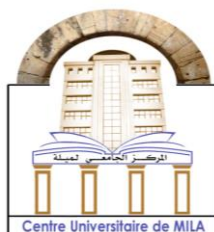


الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique



N° Réf :.....

Centre Universitaire de Mila

Institut des Sciences et de la Technologie

Département de Mathématiques et Informatique

Mémoire préparé En vue de l'obtention du diplôme de licence
En : - Filière : Informatique générale

Thème

Conception d'une solution web assistant les administrateurs à la planification des réseaux IPV4, IPV6 et les Réseaux Hybrides

Préparé par :

- BENZERAFA BILAL
- MEZHOUD SEYF-EDDINE
- MEGHLAOU TOUWFIQ

Encadré par:

- BENCHEIKH EL HOUCIN MADJED
- Grade : M.A.B

Année universitaire : 2013/2014

Sommaire

Introduction générale	01
Chapitre 01 : Le protocole IP	04
I. Introduction	06
II. L'adressage IP	07
III. Le protocole IPv4	07
III.1. Datagramme	07
III.2. Le format des adresses IPv4	09
III.3. Les classes des adresses IPv4	10
III.3.1. Les adresses IPv4 de classe A	10
III.3.2. Les adresses IPv4 de classe B	11
III.3.3. Les adresses IPv4 de classe C	11
III.3.4. Les adresses IPv4 de classe D	12
III.3.5. Les adresses IPv4 de classe E	12
III.4. Les types d'adresses IPv4	13
III.5. Le masque réseau	14
III.6. Les sous-réseaux (Subnetting)	15
III.6.1. Les avantages du découpage en sous-réseaux	15
III.6.2. Technique de découpage sous-réseaux	15
III.6.3. Le masque de sous-réseau	16

III.7. Le principe du NAT (Network Address Translation)	17
III.7.1. Les types de translation	18
III.7.1.a. NAT statique	18
III.7.1.b. NAT dynamique	19
III.8. L'attribution des adresses IP	19
IV. Le protocole IPv6	20
IV.1. Format de paquet et fonctionnalités d'IPv6	22
IV.2. L'adressage IPv6	22
IV.2.1. Représentation des adresses IPv6	22
IV.2.2. Les types d'adresses IPv6	23
V. Les réseaux Hybrides	25
V.1. Définition	25
V.2. Les mécanismes de la transition d'IPv4 vers IPv6	25
V.2.1. Double pile	25
V.2.2. Les tunnels IPv6 dans IPv4	26
V.2.2.a. Les tunnels statiques	26
V.2.2.b. Les tunnels dynamiques	26
VI. Conclusion	31
Chapitre 02 : Planification des réseaux	32
I. Introduction	34
II. Problématique	35
III. Approche proposée	36

IV. Maquette du projet	37
V. Conclusion	46
Chapitre 03 : Conception du site web	47
I. Introduction	59
II. UML	50
II.1. Définition	50
II.2. Utilité d'UML	50
II.3. Caractéristiques du langage UML	51
II.3.1. UML n'est pas une méthode ou un processus !	51
II.3.2. UML est un langage pseudo-formel	51
II.3.3. UML cadre l'analyse objet	51
II.3.4. UML est un support de communication	52
II.4. Les points fort d'UML	52
II.5. Les points faibles d'UML	52
II.6. Les diagrammes UML	53
II.6.1. Diagrammes structurels ou diagrammes statiques (UML structure)	53
II.6.2. Diagrammes comportementaux ou diagrammes dynamiques	53
II.6.3. Diagrammes d'interaction (Interaction diagrams)	53
II.7. Mise en œuvre d'UML	53
II.7.1. Les étapes de la démarche	54
II.7.1.a. Phase d'identification des besoins et spécialisation des fonctionnalités	54

II.7.1.b. Phase d'analyse	54
II.7.1.c. Phase de conception	54
III. Le modèle des besoins	54
III.1. Identification des acteurs	54
III.2. Le diagramme de cas d'utilisation	55
III.2.1. Cas se renseigner sur une adresse IP	56
III.2.2. Cas segmentation en sous-réseaux d'une adresse IPv4	60
III.2.3. Cas Compression/Décompression d'une adresse IPv6	64
III.2.4. Cas assistance pour le choix des tunnels	68
IV. Conclusion	72
Chapitre 04 : Implémentation	73
I. Introduction	75
II. Langages de programmation	76
II.1. Le langage HTML	76
II.2. Le langage CSS	76
II.3. Le langage JavaScript	77
II.4. Le langage << Personal Home Page >>	77
III. Outils de développement	78
III.1. Adobe DreamWeaver	78
III.2. WampServer	78
IV. Conclusion	79
Conclusion générale	80

Annexe	82
Liste des Tableaux	85
Liste des Figures	86
Références Bibliographiques	90

Introduction

Générale

L'évolution technologique de ces dernières années conduit la société moderne à adopter de nouvelles habitudes face à la communication.

Depuis bien longtemps, les hommes à travers diverses structures éprouvent le besoin de partager les informations en temps réel. Face à cette obsession, plusieurs études ont été menées pour concevoir un système de diffusion des informations capable de couvrir des vastes étendus afin de révolutionner le système de communication de l'ancien temps en un système de communication intégrant la nouvelle technologie de l'information et de communication dont le plus récent serait l'interface web [1].

Actuellement les réseaux informatiques représentent le noyau de communication pour notre vie personnelle ou professionnelle, c'est un système très compliqué qui permet, à partir de l'interconnexion de différents équipements, de transporter l'information quel que soit son type (Texte, audio ou vidéo). L'utilisation des services réseaux est devenue un mode de vie pour la société, en parle d'Internet ou bien de la téléphonie mobile.

La planification et la gestion des réseaux informatiques représentent des tâches très critiques au niveau des entreprises et des compagnies de télécommunication afin de veiller sur la continuité des services offerts aux clients. Pour cela, ces structures engagent des administrateurs qualifiés assurant le bon fonctionnement des réseaux.

L'objectif de notre projet est de concevoir un site web dynamique, à accès libre, destiné à toute personne intéressée par le domaine des réseaux, dans un cadre d'étude ou bien professionnel, offrant un ensemble de services concernant la planification des réseaux IP.

Ce travail vise à réduire le temps nécessaire pour l'établissement des opérations arithmétiques binaires utilisées dans la segmentation des réseaux IPv4, offre un support très riche détaillant les caractéristiques de n'importe quelle adresse IP (Version 4 / Version 6) et enfin propose un assistant bien étudié pour le choix des tunnels IPv4/IPv6.

Les chapitres de ce mémoire sont organisés comme suit :

Chapitre 01 présente de façon générale les notions de base du protocole IP et détaille les techniques d'adressages utilisées.

Chapitre 02 expose les problématique liées à la planification des réseaux, motivant les besoins de ce projet. Ensuite présente une maquette simulant notre vision du futur site Web.

Chapitre 03 détaille la conception de notre site Web, à partir des diagrammes UML afin de passer à la phase finale qui est l'implémentation.

Le chapitre 05 présente l'environnement de développement ainsi que les outils qui nous ont permis la réalisation de ce travail.

CHAPITRE 01

Le protocole IP



Le chapitre 01 couvre les points suivants :

- I. Introduction**
- II. L'Adressage IP**
- III. Le Protocole IPv4**
- IV. Le Protocole IPv6**
- V. Les Réseaux Hybrides**
- VI. Conclusion**

I. Introduction :

Le protocole IP fait partie de la famille des protocoles réseau du modèle OSI. C'est un des protocoles les plus importants d'internet car il permet l'élaboration et le transport des datagrammes IP (les paquets de données), sans toutefois en assurer la « livraison ». En réalité, le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition [2].

Dans ce premier chapitre nous sommes intéressés à présenter le protocole IP, tout en détaillant le système d'adressage utilisé dans ses deux versions IPv4 et IPv6, ainsi que les différentes techniques permettant la communication entre ces versions.

II. L'Adressage IP :

L'adressage est l'une des premières fonctions des protocoles de la couche réseau. Il permet de mettre en œuvre la transmission de données entre des hôtes situés sur le même réseau ou sur des réseaux différents.

L'adresse IP est basée sur le concept d'hôtes et de réseaux un hôte est tout ce qui peut envoyer ou recevoir des paquets sur le réseau, comme une station de travail ou un routeur.

L'adresse IP est utilisée :

- pour acheminer des paquets IP entre les différents réseaux IP (appelé routage).
- Identifier chaque élément sur la totalité du système d'information (ordinateurs, imprimantes, caméras...) [3].

III. Le protocole IPV4 :

Le protocole internet version 4 (ipv4) permet un adressage hiérarchique des paquets qui transportent les données.

L'élaboration, la mise en œuvre et la gestion d'un modèle d'adressage IPv4 garantissent un fonctionnement optimal pour les réseaux [3].

III.1.Datagramme :

Les données circulent sur Internet sous forme de datagrammes (on parle aussi de paquets). Les datagrammes sont des données encapsulées, c'est-à-dire des données auxquelles on a ajouté des en-têtes correspondant à des informations sur leur transport (telles que l'adresse IP de destination).

Les données contenues dans les datagrammes sont analysées (et éventuellement modifiées) par les routeurs permettant leur transit [3].

Le tableau suivant présente le format d'un datagramme :

32 bits				
Version (4 bits)	Longueur d'en-tête (4 bits)	Type de service (8 bits)	Longueur totale (16 bits)	
Identification (16 bits)			Drapeau (3 bits)	Décalage fragment (13 bits)
Durée de vie (8 bits)		Protocole (8 bits)	Somme de contrôle en-tête (16 bits)	
Adresse IP source (32 bits)				
Adresse IP destination (32 bits)				
Données				

Tableau 1.1 : Table de datagramme IPv4 [3].

Voici la signification des différents champs :

- **Version** (4 bits) : il s'agit de la version du protocole IP que l'on utilise (actuellement on utilise la version 4 *IPv4*) afin de vérifier la validité du datagramme. Elle est codée sur 4 bits.
- **Longueur d'en-tête**, ou *IHL* pour *Internet Header Length* (4 bits) : il s'agit du nombre de mots de 32 bits constituant l'en-tête (la valeur minimale est 5). Ce champ est codé sur 4 bits.
- **Type de service** (8 bits) : il indique la façon selon laquelle le datagramme doit être traité.
- **Longueur totale** (16 bits) : il indique la taille totale du datagramme en octets. La taille de ce champ étant de 2 octets, la taille totale du datagramme ne peut dépasser 65536 octets. Utilisé conjointement avec la taille de l'en-tête, ce champ permet de déterminer où sont situées les données.
- **Identification, drapeaux (flags) et déplacement de fragment** sont des champs qui permettent la fragmentation des datagrammes, ils sont expliqués plus bas.
- **Durée de vie** appelée aussi **TTL**, pour *Time To Live* (8 bits) : ce champ indique le nombre maximal de routeurs à travers lesquels le datagramme peut

passer. Ainsi ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit le datagramme. Cela évite l'encombrement du réseau par les datagrammes perdus.

- **Protocole** (8 bits) : ce champ, en notation décimale, permet de savoir de quel protocole est issu le datagramme
 - ICMP : 1
 - IGMP : 2
 - TCP : 6
 - UDP : 17
- **Somme de contrôle de l'en-tête, ou en anglais *header checksum* (16 bits)** : ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission. La somme de contrôle est le complément à un de tous les mots de 16 bits de l'en-tête (champ *somme de contrôle* exclu). Celle-ci est en fait telle que lorsque l'on fait la somme des champs de l'en-tête (somme de contrôle incluse), on obtient un nombre avec tous les bits positionnés à 1.
- **Adresse IP source** (32 bits) : Ce champ représente l'adresse IP de la machine émettrice, il permet au destinataire de répondre.
- **Adresse IP destination** (32 bits) : adresse IP du destinataire du message [3].

III.2. Le format des adresses IPv4 :

Une adresse IP version 4 est une séquence de 32 bits composée de 1 et de 0.

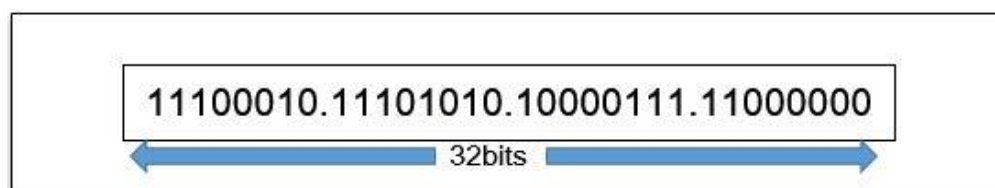


Figure 1.1 : Le format des adresses IPv4.

Afin de faciliter leur lecture, les adresses IP sont généralement exprimées sous forme de quatre nombres décimaux séparés par des points.

Exemple :

L'adresse IP d'un ordinateur : 192.168.1.8 correspond à la valeur : 11000000.10101000.00000001.00001000 en notation binaire.

Chaque élément d'une adresse est un octet, donc, il représente une valeur comprise entre 0 et 255.

Chaque adresse IP comporte également deux parties :

- La première partie « partie réseau » identifie le réseau auquel la machine est connectée.
- La seconde partie « partie hôte » identifie la machine [5].

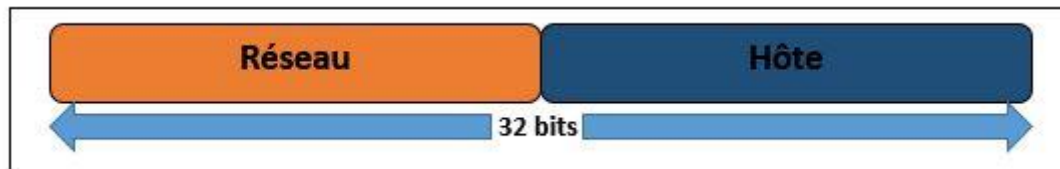


Figure 1.2 : Le format des adresses IPv4.

III.3. Les Classes des Adresses IPv4 :

À l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser le cheminement (ou le routage) des paquets entre les différents réseaux et de permettre l'adaptation à des réseaux de différentes tailles (grande, moyenne et petite taille) et de faciliter leur classification.

Un bit, ou une séquence de bits, situé en début d'adresse détermine la classe de l'adresse. Il existe cinq classes d'adresses IP [5] :

III.3.1. Les adresses IPv4 de Classe A :

Elles utilisent le premier octet pour indiquer l'adresse réseau. Les trois octets suivants sont utilisés pour définir les adresses hôte.



Figure 1.3 : Le format des adresses IPv4 de la classe A [2].

Le premier bit d'une adresse de classe A est toujours « 0 ». Les adresses sont entre : 00000000 (0 en décimal) et 01111111 (127 en décimal). Les valeurs 0 et 127 sont réservées et ne peuvent pas être utilisées comme adresses réseau. Ainsi, toute adresse commençant par une valeur comprise entre 1 et 126 dans le premier octet est une adresse de classe A.

Les adresses de la classe A sont réservées aux réseaux de très grande taille, avec plus de 16 millions d'adresses hôte disponibles [5].

III.3.2. Les adresses IPv4 de Classe B :

Elles utilisent les deux premiers octets pour indiquer l'adresse réseau. Les deux autres sont utilisés pour les adresses hôte.



Figure 1.4 : Le format des adresses IPv4 de la classe B [2].

Les deux premiers bits du premier octet d'une adresse de classe B sont toujours « 10 ». L'adresse la plus faible 10000000 (128 en décimal) et la plus élevée est 10111111 (191 en décimal). Toute adresse commençant par une valeur comprise entre 128 et 191 dans le premier octet est une adresse de classe B.

Les adresses de la classe B sont réservées aux réseaux de taille moyenne ou grande [5].

III.3.3. Les Adresses IPv4 de Classe C :

Elles constituent l'espace le plus utilisé des classes d'adresses. Elles utilisent trois octets pour représenter l'adresse réseau et un octet pour définir l'adresse hôte.



Figure 1.5 : Le format des adresses IPv4 de la classe C [2].

Une adresse de classe C commence par la valeur binaire « 110 ». L'adresse la plus faible 11000000 (192 en décimal) et la plus élevée est 11011111 (223 en décimal). Toute adresse contenant un nombre compris entre 192 et 223 dans le premier octet est une adresse de classe C.

Les adresses de classe C sont réservées aux réseaux de petite taille (254 hôtes maximum) [5].

III.3.4. Les Adresses IPv4 de Classe D :

Réservées à la diffusion multicast d'une adresse IP. Les quatre premiers bits doivent correspondre à « 1110 ». Par conséquent, le premier octet d'une adresse de classe D est compris entre 11100000 et 11101111 (soit 224 et 239 en décimal).



Figure 1.6 : Le format des adresses IPv4 de la classe D [2].

Toute adresse IP commençant par une valeur comprise entre 224 et 239 dans le premier octet est une adresse de classe D. Une adresse de multicast est une adresse réseau unique qui achemine les paquets associés à une adresse de destination vers des groupes prédéfinis d'adresses IP [5].

III.3.5. Les Adresses IPv4 de Classe E :

Utilisées à des fins expérimentales par IETF. Les quatre premiers bits d'une adresse de classe E sont toujours des « 1 ». Par conséquent, le premier octet d'une adresse de classe E est compris entre 11110000 et 11111111 (soit 240 et 255 en décimal). Aucune adresse de classe E n'est disponible sur Internet [5].



Figure 1.7 : Le format des adresses IPv4 de la classe E [2].

Le tableau suivant récapitule la plage d'adresses IP du premier octet (sous forme binaire et décimale) de chaque classe d'adresse IP :

Classe d'@ IP	Plage d'adresses	Nbr des bits Partie Net	Nbr des réseaux	Nbr d'hôtes par réseau
Classe A	1-126	8	126	16777216
Classe B	128-191	16	16384	65535
Classe C	192-223	24	2097152	254
Classe D	224-239	/		
Classe E	240-255	/		

Tableau 1.2 : La plage d'adresse IPv4.

Remarque :

Il existe des exceptions :

- La plage d'adresses 127.x.x.x est réservée : utilisée pour les tests et diagnostics.
- Le réseau 0.0.0.0 est réservé : utilisée notamment pour définir une route par défaut sur un routeur.
- Pour déterminer la partie de l'adresse qui correspond au réseau et celle qui correspond à l'hôte, vous devez d'abord identifier la classe de l'adresse IP [5].

III.4. Les types d'adresses IPv4 :

Il existe trois types d'adresses IP :

- **Adresse IPv4 publique :**

Les adresses IP publiques sont utilisées uniquement sur internet. Les routeurs disposent d'une adresse IP publique côté internet, ce qui le rend visible sur ce réseau. Mais aussi, lorsque vous accédez à un site web vous utilisez l'adresse publique du serveur web.

Une adresse IP publique est unique dans le monde, elle fait partie des classes A, B et C à l'exception des adresses privées ou bien réservées.

- **Adresse IPv4 privé :**

Les adresses IP privées représentent toutes les adresses IP de classe A, B et C que l'on peut utiliser dans un réseau local (LAN) c'est-à-dire dans le réseau de votre entreprise ou dans le réseau domestique. De plus, les adresses IP privées ne peuvent pas être utilisées sur internet (car elles ne peuvent pas être routées sur internet), les hôtes qui les utilisent sont visibles uniquement dans

vosre réseau local, les classes A, B et C comprennent chacune une plage d'adresses IP privées à l'intérieur de la plage globale.

- Les Adresses privées de la classe A : **10.0.0.0** à **10.255.255.255**.
- Les adresses privées de la classe B : **172.16.0.0** à **172.31.255.255**.
- Les adresses privées de la classe C : **192.168.1.0** à **192.168.255.255** [5].

- **Adresse IPv4 réservé :**

Certaines adresses hôte sont réservées et ne peuvent pas être affectées aux équipements du réseau. Ces adresses sont :

- **L'adresse réseau (IPv4) :** L'adresse réseau est celle dont tous les bits hôte sont à 0. Elle est utilisée pour identifier le réseau lui-même.

Exemple : Dans un réseau de classe B, les 16 derniers bits forment la partie hôte, ainsi, l'adresse 176.10.0.0 est une adresse réseau.

- **L'adresse de broadcast (IPv4) :** Est une adresse IP dont tous les bits hôtes sont à 1. Elle est utilisée pour diffuser des paquets vers tous les équipements d'un réseau.

Exemple : dans l'exemple précédent, les 16 derniers bits forment la partie hôte, ainsi, l'adresse de broadcast est 176.10.255.255 (255 correspond à la valeur décimale d'un octet contenant 11111111).

III.5. Le Masque réseau :

Une adresse IP comporte une partie réseau et une partie hôte. Afin de différencier ces deux numéros, un masque de réseau est nécessaire.

Le masque de réseau est une adresse IP dont les bits de la partie réseau sont à 1 et ceux de la partie hôte à 0. Ce masque permet d'obtenir l'adresse réseau en effectuant une opération **AND logique** sur l'adresse et le masque de réseau. Le masque est très important dans le cas d'un découpage en sous réseaux [5].

Remarque :

Dans une adresse IP de classe B, la partie réseau comporte les deux premiers octets, et les deux derniers sont ceux de la partie machine, le masque de réseau d'une adresse de classes B est : 11111111.11111111.00000000.00000000 --> 255.255.0.0

Soit l'adresse IP : 176.11.16.1, pour avoir l'adresse réseau, on fait : (176.11.16.1) AND (255.255.0.0) = 176.11.0.0 [5].

III.6. Les Sous-réseaux (Subnetting) :

En 1992 l'IETF a identifié deux problèmes :

- 1) Pénurie d'adresses réseaux IPv4 non affectées.
- 2) Augmentation rapide de la taille des tables de routage d'Internet.

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 [6].

Si cette technique est ancienne, elle n'en est pas moins efficace face aux problèmes d'exploitation des réseaux contemporains.

Le découpage d'un réseau en sous-réseaux permet de fragmenter un réseau de grande taille en segments (ou sous-réseaux) plus petits, plus faciles à gérer et plus efficaces.

III.6.1. Les Avantages du découpage en sous-réseaux :

- Faciliter la gestion du réseau.
- Confiner le broadcast.
- Garantir une certaine sécurité sur le réseau LAN. (autoriser ou refuser l'accès à un sous-réseau en fonction de plusieurs critères) [5].

III.6.2. Technique de découpage sous-réseaux :

Pour créer une adresse de sous-réseau, il faut emprunter des bits au champ d'hôte et les désigner comme champ de sous-réseau.

Le nombre de bits à sélectionner dans le processus de découpage en sous-réseaux dépend du nombre maximal d'hôtes requis par sous-réseau.

Pour savoir combien de bits doivent être empruntés, il faut :

- Calculer le nombre de sous-réseaux requis ainsi que le nombre d'hôtes nécessaires au sous-réseau le plus vaste.
- Il faut savoir l'emprunt de N bits donne combien de sous-réseaux utilisables, et combien d'hôtes utilisables pour chaque sous-réseau. Il y a une différence entre les hôtes utilisables et le nombre total d'hôtes (y compris les deux adresses réservées, l'adresse du réseau et celle de broadcast), pour ce faire, la méthode se base sur la formule suivante :

- Nbr sous-réseaux utilisables = $2^{\text{nombre de bits empruntés}} - 2$
- Nbr hôtes utilisables = $2^{\text{nombre de bits hôtes restants}} - 2$

Conditions à respecter :

Le nombre minimal de bits pouvant être empruntés est deux.

L'emprunt d'un seul bit donne : L'adresse du réseau (0) et l'adresse de broadcast (255).

Le nombre maximal de bits pouvant être empruntés est égal au nombre de bits hôte – 2. Si on utilise ce nombre maximal de bits, les sous-réseaux créés ne comporteront que deux hôtes.

Remarque :

- Dans le cas de réseaux de petite taille, il n'est pas toujours utile de créer des sous-réseaux. Cette opération s'impose dans le cas des réseaux de grande taille.
- Il est possible d'itérer ce découpage plusieurs fois (on aura des sous- sous-réseau, etc.) ➡ d'où la notion d'adressage hiérarchique [5].

III.6.3. Le masque de sous-réseau :

Il est possible de diviser une adresse de réseau en plusieurs adresses de sous-réseaux. La création de sous-réseaux permet de résoudre les problèmes organisationnels ou de topologie.

L'application d'un masque des bites appelé « un masque du sous-réseau » (Subnetmask) à l'adresse IP permet de définir un sous-réseau. Le masque de sous-réseau divise le champ host-id en un numéro de sous-réseau et un numéro d'hôtes. Le masque est un nombre à 32 bits dont les valeurs sont définies selon les règles suivantes :

Dans un masque de sous réseau la suite de bits à « 1 » définit la partie réseau. La suite de bits à « 0 » définit la partie Hôte [2].

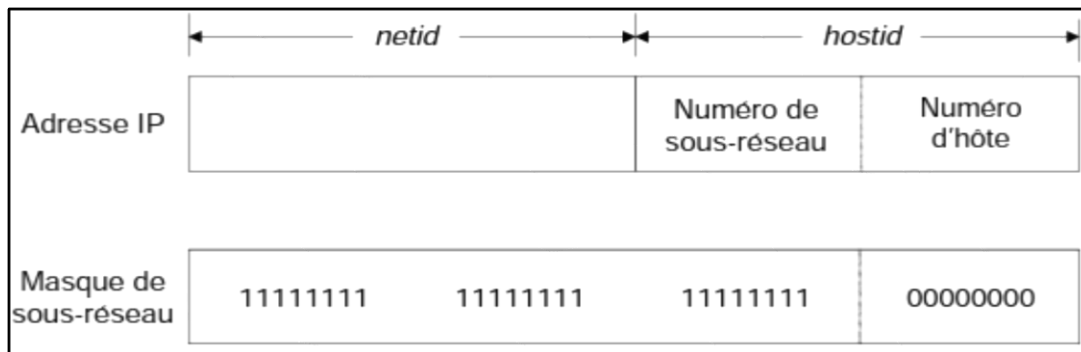


Figure 1.8 : Le format du masque sous-réseau de la classe C [2].

Le sous-réseau n'est reconnu que localement. Dans le reste d'Internet, l'adresse est toujours interprétée comme étant une adresse IP standard [2].

III.7. Le Principe du NAT (Network Adresses Translation) :

Le mécanisme de translation d'adresses (en anglais *Network Address Translation* noté **NAT**) a été mis au point afin de répondre à la pénurie d'adresses IPV4.

En effet, en adressage IPv4, le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines d'être connectées à internet. Le principe du NAT consiste donc à utiliser une passerelle de connexion à internet, possédant au moins une interface réseau connectée sur le réseau local et au moins une interface réseau connectée à Internet (possédant une adresse IP routable), pour connecter l'ensemble des machines du réseau [7].

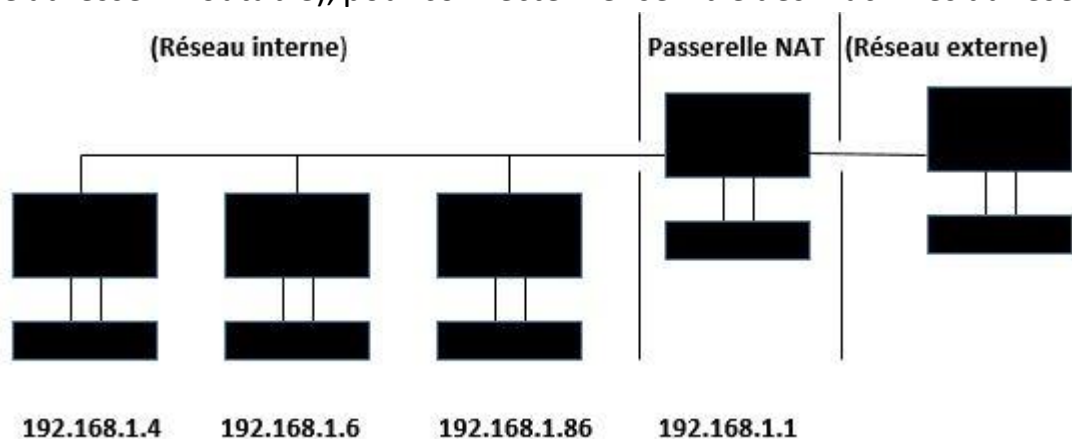


Figure 1.9 : Un exemple sur la structure d'un réseau utilise le NAT.

Il s'agit de réaliser, au niveau de la passerelle, une translation (littéralement une « traduction ») des paquets provenant du réseau interne vers le réseau externe.

Ainsi, chaque machine du réseau nécessitant d'accéder à internet est configurée pour utiliser la passerelle NAT (en précisant l'adresse IP de la passerelle dans le champ « Gateway » de ses paramètres TCP/IP). Lorsqu'une machine du réseau effectue une requête vers Internet, la passerelle effectue la requête à sa place, reçoit la réponse, puis la transmet à la machine ayant fait la demande [7].

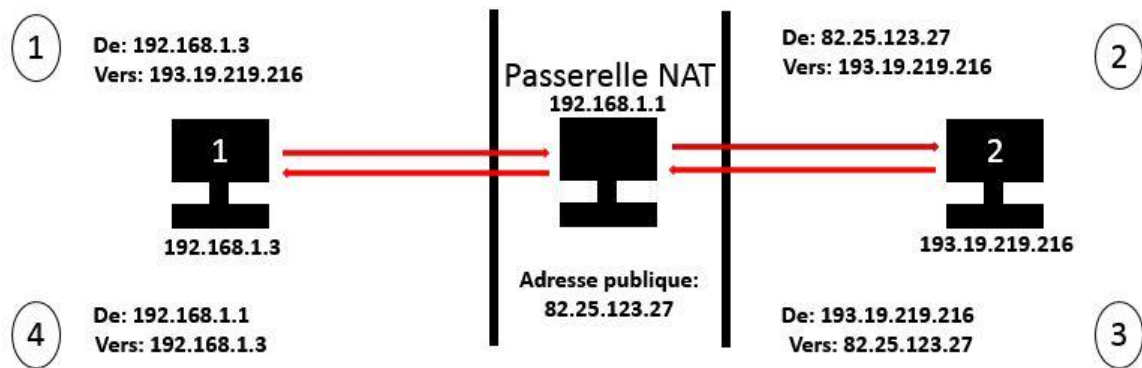


Figure 1.10 : Envoi et réception de données entre deux hôtes utilisent le NAT.

Étant donné que la passerelle camoufle complètement l'adressage interne d'un réseau, le mécanisme de translation d'adresses permet d'assurer une fonction de sécurisation. En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de l'adresse IP de la passerelle [7].

III.7.1. Les types de Translation :

III.7.1.a. NAT statique :

Le principe du NAT statique consiste à associer une adresse IPV4 publique à une adresse IP privée interne au réseau. Le routeur (ou plus exactement la passerelle) permet donc d'associer à une adresse IPv4 privée (par exemple 192.168.0.1) une adresse IPv4 publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IPv4 [7].

La translation d'adresse statique permet ainsi de connecter des machines du réseau interne à internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où n adresses IPv4 routables sont nécessaires pour connecter n machines du réseau interne [7].

III.7.1.b. NAT dynamique :

Le NAT dynamique permet de partager une adresse IPV4 routable (ou un nombre réduit d'adresses IPv4 routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement la même adresse IPv4. C'est la raison pour laquelle le terme de « **mascarade IP** » (en anglais *IP masquerading*) est parfois utilisé pour désigner le mécanisme de translation d'adresse dynamique.

Afin de pouvoir « multiplexer » (partager) les différentes adresses IPv4 sur une ou plusieurs adresses IP routables le NAT dynamique utilise le mécanisme de translation de port (**PAT** - *Port Address Translation*), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IPv4 du routeur [7].

III.8. L'attribution des adresses IPv4 :

Dans Internet l'adresse IPv4 publique d'un équipement est unique. Afin de garantir qu'une même adresse IPv4 publique n'est pas utilisée deux fois, un organisme IANA (Internet Assigned Numbers Authority) gère scrupuleusement les adresses IPv4 disponibles.

Les adresses IPv4 publiques doivent être obtenues auprès d'un fournisseur d'accès Internet (FAI).

Il existe plusieurs façons d'attribuer une adresse IPv4 à un équipement :

- Statique : L'équipement possède toujours la même adresse.
- Dynamique : L'équipement se voit attribuer une adresse différente à chaque connexion au réseau [8].

Remarque :

- Un ordinateur peut être connecté à plusieurs réseaux. Ainsi, il reçoit plusieurs adresses.
- Chaque point de connexion, ou interface, dispose d'une adresse [5].

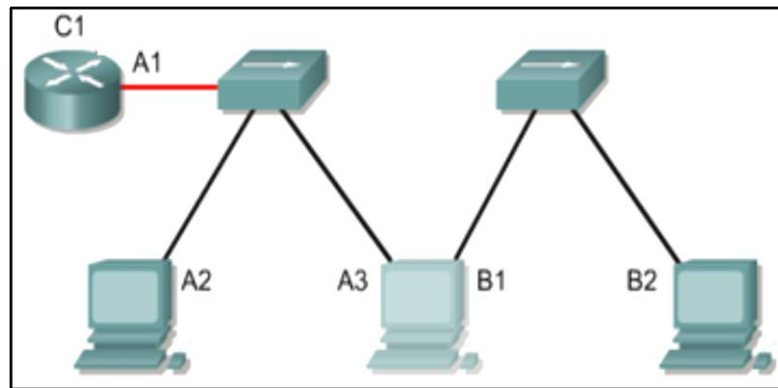


Figure 1.11 : Exemple d'une topologie réseau [5].

IV. Le protocole IPv6 :

La croissance du nombre d'utilisateurs et des serveurs d'Internet s'accompagne d'un épuisement des adresses IPv4, c'est-à-dire de la saturation progressive de la quantité d'adresses IPv4 publiques disponibles. La saturation menace la croissance du réseau Internet. En février 2011, la réserve de blocs libres d'adresses publiques IPv4 est arrivée à épuisement.

Une adresse IPV4 comporte 32 bits, ce qui permet de créer jusqu'à 4 milliards ($4\,294\,967\,296 = (2^{32})$) de numéros. Certaines adresses ne sont cependant pas assignables à des ordinateurs parce qu'elles sont réservées à des usages particuliers (comme les adresses de groupe multicast ou le bloc 240.0.0.0/4).

D'autre part, la technique d'assignation aux utilisateurs ne permet pas d'utiliser toutes les adresses possibles en raison de contraintes liées au découpage en sous-réseaux.

L'économie des adresses IP n'a pas été une préoccupation du début d'Internet. Certaines entreprises se sont vu attribuer des blocs « /8 » (soit 16 millions d'adresses) ou « /16 » (65536 adresses) qui dépassaient souvent largement leurs besoins réels.

La multiplication des équipements mobiles et connectés en permanence a également augmenté la demande en adresses.

Plusieurs techniques ont été proposées pour résoudre le problème ou repousser l'échéance de l'épuisement complet des adresses IP :

- l'adressage *classless* a permis une meilleure efficacité dans l'utilisation des adresses IP.

- les registres Internet régionaux (RIR) ont développé des politiques d'assignation d'adresses plus contraignantes, qui tiennent compte des besoins réels à court terme. L'assignation de blocs d'adresses plus petits diminue cependant l'efficacité de l'agrégation des adresses.
- NAT, qui permet à de nombreux ordinateurs d'un réseau privé de partager une adresse publique, mais qui nuit au bon fonctionnement de certains protocoles.
- l'utilisation de blocs d'adresses autrefois réservés (comme 14.0.0.0/8).
- la récupération, sur base volontaire, des blocs attribués généreusement autrefois.
- la récupération des blocs assignés autrefois et qui ne sont pas annoncés sur Internet.
- le commerce de blocs d'adresses IP dans un *marché* entre clients, prédit par certains.
- **IPv6**, la nouvelle version du Protocole Internet développée dans ce but pendant les années 1990, et dont la capacité d'adressage est considérable.

IPv6 est l'aboutissement des travaux menés au sein de l'IETF au cours des années 1990 pour succéder à IPv4 et ses spécifications ont été finalisées dans la RFC 2460 en décembre 1998.

Grâce à des adresses de 128 bits au lieu de 32 bits, IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4. Cette quantité d'adresses considérable permet une plus grande flexibilité dans l'attribution des adresses et une meilleure agrégation des routes dans la table de routage d'Internet. La traduction d'adresse, qui a été rendue populaire par le manque d'adresses IPv4, n'est plus nécessaire.

IPv6 dispose également de mécanismes d'attribution automatique des adresses et facilite la renumérotation. La taille du sous-réseau, variable en IPv4, a été fixée à 64 bits en IPv6. L'en-tête du paquet IPv6 a été simplifié et des types d'adresses locales facilitent l'interconnexion de réseaux privés [3].

IV.1. Format de paquet et fonctionnalités d'IPv6 :

Les paquets IPv6 ont la forme générale suivante :

Entête IPv6 (40 octets)	Extension de l'entête (0 ou n octets)	PDU – niveau transport
----------------------------	--	------------------------

Figure 1.12 : Le Format de paquet IPv6.

IV.2. L'adressage IPv6 :

L'adressage sous IPv6 se fait désormais sur 128 bits (au lieu de 32 bits sur IPv4). Cette version n'utilise pas la notion de classes, on a seulement un adressage hiérarchique par préfixe. L'adressage se fait désormais par l'attribution d'une partie d'adresse fixe qui définit le réseau, cette partie est appelée le préfixe.

Cet adressage hiérarchique consiste en l'attribution d'un préfixe au premier routeur d'un réseau, sur 10 bits par exemple. Le routeur du sous réseaux aura lui une partie fixe qui sera celle de son père plus un complément de préfixe qui lui sera imposé. Et ainsi de suite l'attribution des adresses se fait de manière hiérarchique [3].

IV.2.1. Représentation des adresses IPv6 :

La taille des adresses IPv6 a donc été quadruplée comparativement à celle d'IPv4, Ce qui permet d'obtenir un espace adressable nettement plus large.

Une adresse sur IPv6 est un ensemble de 8 mots de 2 octets, qui sont en fait, 8 groupes de 4 lettres hexadécimales séparés par « : ».

(Ex : FEDC:BA98:7654:3210:FEDC:BA98:7654:3210).

Dans un champ, il n'est pas nécessaire d'écrire les zéros placés en tête. En outre plusieurs champs nuls consécutifs peuvent être abrégés par « :: ».

Ainsi les deux notations suivantes sont équivalentes :

FEDC:0000:0000:0000:0400:A987:0043:210F .

FEDC::400:A987:43:210F .

Plus particulièrement, l'adresse formée uniquement par des zéros est représentée comme suit « :: ».

Naturellement, pour éviter toute ambiguïté, l'abréviation «::» ne peut apparaître qu'une fois au plus dans une adresse.

La représentation des préfixes IPv6 est similaire à la notation CIDR utilisée pour les préfixes IPv4.

Un préfixe IPv6 est donc représenté par la notation :
adresse-ipv6 / longueur-du-préfixe -en-bits.

Les formes abrégées avec «::» sont autorisées :

Exemple :

```
3EDC:BA98:7654:3210:0000:0000:0000:0000/64
3EDC:BA98:7654:3210:0:0:0:0/64
3EDC:BA98:7654:3210::/64
::/0 (défaut) .
```

Enfin on peut combiner l'adresse d'une interface et la longueur du préfix réseau associé en une seule notation :

3EDC:BA98:7654:3210:945:1321:ABA8:F4E2/64 [9].

IV.2.2. Les types d'adresses IPV6 :

IPv6 reconnaît trois types d'adresses :

- **Adresses Globales UNICAST : Découpage géographique Grace aux préfix :**

L'utilisation de préfixes séparés pour les adresses affectées à un fournisseur et les adresses affectées à une zone géographique constitue un compromis entre deux différentes visions du futur réseau Internet. Chacun de ces fournisseurs dispose d'une fraction réservée de l'espace d'adressage (adresses unicast = 1/8 de cet espace). Les 5 premiers bits qui suivent le préfixe « 0010 » (2000::/3) sont utilisés pour indiquer dans quel " registre " se trouve le fournisseur d'accès. Actuellement, trois registres sont opérationnels, pour l'Amérique du nord, l'Europe et l'Asie. Jusqu'à 29 nouveaux registres pourront être ajoutés ultérieurement.

Chaque registre est libre de diviser les 15 octets restants comme il l'entend. Une autre possibilité est d'utiliser un octet pour indiquer la nationalité du fournisseur et de laisser toute liberté aux octets suivant pour définir une structure d'adresses spécifique.

Le modèle géographique est le même que celui du réseau Internet actuel, dans lequel les fournisseurs d'accès ne jouent pas un grand rôle. Dans ce cadre, IPv6 peut gérer deux types d'adresses :

A. Les adresses unicast Locales(ULA) : Utilisent le préfixe FC00::/7, elles sont équivalentes aux adresses IPV4 privées . Elles peuvent être réutilisées par d'autres organisations sans qu'il y ait de conflit. Elles ne peuvent pas être propagées hors des limites des organisations, ce qui les rend bien adaptées à celles qui utilisent des gardes-barrières pour protéger leur réseau privé du réseau Internet.

Si elles sont correctement générées (tirage aléatoire des 40 bits suivant le préfixe FD00::/8) elles permettront d'interconnecter des réseaux par VPN avec moins d'une chance sur mille milliards de conflit .

B. Les adresses de liens locaux : (préfixe FE80::/10) Il n'ont qu'une spécification locale sur l'interface.

Toutes ces adresses, si elles utilisent la procédure de création automatique ont généralement 8 octets qui représentent le réseau et 8 octets représentant l'interface sur ce réseau.

- **Adresses MULTICAST :**

Ayant un préfixe de "FF00::/8 ", les adresses de diffusion multidentinaire disposent d'un champ Drapeau (4 bits) et d'un champ *Envergure* (4 bits) à la suite du préfixe, puis d'un champ Identificateur de groupe (112 bits). L'un des bits du drapeau distingue les groupes permanents des groupes transitoires.

Le champ Envergure permet une diffusion limitée sur une zone.

- **Adresses ANYCAST :**

En plus de supporter l'adressage point à point classique (unicast) et l'adressage de diffusion multidentinaire (multicast) IPv6 supporte un nouveau type d'adressage de diffusion au premier vu (anycast).

Cette technique est similaire à la diffusion multidentinaire dans le sens où l'adresse de destination est un groupe d'adresses, mais plutôt que d'essayer de livrer le datagramme à tous les membres du groupe, il essaie de le livrer à un seul membre du groupe, celui le plus proche ou le plus à même de le recevoir [7].

Remarque :

Il existe d'autres types d'adresses :

- Adresse indéterminée : l'adresse indéterminée est utilisée comme adresse source par un équipement du réseau pendant son initialisation, avant d'acquérir une adresse. Sa valeur est 0:0:0:0:0:0:0:0 (ou en abrégé « :: »).
- Adresse de bouclage (loopbackaddress) : L'adresse de bouclage vaut 0:0:0:0:0:0:0:1, soit en abrégé « :: 1 ». Il s'agit de l'équivalent de l'adresse 127.0.0.1 d'IPv4. Elle est utilisée par un équipement du réseau pour envoyer un paquet IPv6 à lui-même [10].

V. Les Réseaux Hybrides :

V.1. Définition :

Un réseau hybride est un réseau qui est reposé à la fois à des réseaux qui utilisent le protocole IPv4 et d'autres qui utilisent le protocole IPv6.

Afin de garantir une transition le plus en douceur possible, IPv6 permet une certaine compatibilité avec IPv4. Un certain nombre de mécanismes sont chargés d'effectuer des opérations de « conversion » entre les adresses sur 128bits d'IPv6 et celles d'IPv4 [11].

V.2. Les mécanismes de la transition d'IPv4 vers IPv6 :

V.2.1. Double pile :

Ce principe consiste à avoir un système capable de gérer en même temps les deux protocoles simultanément. Aujourd'hui, les systèmes d'exploitation modernes et un certain nombre d'équipements sont capables de faire cela.

Les deux piles cohabitent en même temps et indépendamment sur le système et en fonction du service demandé, le système va utiliser la pile IPv4 ou la pile IPv6 indifféremment. Ce système implique d'avoir les deux piles configurées correctement et est entièrement transparent pour l'utilisateur. Cette solution est actuellement la meilleure et doit être utilisée en priorité.

Une machine IPv6 est capable de communiquer aussi bien avec une machine IPv4 qu'avec une machine IPv6 en utilisant ces deux types d'adresses :

A. Adresses IPv4 mappées :

Une machine IPv6 est capable de communiquer avec une machine IPv6 aussi bien qu'avec une machine IPv4 en utilisant des adresses IPv4 mappées. Il s'agit seulement d'une représentation des adresses IPv4 dans IPv6. En réalité, ces adresses n'apparaissent jamais sur le réseau. Ces adresses sont de la forme ::FFFF:a.b.c.d, par exemple : (::FFFF:192.168.216.1).

B. Adresses IPv4 compatibles :

Une machine IPv6 communiquant avec une autre machine IPv6 via un tunnel automatique IPv6 sur IPv4 peut utiliser des adresses IPv4 compatibles IPv6. Ces adresses sont notées la manière suivante : ::a.b.c.d, par exemple : (::192.168.1.4).

V.2.2. Les tunnels IPv6 dans IPv4 :

Cette technologie consiste à créer des « tunnels ». Cela signifie que lors d'un transfert de paquets IPv6 entre deux équipements, celles-ci seront encapsulées à l'intérieur d'un paquet IPv4. Il existe deux types de tunnels : les tunnels statiques et les tunnels automatiques.

V.2.2.a. Les tunnels statiques :

Les tunnels statiques fonctionnent suivant le même principe que les réseaux privés virtuels (VPN). Cette technique impose de connaître les adresses IPv4 de chaque extrémité du tunnel.

L'utilisation de tunnels ne permet pas de profiter de toutes les innovations du protocole IPv6. L'intérêt de cette technologie est de pouvoir faire communiquer entre eux deux sites IPv6 distants à travers un réseau ne supportant que le protocole IPv4.

V.2.2.b. Les tunnels dynamiques :

Les tunnels dynamiques permettent la création automatique de tunnels IPv6 sur IPv4 en cas d'absence de connectivité IPv6 native. Il existe divers protocoles pour réaliser cette opération :

- **Le 6to4 :** Ce système est décrit dans la RFC 3056 et 3068 et est dédié à la communication entre deux sites IPv6 distants via un réseau IPv4. Il permet à 2 réseaux IPv6 de communiquer entre eux en passant par l'intermédiaire d'un réseau IPv4.

La présence d'un routeur est nécessaire. Ce routeur attribue à l'équipement une adresse IPv6 constituée à partir de son adresse IPv4. Par exemple, si l'adresse publique du routeur est 23.54.65.123 et le préfixe du réseau IPv6 est FEC0, les opérations suivantes seront réalisées :

Transformation de l'adresse IPv4 en notation hexadécimale (1736:417B) puis ajout de cette adresse au préfixe IPv6 (FEC0:1736:417B). A cette adresse de réseau sera ajoutée les identifiants de chaque équipement. Le paquet sera ensuite encapsulé dans un paquet IPv4 puis transmis au routeur 6to4 distant.

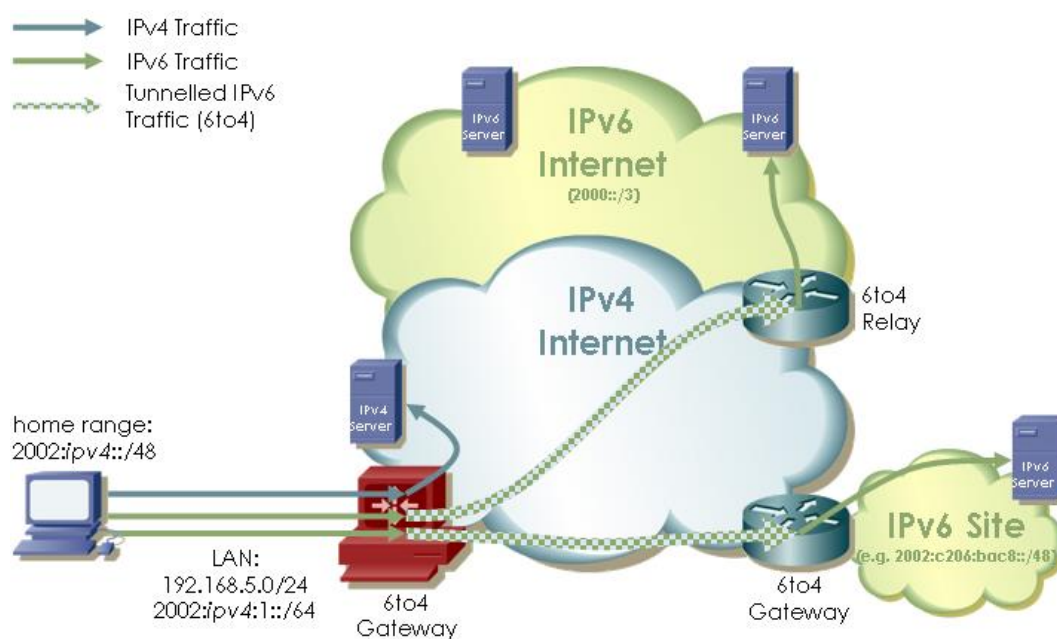


Figure 1.13 : Schéma d'un tunnel 6to4 [13].

- **Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) :**

Ce système est conçu pour permettre à un équipement IPv6 isolé dans un réseau IPv4 de communiquer avec un réseau IPv6 distant via une passerelle supportant IPv6.

Une adresse ISATAP sera composée ainsi :

[Préfix du réseau distant]:0000:5EFE :[adresse IPv4 de l'équipement].

Après encapsulation dans un paquet IPv4, les données seront envoyées vers la passerelle qui les retransmettra à leur destinataire.

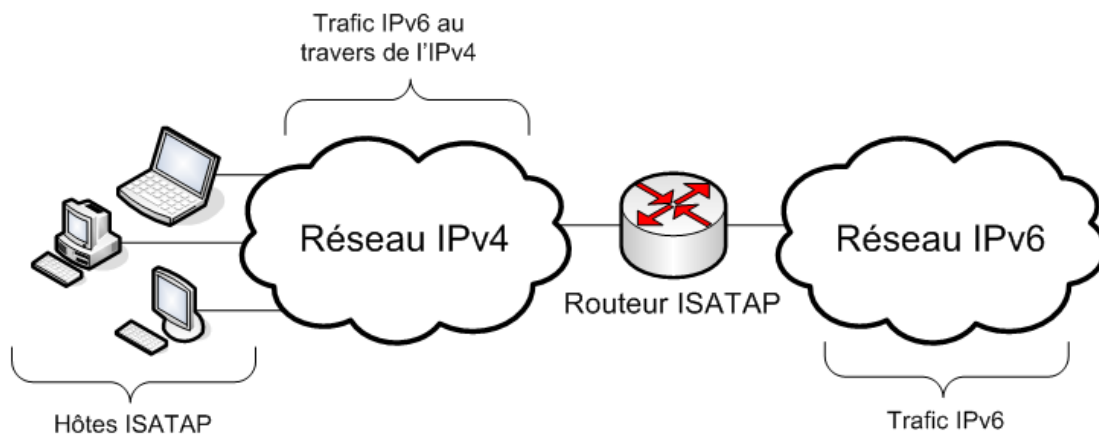


Figure 1.14 : Schéma d'un tunnel ISATAP[13].

- **Teredo** : Cette technologie a été développée par Microsoft pour pallier aux défauts de 6to4.

6to4, le protocole d'encapsulation IPv6 sur IPv4 le plus courant, nécessite que le matériel au bout du tunnel d'encapsulation ait une adresse IPv4 publique. Pourtant actuellement et pour combler l'épuisement des adresses IPv4, la plupart de ses hôtes sont reliés au réseau IPv4 par un périphérique faisant du NAT. Ainsi, l'adresse publique est assignée à ce périphérique NAT et c'est donc lui qui doit implémenter le protocole 6to4. Malheureusement, une grande partie de ces équipements ne peuvent pas être mis à jour pour fournir le support de 6to4 pour des raisons techniques ou économiques.

Teredo permet de résoudre ce problème en encapsulant les paquets IPv6 dans des datagrammes UDP/IPv4, que la plupart des NAT peuvent transmettre correctement. Ainsi, les hôtes IPv6 derrière des NAT peuvent être utilisés comme points de terminaison du tunnel Teredo, même quand ils n'ont pas une adresse IPv4 publique dédiée. En effet, un hôte implémentant le protocole Teredo peut acquérir une connectivité IPv6 sans la coopération de l'environnement du reste du réseau local [12].

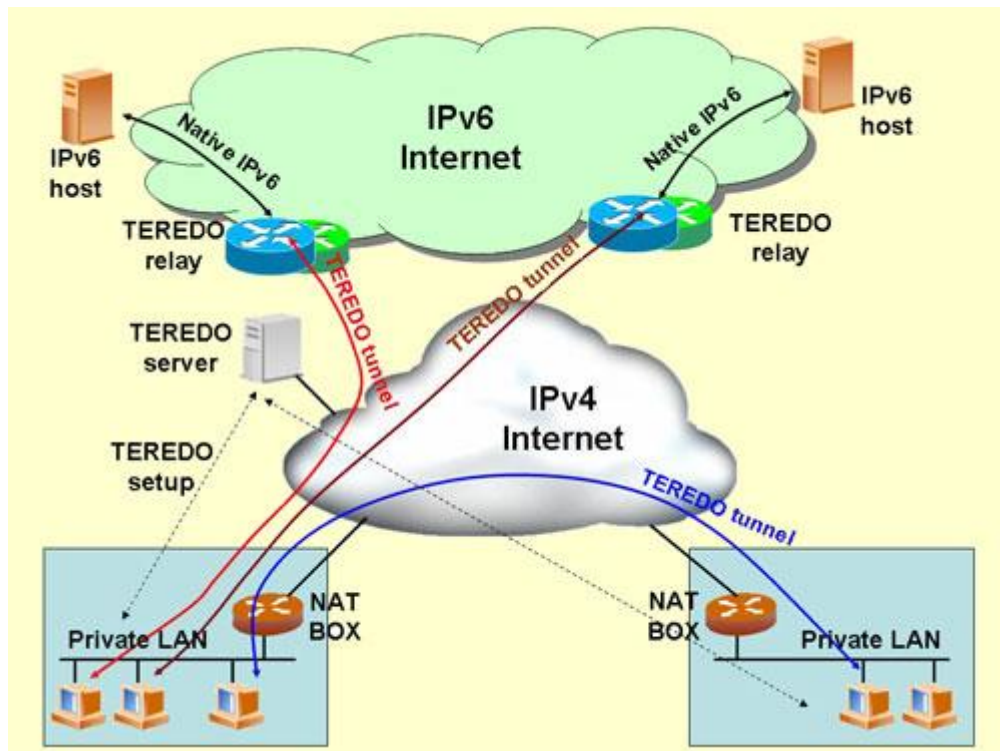


Figure 1.15 : Schéma d'un tunnel TOREDO [13].

- **GRE :** est un protocole de tunnel qui a été à l'origine développé par Cisco, et qui peut réaliser plus de choses que le tunnel IP. Par exemple : vous pouvez aussi transporter du trafic multi-diffusion (*multicast*) et de l'IPv6 à travers un tunnel GRE [11].

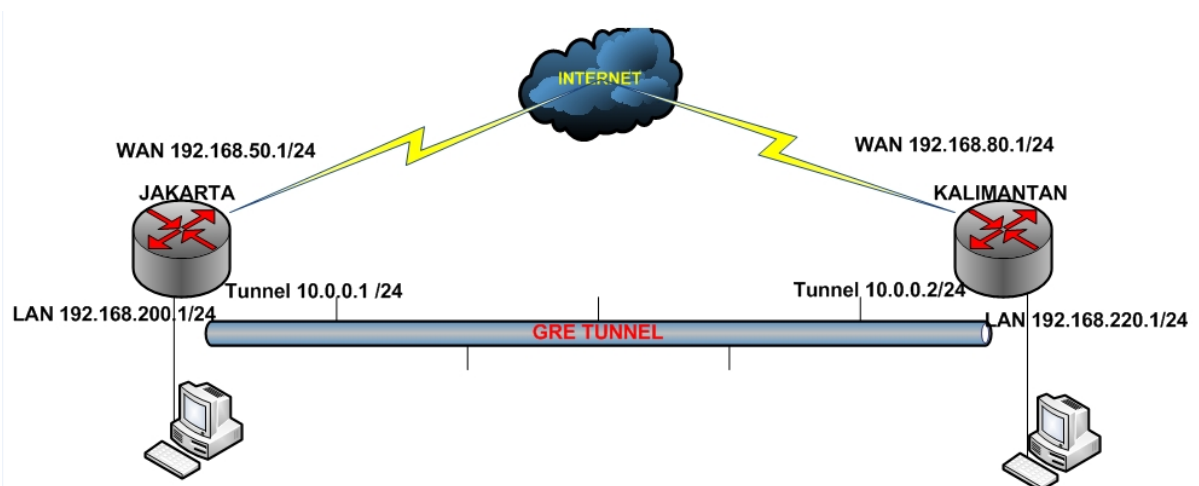


Figure 1.16 : Schéma d'un tunnel GRE [13].

Tunnel	Config	Utilisation suggéré	Avantage	Inconvénient
GRE	manuel	Simple tunnels point-à-point.	Un control maximal du réseau à cause de la configuration manuel qui va faciliter le diagnostic.	Complexité de la configuration.
ISATAP	Automatique	Un tunnel point-à-multipoint qui peut être utilisé pour connecter des systèmes à l'intérieur d'un site.	permet aux entreprises de déployer IPv6 de façon simple et gérable au sein de leur infrastructure avec peu de temps et d'efforts.	Nécessite une configuration dual-stack.
TORERO		Un tunnel point-à-multipoint qui peuvent être utilisés pour connecter des sites IPv6 isolées.	Peut passer à travers presque tous les Nat.	Le taux d'échec pour Teredo est certainement élevé. Environ 37%. Affecte la sécurité.
6TO4		établir des tunnels de type point-to-multipoint de façon totalement dynamique.	pouvoir par exemple, ajouter 100 routeurs dans votre topologie sans pour autant remettre en cause la configuration de vos routeurs existants puisque tout s'établit de façon dynamique.	il ne prend pas en charge les IGP, et ne supporte pas le NAT. Requièrre une adresse ipv4 publique.

Tableau 1.3 : Tableau comparatif des tunnels.

VI. Conclusion :

Dans ce chapitre, nous avons présenté le protocole de la couche internet du modèle TCP/IP, c'est le noyau de communication dans la pluparts des réseaux qui existe dans le monde. Ensuite nous avons détaillé le concept d'adressage utilisé dans les différentes versions de ce protocole, IPv4 et IPv6 et en fin nous avons abordé les techniques permettant la conception des réseaux complexe combinant IPv4 avec IPv6.

CHAPITRE 02

Planification des réseaux



Le chapitre 02 couvre les points suivants :

- I. Introduction**
- II. Problématique**
- III. Approche proposée**
- IV. Maquette du projet**
- V. Conclusion**

I. Introduction :

Après avoir présenté dans le chapitre précédent, les différents systèmes d'adressages des réseaux (IPv4, IPv6 ainsi que les réseaux hybrides combinant les deux versions d'IP), nous nous concentrons dans ce qui suit à spécifier les problématiques liées à la planification des réseaux informatiques afin de cibler les orientations de notre étude.

Ce chapitre a pour objectif majeur de présenter une vision sur la solution WEB que nous proposons dans ce projet afin de développer un assistant ou bien un outil d'aide à la planification des topologies réseaux.

II. Problématique :

Les réseaux informatiques sont des infrastructures très complexes qui doivent faire l'objet d'une bonne planification, de manière à optimiser les coûts d'investissement que nécessite leur mise en place tout en respectant les contraintes liées à la qualité de service à offrir.

Cette planification est un processus délicat visant à déterminer les composants (matérielle et logicielles) dans le but de minimiser le coût d'exploitation des ressources. Une bonne planification nécessite une large connaissance dans le domaine des réseaux.

Une mauvaise planification du réseau peut nuire au bon fonctionnement du réseau, entraînant parfois des pertes catastrophiques pour les grandes firmes et entreprises. Les problèmes les plus fréquents dont l'utilisateur ou l'administrateur réseaux font face sont :

- Conflit d'adresses IP.
- Problème d'accès aux ressources matérielles et logicielles.
- Diffusion non autorisée des informations.
- Problème de sécurité.
- Mauvaise gestion de la bande passante.

III. Approche Proposée :

Au cœur de tous ces problèmes se situe la nécessité de développer un site web dynamique assurant des services destinés aux clients suivants :

- 1) Etudiant : offrant un guide très pratique pour les travaux dirigés et motivant les étudiants pour le Self-Learning.
- 2) Administrateur réseau : assurant un support d'aide à la planification des réseaux pour les non expérimentés dans ce domaine.

Notre solution regroupe les fonctionnalités suivantes :

- **Se renseigner sur une adresse IP** : Fournir toutes les informations sur une adresse IP (Version 6/Version 4).
- **La segmentation d'un réseau IPv4 en sous réseaux** : Un service très important visant à économiser le temps nécessaire pour effectuer des opérations arithmétiques binaire par un simple clic de bouton affichant des résultats fiables instantanément.
- **L'assistance au choix des tunnels** : Permet d'assister le client pour le choix du meilleur tunnel adapté à son réseau hybride.
- **La documentation** : notre site offre une documentation très riche sur les deux versions du protocole IP ainsi que les techniques utilisées dans les réseaux hybrides.

IV. Maquette du projet :

Notre site est composé de trois volets principaux :

- IPv4 (protocole IP version 4).
- IPv6 (protocole IP version 6).
- IPv4/IPv6 (réseau hybride).

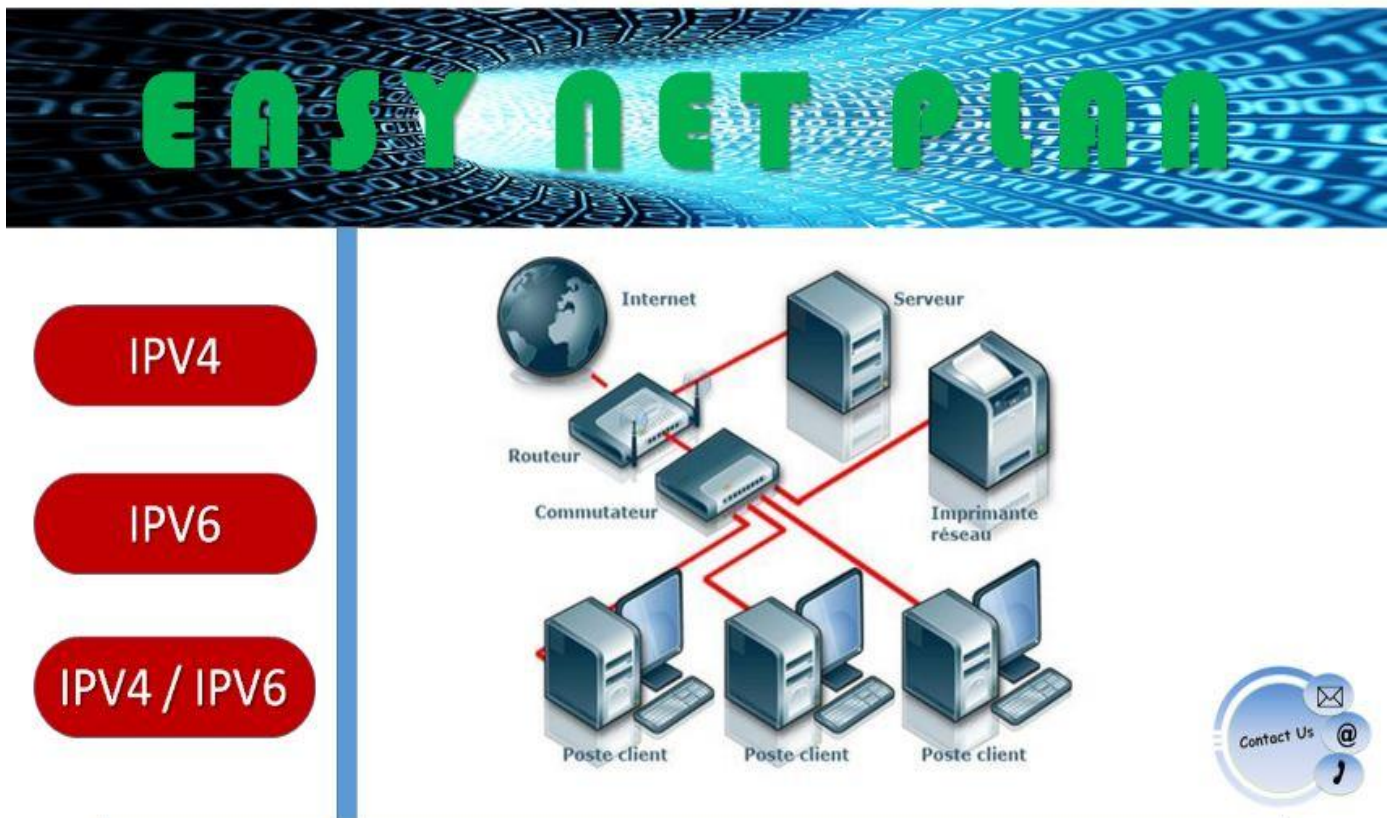


Figure 2.1 : Page d'accueil.

- Page protocole IPv4 :

Cette page offre des services concernant le protocole IPv4 :

- 1) Se renseigner sur une adresse IPv4.
- 2) Segmentation des réseaux IPv4 en sous réseaux.



Figure 2.2 : Les services du protocole IPv4.

- Page se renseigner sur une adresse IPv4 :

Cette page permet à l'utilisateur de lister les informations liées à une adresse IPv4 (type, classe, masque sous réseaux) comme le montre la figure suivante :

The screenshot shows the 'EASY NET PLAN' web application. On the left, there are three buttons: 'IPv4' (highlighted in red), 'IPv6', and 'IPv4 / IPv6'. The main content area is titled 'Se renseigner sur un réseau IPv4'. It features an input field for an IPv4 address with the example '192.168.0.30' and a 'Valider' button. Below the input field, a table displays the calculated network information for the entered address '192.168.1.12'.

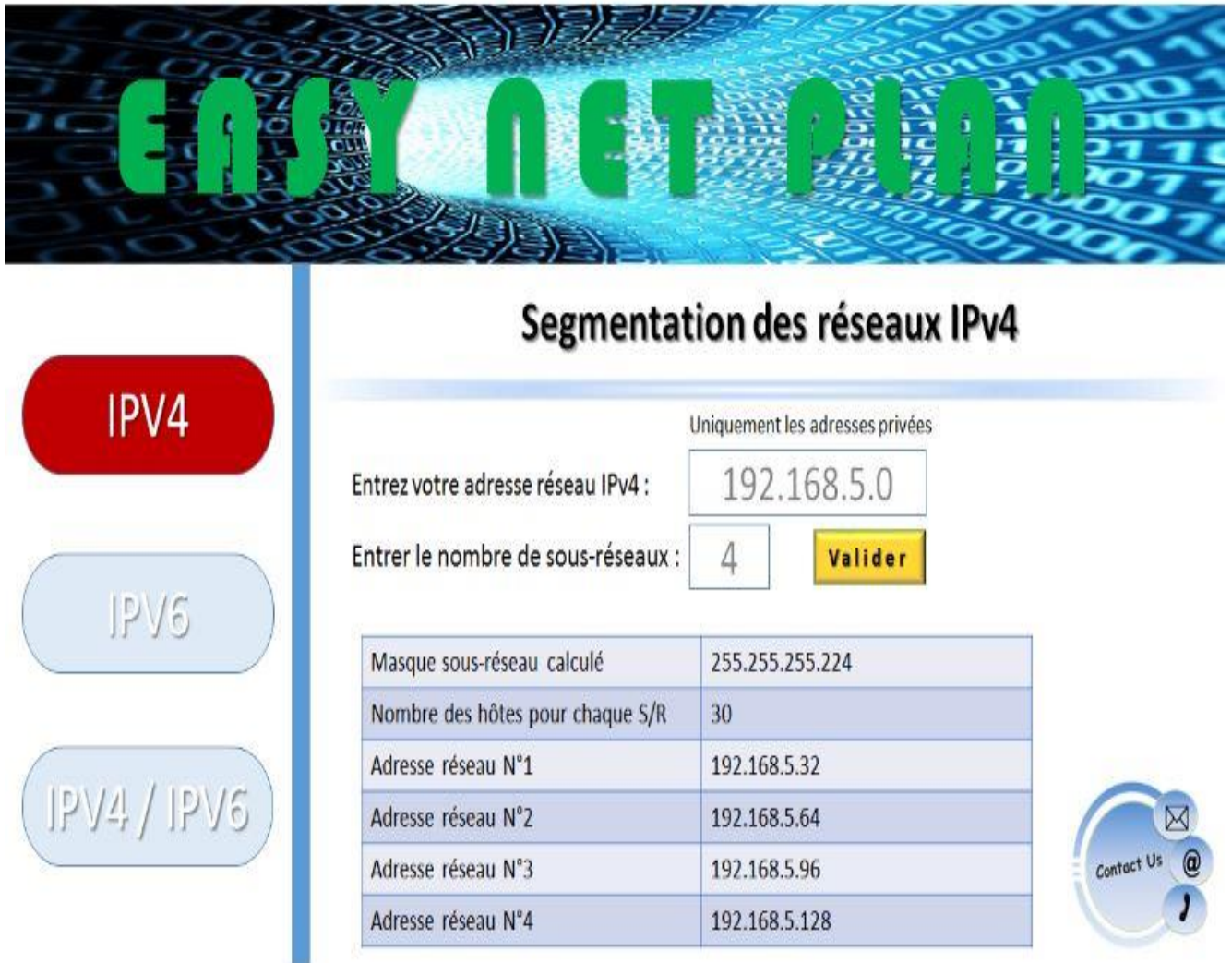
L 'adresse IP:	192.168.1.12
Classe :	C
Type (@ Privée / @ Publique):	Privée
Adresse réseau :	192.168.1.0
Le masque réseau :	255.255.255.0
Adresse du broadcast	192.168.1.255
Nombre des adresses IP clients	254

In the bottom right corner, there is a circular 'Contact Us' button with an email icon and a question mark icon.

Figure 2.3 : Se renseigner sur un réseau IPv4.

- Page segmentation d'une adresse IPv4 :

Depuis cette page l'utilisateur peut segmenter un réseau IPv4 en sous réseaux selon le nombre de sous réseaux dont il a besoin.



Segmentation des réseaux IPv4

Uniquement les adresses privées

Entrez votre adresse réseau IPv4 :

Entrer le nombre de sous-réseaux :

Masque sous-réseau calculé	255.255.255.224
Nombre des hôtes pour chaque S/R	30
Adresse réseau N°1	192.168.5.32
Adresse réseau N°2	192.168.5.64
Adresse réseau N°3	192.168.5.96
Adresse réseau N°4	192.168.5.128

Contact Us

Figure 2.4 : Segmentation d'un réseau IPv4.

- **Page protocole IPv6 :**

À partir de cette page l'utilisateur peut bénéficier de deux services :

- 1) Se renseigner sur une adresse IPv6.
- 2) Compression et décompression d'une adresse IPv6.



Figure 2.5 : Les services de la page du protocole IPv6.

- **Page se renseigner sur une adresse IPv6 :**

Cette page permet à l'utilisateur de connaître différente information Sur une adresse (type, longueur préfix) IPv6 comme le montre la figure suivante :

EASY NET PLAN

Se renseigner sur un réseau IPV6

Entrer votre adresse IPv6 :

L 'adresse IP:	2002:9b99:7b0c::45dd:eefe:4520
Type:	GLOBAL-UNICAST
Longueur du préfix	64

Contact Us

Figure 2.6 : Se renseigner sur une adresse IPv6.

- Page compression/décompression :

Cette page permet à l'utilisateur de compresser une adresse IPv6 ou de la rendre dans sa forme standard.

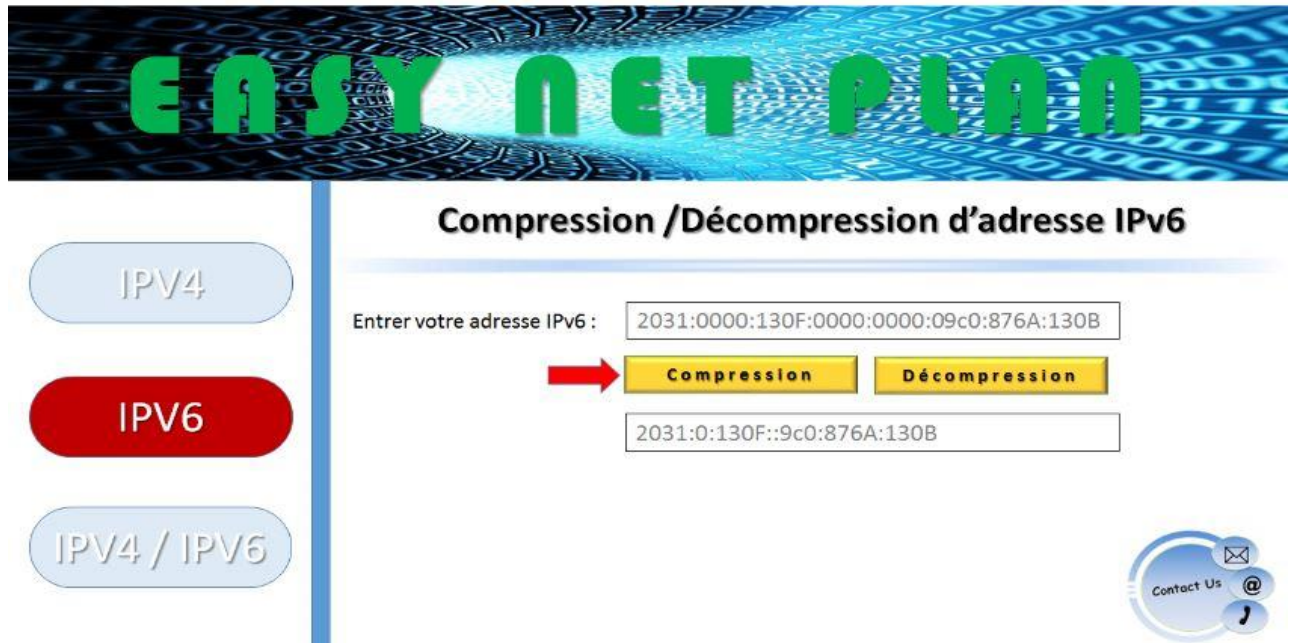


Figure 2.7 : Compression d'une adresse IPv6.

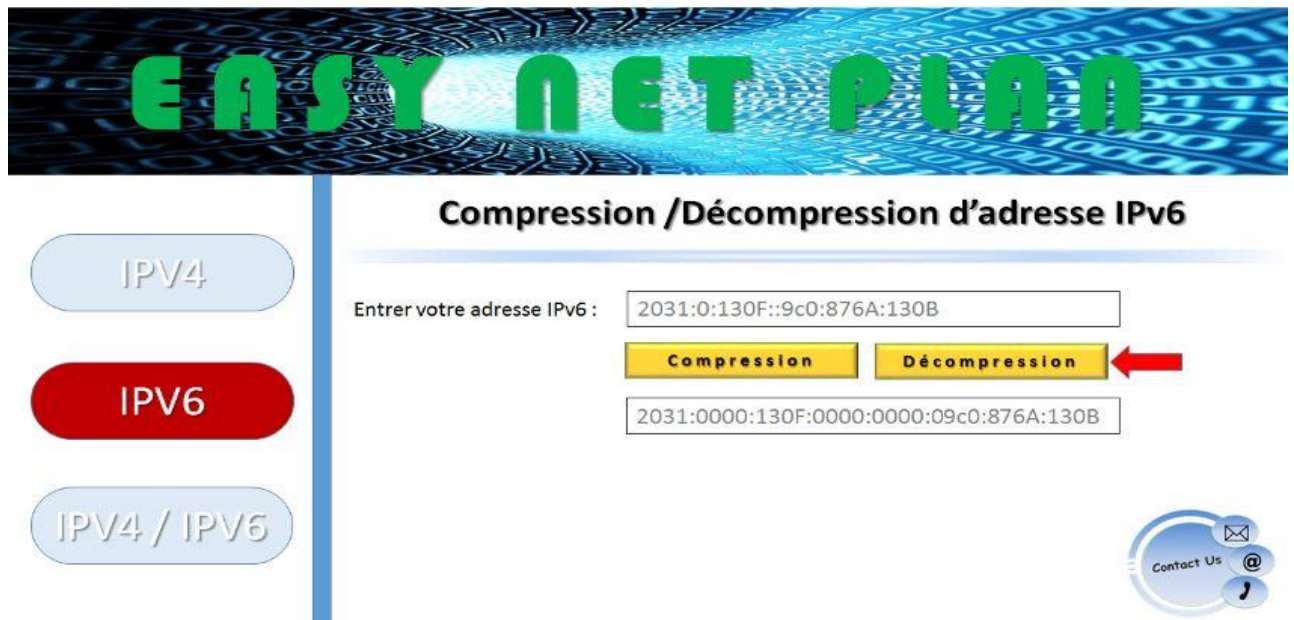


Figure 2.8 : Décompression d'une adresse IPv6.

- **Page IPv6/ipv4 :**

Ce volet assiste au choix du meilleur tunnel à utiliser pour la topologie hybride, afin d'assurer la communication entre les réseaux IPv4 et IPv6, il offre le service d'assistance au choix des tunnels.

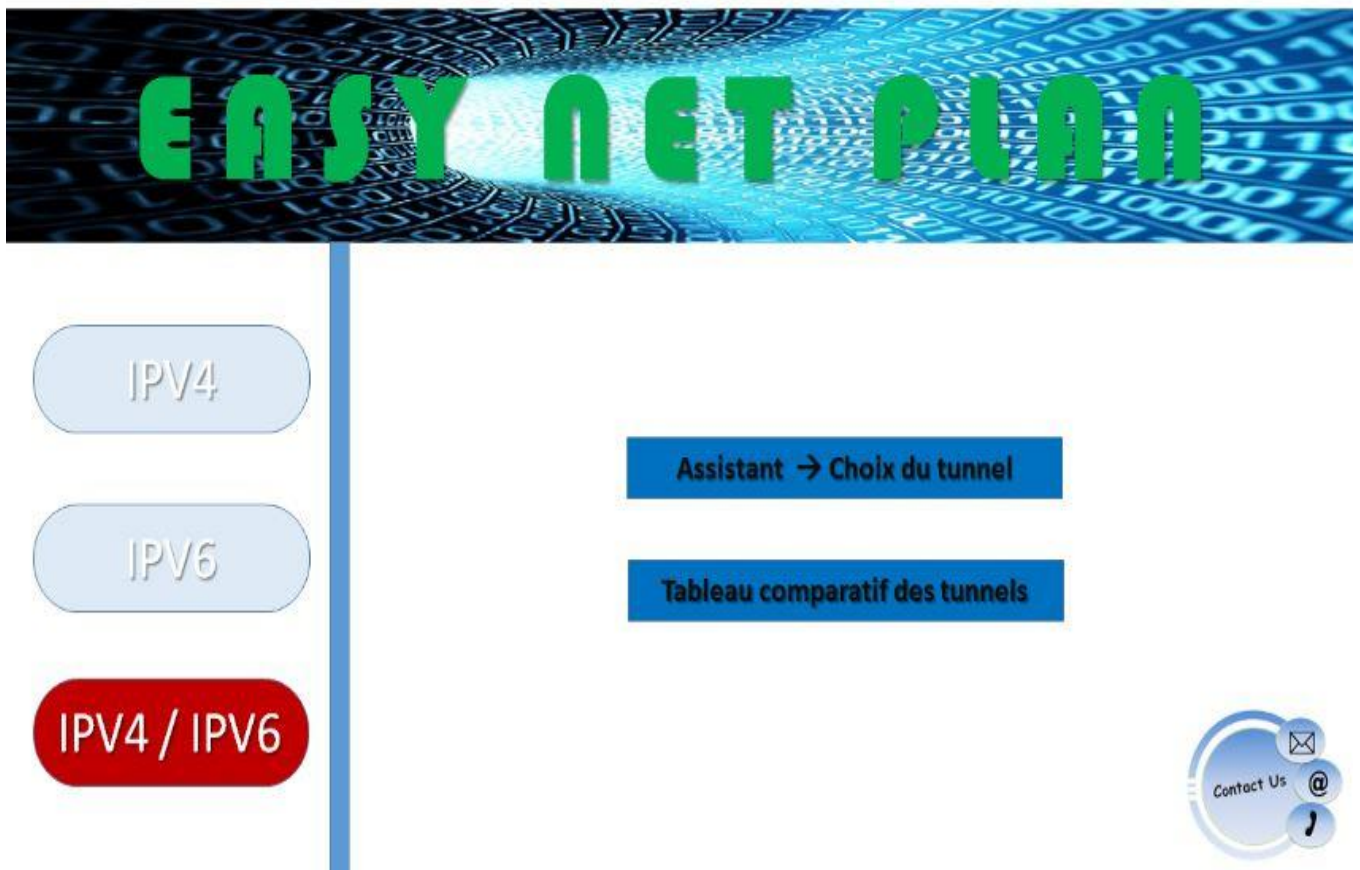


Figure 2.9 : Les services du volet IPv4/IPv6.

- page assistance au choix des tunnels :

Cette page permet à l'utilisateur de bénéficier d'un aide au meilleur choix de tunnels selon ses besoins.



Figure 2.10 : Assistance au choix du meilleur tunnel.



Figure 2.11 : Exemple d'une assistance au choix des tunnels.

V. Conclusion :

Dans ce chapitre nous avons décrit les différentes difficultés et les problèmes que l'administrateur du réseau peut rencontrer durant ses activités de routine.

Cette étude nous a permis de bien tracer les objectifs de notre recherche, à travers une vision concrétisée par une maquette démontrant les différentes fonctionnalités de notre solution WEB.

CHAPITRE 03

Conception du Site WEB



Le chapitre 03 couvre les points suivants :

- I. Introduction**
- II. UML**
- III. Le Modèle des besoins**
- IV. Conclusion**

I. Introduction :

La réalisation d'un site web doit être impérativement précédée d'une méthodologie d'analyse et de conception qui a pour objectif de permettre la formalisation des étapes préliminaires du développement d'un site pour rendre ce développement plus fidèle aux besoins du client.

Pour notre projet nous avons choisi le langage UML (Unified modeling language) que nous allons définir et présenter dans le début de ce chapitre, ensuite nous passerons à la phase de conception qui permet de décrire de manière claire, le fonctionnement futur du système, afin d'en faciliter la réalisation, l'outil utilisé est « Paocestar UML Diagrammer 6.2 » qui offre un ensemble d'outils de modélisation graphique facilitant la conception et simplifiant la réalisation .

II. UML :

II.1. Définition :

UML « Unified Modeling Language » ou « langage de modélisation unifié » est un langage de modélisation graphique à base de pictogrammes. UML n'est pas une méthode mais un ensemble d'outils permettant la modélisation de la future application informatique.

Il est apparu dans le monde du génie logiciel, dans le cadre de la « conception orientée objet ». Couramment utilisé dans les projets logiciels, il peut être appliqué à toutes sortes de systèmes ne se limitant pas au domaine informatique.

II.2. Utilité d'UML :

UML est utilisé pour spécifier, visualiser, modifier et construire les documents nécessaires au bon développement d'un logiciel orienté objet. UML offre un standard de modélisation, pour représenter l'architecture logicielle. Les différents éléments représentables sont :

- Activité d'un objet/logiciel
- Acteurs
- Processus
- Schéma de base de données
- Composants logiciels
- Réutilisation de composants

Grâce aux outils de modélisation UML, il est également possible de générer automatiquement une partie de code, par exemple en langage java, à partir des divers documents réalisés.

UML est donc bien plus qu'un simple outil qui permet de "dessiner" des représentations mentales... Il permet de parler un langage commun, normalisé mais accessible, car visuel.

II.3. Caractéristiques du langage UML :

II.3.1. UML n'est pas une méthode ou un processus !

Si l'on parle de méthode objet pour UML, c'est par abus de langage car une méthode propose aussi un processus, qui régit notamment l'enchaînement des activités de production d'une entreprise.

UML a été pensé pour permettre de modéliser les activités de l'entreprise, pas pour les régir.

L'expérience a prôné que la proposition d'un processus de développement logiciel universel est une utopie car il est :

- Impossible de prendre en compte toutes les organisations et cultures d'entreprises.
- Un processus est adapté au domaine d'activité de l'entreprise, même si un processus constitue un cadre général, il faut l'adapter de manière précise au contexte de l'entreprise [14].

II.3.2. UML est un langage pseudo-formel :

UML est fondé sur un méta modèle, qui définit :

- Les éléments de modélisation.
- La sémantique de ces éléments.

Un méta modèle est une description très formelle de tous les concepts d'un langage. Il limite les ambiguïtés et encourage la construction d'outils.

Le méta modèle d'UML permet de classer les concepts du langage (selon leur niveau d'abstraction ou domaine d'application) et expose sa structure.

UML propose aussi une notation, qui permet de représenter graphiquement les éléments de modélisation du modèle. Cette notation graphique est le support du langage UML [14].

II.3.3. UML cadre l'analyse objet :

UML offre différentes vues (perspectives) complémentaires d'un système, afin de guider son utilisation ainsi que plusieurs niveaux d'abstraction, qui permettent de mieux contrôler la complexité dans l'expression des solutions objets [14].

II.3.4. UML est un support de communication :

La notation graphique d'UML permet d'exprimer visuellement une solution objet, tandis que l'aspect formel de ses notations limite les ambiguïtés et les incompréhensions [14].

II.4. Les points forts d'UML :

- UML est un langage formel et normalisé : il permet un gain de précision et de stabilité.
- Permet une meilleure précision.
- UML est un support de communication performant : il permet grâce à sa représentation graphique, d'exprimer visuellement une solution objet, de faciliter la comparaison et l'évolution de solution.
- Il cadre l'analyse et facilite la compréhension de représentations abstraites complexes.
- Son caractère polyvalent et sa souplesse en font un langage universel [14].

II.5. Les points faibles d'UML :

- La mise en pratique d'UML nécessite un apprentissage et passe par une période d'adaptation.
- Même si l'Espéranto est une utopie, la nécessité de s'accorder sur des modes d'expression communs est vitale en informatique. UML n'est pas à l'origine des concepts objets, mais en constitue une étape majeure, car il unifie les différentes approches et en donne une définition plus formelle.
- Le processus (non couvert par UML) est une autre clé de la réussite d'un projet. Or, l'intégration d'UML dans un processus n'est pas triviale et améliorer un processus est une tâche complexe et longue. Les auteurs d'UML sont tout à fait conscients de l'importance du processus, mais l'acceptabilité industrielle de la modélisation objet passe d'abord par la disponibilité d'un langage d'analyse [14].

II.6. Les diagrammes UML :

UML 2.0 comporte treize types de diagrammes représentant autant de vues distinctes pour représenter des concepts particuliers du système d'information. Ils se répartissent en trois grands groupes :

II.6.1. Diagrammes structurels ou diagrammes statiques (UML structure) :

- Diagramme de classes (Class diagram).
- Diagramme d'objets (Object diagram).
- Diagramme de composants (Component diagram).
- Diagramme de déploiement (Deployment diagram).
- Diagramme de paquetages (Package diagram).
- Diagramme de structures composites (Composite structure diagram) [14].

II.6.2. Diagrammes comportementaux ou diagrammes dynamiques :

- Diagramme de cas d'utilisation (Use case diagram).
- Diagramme d'activités (Activity diagram).
- Diagramme d'états-transitions (State machine diagram).

II.6.3. Diagrammes d'interaction (Interaction diagrams) :

- Diagramme de séquence (Sequence diagram)
- Diagramme de communication (Communication diagram)
- Diagramme global d'interaction (Interaction overview diagram)
- Diagramme de temps (Timing diagram).

Il est très important de noter que la modélisation d'un projet n'exige pas forcément l'utilisation de tous ces diagrammes. Le concepteur à l'intérêt de choisir parmi ces diagrammes ceux qui jugent utiles à son projet [14].

II.7. Mise en œuvre d'UML :

Trouver un "bon" modèle est une tâche difficile mais capitale, parmi les points à respecter pendant la phase de modélisation on cite :

- Opter pour une approche itérative et incrémentale.
- Se concentrer sur l'analyse des besoins des utilisateurs.
- Définition de l'architecture de l'application [14].

II.7.1. Les étapes de la démarche :

Nous présentons dans ce qui suit, l'enchaînement de quelques diagrammes UML, que nous jugeons utile pour la modélisation de notre application.

II.7.1.a. Phase d'identification des besoins et spécialisation des fonctionnalités :

Cette phase regroupe les diagrammes suivants :

- diagramme de cas d'utilisation.
- diagrammes de séquence système.

II.7.1.b. Phase d'analyse :

C'est la phase qui regroupe :

- Model du domaine.
- Diagrammes d'activités de navigation.

II.7.1.c. Phase de conception :

Cette phase est basée sur les diagrammes d'interaction.

III. Le Modèle des besoins :

III.1. Identification des acteurs :

Avant de commencer notre présentation des diagrammes UML nous devons d'abord identifier l'acteur interagissant avec notre système.

Notre site WEB est ouvert au grand public, mais destiné principalement aux étudiants (universitaire ou bien de formation professionnelle) et aux administrateurs réseau.

L'acteur (Etudiant/Administrateur) peut bénéficier et explorer toute les fonctionnalités et services offerts par notre site :

- Se renseigner sur des adresses IPv4 /IPv6.
- Segmentation des sous réseaux IPv4.
- Compression / Décompression des adresses IPv6.
- Assistant au choix des tunnels utilisable dans les réseaux hybride.

III.2. Le diagramme de cas d'utilisation :

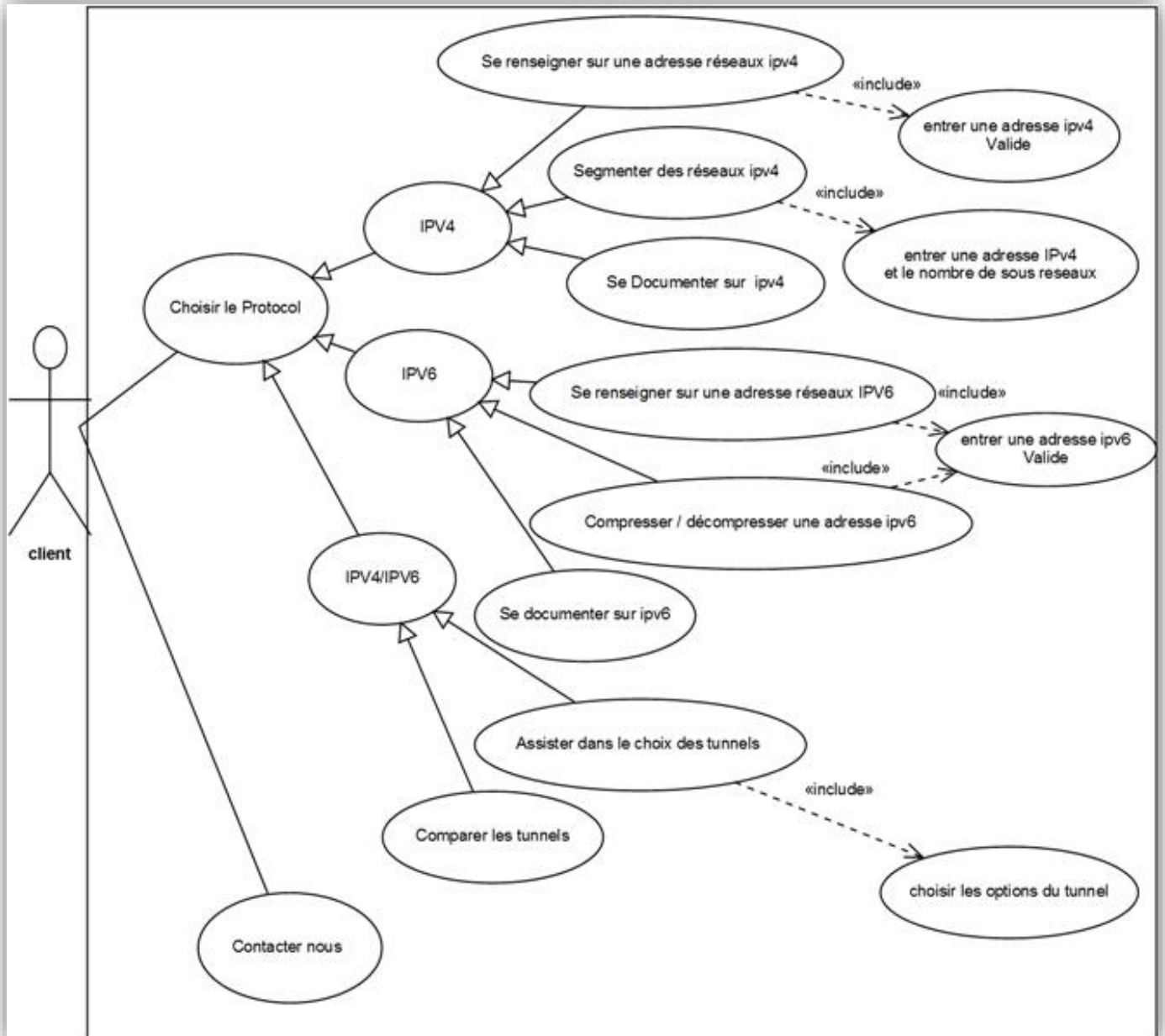


Figure 3.1 : Diagramme de cas d'utilisation.

III.2.1. Cas se renseigner sur une adresse IP :

Cas d'utilisation	Ce cas permet au client de se renseigner sur une adresse IP.
Acteur	Client.
Pré condition	L'adresse IP saisie est valide.
Post condition	Utilisation du service se renseigner sur une adresse IP.
Scénario nominal	1. Le client demande des informations sur une adresse IP 2. Le système demande à l'utilisateur d'introduire son adresse IP 3. Le client saisit son adresse IP et valide. 4. Le système procure les informations sur l'adresse IP introduite par le client.
Scénario alternative	1. L'adresse IP introduite est non valide (champ vide ou adresse incorrecte). 2. Retour à l'étape 2 du scénario nominal

Tableau 3.1 : La fiche descriptive du cas d'utilisation s'informer sur une adresse IP.

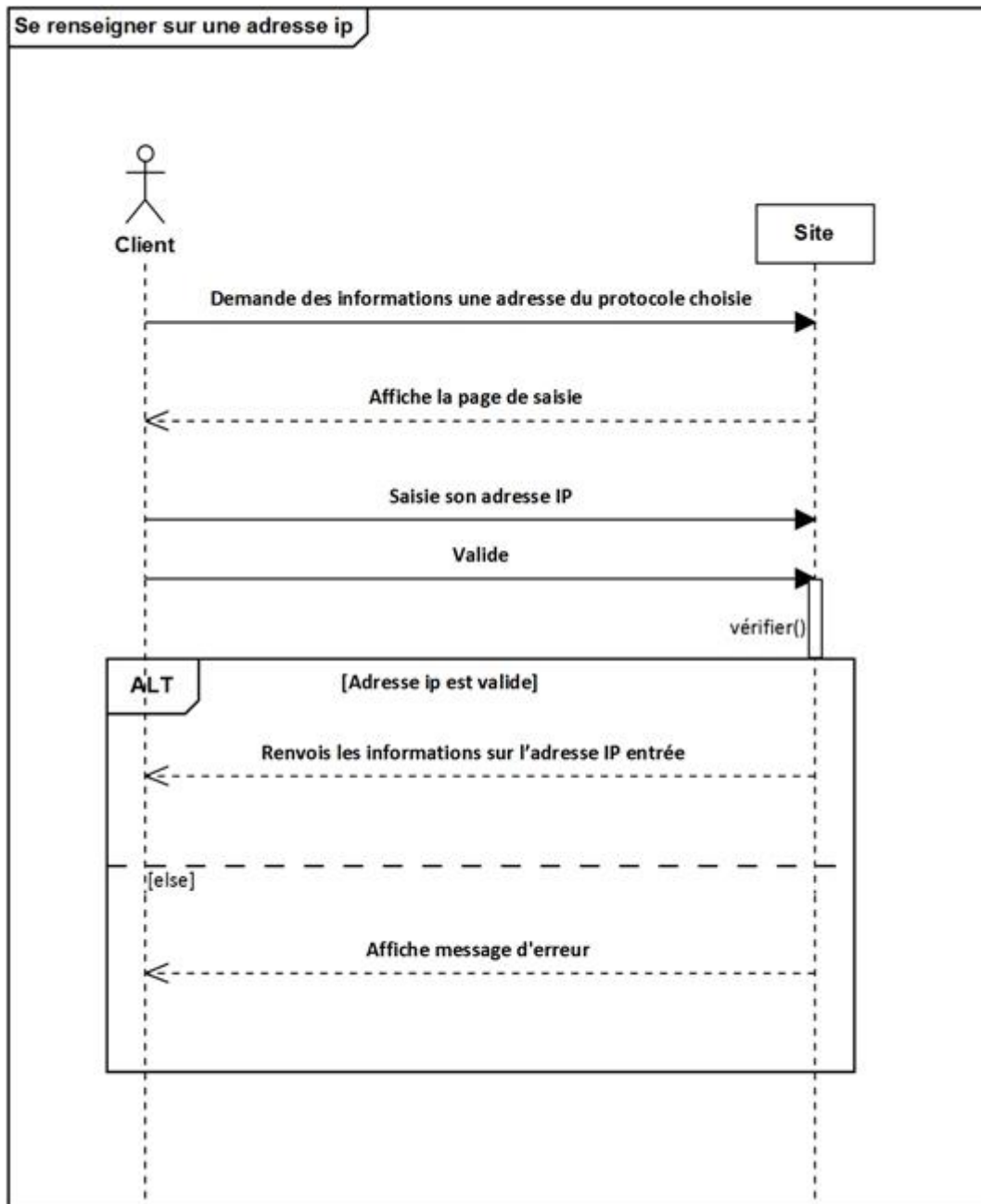


Figure 3.2 : Diagramme de séquence système de cas d'utilisation s'informer sur une adresse IP.

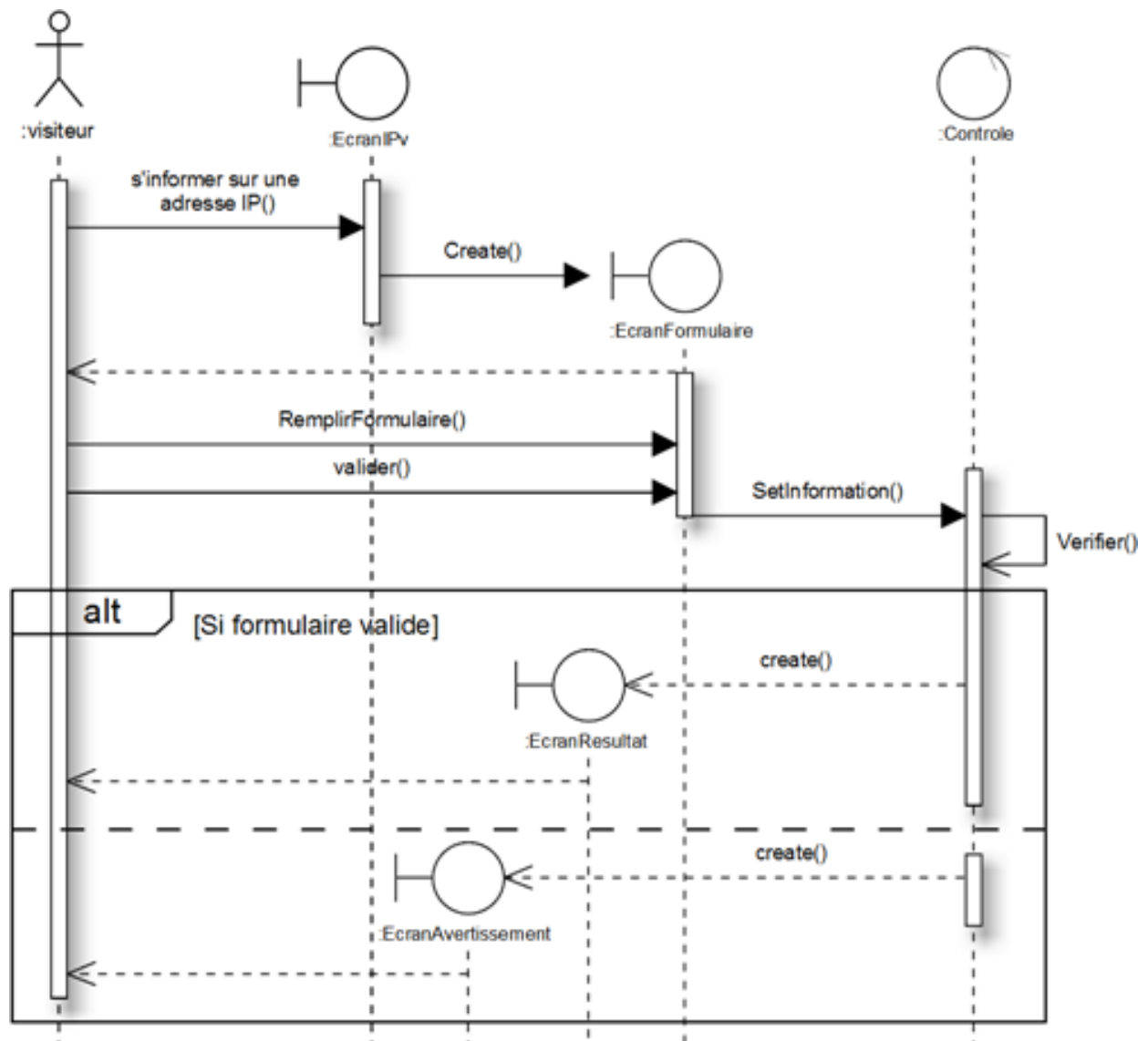


Figure 3.3 : Diagramme de séquence de cas d'utilisation s'informer sur une adresse IP.

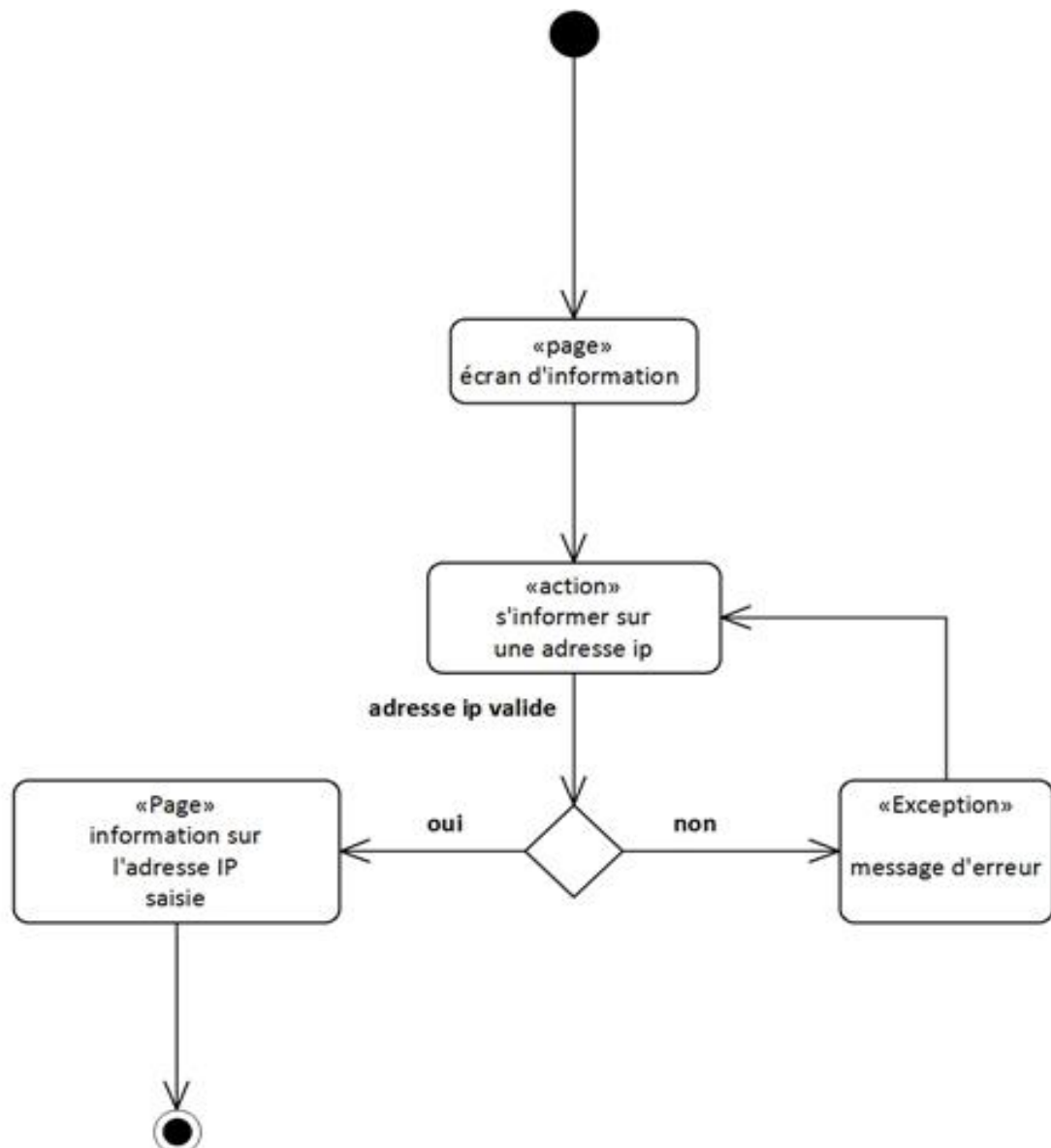


Figure 3.4 : Diagramme de navigation de cas se renseigner sur une adresse IP.

III.2.2. Cas segmentation en sous-réseaux d'une adresse IPv4 :

Description	Ce cas permet au client de segmenter des adresses réseaux ipv4.
Acteur	Client.
Pré condition	L'adresse IPv4 saisie est valide et le nombre de sous réseau introduit est conforme à la classe de cette adresse IPv4.
Post condition	Utilisation du service segmenter un réseau IPv4.
Scénario nominal	1. Le client demande une segmentation de son réseau IPv4. 2. Le système demande au client d'introduire une adresse ipv4 et le nombre de sous réseaux. 3. Le client saisit l'adresse ipv4 et le nombre de sous réseau. 4. Le système procure la segmentation au client.
Scénario alternative	1. Le client a laissé un champ vide ou l'adresse IPv4 est incorrecte ou bien le nombre de sous réseau n'est pas conforme au limite de la classe de l'adresse IPv4. 2. Retour à l'étape 2.

Tableau 3.2 : La fiche descriptive du cas d'utilisation segmentation en sous-réseaux d'une adresse IPv4.

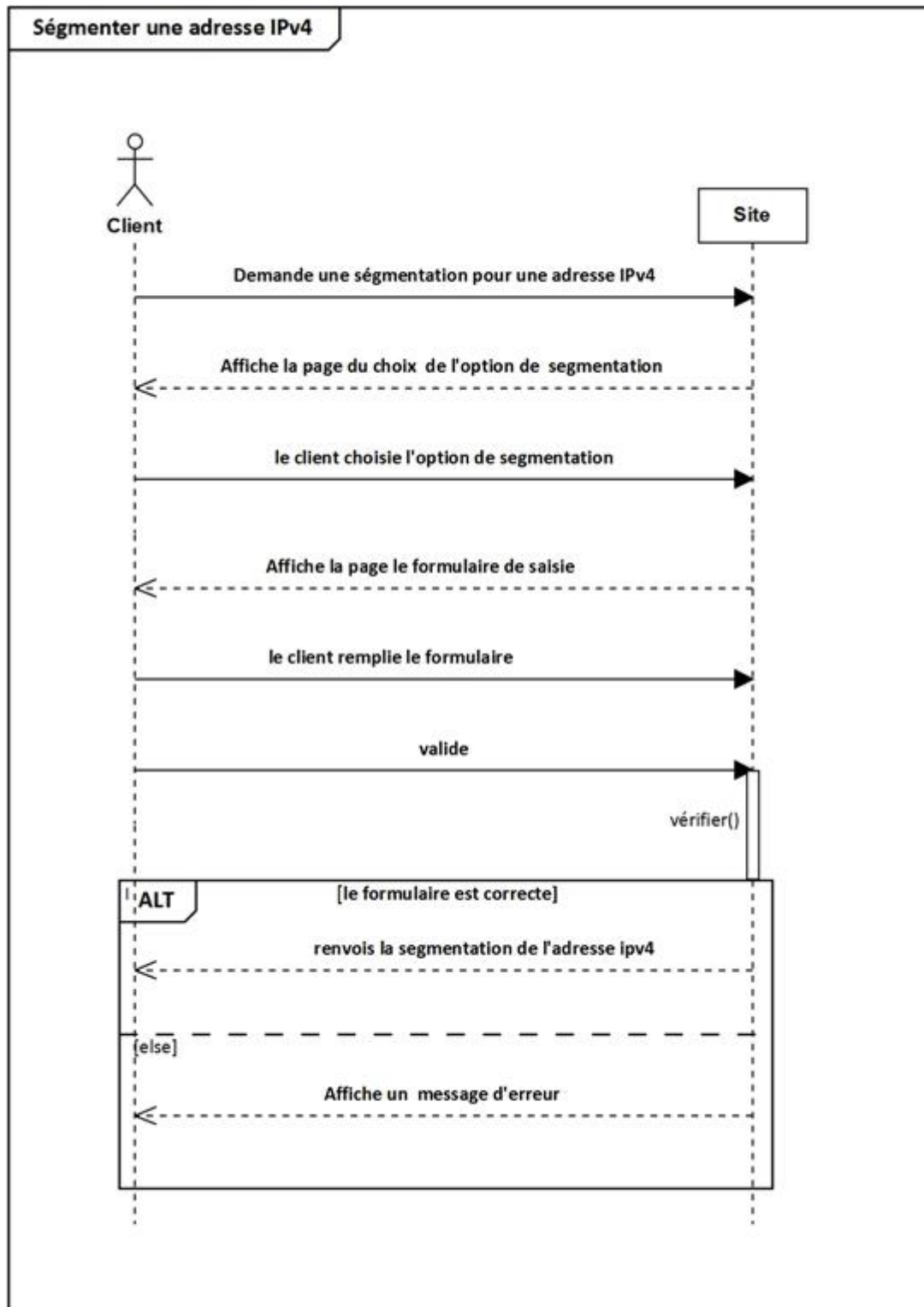


Figure 3.5 : Diagramme de séquence système de cas d'utilisation segmentation en sous-réseaux d'une adresse IPv4.

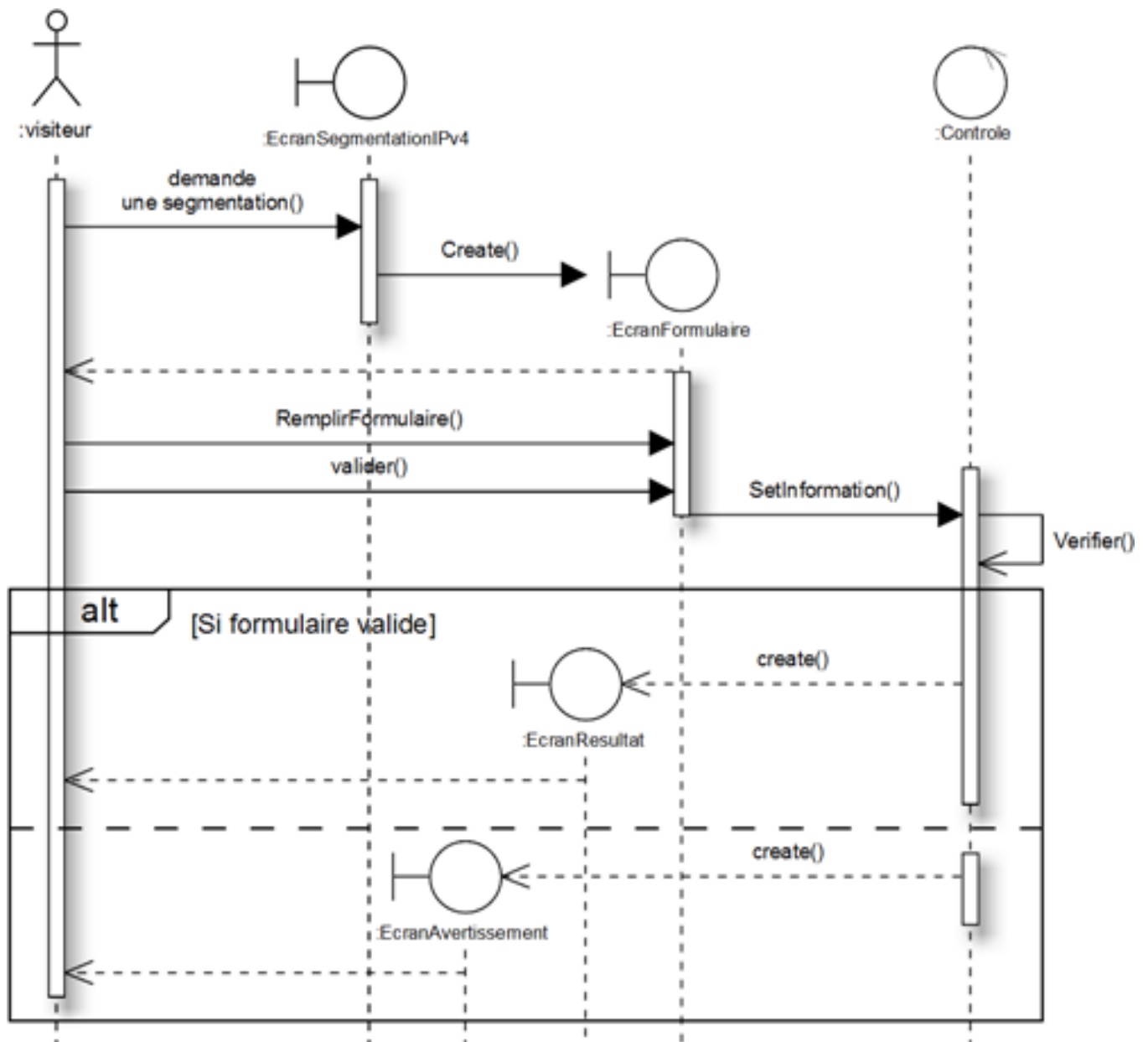


Figure 3.6 : Diagramme de séquence de cas d'utilisation segmentation en sous-réseaux d'une adresse IPv4.

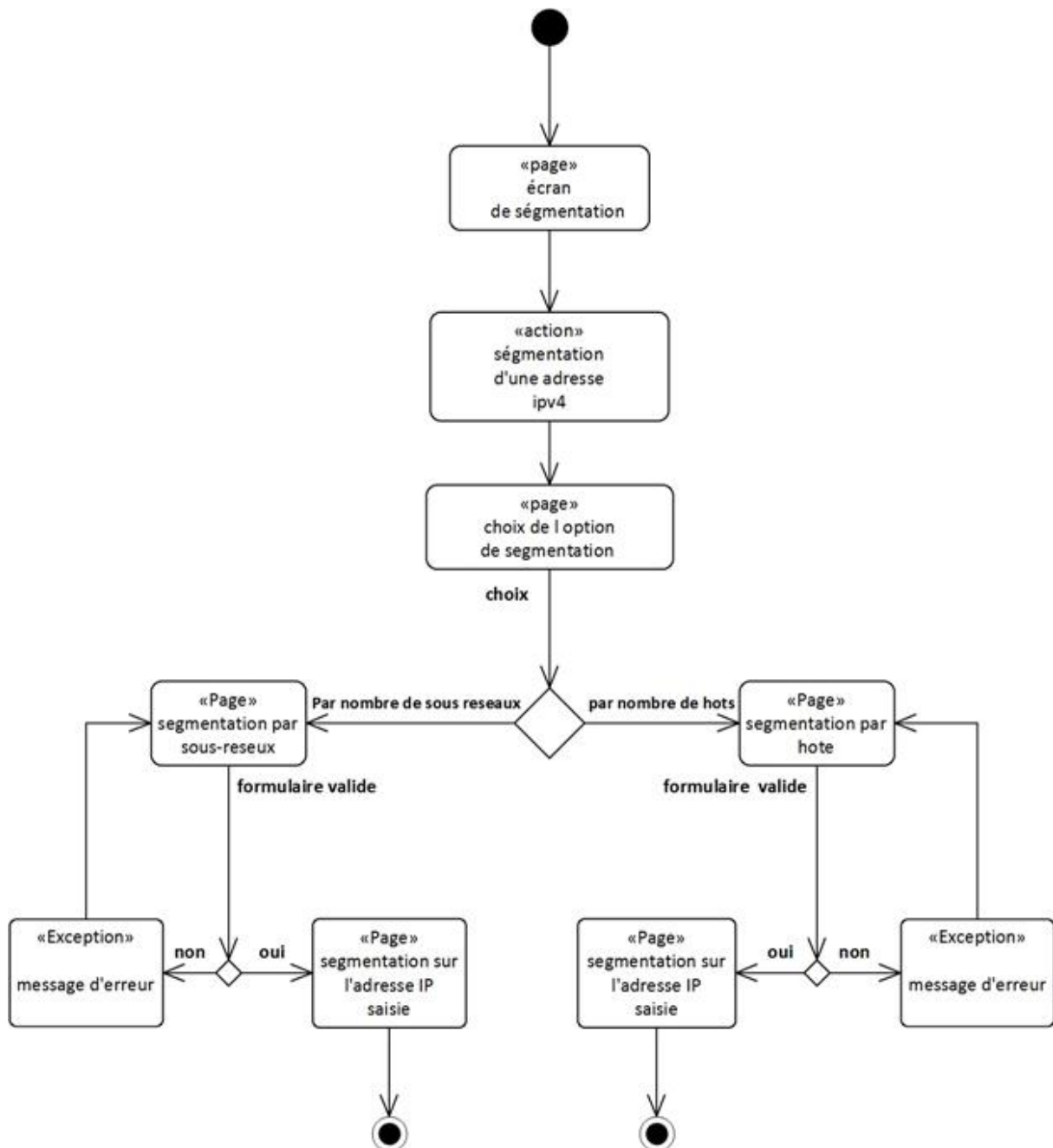


Figure 3.7 : Diagramme de navigation de cas d'utilisation segmentation en sous-réseaux d'une adresse IPv4.

III.2.3. Cas compression/décompression d'une adresse IPv6 :

Description	Ce cas permet au client de compresser / décompresser une adresse ipv6.
Acteur	Client.
Pré condition	L'adresse IPv6 saisie est valide.
Post condition	Le système compresse ou décompresse une adresse ipv6.
Scénario nominal	1. Le client demande une compression ou décompression. 2. Le système demande au client d'introduire son adresse ipv6. 3. Le client saisit l'adresse ipv6. 4. Le système procure la décompression ou la compression de l'adresse ipv6.
Scénario alternative	1. L'adresse IP introduite est non valide (champ vide ou adresse incorrecte). 2. Retour à l'étape 2.

Tableau 3.3 : La fiche descriptive du cas d'utilisation compression/décompression d'une adresse IPv6.

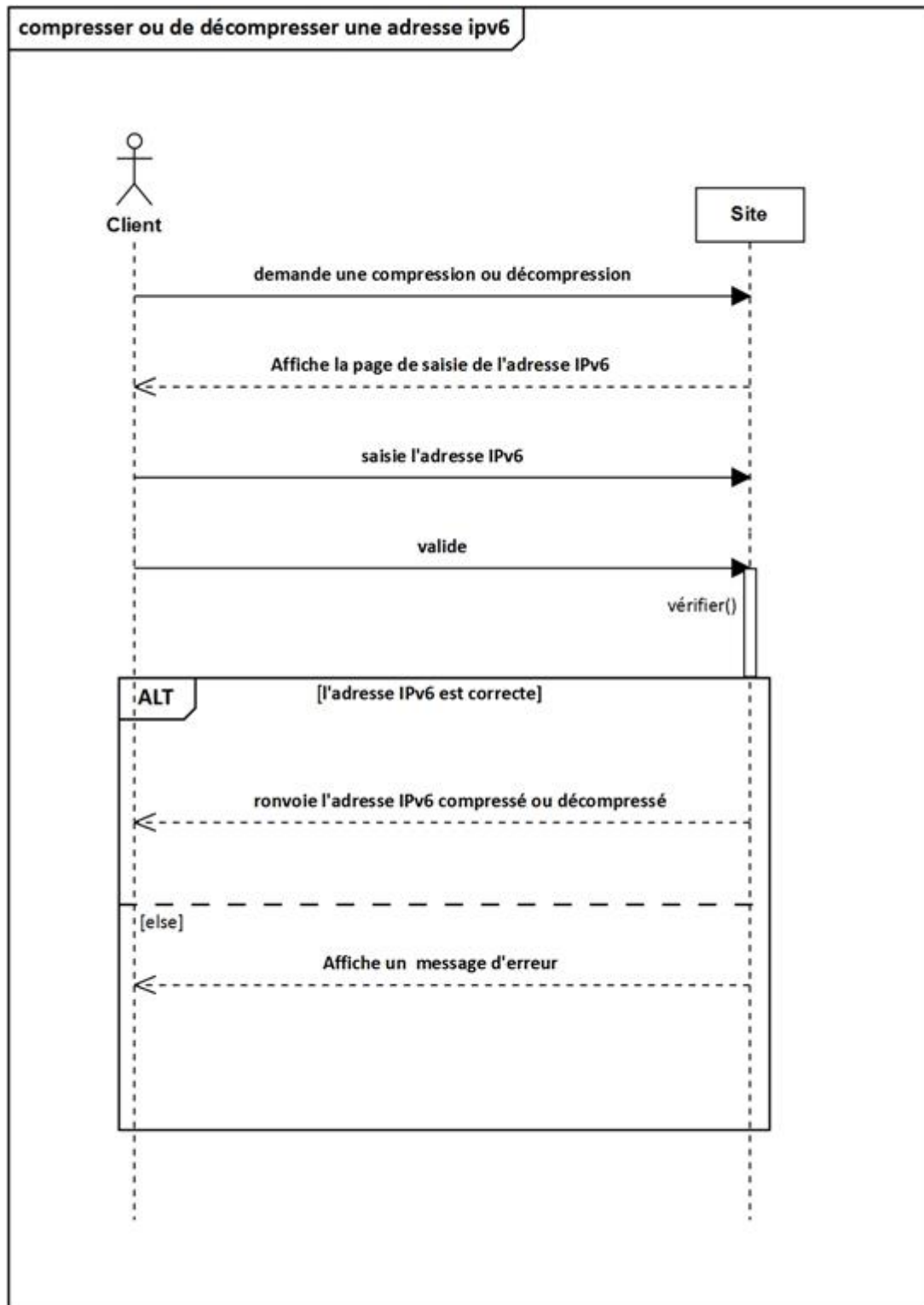


Figure 3.8 : Diagramme de séquence système de cas d'utilisation compression/décompression d'une adresse IPv6.

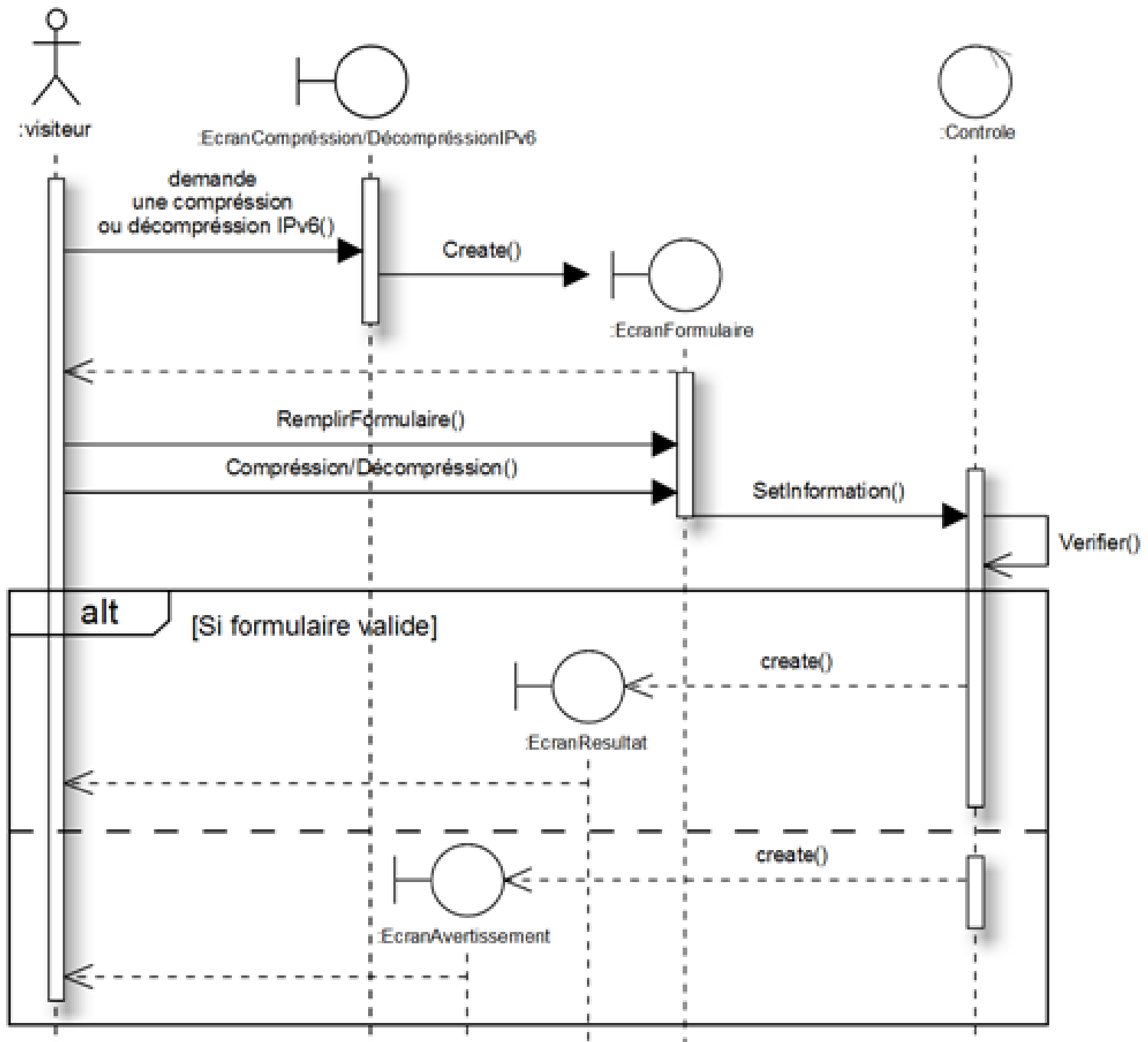


Figure 3.9 : Diagramme de séquence de cas d'utilisation compression/décompression d'une adresse IPv6.

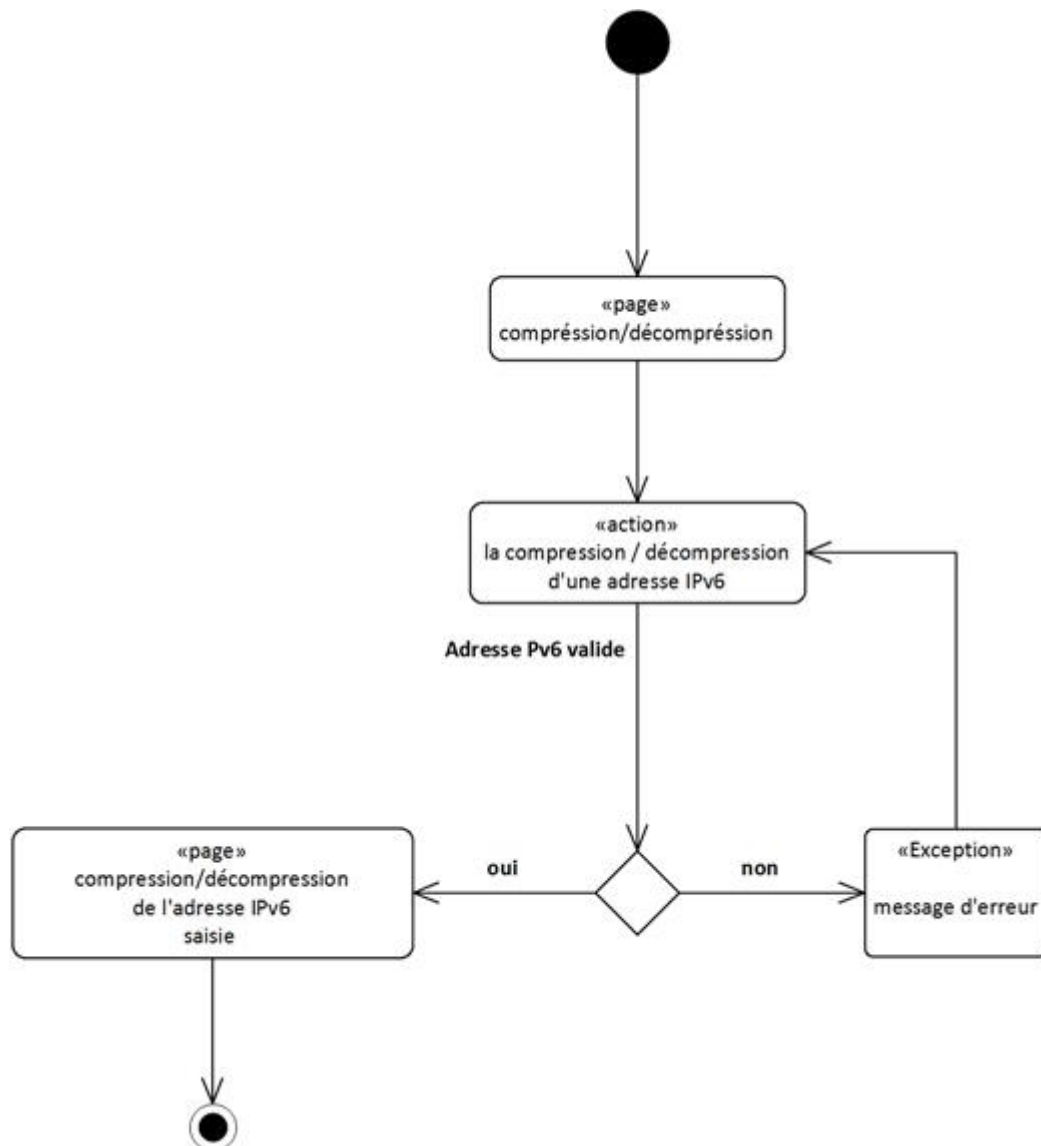


Figure 3.10 : Diagramme de navigation de cas d'utilisation compression/décompression d'une adresse IPv6.

III.2.4. Cas assistance pour le choix des tunnels :

Description	Ce cas permet au client d'utiliser un assistant pour le choix du tunnel.
Acteur	client
Précondition	Le formulaire est correct
Post condition	Le système choisit le meilleur tunnel pour le réseau du client
Scénario nominal	1. Le client demande une assistance pour choisir le tunnel le plus adapté à son réseau. 2. Le système affiche un formulaire pour le client. 3. Le client remplit le formulaire et valide. 4. Le système affiche le meilleur tunnel pour le réseau du client
Scénario alternative	1. Le client n'a pas coché un choix du formulaire. 2. Retour à l'étape 2.

Tableau 3.4 : La fiche descriptive du cas d'utilisation assistance pour le choix du tunnel.

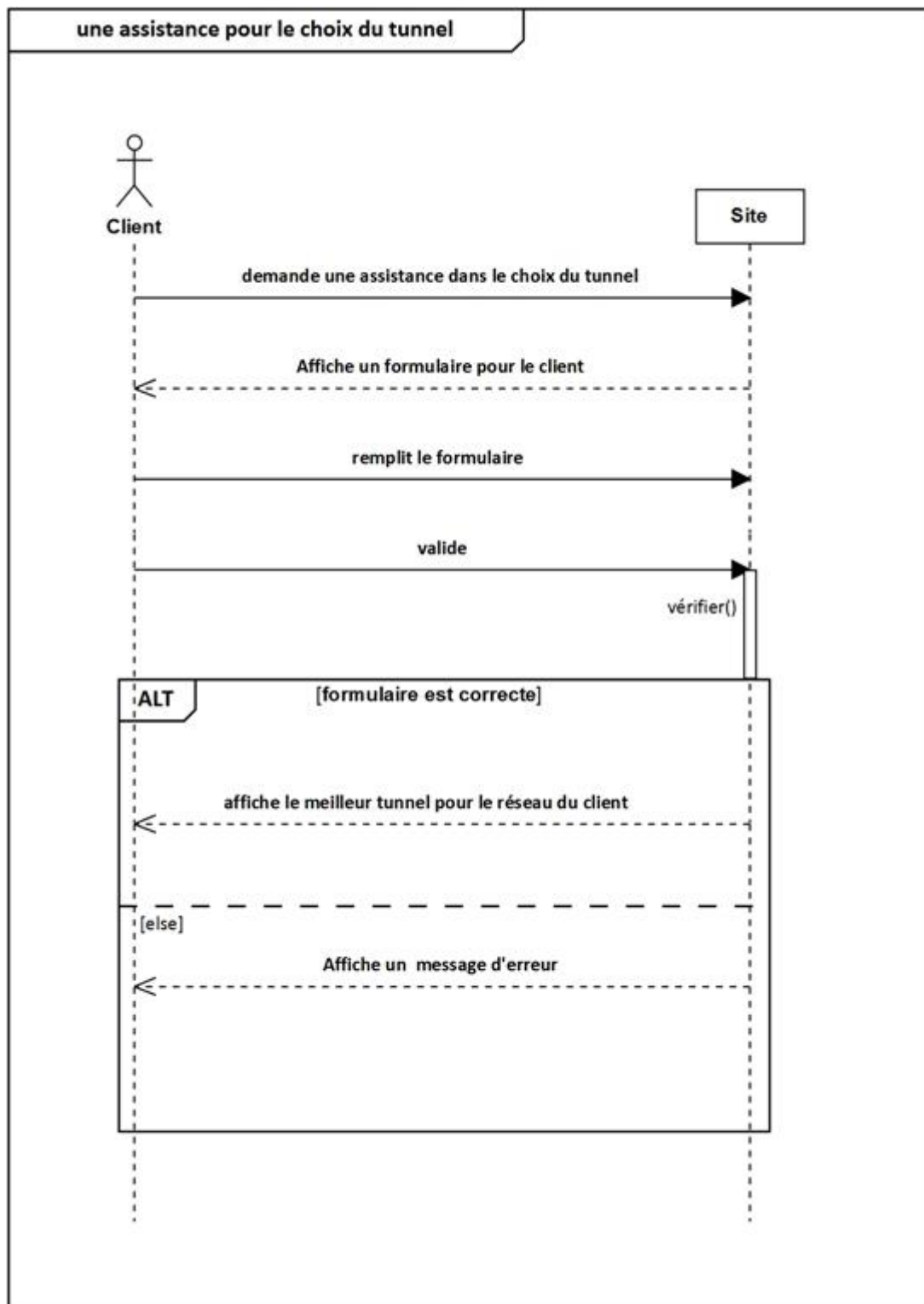


Figure 3.11 : Diagramme de séquence système de cas d'utilisation assistance pour le choix du tunnel.

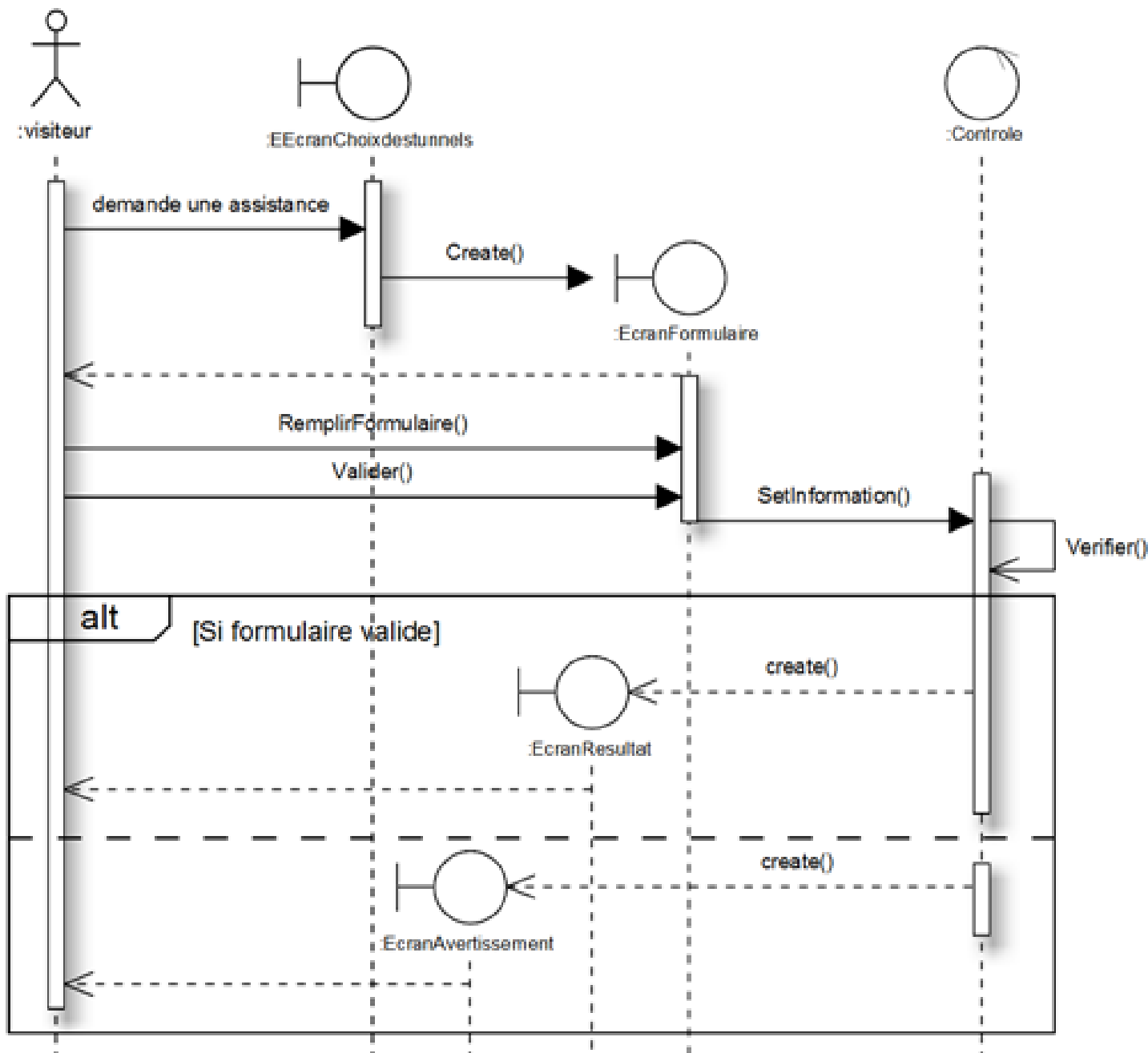


Figure 3.12 : Diagramme de séquence de cas d'utilisation assistance pour le choix du tunnel.

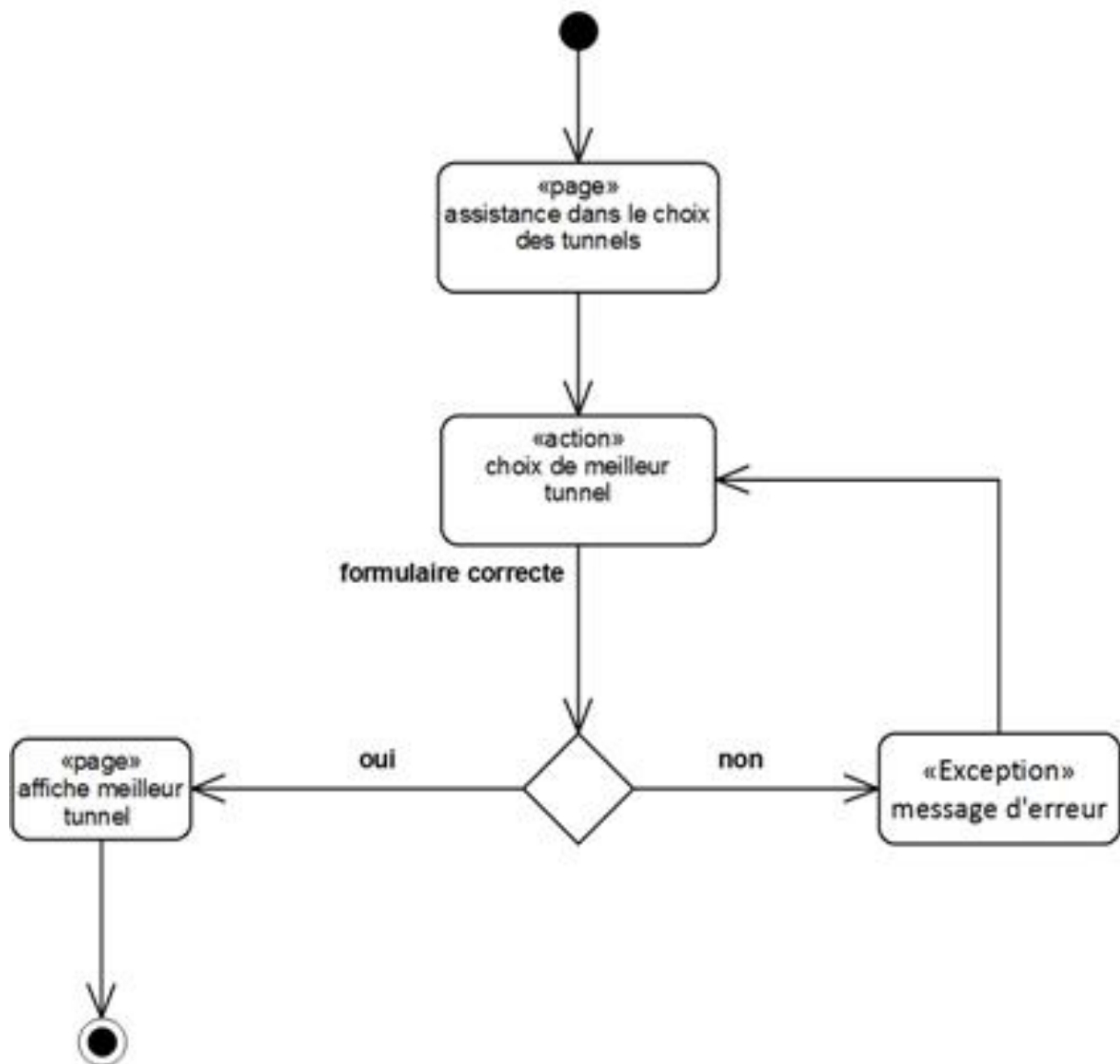


Figure 3.13 : Diagramme de navigation de cas d'utilisation assistance pour le choix du tunnel.

IV. Conclusion :

Dans ce chapitre, nous avons présenté les diagrammes nécessaires à la modélisation de notre site WEB, en utilisant le langage UML qui nous a permis de définir tous les concepts participants à la dernière phase de réalisation de ce travail, c'est la phase implémentation que nous allons aborder dans le prochain chapitre.

CHAPITRE 04

Implémentation



Le chapitre 04 couvre les points suivants :

- I. Introduction**
- II. Langage de programmation**
- III. Outils de développement**
- IV. Conclusion**

I. Introduction :

Le développement de notre site WEB a été basé sur l'étude, réalisée dans le chapitre précédent, qui nous a permis de cerner les besoins et les perspectives de notre système.

Dans ce chapitre, nous allons présenter les langages de programmation ainsi que l'ensemble des outils qui nous ont permis la réalisation de ce travail.

II. Langages de programmation :

Dans ce qui suit nous allons citer les langages utilisés dans la phase d'implémentation :

II.1. Le langage HTML :

C'est un langage de balise permettant le codage des pages WEB. HTML permet également de structurer sémantiquement et de mettre en forme l'interface des sites, d'inclure des ressources multimédias telles que les images, les formulaires de saisie, et les programmes informatiques. Il permet de créer des documents interopérables avec des équipements très variés de manière conforme aux exigences de l'accessibilité du web.

Il est souvent utilisé conjointement avec des langages de programmation et des formats de présentation (feuilles de style en cascade).

HTML est initialement dérivé du « Standard Generalized Markup Language » (SGML) [16].

II.2. Le langage CSS :

Le langage CSS c'est le langage de décoration d'une page web Le terme **CSS** est l'acronyme anglais de *Cascading Style Sheets* qui peut se traduire par "feuilles de style en cascade". Le CSS est un langage informatique utilisé sur l'internet pour mettre en forme les fichiers HTML ou XML. Ainsi, les feuilles de style, aussi appelé les fichiers CSS, comprennent du code qui permet de gérer le design d'une page en HTML.

Bien que l'HTML puisse être mis en forme à l'aide de balises prévus à cet effet, de nos jours il est plus judicieux d'utiliser le CSS et de n'utiliser le XHTML que pour le contenu.

L'avantage de l'utilisation d'un fichier CSS pour la mise en forme d'un site réside dans la possibilité de modifier tous les titres du site en une seule fois en modifiant une seule partie du fichier CSS. Sans ce fichier CSS, il serait nécessaire de modifier chaque titre de chaque page du site (difficilement envisageable pour les énormes sites de plusieurs milliers de pages).

D'autres points forts sont perceptibles. Il est par exemple possible de créer une feuille de style spécifique pour l'impression des documents, ce qui permet de retirer tous les effets de style et toutes les parties inutile lors de l'impression. De même, une feuille de style peut être utilisée pour les utilisateurs d'un téléphone portable, ce qui permet de mieux gérer la mise en forme particulièrement pour les petits écrans de ces appareils [16].

II.3. Le langage JavaScript :

JavaScript est un langage de programmation de scripts principalement utilisé dans les pages web interactives. C'est un langage orienté objet à prototype, c'est-à-dire que les bases du langage et ses principales interfaces sont fournies par des objets qui ne sont pas des instances de classes, mais qui sont chacun équipés de constructeurs permettant de créer leurs propriété [3].

II.4. Langage <<Personal Home Page >> :

Plus connu sous le nom de PHP, c'est un langage de programmation WEB principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP (ex : Apache), on désigne parfois PHP comme une plateforme plus qu'un simple langage.

Les codes du PHP sont appelés « scripts », et ils sont inclus dans le code HTML [14].

Exemple (script) :

```
<? php  
Echo 'Easy net plan' ;  
?>
```

III. Outils de développement :

III.1. Adobe DreamWeaver :

Adobe Dreamweaver (anciennement Macromedia Dreamweaver) est un éditeur de site web de type «tel écrit tel écran» cette excellente formule remplaçant désormais dans la terminologie informatique le sigle anglophone WYSIWYG («What You See Is What You Get» : «ce que vous voyez est ce que vous obtiendrez»).

Dreamweaver offre deux modes de conception par son menu affichage :

- Mode création : mise en page directement à l'aide d'outils simples, comparables à un logiciel de traitement de texte (insertion de tableau, d'image, etc.).
- Mode code : éditer directement le code (HTML ou autre) qui compose la page.

On peut passer très facilement d'un mode d'affichage à l'autre ou opter pour un affichage mixte. Cette dernière option est particulièrement intéressante pour les débutants, qui à terme, souhaitent se familiariser avec le langage HTML [17].

III.2. WampServer :

WampServer 2 (anciennement WAMP5) est une plateforme de développement Web de type WAMP, servant à faire fonctionner localement (sans se connecter à un serveur externe) des scripts PHP. WampServer n'est pas en soi un logiciel, mais un environnement comprenant deux serveurs (Apache et MySQL), un interpréteur de script (PHP), ainsi qu'une administration pour les deux bases SQL PhpMyAdmin et SQLiteManager.

Il dispose d'une interface d'administration servant à gérer et d'administrer ses serveurs au travers d'un trayicon (icône près de l'horloge de Windows).

La grande nouveauté de WampServer 2 réside dans la possibilité d'y installer et d'utiliser n'importe quelle version de PHP, Apache ou MySQL en un clic. Ainsi, chaque développeur peut reproduire scrupuleusement son serveur de production sur sa machine locale [15].

IV. Conclusion :

La phase d'implémentation a été concrétisée par la réalisation du site WEB, en respectant les digrammes qu'on a défini afin de modéliser la conception de notre projet.

Les tests effectués, durant l'étape finale, confirment que la solution proposée répond aux besoins, néanmoins notre étude couvre juste une partie de la problématique, avec la possibilité d'effectuer des extensions afin d'enrichir les services offerts, tels que : la segmentation en sous réseaux selon le nombre de hôtes.

Conclusion Générale

L'évolution des réseaux représente un axe de recherche très important dans le monde Informatique, nécessitant un suivi constant des nouveautés, afin d'être à jour avec la technologie exploitée par les différents secteurs et surtout les entreprises.

La recherche effectuée durant la réalisation de ce mémoire, nous a permis d'enrichir nos connaissances dans le monde des réseaux, elle nous a, de même, inspirée à améliorer notre travail avec d'autres idées.

Nous vison à l'avenir de mettre en place un système autonome permettant de configurer des équipements réseaux à distance en se basant sur les résultats obtenus dans notre projet.

La réalisation d'un tel travail nécessite la collaboration de plusieurs équipes ayant un niveau très avancé dans les réseaux afin de produire une solution pratique pour les entreprises.

Annexe

Simulation de notre solution WEB par imprime écran :



Figure 4.1 : La page d'accueil du site web.



Figure 4.2 : La page des services IPv4.

Easy NET Plan ACCUEIL SERVICES A PROPOS

Se renseigner sur un réseau IPv4

Exemple: 192.168.0.30
Entrez votre adresse IPv4 :

L'adresse IP	192.160.3.2
Classe	classe C
Type	Adresse publique
Adresse réseau	192.160.3.0
Le masque réseau	255.255.255.0
Adresse du broadcast	192.160.3.255
Nombre des adresses IP clients	254

Appel
+213-664 200 808
+213-699 305 569
+213-778 193 235

Contact
memoire.ipv.2013@gmail.com

© par Benzerafa
Mezhoud
& Meghlaoui

Figure 4.3 : Se renseigner sur un réseau IPv4.

Easy NET Plan ACCUEIL SERVICES A PROPOS

Segmentation des réseaux IPv4

Exemple: 192.168.0.30
Entrez votre adresse IPv4 :
Entrez le nombre des sous-réseaux :

Segmentation du réseau 10.12.4.1 en 1000 sous-réseaux.

Masque sous-réseau calculé	255.255.192.0
Nombre des hôtes pour chaque S/R	16384
Adresse réseau N°: 1	10.0.64.1
Adresse réseau N°: 2	10.0.128.1
Adresse réseau N°: 3	10.0.192.1
Adresse réseau N°: 4	10.1.0.1
Adresse réseau N°: 5	10.1.64.1
Adresse réseau N°: 6	10.1.128.1

Appel
+213-664 200 808
+213-699 305 569
+213-778 193 235

Contact
memoire.ipv.2013@gmail.com

© par Benzerafa
Mezhoud
& Meghlaoui

Figure 4.4 : Segmentation d'un réseau IPv4.



[ACCUEIL](#)
[SERVICES](#)
[A PROPOS](#)

Compression /Décompression d'adresse IPv6

Exemple: 2002:9b99:7b0c::45dd:eefe:4520

Entrez votre adresse IPv6 :

Appel

+213-664 200 808
+213-699 305 569
+213-778 193 235

Contact

memoire.ipv.2013@gmail.com

© par Benzerafa
Mezhoud
& Meghlaoui

Figure 4.5 : Compression d'une adresse IPv6.



[ACCUEIL](#)
[SERVICES](#)
[A PROPOS](#)

Choix du tunnel.

Meilleur tunnel à utiliser	IPv6 over IPv4 GRE
Plus d'information sur ce tunnel	



Appel

+213-664 200 808
+213-699 305 569
+213-778 193 235

Contact

memoire.ipv.2013@gmail.com

© par Benzerafa
Mezhoud
& Meghlaoui

Figure 4.6 : Exemple d'une assistance au choix des tunnels.

Liste des Tableaux

<i>N° du Tableau</i>	<i>Titre</i>	<i>N° de Page</i>
<i>Tableau 1.1</i>	<i>Table de datagramme IPv4</i>	<i>08</i>
<i>Tableau 1.2</i>	<i>La plage d'adresse IPv4</i>	<i>13</i>
<i>Tableau 1.3</i>	<i>Tableau comparatif des tunnels</i>	<i>30</i>
<i>Tableau 3.1</i>	<i>La fiche descriptive du cas d'utilisation s'informer sur une adresse IP</i>	<i>56</i>
<i>Tableau 3.2</i>	<i>La fiche descriptive du cas d'utilisation segmentation en sous-réseaux d'une adresse IPv4</i>	<i>60</i>
<i>Tableau 3.3</i>	<i>La fiche descriptive du cas d'utilisation compression/décompression d'une adresse IPv6</i>	<i>64</i>
<i>Tableau 3.4</i>	<i>La fiche descriptive du cas d'utilisation assistance pour le choix du tunnel</i>	<i>68</i>

Liste des Figures

<i>N° de Figure</i>	<i>Titre</i>	<i>N° de Page</i>
<i>Figure 1.1</i>	<i>Le format des adresses IPv4</i>	<i>09</i>
<i>Figure 1.2</i>	<i>Le format des Adresses IPv4</i>	<i>10</i>
<i>Figure 1.3</i>	<i>Le format des Adresses IPv4 de la classe A</i>	<i>10</i>
<i>Figure 1.4</i>	<i>Le format des Adresses IPv4 de la classe B</i>	<i>11</i>
<i>Figure 1.5</i>	<i>Le format des Adresses IPv4 de la classe C</i>	<i>11</i>
<i>Figure 1.6</i>	<i>Le format des Adresses IPv4 de la classe D</i>	<i>12</i>
<i>Figure 1.7</i>	<i>Le format des Adresses IPv4 de la classe E</i>	<i>12</i>
<i>Figure 1.8</i>	<i>Le format du masque de sous-réseau de la classe C</i>	<i>17</i>
<i>Figure 1.9</i>	<i>Un exemple sur la structure d'un réseau utilise le NAT</i>	<i>17</i>
<i>Figure 1.10</i>	<i>Envoi et réception de données entre deux hôtes utilisent le NAT</i>	<i>18</i>
<i>Figure 1.11</i>	<i>Exemple d'une topologie réseau</i>	<i>20</i>
<i>Figure 1.12</i>	<i>Le format du paquet IPv6</i>	<i>22</i>

<i>Figure 1.13</i>	<i>Schéma d'un tunnel 6to4</i>	<i>27</i>
<i>Figure 1.14</i>	<i>Schéma d'un tunnel ISATAP</i>	<i>28</i>
<i>Figure 1.15</i>	<i>Schéma d'un tunnel TOREDO</i>	<i>29</i>
<i>Figure 1.16</i>	<i>Schéma d'un tunnel GRE</i>	<i>29</i>
<i>Figure 2.1</i>	<i>Page d'accueil</i>	<i>37</i>
<i>Figure 2.2</i>	<i>Les services du protocole IPv4</i>	<i>38</i>
<i>Figure 2.3</i>	<i>Se renseigner sur un réseau IPv4</i>	<i>39</i>
<i>Figure 2.4</i>	<i>Segmentation d'un réseau IPv4</i>	<i>40</i>
<i>Figure 2.5</i>	<i>Les fonctionnalités de la page du protocole IPv6</i>	<i>41</i>
<i>Figure 2.6</i>	<i>Se renseigner sur une adresse IPv6</i>	<i>42</i>
<i>Figure 2.7</i>	<i>Compression d'une adresse IPv6</i>	<i>43</i>
<i>Figure 2.8</i>	<i>Décompression d'une adresse IPv6</i>	<i>43</i>
<i>Figure 2.9</i>	<i>Les services du volet IPv4/IPv6</i>	<i>44</i>
<i>Figure 2.10</i>	<i>Assistance au choix du meilleur tunnel</i>	<i>45</i>
<i>Figure 2.11</i>	<i>Exemple d'une assistance au choix des tunnels</i>	<i>45</i>

<i>Figure 3.1</i>	<i>Diagramme de cas d'utilisation</i>	<i>55</i>
<i>Figure 3.2</i>	<i>Diagramme de séquence système de cas d'utilisation s'informer sur une adresse IP</i>	<i>57</i>
<i>Figure 3.3</i>	<i>Diagramme de séquence de cas d'utilisation s'informer sur une adresse IP</i>	<i>58</i>
<i>Figure 3.4</i>	<i>Diagramme de navigation de cas s'informer sur une adresse IP</i>	<i>59</i>
<i>Figure 3.5</i>	<i>Diagramme de séquence système de cas d'utilisation segmentation en sous-réseaux d'une adresse IPv4</i>	<i>61</i>
<i>Figure 3.6</i>	<i>Diagramme de séquence de cas d'utilisation segmentation en sous-réseaux d'une adresse IPv4</i>	<i>62</i>
<i>Figure 3.7</i>	<i>Diagramme de navigation de cas d'utilisation segmentation en sous-réseaux d'une adresse IPv4</i>	<i>63</i>
<i>Figure 3.8</i>	<i>Diagramme de séquence système de cas d'utilisation compression/décompression d'une adresse IPv6</i>	<i>65</i>
<i>Figure 3.9</i>	<i>Diagramme de séquence de cas d'utilisation compression/décompression d'une adresse IPv6</i>	<i>66</i>
<i>Figure 3.10</i>	<i>Diagramme de navigation de cas d'utilisation compression/décompression d'une adresse IPv6</i>	<i>67</i>
<i>Figure 3.11</i>	<i>Diagramme de séquence système de cas d'utilisation assistance pour le choix du tunnel</i>	<i>69</i>
<i>Figure 3.12</i>	<i>Diagramme de séquence de cas d'utilisation assistance pour le choix du tunnel</i>	<i>70</i>
<i>Figure 3.13</i>	<i>Diagramme de navigation de cas d'utilisation assistance pour le choix du tunnel</i>	<i>71</i>
<i>Figure 4.1</i>	<i>La page d'accueil du site web</i>	<i>82</i>
<i>Figure 4.2</i>	<i>La page des services IPv4</i>	<i>82</i>

<i>Figure 4.3</i>	<i>Se renseigner sur un réseau IPv4</i>	83
<i>Figure 4.4</i>	<i>Segmentation d'un réseau IPv4</i>	83
<i>Figure 4.5</i>	<i>Compression d'une adresse IPv6</i>	84
<i>Figure 4.6</i>	<i>Exemple d'une assistance au choix des tunnels</i>	84

Références Bibliographiques

<i>Code</i>	<i>Référence</i>
[1]	Mémoire de fin d'étude : Conception et réalisation d'un site web dynamique d'une entreprise publique par Mr.MWAMBA Edouard
[2]	Livre : Le protocole IP de Cristian Bolton.
[3]	Fr.wikipedia.org
[4]	www.lille.labo-cisco.com
[5]	Cours Réseaux 3 ^{ème} année informatique de Madame Benabdarrahmane.
[6]	www.inetdoc.net
[7]	www.commentcamarche.net
[8]	www.mrim.forumpro.fr
[9]	www.sectiontelecom.pagesperso-orange.fr
[10]	www.users.polytech.unice.fr

[11]	www.junon.univ-cezanne.fr
[12]	www.geekz.fr
[13]	www.ccie.julienberton.fr
[14]	Mémoire fin d'étude, par Mr.BEN CHEIKH EL HOUCIN MADJED 2012/2013
[15]	www.standard-du-web.com
[16]	www.hal.archives-ouvertes.fr
[17]	Livre : DreamWeaver : les fonctions essentielles d'Éric Morasse.