombre d'hôtes :

Etant donné que le masque détermine le nombre de machines qu'il pourra y avoir sur un réseau, c'est souvent de cette information que l'on part pour choisir le masque. Etant donné que l'on travaille en binaire, le nombre de machines possible au sein d'un réseau sera une puissance de 2. Pour un nombre donné de machines, il faudra donc choisir la puissance de 2 immédiatement supérieure pour pouvoir adresser les machines.

De plus, il faudra prévoir un certain nombre d'adresses supplémentaires pour accueillir de nouvelles machines. Il va donc falloir résoudre la petite équation :

$$2^n - 2 \geq M \quad (\text{III.1})$$

Tel que ***n*** représente le nombre de bits dans la partie hôtes (en partant de la fin) où va être codé le masque et ***M*** représente le nombre de machines [26].

La meilleure façon pour expliquer la méthode de *subnetting* (ou la création de sous-réseaux) consiste à utiliser un exemple. Par exemple, l'adresse réseau **192.168.116.0** est associée au masque de sous-réseau par défaut **255.255.255.0**. L'exigence est de réaliser des sous-réseaux de manière à pouvoir créer autant de sous-réseaux que possible avec **30 hôtes** dans chaque sous-réseau.

Notre première étape consistera à déterminer le nombre de bits que nous devons emprunter pour la partie hôte de manière à satisfaire à l'exigence d'au moins 30 hôtes par sous-réseau en utilisant la formule (III.1).

Nous pouvons calculer le nombre de bits requis pour que chaque sous-réseau ait 30 adresses d'hôte. $2^5 - 2 = 30$, donc **5 bits** au moins doivent être disponibles pour l'adressage hôte et le reste peut être emprunté pour créer des adresses de sous-réseau Le - 2 dans la

formule représente les deux adresses l'adresse de sous-réseau et l'adresse de diffusion qui ne peuvent pas être attribuées à des hôtes.

Le réseau **192.168.116.0** a **8 bits** pour la partie hôte et nous allons réserver **5 bits** pour la nouvelle partie hôte. Les **3 bits** restants peuvent maintenant être utilisés pour créer des sous-réseaux. Pour déterminer le nombre de sous-réseaux **N** que nous pouvons créer, utilisez la formule suivante :

$$N = 2^n \quad (\text{III.2})$$

où l'exposant n est constitué de bits empruntés de la partie hôte. Ainsi, dans ce cas, nous pouvons créer $2^3 = 8$ sous-réseaux.

Notre deuxième étape consistera à calculer le nouveau masque de sous-réseau. Notre précédent masque était de **255.255.255.0** ou **11111111.11111111.11111111.00000000** en binaire. Comme nous avons emprunté **3 bits** de la partie hôte, notre nouveau masque de sous-réseau sera **11111111.11111111.11111111.11100000**, soit **255.255.255.224** lorsqu'il est converti en notation décimale.

Notre dernière étape consistera à lister l'adresse du sous-réseau, la plage d'hôtes et l'adresse de diffusion. La première adresse de sous-réseau sera 192.168.116.0/27 et les sous-réseaux suivants auront des incréments de 32 (Le nombre d'adresses maximal dans chaque sous-réseau).

Le tableau ci-dessous présente les adresses de sous-réseau, leurs plages d'adresses utilisables respectives et les adresses de diffusion.

Sous-réseau	Adresse de sous-réseau	Plage d'adresses utilisables	Diffusion
1	192.168.116.0/27	192.168.116.1 – 192.168.116.30	192.168.116.31
2	192.168.116.32/27	192.168.116.33 – 192.168.116.62	192.168.116.63
3	192.168.116.64/27	192.168.116.65 – 192.168.116.94	192.168.116.95
4	192.168.116.96/27	192.168.116.97 – 192.168.116.126	192.168.116.127
5	192.168.116.128/27	192.168.116.129 – 192.168.116.158	192.168.116.159
6	192.168.116.160/27	192.168.116.161 – 192.168.116.190	192.168.116.191
7	192.168.116.192/27	192.168.116.193 – 192.168.116.222	192.168.116.223
8	192.168.116.224/27	192.168.116.225 – 192.168.116.254	192.168.116.255

Tableau III.1 : Résultat de calcul des sous-réseaux.

Comme indiqué dans le tableau, l'adresse de diffusion sera la dernière adresse du sous-réseau. Par exemple, pour le sous-réseau **192.168.116.0**, l'adresse de diffusion sera **192.168.1.31**, qui est la dernière adresse de ce sous-réseau.

III.3.3 Selon le nombre de sous-réseaux :

Comme nous avons expliqué précédemment, chaque réseau IP utilise deux adresses qui ne sont plus disponibles pour les adresses d'interfaces (hôtes), le numéro de réseau IP lui-même, et l'adresse de diffusion sur ce réseau. Quand vous découpez en sous-réseaux, chaque sous-réseau a besoin de ses propres adresses de réseau et de diffusion et celles-ci doivent être des adresses valides, dans l'intervalle fourni par le réseau IP que nous découpons.

Donc, en découpant un réseau IP en 2 sous-réseaux séparés, on a alors deux adresses de réseau et 2 adresses de diffusion, augmentant le nombre d'adresses 'inutilisables' pour les interfaces (hôtes). Créer 4 sous-réseaux crée 8 adresses inutilisables, et ainsi de suite...

En fait, le plus petit sous-réseau utilisable est composé de 4 adresses IP :

- Deux adresses IP d'hôtes
- Une adresse de réseau.
- Une adresse de diffusion

On peut découper l'adresse de réseau IP en 2^n sous-réseaux de tailles égales (où n est le nombre de bits de la partie hôtes dans notre numéro de réseau).

Pour mettre en œuvre le découpage en sous-réseaux, on réserve n bits parmi les bits de la partie hôtes, et on les interprète localement comme faisant partie des bits de réseau. Donc, pour diviser une adresse de réseau en **2 sous-réseaux**, on réservera **1 bit** de la partie hôtes en positionnant à '1' le bit approprié dans le masque des **2 sous-réseaux** (le premier bit gauche de la partie d'hôtes).

Pour notre adresse de réseau de classe C : **192.168.116.0**, voici quelqu'une des options de découpage en sous-réseaux possibles :

Nombre n	Nombre de sous-réseaux	Nombre d'hôtes par sous-réseau	Masque de sous-réseaux	4 ^{eme} octet du masque
1	2	126	255.255.255.128	10000000
2	4	62	255.255.255.192	11000000
3	8	30	255.255.255. 224	11100000
4	16	14	255.255.255.240	11110000
5	32	6	255.255.255.248	11111000
6	64	2	255.255.255.252	11111100

Tableau III.2 : Options de découpage en sous-réseaux possibles.

Pour réaliser un découpage en **8 sous-réseaux**, On réserve **3 bits** supplémentaires du 4^{ème} octet en complétant le masque réseau. De cette façon on augmente la partie réseau de **3 bits** et on diminue la partie hôte à **5 bits**. Pour ces 5 bits de la nouvelle partie hôtes, le nombre d'hôtes pour chaque sous-réseau est $2^5 - 2 = 30$.

vous devez maintenant trouver facilement quelles sont les différentes adresses de sous-réseau et de diffusion et la plage d'adresses utilisables pour chacun de ces réseaux.

III.4 Découpage en des sous-réseaux sans classe :

III.4.1 Le CIDR :

Les RFC1518 (historique) et RFC4632 (technique) consacrent la méthode CIDR, routage sans classe inter-domaine, comme méthode de gestion et d'organisation plus efficace des adresses Internet. Concrètement cela signifie que [18] :

- Une adresse est toujours accompagnée de son masque identifiant son appartenance à un réseau (domaine de Broadcast)
- La notion de classe d'adresse IPv4 disparaît dans la pratique.
- La notion de blocs identifiant des domaines de routage remplace la notion de classe d'adresse IPv4, rendant l'usage d'un masque indispensable.
- Pour simplifier la notation, on préfère représenter un slash / + le nombre de bits à 1 dans le masque. Par exemple **/26** au lieu de **255.255.255.192**.
- Les blocs sont variables, peuvent être agrégés ou découpés dans les informations de routage ou dans les plans d'adressage.
- Ces blocs sont des ensembles homogènes (les adresses se suivent) d'adresses en base 2 : 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, ..., 65536, ... adresses.
- Le RFC950 reste une référence en matière de calculs (numéro de réseau, Broadcast, plage d'adresses).

III.4.1.1 La notion CIDR

La notation CIDR (*Classless Inter-Domain Routing*) permet de spécifier dans l'adresse IP elle-même le nombre de bits significatifs constituant la partie réseau de l'adresse, elle représente le nombre de bits pris par la partie réseau du masque.

Au lieu de représenter le masque d'une adresse en notation décimale pointée, le CIDR propose de noter une adresse suivie de /"nombre de bits à 1", le nombre de bits à zéro qui reste représente la taille du bloc [21].

Par exemple, la notation CIDR pourrait ressembler à ceci: 255.255.255.192 /26. Le /26 vous indique que les 26 premiers bits de l'adresse IP sont utilisés pour le routage réseau et que celui du masque de sous-réseau contient 26 bits binaires définis sur 1, ce qui est également vrai pour chaque adresse IP d'hôte.

À partir du préfixe /26, vous pouvez également déterminer le nombre d'adresses IP dédiées à la spécification d'un ID d'hôte. Etant donné qu'une adresse IPv4 contient 32 bits, cela signifie que les 6 bits restants sont utilisés pour calculer les ID d'hôte. Il est utile de connaître les masques par défaut :

- Classe A : 255.0.0.0 : /8
- Classe B : 255.255.0.0 : /16
- Classe C : 255.255.255.0 : /24

Le tableau suivant récapitule le nombre d'adresses hôtes disponibles pour chaque type de notation CIDR. Vous pouvez l'utiliser pour convertir entre la notation CIDR, le masque de réseau et les informations d'hôte.

Il y a deux adresses hôtes supprimés, car ces deux adresses sont toujours réservées pour le réseau et broadcast [23].

Notation CIDR	Nombre total d'adresses	Nombre d'hôtes	Masque de réseau
/30	4	2	255.255.255.252
/29	8	6	255.255.255.248
/28	16	14	255.255.255.240
/27	32	30	255.255.255.224
/26	64	62	255.255.255.192
/25	128	126	255.255.255.128
/24	256	254	255.255.255.0
/23	512	510	255.255.254.0
/22	1,024	1,022	255.255.252.0
/21	2,048	2,046	255.255.248.0
/20	4,096	4,094	255.255.240.0
/19	8,192	8,190	255.255.224.0
/18	16,384	16,382	255.255.192.0
/17	32,768	32,766	255.255.128.0
/16	65,536	65,534	255.255.0.0
/15	131,072	131,070	255.254.0.0
/14	262,144	262,142	255.252.0.0
/13	524,288	524,286	255.248.0.0
/12	1,048,576	1,048,574	255.240.0.0
/11	2,097,152	2,097,150	255.224.0.0

/10	4,194,304	4,194,302	255.192.0.0
/9	8,388,608	8,388,606	255.128.0.0
/8	16,777,216	16,777,214	255.0.0.0
/7	33,554,432	33,554,430	254.0.0.0
/6	67,108,864	67,108,862	252.0.0.0
/5	134,217,728	134,217,726	248.0.0.0
/4	268,435,456	268,435,454	240.0.0.0
/3	536,870,912	536,870,910	224.0.0.0
/2	1,073,741,824	1,073,741,822	192.0.0.0
/1	2,147,483,648	2,147,483,646	128.0.0.0
/0	4,294,967,296	4,294,967,294	0.0.0.0

Tableau III.3 : Le nombre d'adresses hôtes disponibles pour chaque type de notation CIDR.

III.4.1.2 Principe de CIDR

Le CIDR a été mis au point afin (principalement) de diminuer la taille de la table de routage contenue dans les routeurs. Ce but est atteint en agrégeant plusieurs entrées de cette table en une seule.

Avec l'ancien système, à chaque fois qu'un fournisseur d'accès désirait se voir attribuer plusieurs " classe C ", cela créait autant d'entrées dans la table de routage (vers lui) que de réseaux alloués. D'autre part, les plages d'adresses de classe A et B étaient (et sont encore...) largement sous-utilisées.

La première évolution a été de rendre obsolète (et en fait abolir) la distinction entre les adresses de classe A, B ou C, de sorte que l'ensemble de l'espace puisse être géré comme une collection unique de sous-réseaux de classe A, B ou C. Avec cette évolution, il est devenu impossible de déduire la classe effective (ou le masque de sous-réseau) d'une adresse IPv4 simplement en comptant les premiers bits de poids fort positionnés à 1.

Depuis lors, pour connaître la taille maximale du sous-réseau contenant une adresse IPv4, il faut consulter le serveur whois du registre régional où le bloc d'adresses a été réservé, mais ce bloc peut encore être lui-même sous-divisé localement en sous-réseaux par le réservataire. Les protocoles nécessitant la connaissance de la taille du sous-réseau ont été revus en rendant nécessaire la spécification effective du masque de sous-réseau (l'ancien algorithme de détermination ne fonctionne plus).

Cependant cette évolution était insuffisante pour servir la communauté des utilisateurs Internet. Il était nécessaire de pouvoir créer des sous-réseaux indépendants plus petits que /24, ou plus grands sans atteindre toutefois la taille d'un réseau /16 (ce qui aurait gaspillé des ressources d'adressage).

Le CIDR, au contraire, permet le regroupement de plusieurs " classe C " pour les considérer comme un seul bloc, et donc avec l'effet de ne créer qu'une seule entrée dans la table de routage là où il y en avait plusieurs. De même il permet de gérer une granularité plus fine des allocations, avec un choix nettement plus étendu de tailles de sous-réseaux [27].

III.4.2 Le VLSM :

La technique VLSM (*Variable-Length Subnet Masks*) est une simple extension du découpage en sous-réseaux de base, où une même adresse de classe A, B ou C est découpée en sous-réseaux à l'aide de masques de longueurs différentes.

La VLSM permet d'optimiser l'attribution des adresses IP et offre davantage de souplesse dans l'affectation du nombre adéquat d'hôtes et de sous-réseaux, à partir d'un nombre limité d'adresses IP.

Au fur et à mesure de l'expansion des sous-réseaux IP, les administrateurs ont cherché des solutions pour utiliser l'espace d'adressage plus efficacement. Une des techniques existantes s'appelle VLSM. Avec VLSM, un administrateur réseau peut utiliser un masque long sur les réseaux qui ne comportent pas beaucoup d'hôtes et un masque court sur les sous-réseaux qui comportent beaucoup d'hôtes.

La technique VLSM permet à une entreprise d'utiliser plusieurs sous masques dans le même espace d'adressage réseau. La mise en œuvre de VLSM est souvent appelée « subdivision d'un sous-réseau en sous-réseaux » et peut être utilisée pour améliorer l'efficacité de l'adressage.

VLSM est simplement une fonction qui permet à un système autonome unique d'inclure des réseaux avec différents masques de sous-réseau.

Auparavant, il était recommandé de ne pas utiliser le premier et le dernier sous-réseau. L'utilisation du premier sous-réseau (appelé sous-réseau zéro) pour l'adressage d'hôtes était déconseillée en raison de la confusion possible lorsqu'un réseau et un sous-réseau ont la même adresse. Pour la même raison, l'utilisation du dernier sous-réseau (appelé sous-réseau tout à 1) était également déconseillée.

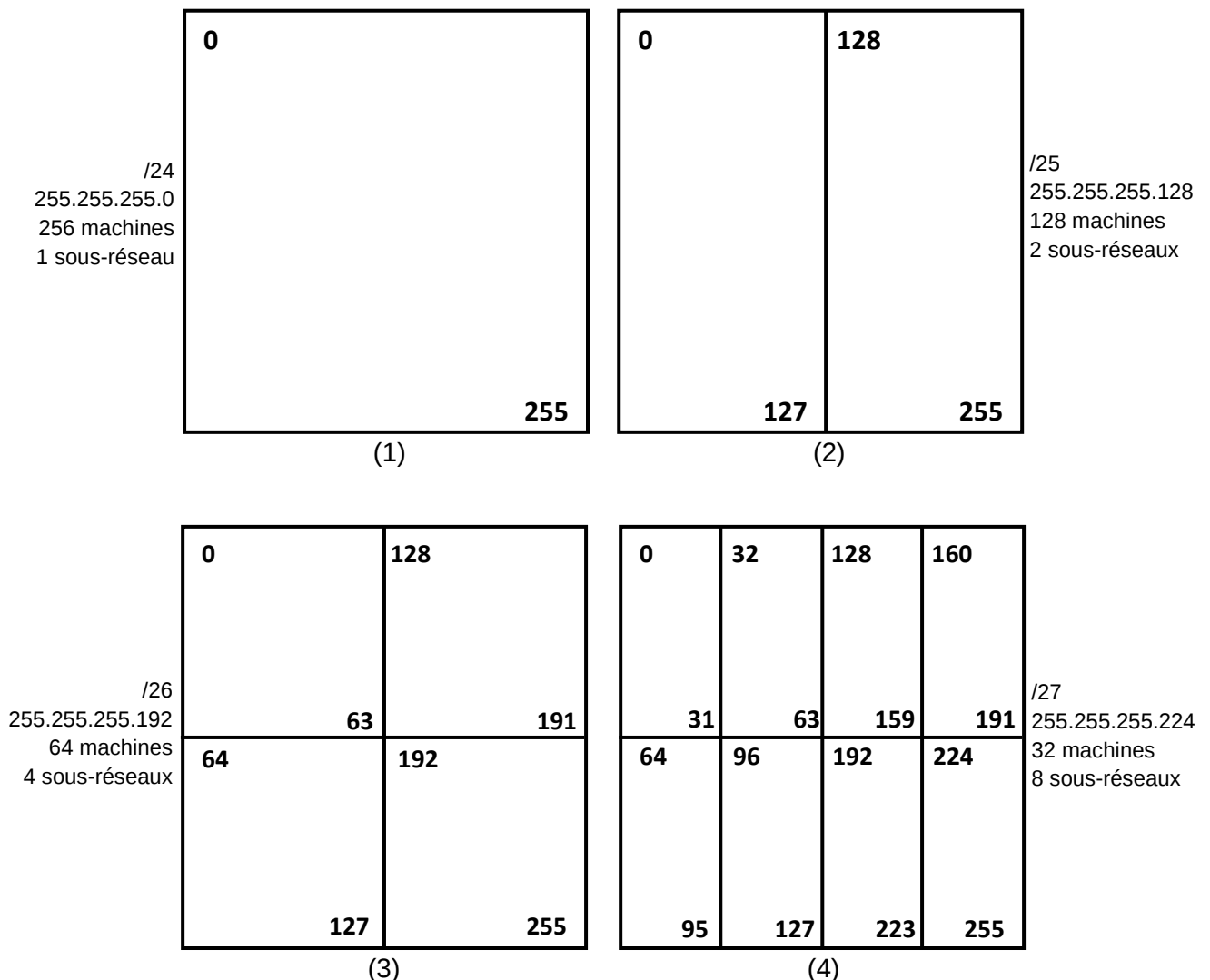
On pouvait utiliser ces sous-réseaux, mais ce n'était pas une pratique recommandée. Avec l'évolution des technologies de réseau et la pénurie anticipée d'adresses IP, il est devenu acceptable d'utiliser le premier et le dernier sous-réseau dans un réseau subdivisé en sous réseaux, en association avec la technique VLSM [28].

III.4.2.1 Les différentes méthodes de VLSM

III.4.2.1.1 Méthode de boîte

La méthode de box (*the box method*) est un moyen simple de visualiser la répartition des sous-réseaux et des adresses en plus petite taille. En ombrant ou en coloriant les cases, on peut facilement caser notre sous-réseau sans chevaucher nos adresses. On ajuste chaque sous-réseau à la taille correcte requise (Figure III.3).

- (1). Commencer par un carré. Le carré entier est un seul sous-réseau composé de 256 adresses.
- (2). Diviser le carré en deux et obtenir 2 sous-réseaux avec 128 adresses chacun.
- (3). Diviser la boîte en quartiers et obtenir 4 sous-réseaux avec 64 adresses.
- (4). Diviser chaque carré individuel et obtenir au moins 8 sous-réseaux avec 32 adresses.
- (5). Diviser à nouveaux la boîte en deux et obtenir 16 sous-réseaux avec 16 adresses.
- (6). La prochaine division donne 32 sous-réseaux avec 8 adresses.
- (7). La dernière division donne 64 sous-réseaux avec 4 adresses chacun.



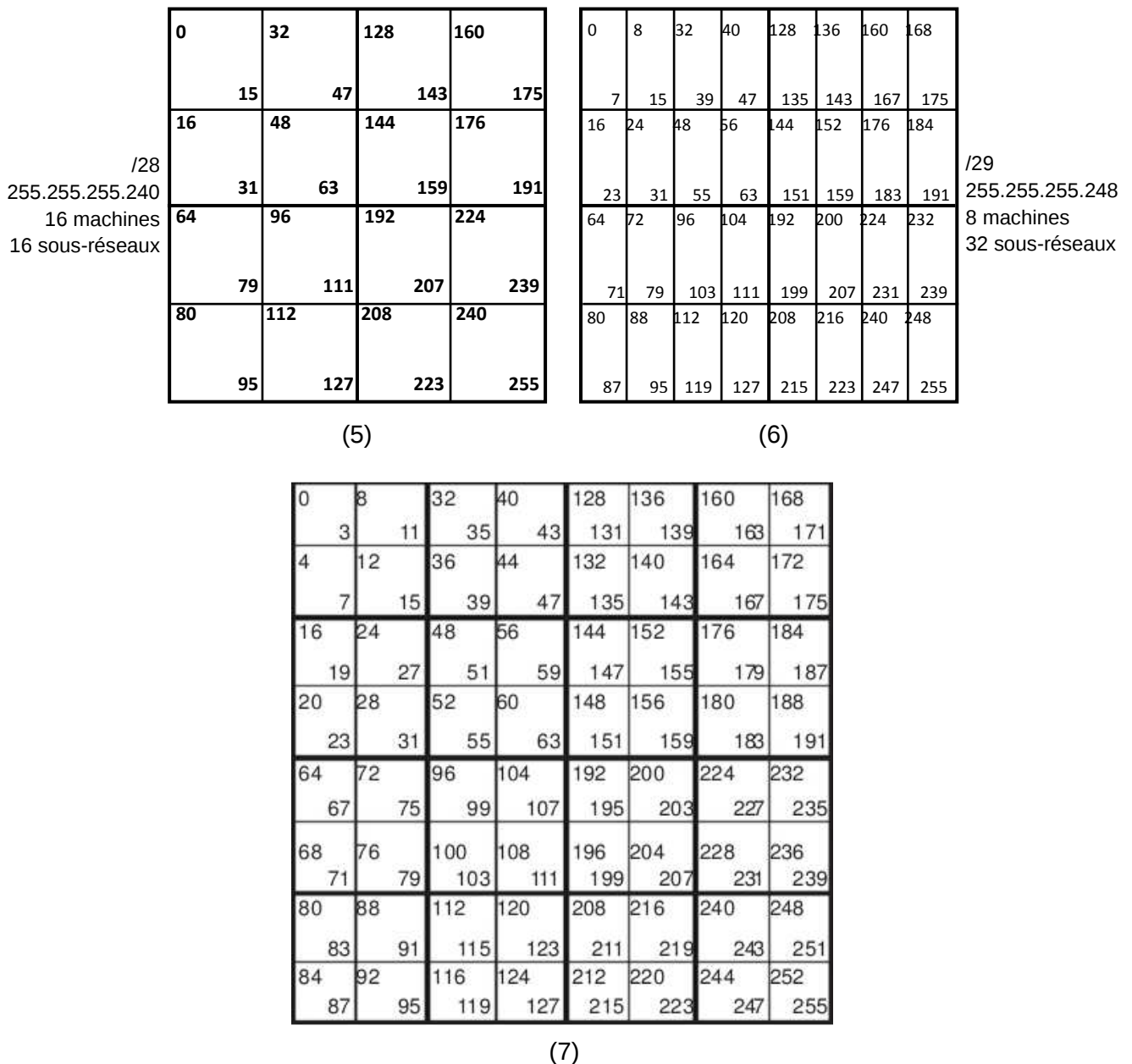


Figure III.3 : Découpage en sous-réseaux par la méthode de boîte.

Exemple :

À l'aide du diagramme de réseau (Figure III.4) et des informations fournies, créez un schéma d'adressage qui utilise des masques de sous-réseau de longueur variable (VLSM). Affichez l'adresse du sous-réseau et le CIDR dans un tableau, coloriez ou ombrez les sous-sous-réseaux utilisés dans la case.

Cette société utilisera l'adresse de classe C : 192.168.16.0. Commencer par le sous-réseau la plus grand en premier.

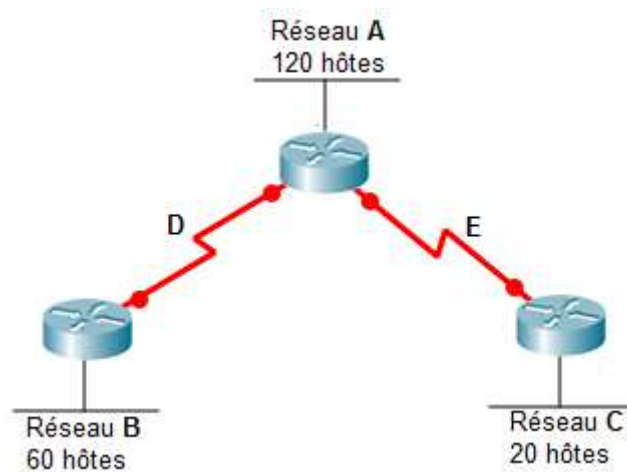


Figure III.4 : Exemple de découpage par la méthode de boî.

Résultat :

S.R	Hôtes	Adresse du S.R /CIDR
A	120	192.168.16.0 /25
B	60	192.168.16.128 /26
C	20	192.168.16.192 /27
D	2	192.168.16.224 /30
E	2	192.168.16.228 /30

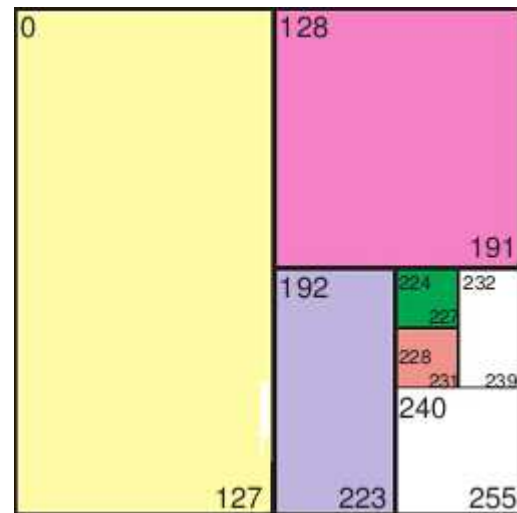


Figure III.5 : Résultat de calcul de découpage par la méthode de boî.

III.4.2.1.2 La méthode numérique

La méthode numérique étend la technique d'adressage IP avec classe et de sous réseaux pour permettre un sous réseaux sans classe. Commence par répertorier les hôtes nécessaires par des sous-réseaux du plus grand au plus petit.

Etape 1 : Dans l'exemple de la figure III.4, le groupe d'hôtes requis est ; 120 Réseau A, 60 Réseau B, 20 Réseau C, 2 Réseau D et 2 Réseau E

Etape 2 : On dispose l'adresse IP de la même manière que dans l'adressage IP avec classe, montrant les valeurs binaires des bits, le nombre de sous-réseaux et le nombre d'hôtes.

	256	128	64	32	16	8	4	2	- Nombre d'hôtes
Nombre de sous-réseaux	2	4	8	16	32	64	128	256	
	128	64	32	16	8	4	2	1	- Valeurs binaires
192. 168 . 16 . 0	0	0	0	0	0	0	0	0	

Etape 3 : On trace une ligne permettant 120 hôtes, en utilisant la valeur du dernier bit gauche ou du nombre magique, on écrit dans la première plage puis on ajoute l'adresse de sous-réseau pour démarrer la deuxième plage.

	256	128	64	32	16	8	4	2	- Nombre d'hôtes
Nombre de sous-réseaux	2	4	8	16	32	64	128	256	
	128	64	32	16	8	4	2	1	- Valeurs binaires
192. 168 . 16 . 0	0	0	0	0	0	0	0	0	
<u>Hôtes</u>	<u>Pages d'adresses</u>							<u>CIDR</u>	
120	192.168.16.0 à 192.168.16.127							/25	
	192.168.16.128 à								

Etape 4 : On trace une deuxième ligne pour les 60 hôtes. Utilisant la valeur du dernier bit gauche ou le nombre magique pour disposer le deuxième plus grand sous-réseau, ajoutant ensuite l'adresse de sous-réseaux qui commencera la troisième plage.

	256	128	64	32	16	8	4	2	- Nombre d'hôtes
Nombre de sous-réseaux	2	4	8	16	32	64	128	256	
	128	64	32	16	8	4	2	1	- Valeurs binaires
192. 168 . 16 . 0	0	0	0	0	0	0	0	0	
<u>Hôtes</u>	<u>Pages d'adresses</u>							<u>CIDR</u>	
120	192.168.16.0 à 192.168.16.127							/25	
60	192.168.16.128 à 192.168.16.191							/26	
	192.168.16.192 à								

Etape 5 : Nous continuons le même processus jusqu'à tous les sous-réseaux sont pris en compte, le CIDR est le nombre de bits empruntés pour la partie réseau et sous-réseau de l'adresse.

	256	128	64	32	16	8	4	2	- Nombre d'hôtes
Nombre de sous-réseaux	2	4	8	16	32	64	128	256	
	128	64	32	16	8	4	2	1	- Valeurs binaires
192. 168 . 16 . 0	0	0	0	0	0	0	0	0	
<u>Hôtes</u>	<u>Pages d'adresses</u>							<u>CIDR</u>	
120	192.168.16.0 à 192.168.16.127							/25	
60	192.168.16.128 à 192.168.16.191							/26	
20	192.168.16.192 à 192.168.16.223							/27	
2	192.168.16.224 à 192.168.16.228							/30	
2	192.168.16.228 à 192.168.16.231							/30	

III.4.2.1.3 La méthode graphique

Le graphique VLSM est la troisième méthode utilisée pour visualiser la répartition des sous-réseaux et des adresses en plus petites tailles. En ombrant ou en colorant les cases pour pouvoir facilement casser les sous-réseaux sans chevaucher les adresses, pouvant ajuster chaque sous-réseau à la taille correcte requise [29].

Exemple :

On prend le même exemple des deux premières méthodes. En utilisant le même diagramme de réseau et les mêmes informations fournis, on crée un schéma d'adressage qui utilise des masque de sous réseau de longueur variable. En affichant l'adresse du sous-réseau et le CIDR dans les cases ci-dessous, coloriez ou ombrez les sous-sous-réseaux utilisés dans le graphique (Figure III.6).

/24	/25	/26	/27	/28	/29	/30
255.255.255.0 256 Hosts	255.255.255.128 128 Hosts	255.255.255.192 64 Hosts	255.255.255.224 32 Hosts	255.255.255.240 16 Hosts	255.255.255.248 8 Hosts	255.255.255.252 4 Hosts
0 - 255	0-127	0-63	0-31	0-15	0-7	0-3
						4-7
			16-31		8-15	8-11
						12-15
		64-127	32-63		16-23	16-19
						20-23
			48-63		24-31	24-27
						28-31
		128-191	64-95		32-39	32-35
						36-39
			80-95		40-47	40-43
						44-47
		192-255	96-127		48-55	48-51
						52-55
			112-127		56-63	56-59
						60-63
		224-255	128-159		64-71	64-67
						68-71
			144-159		72-79	72-75
						76-79
		248-255	160-191		80-87	80-83
						84-87
			176-191		88-95	88-91
						92-95
		252-255	192-207		96-103	96-99
						100-103
			208-223		104-111	104-107
						108-111
		256-259	224-239		112-119	112-115
						116-119
			240-255		120-127	120-123
						124-127
		260-263	248-255			128-131
						132-135
			256-259		128-135	136-139
						140-143
		264-267	260-263		144-151	144-147
						148-151
			264-267		152-159	152-155
						156-159
		268-271	268-271		160-167	160-163
						164-167
			272-275		168-175	168-171
						172-175
		276-279	276-279		176-183	176-179
						180-183
			280-283		184-191	184-187
						188-191
		284-287	284-287		192-199	192-195
						196-199
			288-291		200-207	200-203
						204-207
		292-295	292-295		208-215	208-211
						212-215
			296-299		216-223	216-219
						220-223
		300-303	300-303		224-231	224-227
						228-231
			304-307		232-239	232-235
						236-239
		308-311	308-311		240-247	240-243
						244-247
			312-315		248-255	248-251
						252-255

Figure III.6 : Graphique VLSM des adresses de classe C 24-30 bits (4^{ème} octet) [29].

III.4.2.2 Découpage VLSM d'un réseau :

La technique VLSM n'est pas seulement utile aux principaux fournisseurs d'accès Internet (Internet Service Provider ou ISP). Un administrateur possédant plus d'un sous-réseau peut utiliser cette technique pour utiliser son espace assigné plus efficacement. Considérons l'exemple ci-dessous :

Le fournisseur d'accès a attribué le réseau **198.51.100.0** avec le masque **255.255.255.128** ; soit l'adresse réseau **198.51.100.0 /25**. On dispose donc de la moitié du réseau 198.51.100.0/24.

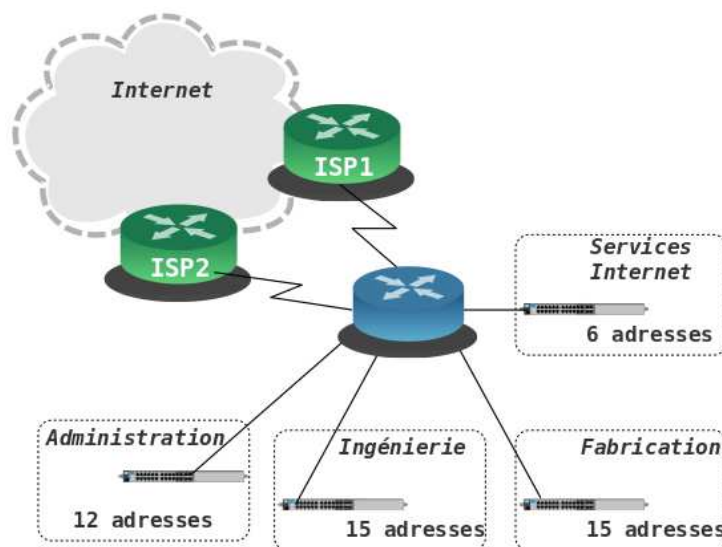


Figure III.7 : Exemple de découpage VLSM d'un réseau.

La figure III.7 donne plusieurs indication qui vont permettre de découper le réseau 198.51.100.0/25 en autant de sous-réseaux que de périmètres définis. Une interface de routeur délimite un domaine de diffusion et un domaine de collision. Chaque interface de routeur de la figure désigne donc un réseau IP distinct.

Chaque périmètre définit le nombre d'hôtes présent dans le domaine de diffusion. Pour permettre une évolution de ce nombre d'hôtes dans le futur, on choisit de le doubler pour chaque périmètre de type LAN (trait droit sur le schéma ci-dessus). On s'intéresse donc en premier lieu à la colonne la plus à droite du tableau ci-dessous pour compléter chaque ligne.

Nom	Sous-réseau	CIDR	Masque	Plage d'adresses	Hôtes
Fabrication	198.51.100.0	/27	255.255.255.224	192.51.100.1 - 192.51.100.30	30
Ingénierie	198.51.100.32	/27	255.255.255.224	192.51.100.33 - 192.51.100.62	30
Administration	198.51.100.64	/27	255.255.255.224	192.51.100.65 - 192.51.100.94	30
Services Internet	198.51.100.96	/28	255.255.255.240	192.51.100.97 - 192.51.100.110	14
Liaison ISP1	198.51.100.112	/30	255.255.255.252	192.51.100.113 - 192.51.100.114	2
Liaison ISP2	198.51.100.116	/30	255.255.255.252	192.51.100.116 - 192.51.100.118	2

Tableau III.4 : Découpage du réseau 198.51.100.0/25 avec VLSM.

On note que le nombre maximum d'adresses d'hôtes disponibles correspond à l'espace d'adressage du sous-réseau moins deux. C'est parce que la première adresse désigne le réseau et que la dernière est l'adresse de diffusion vers tous les hôtes du sous-réseau. Lorsque l'on planifie les espaces d'adressage VLSM, il est préférable de doubler le nombre d'adresses disponibles de chaque sous-réseau pour prévoir les évolutions futures.

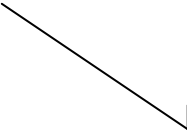
Les techniques de routage inter-domaine sans classe (CIDR) et l'utilisation de masques réseaux de longueur variable (VLSM) ont servi à optimiser l'espace d'adressage IPv4 de tout l'Internet.

III.5 Conclusion :

Avec les numéros de réseau IP devenant rapidement une espèce en voie de disparition, l'utilisation efficace de ces ressources de plus en plus rares est importante. Le présent chapitre décrit comment découper une adresse de réseau IP, afin de l'utiliser pour plusieurs sous-réseaux différents. Ce chapitre est focalisé sur les adresses réseau de classe C, mais les principes s'appliquent de la même manière aux réseaux de classes A et B.

Les découpages en sous-réseaux, que nous avons abordés dans ce chapitre, font partie intégrante du métier d'administrateur réseau. Nous avons traité l'adressage IP et le découpage en sous-réseaux IP en détail, depuis les bases (découpage avec classe) jusqu'aux les notions avancées (CIDR et VLSM). En révélant des méthodes de calcul des sous-réseaux qui ont fait et continuent de faire leurs preuves, soutenues par de nombreux exemples, et des cas pratiques rencontrés fréquemment en entreprise.

CHAPITRE IV :



*Conception et réalisation
de l'application de
segmentation VLSM*

IV.1 Introduction :

En informatique, une application web (aussi appelée *web application*, en anglais) est une application manipulable directement en ligne grâce à un navigateur web et qui ne nécessite donc pas d'installation sur les machines clientes, contrairement aux applications mobiles¹. De la même manière que les sites web, une application web est généralement installée sur un serveur et se manipule en actionnant des *widgets* à l'aide d'un navigateur web, via un réseau informatique (Internet, intranet, réseau local, etc.) [30].

Une application doit résoudre un problème précis. Le meilleur moyen d'y arriver, c'est de se poser beaucoup de questions et de synthétiser au maximum les réponses. Plus la vision est simple, plus l'application le sera et plus elle aura de chances d'être réussie.

Dans ce chapitre, nous présentons l'architecture sur laquelle nous avons développé notre application, les différents outils utilisés pour l'implémentation ainsi que les outils de mise en œuvre de notre projet accompagné de quelques interfaces illustrant les fonctionnalités de l'application développée.

IV.2 Outils de conception :

Utiliser les applications Web hors ligne est la tendance majeure dans ce domaine depuis 2008. Un Framework, Gears, avait été créé pour cela par Google, maintenant remplacé par les fonctions équivalentes dans HTML.

En mode déconnecté les pages et les objets qu'elles affichent sont mises en cache et une base SQL locale (*Indexed DB*) stocke les données sur le poste client en dupliquant la base distante. La balise *Input* peut représenter des types d'objets plus nombreux et dispose de nouveaux attributs comme l'auto-complétion. La balise *Output* affiche le résultat de calculs. L'ajout de contraintes sur les données aide à sécuriser les formulaires.

IV.2.1 Choix de langages de conception :

Les applications web ont l'avantage de donner plus de liberté aux développeurs, que ce soit dans leur champ d'action ou dans leur choix. De plus, les technologies actuelles rendent désormais possible la réalisation d'apps web de haute qualité, semblables à ce que l'on peut trouver sur Smartphones ou autre.

Les applications web sont souvent créées par des équipes composées de développeurs, mais la conception de l'application nécessite diverses compétences transverses et demande l'intervention de designers d'interface (*designer UI*), d'architecte logiciel, mais aussi de chef de produit. Le développement nécessite la connaissance des différents langages utilisés dans les technologies du Web : *HTML* pour la présentation des pages, *CSS* pour la charte graphique,

JavaScript, *Java* ou *ActionScript* pour les automatismes exécutés par le client, ainsi qu'un langage tel que *Java*, *PHP*, *C#* ou *VBScript* pour les automatismes exécutés par le serveur.

Pour développer notre application, nous serons amenés à utiliser trois types de langages de programmation Web ; le HTML, le CSS et le JavaScript.

IV.2.1.1 Langage HTML :

HTML est un langage de description de document utilisé sur Internet pour faire des pages Web. Son sigle signifie « *HyperText Markup Language* » en anglais, littéralement « langage de marquage hypertexte ». Le balisage HTML est incorporé dans le texte du document et est interprété par un navigateur Web. Elle permet ainsi de mettre en forme le contenu des pages web. Ce langage va donc nous servir d'écrire et d'inclure dans les pages web ce que nous souhaitons afficher aux visiteurs du site de notre application.

Un document HTML est avant tout un document texte c'est-à-dire lisible par un humain, qui contient une certaine syntaxe afin de mettre en forme ou de décrire ce document. Son nom de fichier a généralement le suffixe *.html* ou réduit à *.htm* sur certains systèmes d'exploitation ne supportant pas plus de 3 caractères de suffixe.

De nos jours l'immense majorité des gens font leur page Web à l'aide d'un logiciel avec une interface graphique, en utilisant la souris et en ayant un rendu immédiat ; il en existe des gratuits comme *Joomla* ou *Wordpress*, qui génèrent automatiquement les codes HTML. Dans la réalisation de notre portail par contre, pour plus de clarté on va coder tous nos pages que ce soit HTML, CSS, ou JavaScript nous-même. Il existe des éditeurs textes permettant de faire tout cela, pour notre cas on a choisi d'utiliser le logiciel « *Notepad++* » (Figure IV.1) en raison de sa légèreté, gratuité et sa stabilité [31].

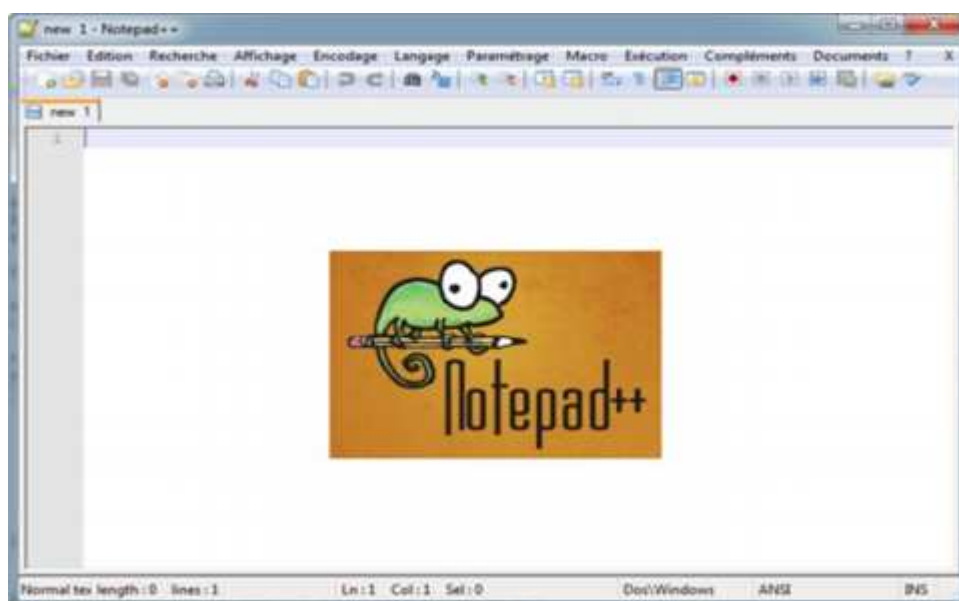


Figure IV.1 : Interface de l'outil Notepad++.

C'est dans cet éditeur de texte donc que l'on va coder tous nos pages. Précisons tout de même à titre de remarque que les documents HTML doivent tous avoir une structure minimale. C'est-à-dire des balises qui sont toujours présentes et au milieu desquelles nous allons ajouter notre propre contenu. Pour qu'une page HTML soit déclarée valide, elle doit obligatoirement comporter certains éléments et suivre un schéma précis.

Voici ci-dessous le code minimum pour créer une page HTML valide. Nous allons dans la suite expliquer le rôle de chaque élément et attribut.

```
<!DOCTYPE html>
<html>
  <head>
    <title> Affiché dans la barre de titre du navigateur </title>
  </head>
  <body>

    <!-- C'est ici que nous mettrons notre contenu >

  </body>
</html>
```

C'est grâce à des balises comme l'on voit ci-dessus que l'on structure les informations et transformer notre code source en document correct affiché à l'écran de l'utilisateur, ainsi qu'elle sert à Intégrer des différents médias comme les images, vidéo ou audio.

La déclaration **DOCTYPE**, obligatoire dans tout document, précise le type de document qui va être créé. La balise **<html>** est la balise racine du document, son contenu est constitué de l'en-tête du document, introduit par la balise **<head>** et terminé par la balise **</head>**, puis par le corps du document introduit par **<body>** et terminé par **</body>** [32].

Plusieurs balises ont été introduite avec HTML pour délimités les différentes zones qui constituent la page web, comme montre la figure IV.2 :

<header> : en-tête.

<footer> : pied de page.

<nav> : liens principaux de navigation.

<section> : section de page.

<aside> : information complémentaire.

<article> : article indépendant.

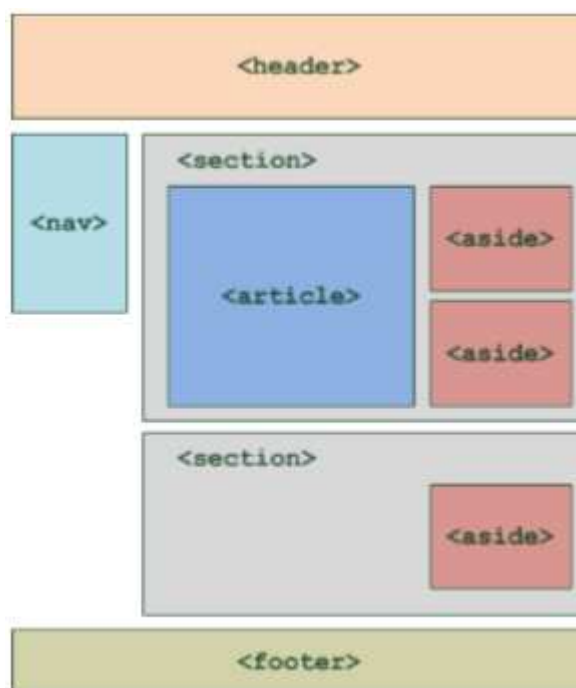


Figure IV.2 : Structure de base d'un document HTML.

A la fin de la rédaction du document HTML qui a constitué la page, le résultat obtenu est assez archaïque et minimaliste [31].

IV.2.1.2 Langage CSS :

Les feuilles de styles en cascade ou CSS pour « *Cascading Style Sheets* », décrivent l'apparence des divers éléments d'une page web par le biais de couples propriété valeur. Étant distinctes du code de la page HTML, elles constituent un moyen pour séparer la structure et la mise en page d'un site web, donc il est rarement approprié de s'en passer dans une page. Elles obéissent à un ensemble de règles que les navigateurs web doivent respecter [31].

CSS est une grammaire de règles pour définir la présentation d'un document HTML. C'est un standard du Web reconnu par tous les navigateurs. Le tutoriel CSS permet avec des démonstrations interactives de mieux connaître les propriétés et la façon dont elles fonctionnent. On peut écrire du code en langage CSS à trois endroits différents [32] :

- 1) **Dans un fichier .css :** Pour indiquer au fichier HTML quel fichier CSS lui est associé pour la mise en forme, on rajoute la ligne suivante dans la balise **<head>** du fichier HTML : **<link rel="stylesheet" href="nom_fichier.css">**, c'est la méthode la plus recommandée.
- 2) **Dans l'en-tête <head> :** Dans l'en-tête du fichier HTML, qui consiste à insérer le code CSS directement dans une balise **<style>** à l'intérieur de l'en-tête **<head>**.

Exemple :

```
<html>
  <head>
    <title>Exemple du deuxième cas</title>
  </head>
  <body style="color : red">
    <p>Cette phrase est rouge</p>
  </body>
</html>
```

- 3) **Directement dans les balises** : Dans les balises du fichier HTML via un attribut style, cela consiste à insérer le code CSS directement dans l'attribut, c'est la méthode la moins recommandée.

Exemple :

```
<body>
  <p style="color : blue ;"> Bonjour! </p>
</body>
```

IV.2.1.3 Langage JavaScript :

JavaScript (« JS » en abrégé) est un langage de programmation dynamique complet qui, appliqué à un document HTML, peut fournir une interactivité dynamique sur les sites Web [33].

Le langage JavaScript permet une répartition des tâches entre le " www " et le client accèdent à la ressource. Il permet d'effectuer localement un nombre important de traitements et fournit une interactivité accrue en détectant les actions de l'utilisateur. Le langage JavaScript permet au lecteur le développement d'interfaces HTML interactives. Un nombre important d'exemples illustrent les différentes fonctionnalités de JavaScript et leur utilisation dans des documents HTML [34].

Voici quelques exemples de ce qui est réalisable grâce au JavaScript :

- Un système de chat, comme celui de Facebook.
- Une suggestion lors de la frappe dans un champ de texte, comme lors d'une recherche avec Google.
- Un lecteur de vidéos ou de musiques, aussi puissant que celui de Youtube.
- Des jeux exploitant la balise <canvas>, comme Torus, un Tetris en 3D.
- Les formules mathématiques et les fonctions de calcul, comme notre cas.
- et bien d'autres choses...

IV.2.2 Tableau récapitulatif :

Pour bien comprendre les rôles que prend chaque langage dans l'édification du site Web portail de notre application, voici un tableau récapitulatif qui résume ce qu'on ait précédemment à leur propos.

Langage	Rôles	Commentaires
HTML	Sert à écrire la page Web proprement dite.	Emploie des balises pour structurer le contenu de la page.
CSS	Changement agencement, positionnement, et propriété des éléments de la page HTML.	Langage complémentaire de HTML.
JavaScript	Soigner le rendu de nos pages Web.	Langage interprété qui est exécuté par le navigateur de l'utilisateur.

Tableau IV.1 : Différences entre les langages HTML, CSS et JS.

IV.3 Le site Web et l'application Web :

IV.3.1 Le site Web

Un site Web est l'ensemble des pages Web et des ressources inter reliées entre elles par des liens hypertextes, auxquelles l'internaute peut accéder par une adresse Web appelée URL, le tout enregistré sous le même nom de domaine. Un site Web ou site Internet englobe des textes et de multimédia, il est hébergé sur un serveur Web, auquel on peut accéder à travers le réseau internet.

Une page Web peut être défini comme étant l'ensemble des documents HTML structurés, stockés sur un serveur connecté au réseau mondial qu'est internet, cette dernière contient pour son essentiel du texte, que l'on enrichit et accompagne d'images, de vidéos animation, de son parfois et de liens reliant la présente page à d'autres pages Web [34].

IV.3.1.1 Quelle est l'utilité d'un site Web ?

Durant ces dernières années, internet est devenu l'outil le plus utilisé au monde qui relie plusieurs internautes à travers le monde dépassant de loin les médias classiques tels que la télévision. Lorsqu'un internaute atterrit sur un site Web, c'est par ce qu'il cherche à assouvir un désir de partage, communication, s'amusement ou à répondre à des questions dans différents domaines.

Une page Web contient des informations qui permettent de communiquer et de partager des ressources avec les gens qui sont connectés sur internet et ce partout dans le monde. Les

professionnels créent des sites Web pour se faire connaître du grand public et l'intégrer comme étape primordiale dans la mise en place de sa stratégie commerciale, une manière très efficace qui a pour objectif de développer leur réputation et notoriété sur le Web, à travers l'utilisation du site Web comme support de diffusion d'information et de publicité [34].

Il existe essentiellement deux principaux types de sites Web, statique et dynamique.

a) Site statique :

Constitué des pages web avec du contenu fixe. Chaque page est codée en HTML et affiche les mêmes informations à chaque visiteur (Figure IV.3). La modification de ces pages se fait par une intervention de l'administrateur du site Web [35].



Figure IV.3 : Site web statique.

b) Site dynamique :

Les pages du site qui le compose peuvent être modifiables par les visiteurs. De plus, entre deux visites sur un même site, le contenu de la page peut être différent sans action de l'administrateur du site Internet (Figure IV.4). Le serveur qui fait fonctionner le site utilise une technologie de Scripting (comme PHP : *Hypertext Preprocessor*) ainsi qu'une base de données comme MySQL (*My Structured Query Language*) [36].

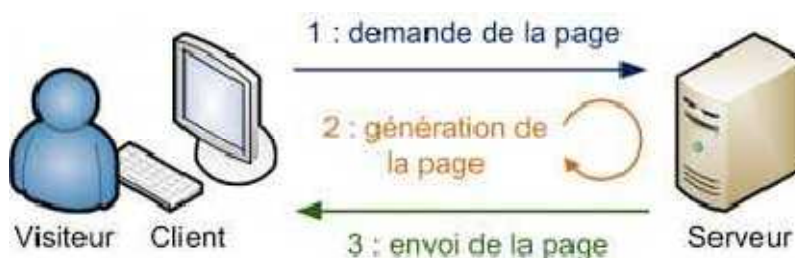


Figure IV.4 : Site web dynamique.

IV.3.2 L'application Web

Une application Web ou *Web App* est une version d'une page web qui a été optimisée, généralement par une équipe de développement, pour être utilisée à partir d'un ordinateur, une tablette ou un téléphone mobile. Grâce à cela, il peut être adapté à n'importe quel appareil.

Une application Web désigne un logiciel applicatif hébergé sur un serveur et accessible via un navigateur Web. Contrairement à un logiciel traditionnel, l'utilisateur d'une application Web n'a pas besoin de l'installer sur son ordinateur. Il lui suffit de se connecter à l'application à l'aide de son navigateur favori. La tendance actuelle est d'offrir une expérience utilisateur et des fonctionnalités équivalentes aux logiciels directement installés sur les ordinateurs. Les technologies utilisées pour développer les applications web sont les mêmes que celles employées dans la création des sites internet.

Une application Web est en général basée sur HTML, JavaScript ou CSS. Etant donné qu'une telle application est chargée depuis un serveur Web et exécutée via un navigateur Web, vous n'avez donc aucune installation à prendre en charge. Néanmoins l'utilisation d'un signet ou raccourci permet l'accès direct à l'application depuis le bureau ou l'écran d'accueil d'un appareil mobile.

IV.3.2.1 Les types d'applications Web

Cette fois, nous voulons faire une classification des types d'applications Web. Cette classification sera faite en fonction de la fonction de la présentation des applications Web avec le contenu qu'elles doivent afficher. Nous distinguons 5 types d'applications Web et ce sont les suivants.

a) Application Web statique

Si nous choisissons de créer une application Web statique, la première chose à savoir est que ce type d'application Web affiche peu d'informations et ne change généralement pas grand-chose. Elles sont généralement développées en HTML et CSS, bien que des objets mobiles tels que des bannières, des GIF animés ou des vidéos puissent également être affichés quelque part dans l'application Web.

Il n'est pas facile de modifier le contenu des applications statiques. Pour ce faire, il est nécessaire d'éditer le HTML et de le mettre à jour sur le serveur. Ces changements seront normalement de la responsabilité du webmaster ou de la société de développement qui a programmé la conception de l'application Web.

b) Application Web dynamique

Les applications web dynamiques sont beaucoup plus complexes sur le plan technique. Elles utilisent des bases de données pour charger des informations et ces contenus sont mis à jour chaque fois que l'utilisateur accède à l'application web.

Il existe de nombreux langages de programmation pour le développement d'applications web dynamiques. Les langages PHP et ASP sont les plus courants car ils permettent une bonne structuration du contenu.

Le processus de mise à jour est très simple et vous n'avez même pas besoin d'entrer sur le serveur pour le modifier. Il vous permet également de mettre en œuvre de nombreuses fonctionnalités, telles que des forums ou des bases de données. La conception des applications Web dynamiques peut également être modifiée pour convenir à l'administrateur.

c) Application Web de type e-shop ou e-commerce

Si, en revanche, l'application Web est une boutique ou un commerce numérique, on peut dire que le développement aura tendance à ressembler à celui d'un m-commerce ou d'un commerce électronique.

Le développement est plus compliqué car il doit permettre les paiements électroniques par carte de crédit, *PayPal* ou autre mode de paiement. Le développeur doit également créer un panel de gestion pour l'administrateur. À partir de là, les produits seront téléchargés, mis à jour ou supprimés et les commandes et les paiements pourront être gérées.

d) Application Web portail

Par portail, nous entendons un type d'application dans laquelle la page d'accueil permet d'accéder à différentes sections, catégories ou rubriques. En voici quelques exemples :

- Forums
- Chats
- Adresse électronique
- Moteurs de recherche
- Zone d'accès avec enregistrement

e) Application Web avec gestionnaire de contenu

Dans le cas d'applications Web dont le contenu doit être mis à jour en permanence, il est préférable d'utiliser un système de gestion de contenu (CMS: *Content Management System*) grâce auquel l'administrateur peut effectuer lui-même les modifications et les mises à jour. Ces gestionnaires sont intuitifs et très simples à gérer.

Comme exemples de systèmes de gestion de contenu (CMS), on trouve : *WordPress*, *Joomla*, *Drupal* ...etc. Ce type d'application web est très courant pour les pages de contenu, telles que les blogs, les pages d'information ou les médias.

IV.4 La structure de l'application VSC :

Après les phases d'étude de l'existant, pour la conception et la modélisation fonctionnelle et organisationnelle, nous avons développé les interfaces de notre application Web, cette dernière nous l'avons nommée VSC (*VLSM Subnet Calculator*), qui correspond à sa fonction de calcul des sous-réseaux de tailles fixes et variables.



Figure IV.5 : Logo de l'application Web (VSC).

IV.4.1 Présentation de l'application :

Notre application VSC (*VLSM SubNet Calculator*) est une application moderne qui fait le calcul de découpage et gestion des adresses IP. L'application VSC est conçue pour gagner du temps et éviter les erreurs coûteuses, elle permet de planifier la structure des adresses IP d'un bloc de réseau IP. Notre application permet d'effectuer des calculs des sous-réseaux à taille variable pour un bloc d'adresse réseau IPv4 donné et calculer le nombre d'adresses disponibles dans le réseau.

Elle peut également générer une table contenant pour chaque sous-réseau le nombre d'adresses disponibles, le masque de sous-réseau, le nombre d'hôtes nécessaires disponibles et inutilisés par sous-réseau et détermine en conséquence l'adresse de diffusion, l'adresse de sous-réseau et la plage d'hôtes disponible dans chaque sous-réseau, tout cela est également possible dans le cas d'un super réseau. Elle permet de découvrir rapidement et automatiquement les adresses réseau qu'elles soient la classe de ces adresses A, B ou C.

Pour compenser les problèmes de distribution de l'espace d'adressage IPv4. Notre application expose deux solutions de découpage en sous-réseaux. La première consiste à segmenter un même réseau, en plusieurs sous-réseaux de taille identiques, en utilisant des masques de sous-réseaux fixe, selon le nombre de hôtes qu'il pourra y avoir sur un sous-réseau ou selon le nombre de sous-réseaux souhaités. La deuxième solution est une simple extension du découpage en sous-réseaux de base, où une même adresse est découpée en sous-réseaux à l'aide de masques de longueurs différentes, permettant une souplesse dans l'affectation du nombre adéquat d'hôtes et de sous-réseaux, basée sur la technique VLSM.

IV.4.2 Présentation des interfaces graphiques :

Après avoir terminé le volet technique de ce chapitre, nous allons désormais consacrer cette partie à la présentation des interfaces graphiques de notre application Web (VSC).

IV.4.2.1 Interface Subnetting (Host) :

Lors de lancement de notre application sur n'importe quel navigateur Web, on se trouve face à l'interface "Subnetting (Host)" illustrée par la figure IV.6. Cette interface effectue des calculs de sous-réseau pour un bloc d'adresse réseau donné; le masque de sous-réseau, le nombre des sous réseaux requis et détermine en conséquence l'adresse de diffusion, l'adresse de chaque sous-réseau, et la plage d'adresses des hôtes.

L'utilisateur de notre application est invité à remplir les inputs demandées, à savoir le bloc d'adresse réseau avec le masque initial (en notation CIDR) et choisir le nombre maximal d'hôtes souhaité par sous-réseau.

Developed by : N. B.Abdellah & N. Bendeddouche | Directed by : Dr. H.Zerrouki.
© 2020 Master R&T, Univ-Tlemcen. All rights reserved.

Figure IV.6 : Interface Subnetting (Host).

En cliquant sur le bouton "Calculer", l'application VSC calculera le nombre de sous-réseaux nécessaire et affichera une interface de "Résultat de calcul", qui génère une table dynamique contenant pour chaque sous-réseau, le ID de sous-réseau, le masque de sous-réseau et détermine en conséquence l'adresse de diffusion, l'adresse de sous-réseau et la plage d'hôtes disponible dans chaque sous-réseau, comme montre la figure IV.7.



Subnet ID	Address de sous-réseau	Plage d'adresses des hôtes	Adresse de diffusion
1	192.168.1.0	192.168.1.1 - 192.168.1.62	192.168.1.63
2	192.168.1.64	192.168.1.65 - 192.168.1.126	192.168.1.127
3	192.168.1.128	192.168.1.129 - 192.168.1.190	192.168.1.191
4	192.168.1.192	192.168.1.193 - 192.168.1.254	192.168.1.255

Developed by : N. B. Abdellah & N. Bendeddouch | Directed by : Dr. H. Zerrouki.
© 2020 Master R&T, Univ-Tlemcen. All rights reserved.

Figure IV.7 : Résultat de calcul des sous-réseaux en Subnetting (Host).

L'application VSC contient un programme défensif, contre un mauvais choix des paramètres ou erreur de frappe. Si le cas, l'application vous affiche une fenêtre "Alert !" et vous indique l'erreur commise. La figure IV.8 représente quelques fenêtres de dialogues d'erreurs.

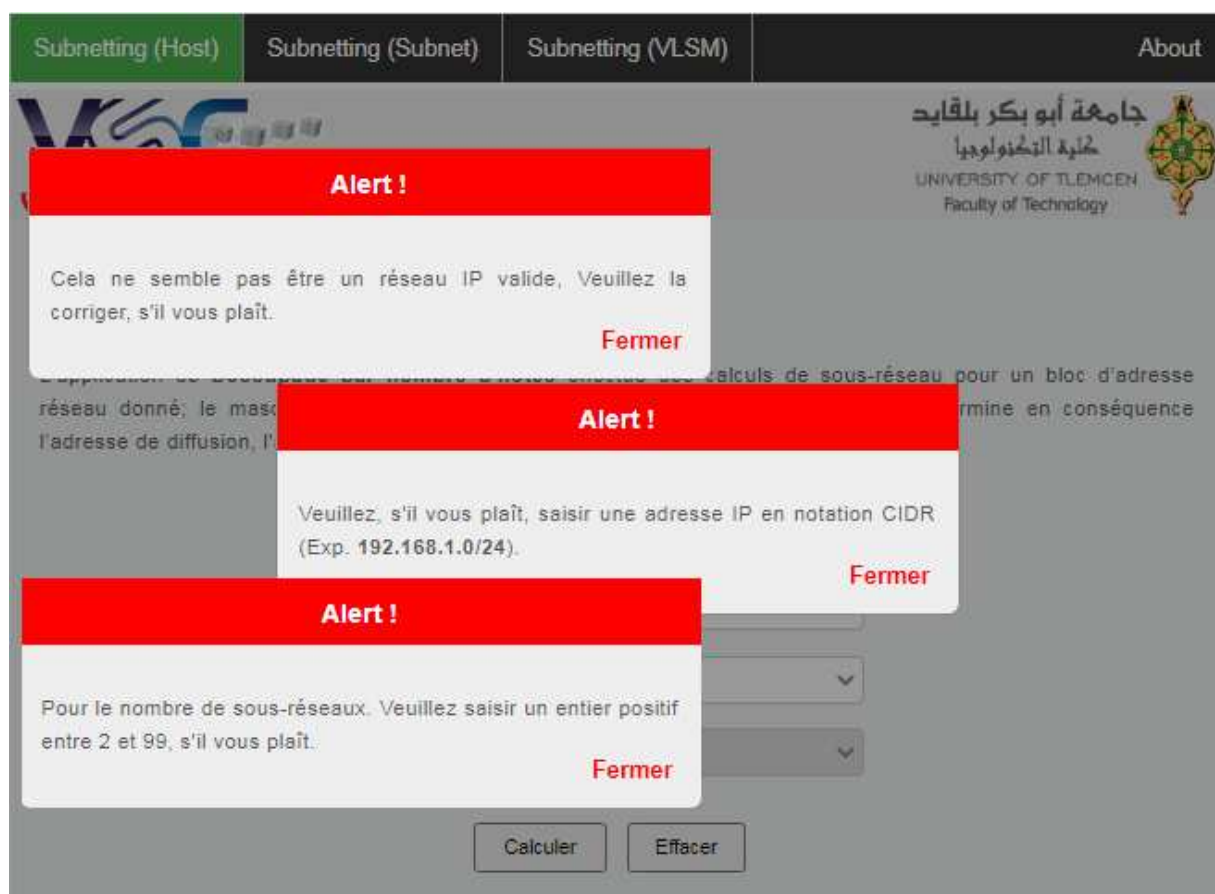


Figure IV.8 : Quelques fenêtres "Alert !" du programme défensif.

De même, notre application contient des valeurs de calcul par défaut pour le premier lancement pour éviter toute erreur d'utilisation. L'utilisateur a la possibilité de modifier les

valeurs de paramètre par défaut à n'importe quel moment et selon leur besoins et la configuration de son réseau.

IV.4.2.2 Interface Subnetting (Subnet) :

L'interface "Subnetting (Host)" (Figure IV.9) effectue des calculs de sous-réseau pour un bloc d'adresse réseau donné; le masque de sous-réseau, le nombre maximum d'hôtes requis par sous-réseau et détermine en conséquence l'adresse de diffusion, l'adresse de chaque sous-réseau, et la plage des hôtes.

The screenshot shows the 'Subnetting (Subnet)' interface of the VLSM SubNet Calculator. The interface has a dark header with four tabs: 'Subnetting (Host)', 'Subnetting (Subnet)' (which is active and highlighted in green), 'Subnetting (VLSM)', and 'About'. Below the header, there is a logo for 'VLSM SubNet Calculator' on the left and the 'UNIVERSITY OF TLEMCEEN Faculty of Technology' logo on the right. The main content area is titled 'Découpage par nombre de sous-réseaux' in blue. Below this title, there is a paragraph explaining the application's function. The form contains four input fields: 'Bloc d'adresse réseau' with the value '192.168.1.0/24', 'Masque de sous-réseau' with the value '255.255.255.0/24', 'Nombre de sous-réseaux' with the value '8', and 'Nbr. Maximal d'hôtes par sous-réseaux' which is currently empty. At the bottom of the form are two buttons: 'Calculer' and 'Effacer'.

Developed by : N. B.Abdellah & N. Bendeddouche | Directed by : Dr. H.Zerrouki.
© 2020 Master R&T, Univ-Tlemcen. All rights reserved.

Figure IV.9 : Interface Subnetting (Subnet).

De la même manière que l'interface de découpage par le nombre d'hôtes, et après avoir renseigné tous les champs nécessaires, en cliquant sur le bouton "Calculer". L'application VSC va calculer le nombre de hôtes maximal dans chaque sous-réseau et génère une table dynamique contenant pour chaque sous-réseau, le ID de sous-réseau, l'adresse de sous-réseau et détermine en conséquence l'adresse de diffusion et la plage d'hôtes disponible dans chaque sous-réseau (Figure IV.10).



Subnet ID	Address de sous-réseau	Plage d'adresses des hôtes	Adresse de diffusion
1	192.168.1.0	192.168.1.1 - 192.168.1.30	192.168.1.31
2	192.168.1.32	192.168.1.33 - 192.168.1.62	192.168.1.63
3	192.168.1.64	192.168.1.65 - 192.168.1.94	192.168.1.95
4	192.168.1.96	192.168.1.97 - 192.168.1.126	192.168.1.127
5	192.168.1.128	192.168.1.129 - 192.168.1.158	192.168.1.159
6	192.168.1.160	192.168.1.161 - 192.168.1.190	192.168.1.191
7	192.168.1.192	192.168.1.193 - 192.168.1.222	192.168.1.223
8	192.168.1.224	192.168.1.225 - 192.168.1.254	192.168.1.255

Developed by : N. B. Abdellah & N. Bendeddouch | Directed by : Dr. H. Zerrouki.
© 2020 Master R&T, Univ-Tlemcen. All rights reserved.

Figure IV.10 : Résultats de calcul des sous-réseaux en Subnetting (Subnet).

IV.4.2.3 Interface Subnetting (VLSM) :

L'interface "Subnetting (VLSM)" permettant aux débutants et aux professionnels et administrateurs des réseaux de diviser les réseaux en sous-réseaux plus petits et plus efficaces pour répondre aux besoins des hôtes variables.

Cette interface comprend également un calculateur de sous-réseau régulier basé sur la technique de masque de sous-réseau de longueur variable (VLSM), qui peut fournir une utilisation plus efficace de l'espace d'adressage IP. Elle permet de découvrir les hôtes nécessaires, disponibles et inutilisés pour chaque sous-réseau, ainsi que la plage d'adresses utilisables, le masque de et l'adresse de sous-réseau et l'adresse de diffusion d'un réseau IPv4 donné avec un utilisation facile pour étendre ou réduire les réseaux. La figure IV.11 schématise une capture de l'interface "Subnetting (VLSM)" avec un exemple de calcul de 4 sous-réseaux de différentes tailles.

La figure IV.12 montre le résultat de calcul de sous-réseaux. Dans cet exemple nous voulons avoir 4 sous-réseaux de tailles variables, le *Subnet 1* avec 100 hôtes, le *Subnet 2* à 40 hôtes, le *Subnet 3* à 70 hôtes et enfin le *Subnet 4* à 50 hôtes. L'application permet de réaliser tout ceci en un clic, après avoir saisi les informations d'entrée, les sous réseaux sont classés en ordre décroissant de taille et attribués en fonction des besoins individuels de chaque sous-réseau. Si la taille des sous-réseaux dépasse la capacité du bloc de réseau initial, l'application propose une solution éventuelle pour surpasser ce problème, cela est indiqué par un message surligné en jaune.

Subnetting (Host)

Subnetting (Subnet)

Subnetting (VLSM)

About



جامعة أبو بكر بلقايد

كلية التكنولوجيا

UNIVERSITY OF TLEMCEN

Faculty of Technology

Découpage par nombre variable d'hôtes

L'application de découpage par nombre variable d'hôtes, nommée "VSC (VLSM Subnet Calculator)", effectue des calculs des sous-réseaux à taille variable pour un bloc d'adresse réseau IPv4 donné; le masque de sous-réseau, le nombre d'hôtes nécessaires, disponibles et inutilisés par sous-réseau et détermine en conséquence l'adresse de diffusion, l'adresse de sous-réseau et la plage d'hôtes disponible dans chaque sous-réseau.

Bloc d'adresse réseau

Nombre de sous-réseaux

Changer

Noms de sous-réseau

Nbr. d'hôtes par sous-réseau

Subnet 1	100
Subnet 2	40
Subnet 3	70
Subnet 4	50

Calculer

Effacer

Developed by : N. B.Abdellah & N. Bendeddouche | Directed by : Dr. H.Zerrouki.
© 2020 Master R&T, Univ-Tlemcen. All rights reserved.

Figure IV.11 : L'interfec Subnetting (VLSM).

VSC VLSM SubNet Calculator

جامعة أبو بكر بلقايد

كلية التكنولوجيا

UNIVERSITY OF TLEMCEN

Faculty of Technology

Résultats de calcul des sous-réseaux VLSM

Fermer

Le réseau 192.168.1.0/24 compte 254 hôtes.
Vos sous-réseaux ont besoin de 260 hôtes.

On dirait que la taille des sous-réseaux est plus grande que le nombre maximum d'hôtes disponible dans votre réseau, mais voici autre solution qui pourrait fonctionner pour vous:

Sous-réseau	Hôtes			Adresse SR	CIDR	Masque	Plage d'adresses utilisable	Diffusion
	Nécessaires	Disponibles	Inutilisés					
Subnet 1	100	126	26	192.168.1.0	/25	255.255.255.128	192.168.1.1 - 192.168.1.126	192.168.1.127
Subnet 3	70	126	56	192.168.1.128	/25	255.255.255.128	192.168.1.129 - 192.168.1.254	192.168.1.255
Subnet 4	50	62	12	192.168.2.0	/26	255.255.255.192	192.168.2.1 - 192.168.2.62	192.168.2.63
Subnet 2	40	62	22	192.168.2.64	/26	255.255.255.192	192.168.2.65 - 192.168.2.126	192.168.2.127

Developed by : N. B.Abdellah & N. Bendeddouche | Directed by : Dr. H.Zerrouki.
© 2020 Master R&T, Univ-Tlemcen. All rights reserved.

Figure IV.12 : Résultats de calcul des sous-réseaux en Subnetting (VLSM).

IV.4.2.4 Interface About :

L'interface "About" permet aux utilisateur de notre application a avoir une connaissance totale pour maîtriser les notions d'adressage IP, les classes, la notion de masque et les méthodes de calcul des adresses IP et ses mécanismes de découpage en sous-réseaux. Cette interface est renforcé par des exemples de calculs pour les deux approches de découpage en sous-réseau citées précédemment.

Subnetting (Host) Subnetting (Subnet) Subnetting (VLSM) **About**

VLSM SubNet Calculator

جامعة أبو بكر بلقايد
كلية التكنولوجيا
UNIVERSITY OF TLEMSEN
Faculty of Technology

Adressage IPv4 et découpage en sous-réseaux

Il est inimaginable de se présenter à un examen Cisco ou à un entretien d'embauche dans le domaine des réseaux sans maîtriser l'adressage IPv4 et ses mécanismes de découpage en sous-réseaux.

I. Introduction aux adresses IPv4

Une adresse IPv4 est un identifiant de 32 bits représentés par 4 octets (8 bits) codés en décimales séparées par des points.

Le masque de réseau lui aussi noté en décimal pointé indique avec les bits à 1 la partie réseau partagée par toutes les adresses d'un bloc et avec les bits à 0 la partie unique qui identifie les interfaces sur la liaison.

Par exemple, **192.168.1.255** **255.255.255.0** indique un numéro de réseau (première adresse) **192.168.1.0** et un numéro de Broadcast **192.168.1.255**. Toutes les adresses comprises entre ces valeurs peuvent être utilisées par les interfaces attachées à une même liaison (un même switch).

À cause du manque d'espace IPv4 disponible, on trouve souvent des masques qui chevauchent les octets, ce qui nécessite de passer par des calculs binaires.

II. Définition

- * Une adresse IPv4 (Internet Protocol version 4) est une identification unique pour un hôte sur un réseau IP.
- * Une adresse IP est un nombre d'une valeur de 32 bits représentée par 4 valeurs décimales pointées ; chacune a un poids de 8 bits (1 octet) prenant des valeurs décimales de 0 à 255 séparées par des points. La notation est aussi connue sous le nom de "décimale pointée".

III. Identification de la classe d'adresse

			195.167.46.223/27
		195.167.46.224/30	195.167.46.225/30 à 195.167.46.226/30 195.167.46.227/30
R1-R2	4 adresses	195.167.46.228/30	195.167.46.229/30 à 195.167.46.230/30 195.167.46.231/30
R1-R3	4 adresses	195.167.46.232/30	195.167.46.233/30 à 195.167.46.234/30 195.167.46.235/30

Cette perspective restrictive correspond aux principes de conservation des adresses IPv4 publiques.

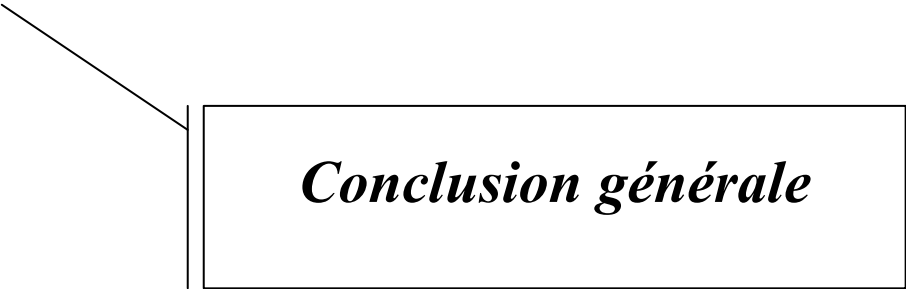
Developed by : N. B. Abdellah & N. Bendeddouche | Directed by : Dr. H. Zerrouki.
© 2020 Master R&T, Univ-Tlemcen. All rights reserved.

Figure IV.13 : L'interface de la page "About".

IV.5 Conclusion :

Dans ce chapitre, nous avons présenté tout d'abord, l'environnement de développement ainsi que l'implémentation de notre application de découpage en sous-réseaux. Nous avons présenté également toutes les interfaces constituant notre application. Elle marie les deux approches pour la mise en sous-réseau d'une adresse IP pour un réseau : avec un masque de sous-réseau de longueur fixe et avec un masque de sous-réseau de longueur variable (VLSM).

Notre application aide les administrateurs réseaux à calculer les adresses IP de sous-réseau VLSM, pour prendre en charge l'administration réseau afin que les utilisateurs puissent résoudre l'ID de réseau en sous-réseaux. Les résultats IP obtenus à partir de notre application peuvent être testés avec VLSM sur divers fournisseurs de services de réseau Internet pour obtenir un tout à fait optimal à des fins d'administration du réseau.



Conclusion générale

Conclusion générale

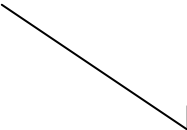
Il existe deux approches pour la mise en sous-réseau d'une adresse IP pour un réseau : un masque de sous-réseau de longueur fixe et un masque de sous-réseau de longueur variable (VLSM). Dans le premier, tous les sous-réseaux sont de taille égale avec un nombre égal d'identificateurs d'hôte. Vous utilisez le même masque de sous-réseau pour chaque sous-réseau et tous les sous-réseaux ont le même nombre d'adresses. Il a tendance à être le plus coûteux car il utilise plus d'adresses IP que nécessaire.

La VLSM est une stratégie de conception de sous-réseau qui permet à tous les masques de sous-réseau d'avoir des tailles variables. Dans le sous-réseau VLSM, les administrateurs réseau peuvent diviser un espace d'adresse IP en sous-réseaux de différentes tailles et l'allouer en fonction des besoins individuels sur un réseau. Ce type de sous-réseau permet une utilisation plus efficace d'une plage d'adresses IP donnée. VLSM est la norme actuelle pour la façon dont chaque réseau est conçu aujourd'hui.

Le problème de la distribution de l'espace d'adressage IP nous a fait l'enthousiasme de trouver une solution par la création d'une application de découpage en sous réseaux. L'objectif de notre mémoire est de développer une application Web pour la segmentation des réseaux IP par la techniques VLSM avec la notion CIDR.

Le développement de notre application Web (VSC : *VLSM SubNet Calculator*) correspond à sa fonction de calcul des sous réseaux de taille fixe et variable et la gestion efficace des adresses IP. Elle génère également un table pour chaque sous réseau contenant le nombre des sous-réseaux, le masque de chaque sous réseau, le nombre d'hôtes, l'adresse de diffusion, l'adresse de sous réseau et la plage d'hôtes disponible.

L'application VSC expose la solution de découpage en sous réseau, la segmentation d'un même réseau en plusieurs sous réseaux de même taille avec masque fixe et le découpage d'une même adresse en sous réseaux de tailles différentes. Notre application fait les preuves de ses résultats obtenus qui peuvent être testés sur des fournisseurs de service réseau internet.



Bibliographie

Bibliographie

- [1]. https://www.pedagogie.ac-aix-marseille.fr/upload/docs/application/pdf/2012-07/formation_reseau.pdf, © Copyright 2003 Jean-François Pillou. Ce document est issu de commentcamarche.net est soumis à la licence GNU FDL, (Consulté le 24/02/2020).
- [2]. Philippe Atelin, José Dordoigne, " *Réseaux informatiques: Notions fondamentales Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, Wi-Fi,...* ", Edition ENI, ISBN : 978-2-7460-4681-8, janvier 2009.
- [3]. Germain Affro Essan, " *Le réseau informatique dans la chaîne de production d'une société de presse* ", Mémoire en ligne, ISCM - Ingenieur 2010 https://www.memoireonline.com/06/10/3578/m_Le-reseau-informatique-dans-la-chaîne-de-production-dune-société-de-pre-sse9.html, (Consulté le 28/02/2020).
- [4]. " *Généralité sur les réseaux informatiques* ", <https://d1n7iqsz6ob2ad.cloudfront.net/document/pdf/533b3e6b0b795.pdf>, (Consulté le 28/02/2020).
- [5]. Danièle Dromard, Dominique Seret, " *Réseaux informatiques* ", Encyclopædia Universalis [en ligne], URL : <http://www.universalis.fr/encyclopedie/reseaux-informatiques/> (Consulté le 03/02/2020).
- [6]. " *Réseau informatique* ", Document en ligne https://sites.google.com/site/reseau_informatiquesocio/home, (Consulté le 03/02/2020).
- [7]. Eldad Kanawa, " *Types de réseaux informatiques* ", Document de réseau informatique et cyber sécurité, janv. 2019, <https://connaitreinfo.com/types-de-reseaux-informatiques/>, (Consulté le 10/03/2020).
- [8]. Mohammed Mourad, " *Exposé sur l'exploitation d'un réseau informatique* ", <https://fr.scribd.com/presentation/442032023/Reseux-pptx>, (Consulté le 12/03/2020).
- [9]. " *Modèle OSI* ", <https://www.frameip.com/osi/>, (Consulté le 20/03/2020).
- [10]. YAO Kouakou Joseph Claver, ADOU Kablan Jérôme, KOUAKOU Guy Charles, " *Migration d'un réseau opérateur télécom vers le all IP : cas du GSM* », Mémoire de Master UFR Mathématiques et Informatique, Université Félix Houphouët Boigny, Abidjan, Octobre 2016.
- [11]. Digital Guides : " *Qu'est-ce que le protocole IP ?* " <https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-que-linternet-protocol-definition-dip/>, (Consulté le 02/04/2020).
- [12]. " *Les bases du réseau : TCP/IP, IPv4 et IPv6 : Le protocole IP* ", Plate-forme de cours sur l'administration systèmes et réseau pour les professionnels de l'informatique, <https://www.it-connect.fr/chapitres/le-protocole-ip/>, (Consulté le 02/04/2020).

- [13]. MADANI Hocine, " *Planification d'un réseau mobile basé sur une technologie IP* " Mémoire de Master en Electronique, option : Télécommunication, Université Abderrahmane MIRA de Bejaia, 2013.
- [14]. Cours Portée et séquence: CCNA Exploration v4.0, <https://www.cours-gratuit.com/cours-packet-tracer/cours-portee-et-sequence-ccna-exploration-v4-0-en-pdf>, (Consulté le 15/04/2020).
- [15]. Guy Pujolle, " *Les réseaux : L'ère des réseaux cloud et de la 5G* (9^e édition) ", Editions Eyrolles, ISBN : 978-2212675351, Juillet 2018.
- [16]. José Dordoigne, " *Réseaux informatiques - Notions fondamentales* (7^e édition) - (Protocoles, Architectures, Réseaux sans fil, Virtualisation, Sécurité, IPv6...) ", Editions ENI, ISBN : 978-2409008955, Août 2017.
- [17]. Philippe Latu " *Adressage IPv4* ", Licence de Documentation Libre GNU (2000), inetdoc.net/pdf/adressage.ipv4.pdf, (Consulté le 20/04/2020).
- [18]. PÉREZ André, " *Les technologies IPv4 et IPv6 : Protocoles et transitions* ", Editions Hermes Science Publications, ISBN : 978-2746238954, Septembre 2012.
- [19]. Douglas Comer, " *TCP/IP - Architecture, protocoles et applications* (5e édition) ", Editions Pearson, ISBN : 2-7440-7186-2, Novembre 2006.
- [20]. Ce document intitulé "Adresse IP " issu de site www.commentcamarche.net est mis à disposition sous les termes de la licence Creative Commons., <https://www.commentcamarche.net/contents/523-adresse-ip>, (Consulté le 10/05/2020).
- [21]. François Goffinet, " *Guide de CCNA 200-301* ", <https://cisco.goffinet.org/ccna/ipv4/adressage-ipv4/>, (Consulté le 10/05/2020).
- [22]. El Hassan EL AMRI, " *Cours le routage statique (ipv4 et ipv6)* ", Formation CISCO, Campus des Réseaux Informatiques et Télécommunications .Janvier 2015.
- [23]. " *Différence entre routage statique et dynamique* ", https://waytolearnx.com/2018/07/difference-entre-routage-statique-et-dynamique.html?fbclid=IwAR2IlxpoowFIh2P9642V6ufbbJh3Ton5fW_VNEBma-mwdftZkc0N_R4ZucM, (Consulté le 23/05/2020).
- [24]. Cisco Systems, " *VLSM et CIDR Protocoles de Routage et Concepts – Chapitre 6* ", CISCO CCNA 2 version 4.0, 2007.
- [25]. Tondeur H, " *Les sous-réseaux (Découpage d'un réseau IP)* ", <http://ashrafbahya.e-monsite.com/medias/files/les-sous-reseaux.pdf>, (Consulté le 21/06/2020).
- [26]. " *Les masques de sous-réseau IP* ", Document en ligne <https://www.frameip.com/masques-de-sous-reseau/>, (Consulté le 21/06/2020).
- [27]. " *Adresse IPv4 - Définition et Explications* ", <https://www.techno-science.net/definition/10887.html>, (Consulté le 24/06/2020).
- [28]. IT NISRO, " *Qu'est-ce que la technique VLSM et à quoi sert-elle?* ", <https://clubtutoinformatique.blogspot.com/2012/12/quest-ce-que-la-technique-vlsm-et-quoi.html?fbclid=IwAR08>

- [xb8bv5y_hLM8vUnoFiKpbqfgEg8f01aK6YIpUqWXxcDlknzhBR1UfqU](#) (Consulté le 17/07/2020).
- [29]. Robb Jones, " *VLSM Workbook IPv4 - Student Edition - ver 2.3*", Frederick County Career & Technology Center, Cisco Networking Academy, Frederick County Public Schools Frederick, Maryland, USA, 2017.
- [30]. Gabriel Boccara, " *La création d'une application réussie de A à Z* ", 27 décembre 2017. <https://www.welcometothejungle.com/fr/articles/conception-application-lunabee>, (Consulté le 24/07/2020).
- [31]. RAMASY Heritier Arantès, " *Conception et réalisation d'une plateforme d'exploitation de données implémentée dans un réseau local* ", Mémoire de fin d'études en vue de l'obtention du diplôme de Licence en Télécommunication, Parcours : Réseaux et Systèmes, Université d'Antananarivo, Mars 2015.
- [32]. " *Apprendre le HTML - Guides et didacticiels : Introduction au HTML* ", https://developer.mozilla.org/fr/docs/Apprendre/HTML/Introduction_%C3%A0_HTML, (Consulté le 05/08/2020).
- [33]. " *Les bases de JavaScript* ", https://developer.mozilla.org/fr/docs/Apprendre/Commencer_avec_le_web/Les_bases_JavaScript, (Consulté le 05/08/2020).
- [34]. Isaac Cohen. " *CGI/Perl et JavaScript, la création de pages HTML interactives* ". Editions Eyrolles, pp.294, 1996.
- [35]. " *Différence entre les pages Web statiques et dynamiques* ", Créé le 7 Septembre 2018, <https://waytolearnx.com/2018/09/difference-entre-les-pages-web-statiques-et-dynamiques.html>, (Consulté le 10/08/2020).
- [36]. " *Tutoriels JAVA*", <https://waytolearnx.com/2020/06/tutoriels-java.html>, et " *Tutoriels PHP* ", <https://waytolearnx.com/2020/06/tutoriels-php.html>, (Consultés le 10/08/2020).