



N° Ref :.....

Centre Universitaire de Mila

Institut des Sciences et de la Technologie

Département 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 :

**BOUNAMOUS MADIHA
CHABBEH LEILA**

Encadré par :

**Mr. BEN CHEIKH ELHOCINE
MADJED**

Grade: M.A.B

Année universitaire : 2013/2014

Remerciements

*Je remercie dieu tout puissant de m'avoir aidé, et
Éclairer le chemin pour Achever mon travail et mes études.*

*Je remercie A ma belle-famille, surtout mon beau père la
belle-mère Qui m'a tout donné pour réussir.*

*Je remercie mes frères et tous les enfants et tout amis
Qui m'encouragé et soutenu durant tout Mon parcours.*

Un remerciement particulier à mon encadreur

Mr. «BENCHAIKH ELHOCINE MADJED»

*Pour sa présence, son aide et surtout pour ses
Précieux conseils qui nous ont Assistés pour
l'accomplissement de ce projet.*

*Je tiens à exprimer mes sincères remerciements à
Tout le personnel de L'institut de sciences et de la
technologie.*

*Enfin je remercie toutes personnes qui ont Contribué
de près ou de loin À l'achèvement de ce travail.*

Sommaire

Sommaire	I.
Les listes de figures	Erreur ! Signet non défini.
Les listes de tableaux	Erreur ! Signet non défini.
Introduction générale	12
Chapitre 01 : le protocole IP	15
I. Introduction	17
II. Protocole IP	18
III. Le protocole IPv4	19
III.1. Présentation d'IPv4	19
III.2. Format du datagramme IPv4	19
III.3. L'adressage d'IPv4	22
III.3.1. les classes d'adressage	22
III.3.2. types de communication dans le protocole IP	27
III.3.3. adresse publiques et privées	28
III.3.4. Les sous-réseaux	29
III.3.5. masque de sous- réseaux	30
III.4. Les lacunes d'IPv4	33

IV. Le protocoleIPv6	35
IV. 1. Présentation d'IPv6	35
IV.2. Format du datagramme IPv6	35
IV.3. Adresse IPv6	37
IV. 3.1. les types d'adresses	38
IV. 3.1.1. adresse unicast	39
IV. 3.1.2. adresse anycast	41
IV. 3.1.3. adresse multicast	42
IV.3.2. adresse particulières	43
V. Transition IPv4 vers IPv6	45
V. 1. Mécanismes de transition	45
V. 1.1. double pile	45
V. 1.2. tunnels IPv6 dans IPv4	45
V. 1.2.1. tunnel statique	46
V. 1.2.2. tunnel dynamique	47
V. 1.3. par translation de protocole	49
V. 2. L'adresse de transition	50
VI. conclusion	51
Chapitre 02 Planification de réseaux	52

I . Introduction	54
II . problématiques	55
III . approche proposée	57
III. 1. Services concernant IPv4	57
III. 2. Services concernant IPv6	59
III. 3. tunneling	60
IV . Maquette du projet	61
IV - 1. La page d'accueil	61
IV - 2. Volet N°1 : Page de services d'adresse IP V4	61
IV - 3. Volet N°2 : Page de services d'adresse IPv6	64
IV - 4. Volet N°3 : Page Tunneling	66
V . Conclusion	68
Chapitre 03 Conception du site WEB	69
I. Introduction	71
II. UML	72
II. 1. Caractéristiques d'UML	72
II. 2. Les points forts d'UML	72
II. 3. Les faibles d'UML	73
II. 4. Les vues UML	73

II. 4.1. vue statique ou structurelle	73
II. 4.2. vue dynamique ou comportement	74
II. 5. Mise en œuvre d'UML	74
II.5.1. les étapes du la démarche	74
III. Modèle de besoin	76
III..1. identification d'un acteur	76
III. 2. Le diagramme de cas d'utilisation	77
III. 2.1. cas d'utilisation « se renseigner sue une adresse IPv4 »	78
III. 2.2. cas d'utilisation « segmenter des réseaux IPv4 »	82
III. 2.3. cas d'utilisation «se renseigner sue une adresse IPv6 »	86
III. 2.4. cas d'utilisation «compresser/décompresser »	90
III. 2.5. cas d'utilisation «assister le choix du tunnel »	94
IV. Conclusion	98
Chapitre 04 l'implémentation	99
I. Introduction	101
II. Langage de programmation	102
II. 1. HTML (HyperText Markup Language)	102
II. 2. CSS	102
II. 3. JavaScript	102

II. 4. langage PHP	103
III. Outils de développement	104
II. 1. Sublime text	104
III. 1. WampServer	105
III. Conclusion	106
Conclusion Générale	108
Références Bibliographiques	109
Annexe	112

Liste des Figures

<i>N° de Figure</i>	<i>Titre</i>	<i>N° de Page</i>
<i>Figure 1.1</i>	<i>Datagramme IPv4</i>	<i>19</i>
<i>Figure 1.2</i>	<i>Format d'adresse IPv4</i>	<i>21</i>
<i>Figure 1.3</i>	<i>Format de la classe A</i>	<i>22</i>
<i>Figure 1.4</i>	<i>Format de la classe B</i>	<i>23</i>
<i>Figure 1.5</i>	<i>Format de la classe C</i>	<i>24</i>
<i>Figure 1.6</i>	<i>Format de la classe D</i>	<i>24</i>
<i>Figure 1.7</i>	<i>Les classes d'adresses IPv4</i>	<i>25</i>
<i>Figure 1.8</i>	<i>Exemple illustrée sous-réseau</i>	<i>29</i>
<i>Figure 1.9</i>	<i>Datagramme d'IPv6</i>	<i>35</i>
<i>Figure 1.10</i>	<i>L'adresse ULA</i>	<i>38</i>
<i>Figure 1.11</i>	<i>L'adresse lien-locale</i>	<i>38</i>

<i>Figure 1.12</i>	<i>L'adresse site-locale</i>	<i>39</i>
<i>Figure 1.13</i>	<i>L'adresse globale unicast</i>	<i>40</i>
<i>Figure 1.14</i>	<i>L'adresse d'anycast</i>	<i>41</i>
<i>Figure 1.15</i>	<i>L'adressage multicast</i>	<i>42</i>
<i>Figure 1.16</i>	<i>Tunnel dans IPv4 et IPv6</i>	<i>46</i>
<i>Figure 1.17</i>	<i>L'adressage IPv4/IPv6</i>	<i>49</i>
<i>Figure 2.1</i>	<i>Page d'accueil.</i>	<i>60</i>
<i>Figure.2.2</i>	<i>page services d'adresse ipv4.</i>	<i>61</i>
<i>Figure.2.3</i>	<i>page «se renseigner une adresse IPV4 ».</i>	<i>61</i>
<i>Figure.2.4</i>	<i>Page « segmentation des réseaux ».</i>	<i>62</i>
<i>Figure 2.5</i>	<i>page services d'adresse IPV6.</i>	<i>63</i>
<i>Figure.2.6</i>	<i>page « se renseigné d'une adresse IPV6 ».</i>	<i>64</i>
<i>Figure.2.7</i>	<i>page « compression/décompression ».</i>	<i>64</i>

<i>Figure.2.8</i>	<i>page tunneling.</i>	<i>64</i>
<i>Figure.2.9</i>	<i>page « assistant choix du tunnel ».</i>	<i>66</i>
<i>Figure.3.1</i>	<i>Diagramme de cas d'utilisation.</i>	<i>78</i>
<i>Figure 3.5</i>	<i>Diagramme de séquence système du cas d'utilisation « segmenter des réseaux IPv4 ».</i>	<i>79</i>
<i>Figure 3.6</i>	<i>Diagramme d'interaction du cas d'utilisation « segmenter des réseaux IPv4 ».</i>	<i>80</i>
<i>Figure 3.7</i>	<i>Diagramme de navigation du cas d'utilisation « segmenter des réseaux IPv4 ».</i>	<i>82</i>
<i>Figure 3.8.</i>	<i>Diagramme de séquence système du cas d'utilisation « Se renseigner l'adresse IPv6 ».</i>	<i>83</i>
<i>Figure 3.9</i>	<i>Diagramme d'interaction du cas d'utilisation « Se renseigner l'adresse IPv6 ».</i>	<i>84</i>
<i>Figure 3.10</i>	<i>Diagramme de navigation du cas d'utilisation « Se renseigner l'adresse IPv6 ».</i>	<i>86</i>
<i>Figure 3.11</i>	<i>Diagramme de séquence système du cas d'utilisation « compresser / décompresser ».</i>	<i>87</i>
<i>Figure 3.12</i>	<i>Diagramme d'interaction du cas d'utilisation « compresser / décompresser ».</i>	<i>88</i>

<i>Figure 3.13</i>	<i>Diagramme de navigation du cas d'utilisation « compresser / décompresser ».</i>	<i>90</i>
<i>Figure 3.14</i>	<i>Diagramme de séquence du cas d'utilisation « Assister le choix du tunnel ».</i>	<i>91</i>
<i>Figure 3.15</i>	<i>Diagramme d'interaction du cas d'utilisation « Assister choix du tunnel ».</i>	<i>92</i>
<i>Figure 3.16</i>	<i>Diagramme de navigation du cas d'utilisation « Assister le choix du tunnel ».</i>	<i>94</i>
<i>Figure A.1</i>	<i>Page d'accueil.</i>	<i>95</i>
<i>Figure A.2</i>	<i>Page services IPv4</i>	<i>96</i>
<i>Figure A.3</i>	<i>Page adresse IPv6 valide</i>	<i>112</i>
<i>Figure A.4</i>	<i>adresse IPv4 non valide</i>	<i>113</i>
<i>Figure A.5</i>	<i>page segmentation de réseaux IPv4.</i>	<i>114</i>
<i>Figure A.6</i>	<i>page de documentation.</i>	<i>115</i>
<i>Figure A.7</i>	<i>Page services IPv6.</i>	<i>116</i>

<i>Figure A.8</i>	<i>page se renseigner sur une adresse IPv6.</i>	<i>117</i>
<i>Figure A.9</i>	<i>page avertissement adresse IPv6.</i>	<i>118</i>
<i>Figure A.10</i>	<i>résultat de compression d'une adresse IPv6.</i>	<i>119</i>
<i>Figure A.11</i>	<i>résultat de décompression d'une adresse IPv6.</i>	<i>120</i>
<i>Figure A.12</i>	<i>page tunneling.</i>	<i>121</i>
<i>Figure A.13</i>	<i>page choix du tunnel</i>	<i>122</i>
<i>Figure A.14</i>	<i>page tableau comparatif du tunnel.</i>	<i>123</i>
<i>Figure A.15</i>	<i>page documentation du tunnels.</i>	<i>124</i>
<i>Figure A.16</i>	<i>page A-propos.</i>	<i>125</i>

Liste des Tableaux

<i>N° du Tableau</i>	<i>Titre</i>	<i>N° de Page</i>
<i>Tableau 2.1</i>	<i>Tableau taille de classe.</i>	<i>77</i>
<i>Tableau 3.1</i>	<i>La fiche descriptive du cas d'utilisation « Se renseigner sur une adresse IPv4 ».</i>	<i>81</i>
<i>Tableau 3.2</i>	<i>La fiche descriptive du cas d'utilisation de « Segmenter des réseaux IPv4.</i>	<i>85</i>
<i>Tableau 3.3</i>	<i>La fiche descriptive du cas d'utilisation de « renseigner sur une adresse IPv6.</i>	<i>89</i>
<i>Tableau 3.4</i>	<i>La fiche descriptive du cas d'utilisation de « compresser / décompresser ».</i>	<i>93</i>
<i>Tableau 3.5</i>	<i>La fiche descriptive du cas d'utilisation « Assister le choix du tunnel ».</i>	<i>97</i>

Introduction Générale

L'histoire d'Internet remonte au développement des premiers réseaux de télécommunication. L'idée d'un réseau informatique, permettant aux utilisateurs de communiquer, se développa par de nombreuses étapes successives. La somme de tous ces développements conduisit au « réseau des réseaux » (*network of networks*) que nous connaissons aujourd'hui en tant qu'Internet. C'est le fruit, à la fois du développement technologique et du regroupement d'infrastructures réseau existantes et des systèmes de télécommunications.

Les premières versions mettant en place ces idées apparurent à la fin des années 1950. L'application pratique de ces concepts commença à la fin des années 1960. Dès les années 1980, les techniques que nous reconnaissons maintenant comme les fondements d'Internet moderne commencèrent à se répandre autour du globe. Dans les années 1990, sa popularisation passa par l'apparition du World Wide Web.

L'infrastructure d'Internet se répandit autour du monde pour créer le large réseau mondial d'ordinateurs que nous connaissons aujourd'hui. Il se répandit au travers des pays occidentaux puis frappa à la porte des pays en voie de développement, créant ainsi un accès mondial à l'information et aux communications sans précédent ainsi qu'une fracture numérique. Internet contribua à modifier fondamentalement l'économie mondiale, y compris avec les retombées de la bulle Internet.

Le protocole d'interconnexion internet « IP », est déployé pratiquement dans la plupart des réseaux qui existe dans le monde, d'où la nécessité de maîtriser toutes ses fonctionnalités, techniques et architectures, afin de devenir un

administrateur qualifié capable de planifier, gérer et entretenir un réseau complexe.

L'objectif de notre projet est de développer un site WEB dynamique assistant les administrateurs dans la phase de planification des réseaux IP.

Les chapitres de ce mémoire sont organisés comme suit :

- Le chapitre 01:** Détaille les concepts d'adressage dans le protocole IP avec ses différentes versions.
- Le chapitre 02:** Expose la problématique liée à la planification des réseaux et propose une solution WEB assistant les administrateurs lors de cette tâche.
- Le chapitre 03:** Vise à détaillé la modélisation de notre site WEB, à partir des diagrammes UML afin de passer à la phase finale qui est l'implémentation.
- Le chapitre 04:** Présente les langages de programmation utilisés ainsi que l'ensemble des 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. Protocole IP

III. Protocole IPv4

IV. Protocole IPv6

V. Transition IPv4 vers IPv6

VI. Conclusion

I. Introduction

Après la guerre froide en 1962, L'Union Soviétique souhaite implanter des missiles nucléaires à Cuba. Dans ce contexte tendu, les Etats-Unis financent des projets de recherche visant au déploiement de réseaux de communication capables de fonctionner en cas d'endommagement partiel. Et dans le milieu des années 1970, le département de la Défense américain DOD (Department Of Defense), décide, devant le foisonnement de machines utilisant des protocoles de communication différents et incompatibles, de définir sa propre architecture. Cette architecture, dite TCP/IP (IP : Internet Protocol, TCP : Transmission Control Protocol).

Dans le cadre de notre projet nous sommes intéressés dans ce premier chapitre à présenter le protocole Internet, et plus particulièrement le système d'adressage utilisé dans ses deux versions IPv4 et IPv6 ainsi que les techniques qui ont permis la communication entre ces deux différentes variantes au sein d'un même réseau hybride.

II. Protocole IP

IP est Le protocole de base du réseau Internet, fournit le service de transmission de paquets commun de base sur lequel les réseaux TCP/IP sont construits, ayant le même format et une adresse commune, compréhensible de toutes les passerelles, dans le cas d'Internet. Toutes les données de TCP/IP traversent IP, entrant et sortant, indépendamment de leur destination finale.

Le protocole IP est avant tout un protocole orienté non connexion, IP délègue aux protocoles des autres couches le soin d'établir la connexion s'ils requièrent un service orienté connexion. IP peut fonctionner de plusieurs technologies différentes : Ethernet, Token-Ring, FDDI, ATM [1].

Il existe deux générations de paquets IP, appelées IPv4 (IP version 4) et IPv6 (IP version 6).

III. Le Protocole IPv4

III.1. Présentation d'IPv4

La première génération du protocole IP c'est-à-dire IPv4 est implémenté dans toutes les stations connectées au réseau Internet. IPv4 a été prépondérant jusqu'à maintenant. IPv4 qui existe depuis l'origine du réseau Internet, À partir du début des années 1980, est encore largement utilisée. Il offre un service non fiable de remise de paquet et fonctionne en mode dit de best effort, dans la mesure où le protocole s'exécute en mode sans connexion [2].

Les messages transmis par IPv4 sont appelés des datagrammes paquet.

III. 2. Format du datagramme IPv4

Les données circulent sur Internet sous forme de datagrammes. Ce 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 IPv4 de destination).

Le datagramme IPv4 va être une suite de 0 et de 1 organisés.

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

Figure 1.1. Datagramme IPv4 [3].

- **Version (VER)** sur 4 bits : il s'agit de la version du protocole que l'on utilise afin de vérifier la validité du datagramme.
- **Longueur d'en-tête (IHL, Internet Header Length)** sur 4 bits : il s'agit du nombre de 5 mots de 32 bits constituant l'en-tête qui contient toutes les informations nécessaires à la transmission de paquet.
- **Type de service (TOS, Type Of Service)** sur 8 bits : il indique la façon selon laquelle le datagramme doit être traité.

- **Longueur totale (LEN, totale LENgth field)** sur 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.
- **Identification, drapeaux (flags) et déplacement de fragment (ID)** sont des champs qui permettent la fragmentation des datagrammes, ils sont expliqués plus bas.
- **Durée de vie (TTL, Time To Live)** sur 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.
- **Protocole** sur 8 bits : ce champ, en notation décimale, permet de savoir de quel protocole est issu le datagramme : ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol), TCP (Transmission Control Protocol)...
- **Somme de contrôle de l'en-tête, (header checksum)** : 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.
- **Adresse IP source** (32 bits) : Ce champ représente l'adresse IPv4 de la machine émettrice.
- **Adresse IP destination** (32 bits) : adresse IPv4 du destinataire (ou le groupe) du message, cette adresse est facultatif [3].

III.3. L'Adressage d'IPv4

A chaque interface réseau d'une machine (host), est associé un mot de 32 bits appelé adresse internet (ou adresse IPv4). Elle est utilisée pour toutes les communications avec l'interface de cette machine. Tous équipements sur à un réseau IPv4 doit disposer d'une adresse IPv4 unique. Cette adresse permet de localiser un équipement sur le réseau.

L'adresse est constituée de deux parties :

La partie réseau (NET-ID, ou identificateur de réseau) et la partie hôte (HOST-ID, identificateur de machine) pour ce réseau. Codée sur 4 octets (1 octet = 8 bits), cette adresse est composée de 4 nombres décimaux de 0 à 255 séparés par un point (.), c'est la notation en décimale pointée [4].

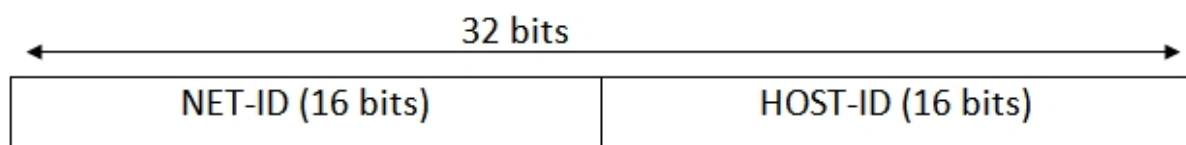


Figure 1.2. Format d'adresse IPv4.

Par exemple l'adresse IPv4

En binaire : **11000001.001100011.10010101.01100100**

En décimale : **193.49.148.100**

III.3.1. Les classes d'adressage

Il existe cinq classes d'adresses, chacune permettant de coder un nombre différent de réseaux et de machines :

- La classe A (réseau de très grande taille).
- La classe B (réseau de taille moyenne).

- La classe C (réseau de petite taille).
- La classe D (diffusion multicast).
- La classe E (expérimentation).

La classe A

S'étendent de **1.0.0.1** à **126.255.255.254**, et le premier bit du premier octet est toujours **0**.

Le premier octet (7 bits utiles) → Adresse réseau.

Les trois derniers octets (24 bits) → Adresse hôte.

Elles permettent de planifier **126** réseaux et plus de **16 millions** machines ($2^{24}-2$, soit **16777214**).

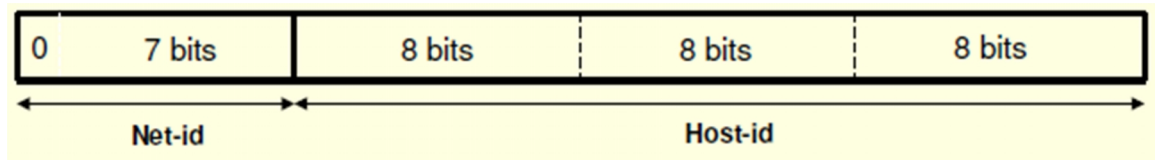


Figure 1.3. Format de la classe A [4].

La classe B

Les adresses sont entre **128.0.0.1** à **191.255.255.254**, et les deux premiers bits du premier octet sont toujours **10**.

Les deux premiers octets (14 bits utiles) → Adresse réseau.

Les deux autres octets (16 bits) → Adresse hôte.

Cela correspond à plus de **16384** réseaux de **65534** machines. Cette classe est la plus utilisée et les adresses sont aujourd'hui pratiquement épuisées.

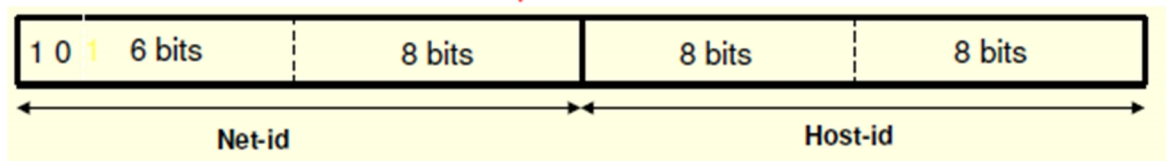


Figure 1.4. Format de la classe B [4].

La classe C

Couvre les adresses **192.0.0.1** à **223.255.255.254**, et les trois premiers bits sont toujours **110**.

Les trois premiers octets (21 bits utiles) → Adresse réseau.

Le dernier octet (8 bits) → Adresse hôte.

Elle adresse plus de **2 millions** de réseaux (**2097152**) et de **254** machines.

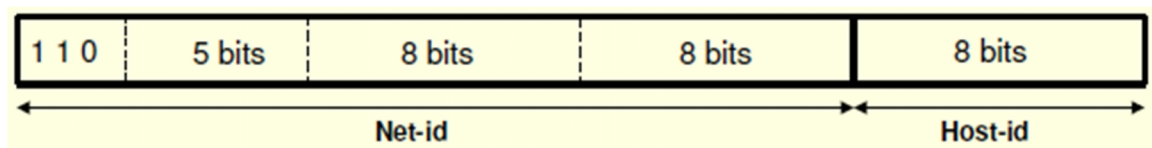


Figure 1.5. Format de la classe C [4].

La classe D

Elles vont de **224.0.0.0** à **239.255.255.255**, et les trois premiers bits sont toujours **111**. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion vers des groupes d'hôtes (*host groups*).

Les 28 bits restants → Adresse hôte.



Figure 1.6. Format de la classe D [4].

La classe E

Elles vont de **240.0.0.0** à **255.255.255.255**, et le premier octet commence par **1111**. Les adresses de cette classe sont réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

Le schéma suivant illustre toutes les classes d'adresse IPv4.

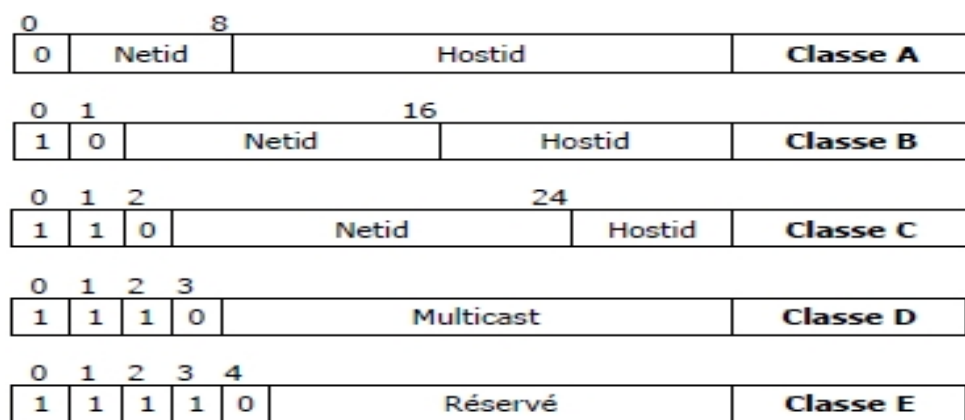


Figure 1.7. Les classes d'adresse IPv4 [2].

Dans la plage d'adresse de chaque réseau IPv4, il y a trois types d'adresses :

- L'adresse réseau.
- L'adresse de diffusion.
- L'adresse d'hôtes.

- **L'adresse réseau**

L'adresse réseau est généralement utilisée pour faire référence à un réseau. C'est un moyen plus pratique et plus représentatif d'identifier le réseau que d'employer un terme de type « le premier réseau ». Tous les hôtes du réseau **10.0.0.0** ont les mêmes bits réseau.

Dans la plage d'adresses IPv4 d'un réseau, la plus petite adresse est réservée à l'adresse réseau. Dans la partie hôte, cette adresse comporte un 0 pour chaque bit d'hôte [5].

- **L'adresse de diffusion**

L'adresse de diffusion IPv4 est une adresse spécifique, attribuée à chaque réseau. Elle permet de transmettre des données à l'ensemble des hôtes d'un réseau. Pour cela, un hôte peut envoyer un seul paquet destiné à l'adresse de diffusion du réseau.

L'adresse de diffusion correspond à la plus grande adresse de la plage d'adresses d'un réseau. Il s'agit de l'adresse dans laquelle les bits de la partie hôte sont tous les « 1 ». Pour le réseau 10.0.0.0 avec 24 bits réseaux, l'adresse de diffusion serait 10.0.0.255. Cette adresse est également désignée sous le nom de diffusion dirigée [5].

- **L'adresse d'hôte**

Comme indiqué précédemment, chaque périphérique final nécessite une adresse unique pour remettre un paquet à un hôte. Dans les adresses IPv4,

nous attribuons les valeurs situées entre l'adresse réseau et l'adresse de diffusion aux périphériques de ce réseau [5].

➤ Préfixes réseaux

Voici une question importante : comment savoir combien de bits représentent la partie réseau et combien représentent la partie hôte ?, pour exprimer une adresse réseau IPv4, nous ajoutons une longueur de préfixe à l'adresse réseau. La longueur de préfixe correspond au nombre de bits de l'adresse qui représentent la partie réseau. Par exemple, dans **172.16.4.0/24**, **24** est la longueur de préfixe. Elle nous indique que les **24 premiers** bits correspondent à l'adresse réseau. Il reste donc **8** bits (le dernier octet) qui correspondent à la partie hôte.

Un numéro de préfixe différent modifie la plage d'hôtes et l'adresse de diffusion pour chaque réseau [5].

III.3.2. Types de communication dans le protocole IP

- **Unicast (point à point)**

Lorsqu'un datagramme IP est envoyé à **une** adresse IPv4 individuelle, on dit qu'il s'agit d'un datagramme IP unicast. L'envoi de ce datagramme est appelé unicasting, On utilise l'unicasting lorsque deux nœuds IP communiquent ensemble.

- **Multicast (point à multipoint)**

Lorsqu'un datagramme IPv4 est envoyé à un **groupe** de destinataires, on parle de multicasting ou multidiffusion. Dans ce cas, on utilise une adresse de classe «D» comme adresse de destination. Les systèmes qui appartiennent au même groupe de multidiffusion, doivent aussi se voir affecter une adresse IPv4 (classe A, B ou C).

Le groupe de multidiffusion peut recevoir un datagramme IPv4 de deux manières :

- ♦ Des datagrammes IPv4 envoyés directement aux adresses individuelles (classes A, B ou C).
- ♦ Des datagrammes IPv4 envoyés à l'adresse de multidiffusion (classe D).

Pour que la multidiffusion fonctionne bien, un hôte doit avoir la capacité de se joindre à un groupe de multicast et de le quitter [6].

- **Broadcast (point à tous les points)**

Lorsqu'un datagramme IPv4 est envoyé à tous les nœuds d'un réseau spécifique, il s'agit d'une diffusion (broadcasting) [6].

III. 3.3. Adresse publiques et privées

- **Les adresse publiques**

Sont dites «routables », c'est-à-dire qu'elles permettent d'être identifier sur le réseau Internet et donc d'échanger des informations via Internet, la majorité des adresses de la plage d'hôtes IPv4 sont des adresses publiques [2].

- **Les adresse privées**

Pour réduire le besoin en nouvelles adresses, un groupe d'adresse par classe à été réservé. Ce sont les adresses privées (non routables), elles sont utilisées dans les réseaux privées, à la maison ou en entreprise. Ces adresses permettent d'identifier et d'échanger des informations avec des équipements situés dans l'entreprise (ou dans un espace privé), on parle alors d'intranet.

Le choix des adresses IPv4 est libre pour les réseaux privés, cependant la norme préconise les adresses suivantes :

- **En classe A** : 10.0.0.0 à 10.255.255.255, soit 1 adresse réseau.
- **En classe B** : 172.16.0.0 à 172.31.255.255, soit 16 adresses réseaux.
- **En classe C** : 192.168.0.0 à 192.168.255.255, soit 255 réseaux.

Afin de pouvoir sortir du réseau, on doit employer un proxy, passerelle NAT (Network Address Translation) ou tout autre équipement permettant l'utilisation de l'adresse publique de cet équipement [2].

III.3.4. Les sous-réseaux

Pour compenser les problèmes de distribution de l'espace d'adressage IP, la première solution utilisée a consisté à découper une classe d'adresses IPv4 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 contemporains. Il ne faut jamais oublier que le découpage en réseaux ou sous-réseaux permet de cloisonner les domaines de diffusion.

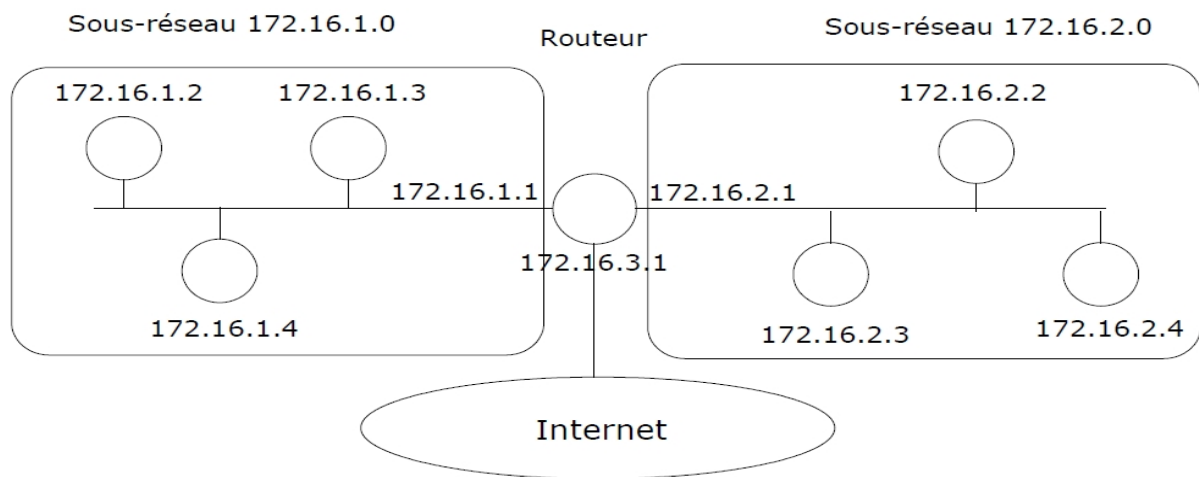


Figure 1.8. Exemple illustrée sous-réseaux.

- **Formule de calcul des sous-réseaux**

Utilisez la formule suivante pour calculer le nombre de sous-réseaux :

$2^n - 2$ ou n = le nombre de bits empruntés

Par exemple, si $n=2$ nous obtenons :

$2^2 - 2 = 2$ sous-réseaux [4].

- **Le nombre d'hôtes**

Pour calculer le nombre d'hôtes par réseau, il faut utiliser la formule $2^n - 2$ ou n = le nombre de bits laissés pour les hôtes.

Après application de cette formule, ($2^6 - 2 = 62$), on déduit que chacun de ces sous-réseaux peut avoir **62** hôtes.

III.3.5. Masque de sous-réseau

Le premier intérêt d'un masque de sous-réseau est de permettre d'identifier simplement le réseau associé à une adresse IPv4. En effet, le réseau est déterminé par un certain nombre d'octets de l'adresse IPv4.

En doit ajouter une information supplémentaire à l'adresse IPv4, le masque de sous-réseau. Ces deux informations, adresse IPv4 et masque, seront inséparables. C'est le masque qui va indiquer quelle est la partie réseau de l'adresse, et quelle est la partie machine, les bits à 1 dans le masque représentent la partie réseau de l'adresse, et les bits à 0 représentent la partie machine de l'adresse.

Chaque classe possède un masque :

- **Pour la classe A**, seul le premier octet doit être conservé. Le masque possède la forme suivante **11111111.00000000.00000000.00000000**, en décimale **255.0.0.0**.

- **Pour la classe B**, les deux premiers octets doivent être conservés, ce qui donne le masque suivant **11111111.11111111.00000000.00000000**, en décimale **255.255.0.0**.
- **Pour la classe C**, les trois premiers octets doit être conservés, Le masque possède la forme suivante **11111111.11111111.11111111.00000000**, en décimale **255.255.255.0**.

Pour déterminer l'identifiant réseau d'une adresse IPv4, on effectue l'opération logique suivante :

$$\text{Adresse réseau} = (\text{adresse IP}) \text{ ET } (\text{masque})$$

Application de l'opération logique ET

L'adresse d'hôte IPv4 est logiquement ajoutée par une opération « ET » à son masque de sous-réseau pour déterminer l'adresse à laquelle l'hôte est associée. Lorsque cette opération « ET » est appliquée entre l'adresse et le masque de sous-réseau, le résultat obtenu est l'adresse réseau.

Opération ET

$$1 \text{ ET } 1 = 1 ; \quad 1 \text{ ET } 0 = 0 ; \quad 0 \text{ ET } 1 = 0 ; \quad 0 \text{ ET } 0 = 0.$$

Exemple : on a l'adresse réseau de l'hôte **172.168.34.80/20**

Adresse d'hôte	172	168	34	80
Adresse d'hôte binaire	10101100	10101000	00100010	01010000
Masque de s-rés binaire	11111111	11111111	11110000	00000000
Adresse réseau binaire	10101100	10101000	00100000	00000000
Adresse réseau	172	168	32	0

III. 4. Les lacunes d'IPv4

IPv4 ne garantit pas :

- La remise des données (perte possible de données, pas de mécanisme de reprise sur erreur).
- L'ordonnancement (séquencement) correct des données à leur réception.
- La confidentialité et l'intégrité des données transmises (les données peuvent être interceptées et copiées, modifiées ou détruites lors de leur transfert).
- L'authentification de la source ou de la destination des paquets.
- N'intègre aucune fonction, mécanisme permettant d'offrir un service de sécurité.
- Limitation en termes de fonctionnalités, d'adressage [1].

Le besoin se fait alors sentir d'aller vers une nouvelle méthode d'adressage beaucoup plus large, des outils interconnectés, en tenant compte de l'évolution rapide et indispensable des technologies utilisées.

IV. Le protocole IPv6

IV. 1. Présentation d'IPv6

Le protocole IPv6 représente la nouvelle génération du protocole IP, d'où le nom d'IPng (Next Generation) qu'on lui donne également. Il maintient les meilleures fonctions d'IPv4.

Pourquoi IPv6 ne s'appelle-t-il pas IPv5 ? Tout simplement, la version 5 d'IP était une version d'expérimentation du protocole STP (Internet Stream Protocol), qui n'a jamais été massivement déployé.

- **Les principales caractéristiques d'IPv6**

- Résoudre le problème de l'épuisement des adresses IPv4.
- Réduire la taille des tables de routage.
- Simplifier le protocole (en simplifiant l'en-tête IP) pour améliorer l'efficacité des routeurs.
- Fournir une meilleure sécurité (authentification et confidentialité).
- Supporter les opérations de diffusion (*multicast*) de manière native (intégration du protocole IGMP dans ICMPv6).

- Amélioration des aspects de diffusion (multicast).
- Intégration de fonctions d'auto-configuration et renumérotation.
- Permettre une coexistence souple avec IPv4 [1].

IV.2. Format du datagramme IPv6

Un paquet IPv6 est composé d'un entête de base auquel peuvent s'ajouter des entêtes d'extension suivant les besoins. Ceci est l'entête de base d'IPv6, La trame IPv6 est :

- plus longue à cause des longueurs d'adresses (128 bits)
- plus simple avec moins de champs.

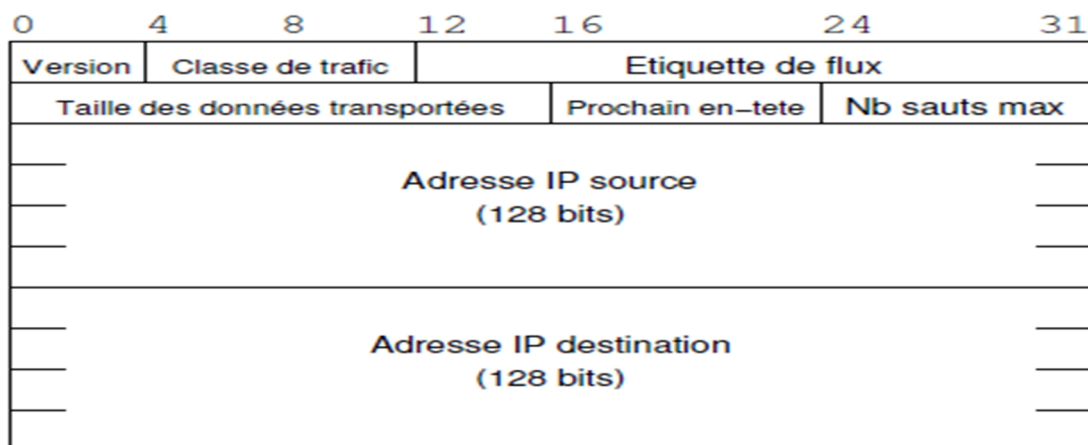


Figure 1.9. Datagramme d'IPv6 [9].

- **Version (14 bits)** version du protocole IP utilisé (IPv6 = 0110).
- **Classe de trafic (8 bits)** identifie le type de contenu encapsulé dans la trame IPv6. Même rôle que le champ TOS en IPv4.
- **Etiquette de flux (20 bits)** : pour faire de la qualité de service.
- **Taille en octet des données transportées (16 bits).**

- **Prochain en-tête (8 bits)** type de l'extension contenu dans les données véhiculées par la trame IPv6.
- **Nombre de sauts maximum (8bits)** nombre de routeurs traversables maximum. Equivalent à TTL IPv4.
- **Adresse IP source (128 bits).**
- **Adresse IP destination (128 bits) [6].**

IV. 3. Adresse IPv6

Une adresse IPv6 est composée de **128** bits contre **32** bits pour IPv4. Ce qui permet d'attribuer un nombre considérable d'adresses ($2^{128} = 3,4 \times 10^{38}$).

La représentation textuelle des adresses IPv6 est faite en utilisant la notation hexadécimale, sur 8 champs de **16** bits séparés par le caractère " : ". On obtient une adresse de la forme :

X:X:X:X:X:X:X:X

Où les **x** représentent les 8 blocs de 16 bits. Considérons l'adresse IPv6.

Exemple : A080:0000:0000:0000:0008:0800:200C:417A

- **Notations :**

- La notation " :: " permet de représenter plusieurs 0 consécutifs au sein de plusieurs mots de 16 bits. Le nombre de 0 peut être retrouvé en examinant le nombre de mots présents dans l'adresse. Cet élément ne peut être présent qu'une fois au sein de l'adresse, par exemple :

A080:0000:0000:0000:0008:0800:200C:417A

→ **A080 :: 0008 :0800 :200C :417A**

- Au sein d'un mot de 16 bits les chiffres hexadécimaux de poids fort positionnés à 0 peuvent être omis.
- Les réseaux IPv6 sont notés en utilisant le CIDR : la première adresse du réseau est suivie par un slash « / » ensuite un nombre qui indique la taille en bits du réseau : c'est le préfixe. Par exemple :

2001 :DB8 :1F89 ::/48 représente l'ensemble des adresses qui commence par **2001 :DB8 :1F89 :0 :0 :0 :0** et finit à **2001 :DB8 :1F89 :ffff:ffff :ffff :ffff :ffff**

- L'utilisation d'une adresse IPv6 comme nom d'hôte doit être encadrée par les caractères « [» et «] ».

Par exemple **[4AD6 :002A :0003 :: 78FF :0000]**.

IV.3.1. Les types d'adresses

IPv6 définit 3 types d'adresses :

IV. 3.1.1. Adresse Unicast (point à point)

Les adresses Unicast sont destinées à la communication avec une interface unique.

- **Adresses unique local (ULA)**

Pour utilisation au sein d'une zone limitée (site ou entre un ensemble limité de sites). Les adresses ULA sont de la forme : **FC00 ::/7** (Figure 1.10).

8 bits	40 bits	16 bits	64 bits
11111101	ID-globale	ID-sous-réseau	ID-interface

Figure 1.10. L'adresse ULA.

• Adresse lien-local

Les adresses de type lien-local sont des adresses dont la validité est restreinte à un lien. Ces adresses sont de la forme FE80::/10 (Figure 1.11).

1111111010	0	ID Interface
10 bits	54 bits	64 bits

Figure : 1.11. L'adresse lien-locale.

Chaque interface réseau possède une adresse de ce type, automatiquement configurée.

Ce type d'adresse permet à 2 machines sur le même lien de communiquer et peut aussi être utilisée pour une connexion ppp ou pour les extrémités d'un tunnel.

• Adresses site-local

Les adresses site-local permettent une utilisation à l'intérieur d'un site sans nécessiter l'utilisation d'un préfixe global. Cet adressage peut être utilisé entre tous les nœuds d'un même site. Ces adresses sont de la forme : (FEC0::/48) (Figure 1.12).

1111111011	0	Subnet-ID	interface-ID
10 bits	38 bits	16 bits	64 bits

Figure 1.12. L'adresse site-locale.

La puissance de l'adressage IPv6, supprime la notion de réseau privé et par conséquent les fonctions de translation (NAT-PAT).

• Adresse global unicast

Le plan d'adressage agrégé, reprend la structure classique d'adressage IPv6, soit un préfixe identifiant le réseau et une partie identifiant local.

Le plan comprend trois niveaux de hiérarchie :

- une topologie publique (48 bits);
- une topologie de site (16 bits) ;
- une topologie d'interface (64 bits) ;

Les adresses de ce type sont de forme :

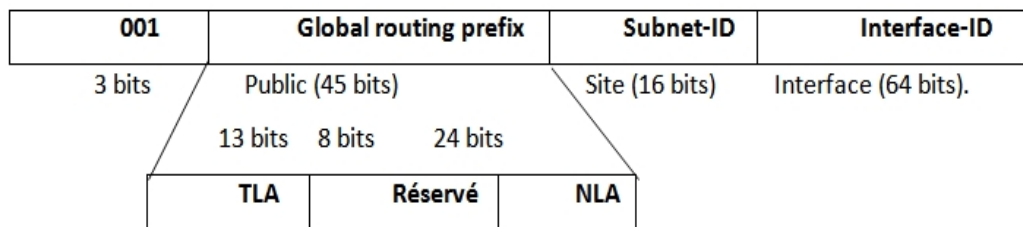


Figure 1.13. L'adresse globale unicast [12].

- **TLA (Top Level Aggregator)** : identifiant l'unité d'agrégation la plus haute ;
- **NLA (Next Level Aggregator)** : identifiant l'unité d'agrégation la plus basse ;
- **Réservé** : sont réservés à un usage futur ;
- **Identifiant d'interface** : Identifiant sur 64 bits pour désigner une interface connectée sur un lien, peut être construit à partir de l'adresse de niveau deux de l'interface réseau.

IV. 3.1.2. Adresses Anycast

Une adresse *Anycast* permet de représenter un service plutôt qu'une interface donnée. On veut ainsi pouvoir joindre une machine fournissant certains services sans se soucier de la machine contactée. Elle est très peu utilisée pour l'instant et pose naturellement des problèmes de sécurité.

Ces adresses sont de la forme suivante :

N bits	128-n bits
Subnet prefix	0

Figure : 1.14. L'adressage d'Anycast.

Les adresses Anycast ont deux points communs avec les adresses unicast : elles sont allouées dans le **même espace d'adressage** et ont les **mêmes formats** [7].

IV.3.1.3. Adresses multicast

La notion de broadcast est remplacé par l'utilisation du multicast à des groupes restreints.

Les adresses multicast IPv6 sont représentées par le préfixe : **FF00::/8** (Figure1.7).

11111111	Flags (000T)	Scope	ID de groupe
8 bits	4bits	4 bits	112 bits

Figure : 1.15. L'adressage multicast.

- Flags représente un groupe de plusieurs valeurs. Les 3 premiers bits doivent être égaux à 0. Le dernier bit représente la validité de l'adresse multicast (T=1 ou T=0).
- scope détermine la portée des adresses multicast :
 - ✓ 0 : réservé ; ✓ 1 : nœud ; ✓ 2 : lien (FF02 ::/8) ;
 - ✓ 3 : sous-réseau ; ✓ 5 : site ; ✓ 8 : organisation ;
 - ✓ E : global ; ✓ F : réservé.

IV. 3.2. Adresse particulières

Comme IPv4, le protocole IPv6 définit un certain nombre d'adresses ou de plages d'adresses dédiées à un usage particulier :

- **::1/128** : la boucle locale.
- **::0 ou ::** : cette adresse indéterminée est utilisée pendant l'initialisation DHCPv6 d'une adresse IPv6.
- **FE80** : l'adresse lien-local servant en local à désigner une interface réseau.
- **FF01::** : la Nœud local. Un paquet émis sur cette adresse ne quitte jamais l'équipement
- **FF02::1** : Lien local. Sert à désigner tous les nœuds IPv6 situés sur le même lien local que l'interface de connexion. Ils ne doivent pas être routés sur un autre réseau.
- **FF02::2** : Sert à désigner tous les routeurs connectés sur le même lien local que l'interface de connexion.
- **FF02::3** : Sert à désigner tous les hôtes situés sur le lien local.
- **FF05::** : Désigne tous les hôtes du réseau local.
- **FEC0::/10** : Adresse de réseau privé [12].

V. Transition IPv4 vers IPv6

V. 1. Mécanismes de transition

Les machines actuelles et à venir devront être capables de traiter des paquets IPv6 autant que les paquets IPv4. Pour transiter de la version 4 à la version 6 d'IP, trois techniques ont été mises au point :

- Sur les hôtes : double pile
- Sur le réseau : tunnels
 - Statique : tunnel broker.
 - Dynamique: TEREDO, 6to4, ISATAP, 6over4.
- Par translation de protocoles
 - NAT-PT : traduire les en-tête des paquets IPv6 en IPv4.

V. 1.1. Double pile (Dual Stack)

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. Ce système implique d'avoir deux piles (la IPv4 et la pile IPv6) configurées correctement et est entièrement transparent pour l'utilisateur. Cette solution est actuellement la meilleure et doit être utilisée en priorité [8].

➤ Inconvénients

- Ne résout pas le problème de pénurie des adresses.
- Routeurs doivent pouvoir acheminer les deux types de paquets.
- Applications doivent être recompilés.

➤ **Avantages**

- Mécanisme de transition le plus simple et le plus souple.

V.1.2. Les tunnels IPv6 dans IPv4

Les paquets IPv6 sont encapsulés dans des paquets IPv4 à l'entrée du tunnel en ajoutant un entête IPv4 (avec champ 'protocole'=41), ensuite ils sont dé-encapsulés et traités comme s'ils provenaient du réseau IPv6 à la sortie du tunnel [9].

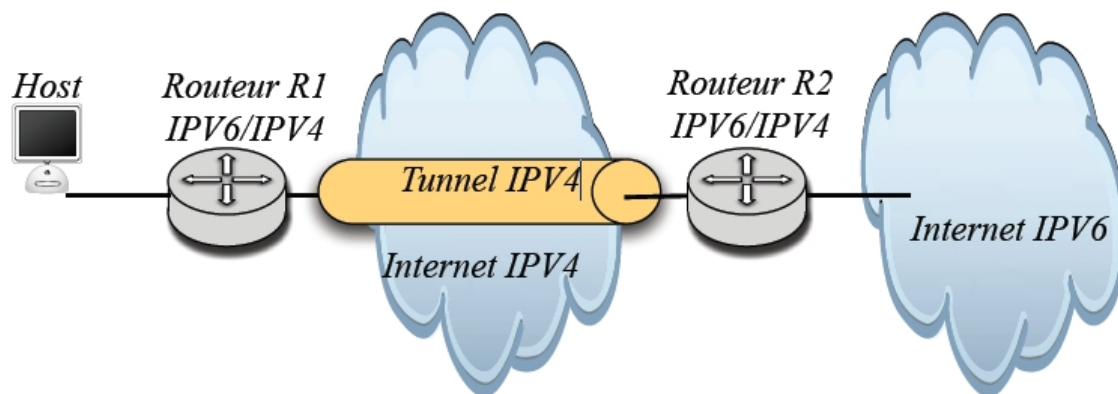


Figure 1.16. Tunnel dans IPv4 et IPv6 [9].

Il existe deux types de tunnels : les tunnels statiques et les tunnels automatiques.

V. 1.2.1. Tunnel statique

- **Tunnel broker**

Tunnel Broker utilise une autre approche basée sur des serveurs dédiés appelés "Tunnel Brokers" qui gèrent automatiquement les demandes de tunnel des Utilisateurs. Tunnel Broker est bien adapté pour les petits sites

IPv6 isolés, et spécialement les machines IPv6 isolées sur l'Internet IPv4, qui veulent se connecter à un réseau IPv6 existant.

Tunnel Broker permet à des FAI IPv6 de facilement gérer les contrôles d'accès des utilisateurs, renforçant ainsi leur politique sur l'utilisation des ressources réseau [8].

V. 2.2.2. Tunnel dynamique

- accès d'une machine isolée à toutes les autres.
- permet la réutilisation de l'infrastructure IPv4 (routeurs Ipv4).
- utilisation d'adresses IPv4 compatibles.

➤ Le 6to4

Le mécanisme 6to4 permet d'interconnecter entre eux des sites IPv6 isolés en créant des tunnels automatiques IPv6 dans IPv4 en fonction du destinataire des données.

- Mieux adapté pour les extranets et les VPN.
- En utilisant des relais 6to4, les sites 6to4 peuvent aussi joindre des sites sur l'Internet IPv6.
- 6to4 ne permet pas l'interopération entre les hôtes uniquement IPv4 et les hôtes uniquement IPv6 [11].

6to4 réalise 3 tâches:

1. Assigne un bloc d'adresses IPv6 à tout hôte ou réseau qui dispose d'une adresse IPv4
2. Encapsule les paquets IPv6 à l'intérieur des paquets IPv4 afin de permettre leur transition sur un réseau IPv4

3. Effectue le transit du trafic entre 6to4 et les réseaux IPv6 « natifs » (agit comme un routeur).

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

ISATAP (qui se prononce ice-a-tap) est en quelque sorte la déclinaison des principes de 6to4 à un réseau local, de façon à permettre un tunneling automatique et l'échanges de flux IPv6 entre terminaux double pile interconnectés via un réseau local IPv4 uniquement. ISATAP permet le déploiement de terminaux dual-stack et d'applications IPv6 sur une infrastructure locale IPv4, comme typiquement celle d'un réseau d'entreprise. ISATAP peut être déployé de plusieurs façons : soit simplement au sein des terminaux concernés afin de leur permettre d'échanger des flux IPv6 alors qu'ils sont connectés sur une infrastructure IPv4, soit en combinaison avec des routeurs 6to4 de façon à échanger des flux IPv6 localement et avec des sites distants.

ISATAP est compatible avec 6to4 [8].

➤ **6 over 4**

6over4, également appelé tunneling multidiffusion IPv4, permet aux nœuds IPv6 et IPv4 de communiquer au moyen du protocole IPv6 via une infrastructure IPv4. Pour que 6over4 fonctionne correctement, l'infrastructure IPv4 doit être en mesure de prendre en charge la multidiffusion IPv4.

➤ **Teredo**

Protocole de tunnelage permettant à un hôte derrière un NAT d'accéder à l'Internet IPv6 par le biais d'un serveur et de relais Teredo.

Teredo est conçu pour permettre un robuste trafic IPv6 à travers les NAT, et le prix de la robustesse est un montant raisonnable des frais généraux, en raison de l'encapsulation UDP et la transmission de bulles. Les nœuds qui veulent se connecter à l'Internet IPv6 ne doivent utiliser le service Teredo qu'en «dernier recours»: ils devraient préférer une connectivité directe IPv6 si elle est disponible sur place [9].

V.2.3. Par translation de protocole

- **NAT-PAT**

Est un outil de migration conçu pour aider les utilisateurs dans la transition de leurs réseaux IPv4 vers IPv6. Il permet la communication directe entre des hôtes utilisant des protocoles réseaux différents.

Les utilisateurs peuvent utiliser un système statique ou des systèmes dynamiques pour l'application du protocole NAT-PAT dans leur réseau.

V. 3. L'adressage de transition

La migration d'IPv4 vers IPv6 ne peut être réalisée que progressivement. Durant un temps assez important les deux versions de protocoles devront cohabiter. Aussi, deux solutions ont été envisagées pour permettre d'utiliser les adresses IPv4 dans le domaine IPv6. La notion IPv4 mappée est une représentation interne des adresses afin de permettre à des programmes IPv6 de fonctionner sur un réseau IPv4. La communication se fait d'une machine IPv4 à IPv4.

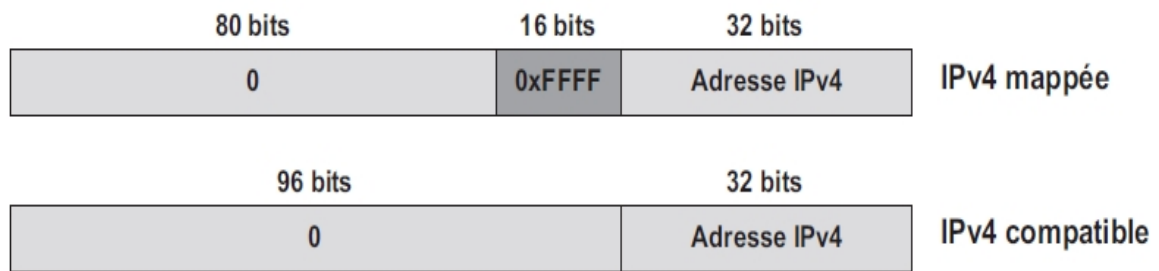


Figure 1.17. L'adressage IPv4/IPv6 [12].

VI. *Conclusion*

Dans ce chapitre nous avons présenté un aperçu général sur le protocole IP, afin d'avoir une vision globale sur celui-ci, ensuite nous avons détaillé le concept d'adressage utilisé dans les différentes versions de ce protocole, IPv4 et IPv6, démontrant que l'administration réseau exige un niveau technique très avancé pour bien planifier et gérer son réseau, surtout lorsqu'il s'agit des topologies complexes.

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

Ce chapitre décrit les problématiques liées à la planification des réseaux dans le but de définir les besoins formant l'objectif de ce projet.

Notre étude vise à développer un site Web destiné aux étudiants universitaire ou bien aux administrateurs réseau, permettant d'offrir des services concernant l'adressage IPv4 et IPv6 de manière très pratique à assister ces clients dans leurs études ou bien dans leurs domaine professionnel.

Afin de bien se préparer à la phase de conception, nous avons élaboré une maquette qui va servir de vision future de notre site Web.

II. Problématique

Mettre en place un réseau ou bien le connecter à d'autres réseaux est une tâche qui nécessite une étude détaillée afin d'éviter des anomalies qui peuvent survenir dans le cycle de vie de ce réseau. Surtout lorsqu'il s'agit de concevoir des réseaux hybride combinant le protocole IPv4 et IPv6.

Notre recherche nous a conduit à déceler quelques problèmes liée à la planification des réseaux IP, particulièrement pour les non expérimentés dans ce domaine :

➤ Problèmes liées à la planification d'un réseau IPv4

- Mauvaise utilisation des adresses IP : Configuration des adresses publiques dans un réseau local.
- Flat Network : Utilisation des adresses de classe A dans un petit réseau.
- Mauvais calcul des sous réseaux.
- Utilisation des adresses IP réservées.
- Connexion d'un nombre de machines dépassant la capacité du sous-réseau.

➤ Problèmes liées à la planification d'un réseau IPv6

- Configuration des adresses IPv6 avec format non valide
- Mauvaise compression d'une adresse IPv6.
- Utilisation d'un préfixe erroné pour une adresse IPv6.

➤ Problèmes liées à la planification des réseaux hybride

Le déploiement d'IPv6 sur Internet est compliqué en raison de l'incompatibilité des adresses IPv4 et IPv6. Les traducteurs d'adresses automatiques se heurtent à des problèmes pratiques importants. Pendant une phase de transition où coexistent IPv6 et IPv4, les hôtes disposent d'une double pile, c'est-à-dire qu'ils disposent à la fois d'adresses IPv6 et IPv4, et des tunnels permettent de traverser les groupes de routeurs qui ne prennent pas encore en charge IPv6.

Le choix du tunnel à utiliser pour assurer la communication dans son réseau hybride, doit être étudié afin de répondre aux besoins des clients (entreprises, fournisseur d'accès à Internet).

III. Approche proposée

Nous projetons dans ce qui suit, un ensemble de services à assurer, dans le but de réduire une grande partie des problèmes cités précédemment.

III.1. Services concernant IPv4

Cette partie permet aux clients (Administrateur / étudiant) de :

- **Se renseigner sur une adresse IPV4**

Ce service assure un support documentaire très riche au client dans le but d'assimiler une topologie réseau existante ou bien valider un projet de planification réseau.

A partir de l'introduction d'une adresse IPv4 valide, le client peut obtenir les informations suivantes :

Classe	Classe A , Classe B , Classe C , Classe D ou Classe E
Type	Privée, Publique
Masque du réseau	Selon la classe
Adresse réseau	Calculée à partir du masque et l'adresse introduite
Adresse broadcast	Calculée à partir du masque et l'adresse introduite

La classe de l'adresse IP introduite est obtenue à partir des bits du poids fort du premier octet de cette adresse, comme suit :

Classe A:	0xxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
Classe B:	10xxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
Classe C:	110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
Classe D:	1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
Classe E:	11110xxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

Pour calculer l'adresse réseau, il faut juste appliquer l'opérateur logique AND entre l'adresse IP introduite et le masque (correspondant à l'adresse IP introduite).

$$\text{IP_H\^OTE AND IP_MASQUE} = \text{IP_RESEAU}$$

L'adresse de diffusion est obtenue en appliquant un OR logique entre l'adresse IP introduite avec l'inverse (NOT logique) du masque réseau.

$$(\text{IP_H\^OTE}) \text{ OR } (\text{NOT IP_MASQUE}) = \text{IP_DIFFUSION}$$

- **Segmentation des réseaux IPv4**

La segmentation d'un réseau en un nombre déterminé de sous-réseaux, consiste à retirer quelques bits de la partie hôte et les rajouter à la partie réseau. Le masque par défaut de l'adresse IP introduite nous aide à repérer la partie hôte.

A partir du nouveau masque de sous-réseau calculé, on détermine pour chacun des sous réseaux :

- 1) L'adresse réseau
- 2) L'adresse de diffusion
- 3) L'adresse IP du premier hôte : $\rightarrow \text{IP_RESEAU} + 1$
- 4) L'adresse IP du dernier hôte: $\rightarrow \text{IP_DIFFUSION} - 1$

Chaque sous-réseau débute après l'adresse de diffusion du sous-réseau précédent.

III.2. Services concernant IPv6

Cette partie permet aux clients (Administrateur / étudiant) de :

- **Se renseigner sur une adresse IPv6**

A partir de l'introduction d'une adresse IPv6 valide, le client peut obtenir les informations suivantes :

Type	Exemple : Global Unicast
Préfixe	Exemple : 64

- **Compression décompression d'une adresse IPv6**

Ce service consiste à compresser une adresse IPv6 en supprimant les zéros non significatifs, ou bien de décompresser une adresse IPv6 en rétablissant son format original codé sur 32 chiffres hexadécimaux.

Notre algorithme de compression passe par deux étapes :

La première étape est nommée « Leading Zero Compression ». Elle consiste à supprimer les zéros placés à gauche pour chaque champ, comme suit :

Adresse IPv6: FE80:0000:0000:0000:0202:B3FF:FE1E:8329

Compression STEP 1: FE80:0:0:0:202:B3FF:FE1E:8329

Dans la deuxième étape, et à partir du résultat obtenu dans l'étape précédente en remplace la plus longue série des zéros par « :: » rien qu'une seule fois, ce qui donne le résultat suivant :

Compression STEP 2: FE80::202:B3FF:FE1E:8329

III. 3. Le tunneling

Le service envisagé pour le tunneling, propose un assistant, qui sert d'un guide, permettant aux clients de déterminer le meilleur tunnel adapté à leur topologie ainsi qu'à leurs besoins, à travers un formulaire listant différentes options justifiant le choix de notre système.

IV. Maquette du projet

Dans cette partie nous allons exposer notre vision pour ce projet à travers une maquette qui va servir d'un guide lors de la conception de notre site.

- **La page d'accueil**

Proposant trois volets principaux IPv4, IPv6 et Tunneling.



Figure 2.1 : Page d'accueil.

Volet N°1 : Page de services d'adresse IP V4

Cette page offre un ensemble de services concernant l'adressage IP version 4 (voire figure2.2, 2.3 et 2.4).



Figure 2.2 : Page services d'adresse ipv4.

Se renseigner sur une adresse IPv4

Entrez votre adresse IP:

Adresse IP:	10.10.10.0
Classe:	A
Type d' adresse:	Adresses privées
Adresse réseau:	10.0.0.0
Le masque réseau:	255.0.0.0
Adresse du broadcast:	10.255.255.255

Figure 2.3 : Page « se renseigner sur une adresse IPV4 »

Segmentation des réseaux IPv4

Entrez votre adresse IP:

Entrer le nombre de s/r:

Sous-réseaux calculés:

adresses S/Réseau	Premier Hôte	Dernier Hôte	Adresse de diffusion
192.168.20.0	192.168.20.1	192.168.20.62	192.168.20.63
192.168.20.64	192.168.20.65	192.168.20.126	192.168.20.127
192.168.20.128	192.168.20.129	192.168.20.190	192.168.20.191
192.168.20.192	192.168.20.193	192.168.20.254	192.168.20.255

Figure 2.4 : Page « segmentation des réseaux ».

Volet N°2 : Page de services d'adresse IPv6

Cette page offre un ensemble de services concernant l'adressage IP version 6 (voire figure 2.5, 2.6 et 2.7).



Figure 2.5 : Page services d'adresse IPV6.

Se renseigner sur une adresse IPv6

Entrez votre adresse IP:

Adresse IP:	2011:ab12:d102:e201:0210:2148:0210:2148
Type:	Global Unicast
Longueur Prefix:	64

Figure 2.6 : Page « se renseigner sur une adresse IPv6 ».

Compression / décompression adresse ipv6

Entrez votre adresse IP:

Figure 2.7 : page « compression /décompression ».

Volet N°3 : Page Tunneling

Conception d'une solution WEB assistant les administrateurs à la planification des réseaux IPv4, IPv6 et les réseaux hybrides.

Cette page assure l'assistance au choix du meilleur tunnel adapté au réseau hybride (IPv4 & IPv6) à travers un formulaire bien étudié dans le but de simplifier cette opération.



Figure 2.8 : Page tunneling.

The form displays the 'Choix du tunnel' section. It includes a 'Topologie' dropdown menu set to 'Point à Point' and a 'Paquets véhiculés' dropdown menu set to 'IPv6'. A 'Validez' button is located below these dropdowns. The 'Tunnel recommandé' section shows 'GRE- and IPv4- compatible' as the recommended tunnel type. A yellow box below this text provides a description: 'Simple point-to-point tunnels that can be used within a site or between sites. Can carry IPv6 packets only.'

Figure 2.9 : Page « assistant choix du tunnel ».

IV Conclusion

Dans ce chapitre, nous avons décrit les problématiques liées à la planification des réseaux IP. 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 de besoin**
- IV. Conclusion**

I. Introduction

Dans ce chapitre, nous allons présenter la phase de conception de notre site WEB, en utilisant le langage de modélisation UML, à travers un ensemble de diagrammes décrivant les différentes fonctionnalités offertes par notre système

II. UML

UML (Unified Modeling Language) se définit comme un langage de modélisation graphique qui permet la spécification des systèmes d'informations à travers une vision orientés objet. UML permet de modéliser un système informatique de façon à simplifier la construction de ses composantes logicielles.

II.1. Caractéristiques d'UML

- UML est un langage formel
- UML n'est pas une méthode ou un processus
- UML cadre l'analyse objet
- UML est un support de communication

II.2. Les points forts d'UML

UML est un langage formel et normalisé :

- Permet une grande précision.
- Assure la pérennité.
- Facilite l'utilisation d'outils.

UML est un outil qui facilite la communication :

- Propose un cadre d'analyse.
- Permet la représentation d'éléments abstraits et complexes.
- Offre une grande expressivité.

- Son caractère polyvalent et son indépendance par rapport aux langages d'implémentation en font un langage universel.

II.3. Les points faibles d'UML

- La mise en pratique d'UML nécessite un apprentissage et passe par une période d'adaptation.
- Le processus (non couvert par UML) est une autre clé de la réussite d'un projet.
- UML est un langage suivant par deux voies soit par une méthode doit fournir un langage de modélisation graphique et une démarche (processeur) à adopter pour développement un logiciel ou par aucune méthode doit être ne définit pas une démarche à suivre, le processus (non couvert par UML) est une autre clé de la réussite d'un projet et Spécifie comment décrire des cas d'utilisation, des classes, des interactions...

II.4. Les vues UML

UML fournit un moyen astucieux permettant de présenter diverses projections d'une même représentation grâce aux vues. Une vue est constituée d'un ou plusieurs diagrammes. Ils se répartissent en trois grands groupes :

II.4.1 Vue statique ou structurelle

Cette vue comporte des diagrammes, au nombre de six, permettant de représenter l'aspect statique d'un système (classes, objets, composants...).

- Diagramme de classe

- Diagramme d'objet
- Diagramme de composant
- Diagramme de paquetage
- Diagramme de déploiement.
- Diagramme de structure composite [14].

II.4.2 Vue dynamique ou de comportement

Les diagrammes de cette vue représentent la partie dynamique d'un système réagissant aux événements et permettant de produire les résultats attendus par les utilisateurs.

- Diagramme des cas d'utilisation
- Diagramme d'activité
- Diagramme d'état-transition
- Diagramme d'interaction :
 - Diagramme de séquence.
 - Diagramme de communication.
 - Diagramme global d'interaction.
 - Diagramme de temps [14].

II.5. Mise en œuvre d'UML

Afin de réussir la phase de conception du système, il faut prendre en compte les points suivants :

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

II.5.1. Les étapes de la démarche

➤ Phase d'identification des besoins

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

➤ Phases d'analyse

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

➤ Phase de conception

- Diagrammes d'interaction.

III. Modèle de besoin

III. 1. Identification des acteurs

Un acteur joue le rôle d'une entité externe (personne, un autre système,...) qui interagit avec le système.

Notre solution WEB est destinée aux étudiants universitaires ainsi qu'aux administrateurs réseau débutant. L'acteur ou bien le client peut accéder aux services offerts par notre site gratuitement (sans passer par la création d'un compte spécifique).

A partir de notre système, le client est capable de :

- Se renseigner sur des adresses IPv4 /IPv6.
- Segmenter des réseaux IPv4.
- Compresser / Décompresser des adresses IPv6.
- Utiliser un assistant au choix des tunnels applicables aux réseaux hybride.

III.2. Le diagramme des cas d'utilisation

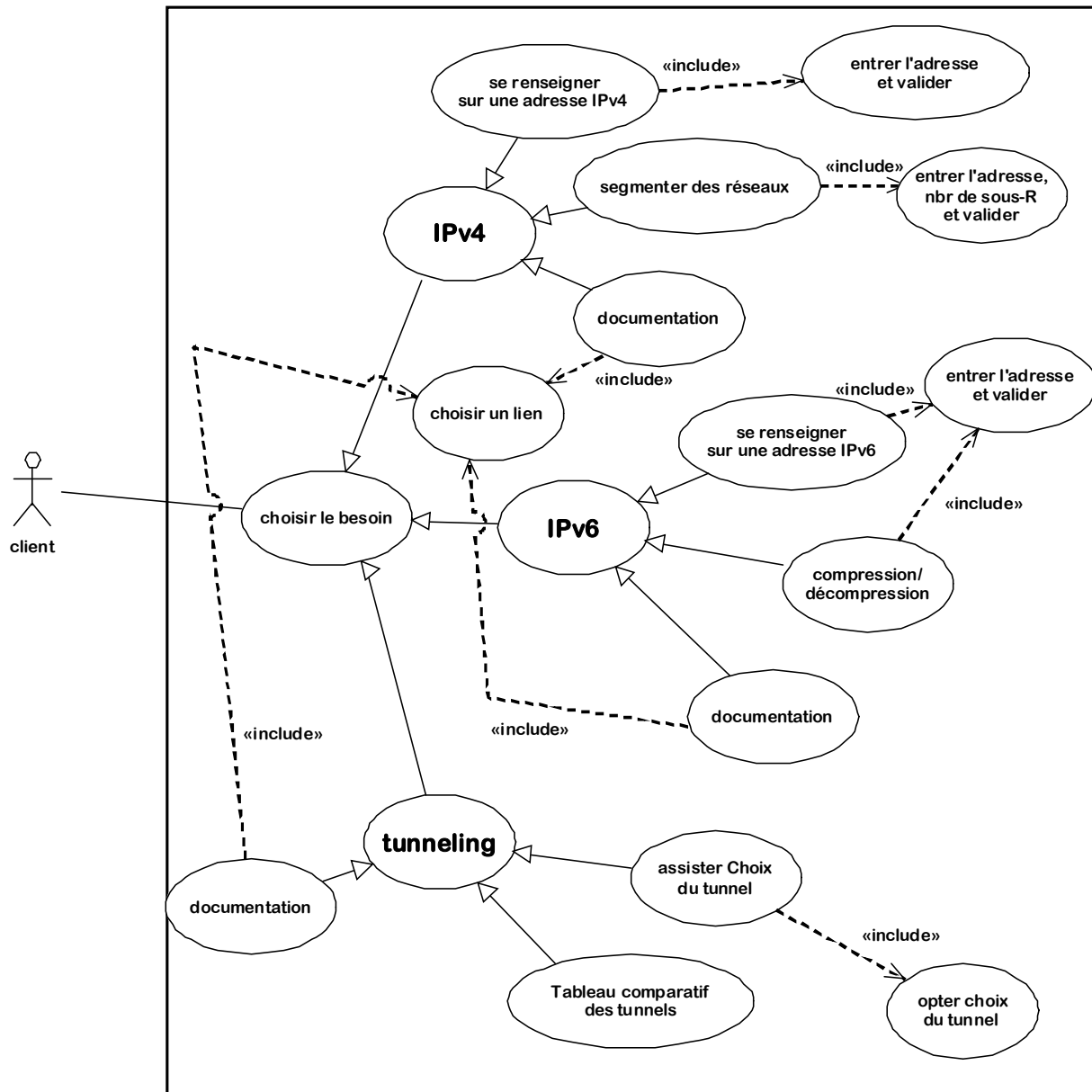


Figure3.1. diagramme de cas d'utilisations.

III.2.1. Cas d'utilisation « se renseigner sur une adresse IPv4 »

Cas d'utilisation	se renseigner sur une adresse IPv4
Acteur	Client
Objectif	Se renseigner sur toutes les informations concernant une adresse IPV4
Pré condition	Validité de l'adresse IPv4 introduite
Post condition	les renseignements sont annoncés.
Scenario nominal	1. Le client demande la page « IPv4 ». 2. Le système affiche la page. 3. Le client demande le formulaire « se renseigner l'adresse IPv4 ». 4. Le système affiche le formulaire. 5. Le client saisit l'adresse IPv4 et valide. 6. Le système afficher le renseignement.
Scenario alternative	1. L'adresse est invalide : Le système affiche un message d'avertissement.
Exception	Néant

Tableau 3.1. La fiche descriptive du cas d'utilisation
« Se renseigner sur une adresse IPv4 ».

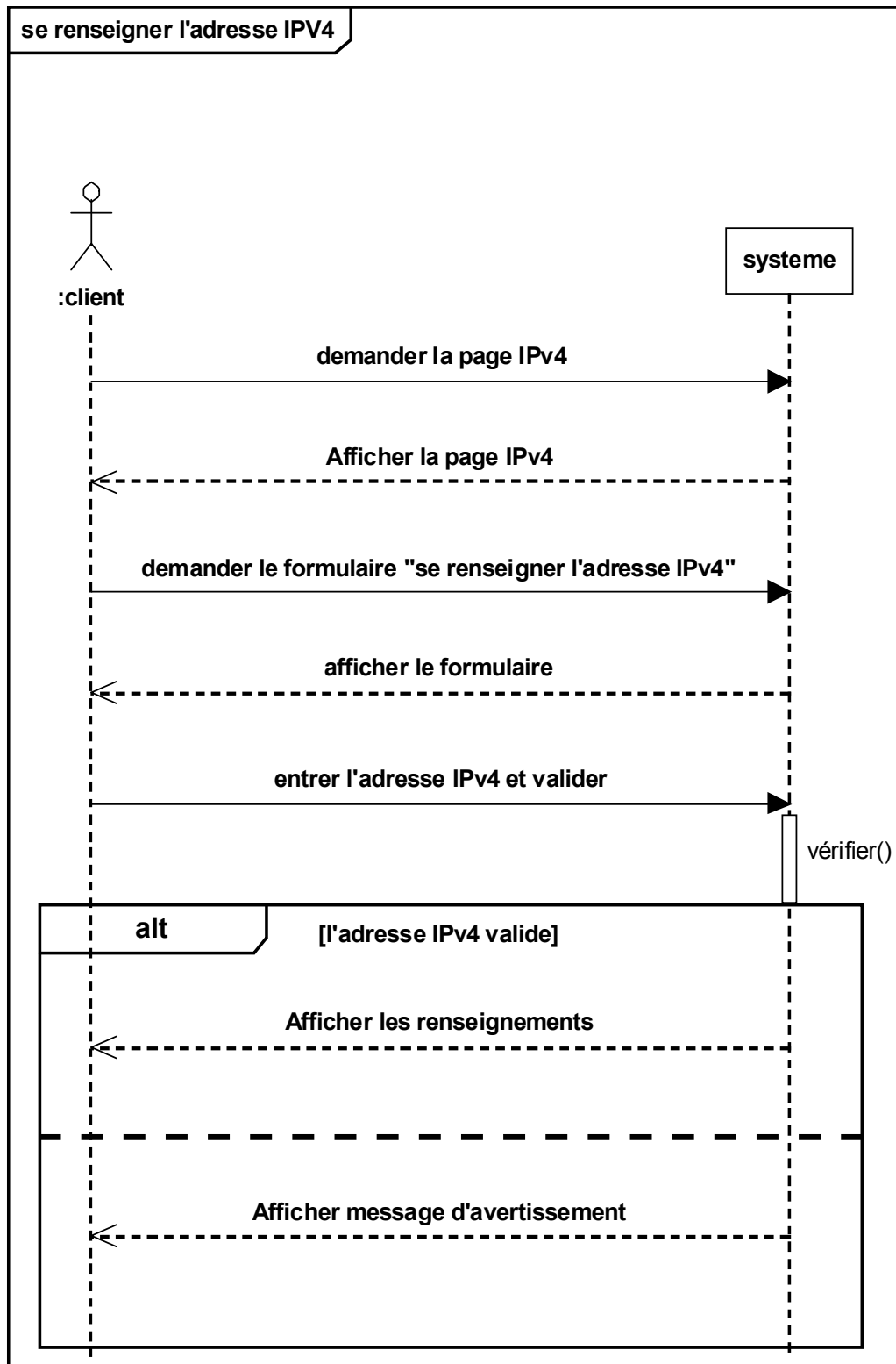


Figure 3.2. Diagramme de séquence système du cas d'utilisation
«Se renseigner sur une adresse IPV4 ».

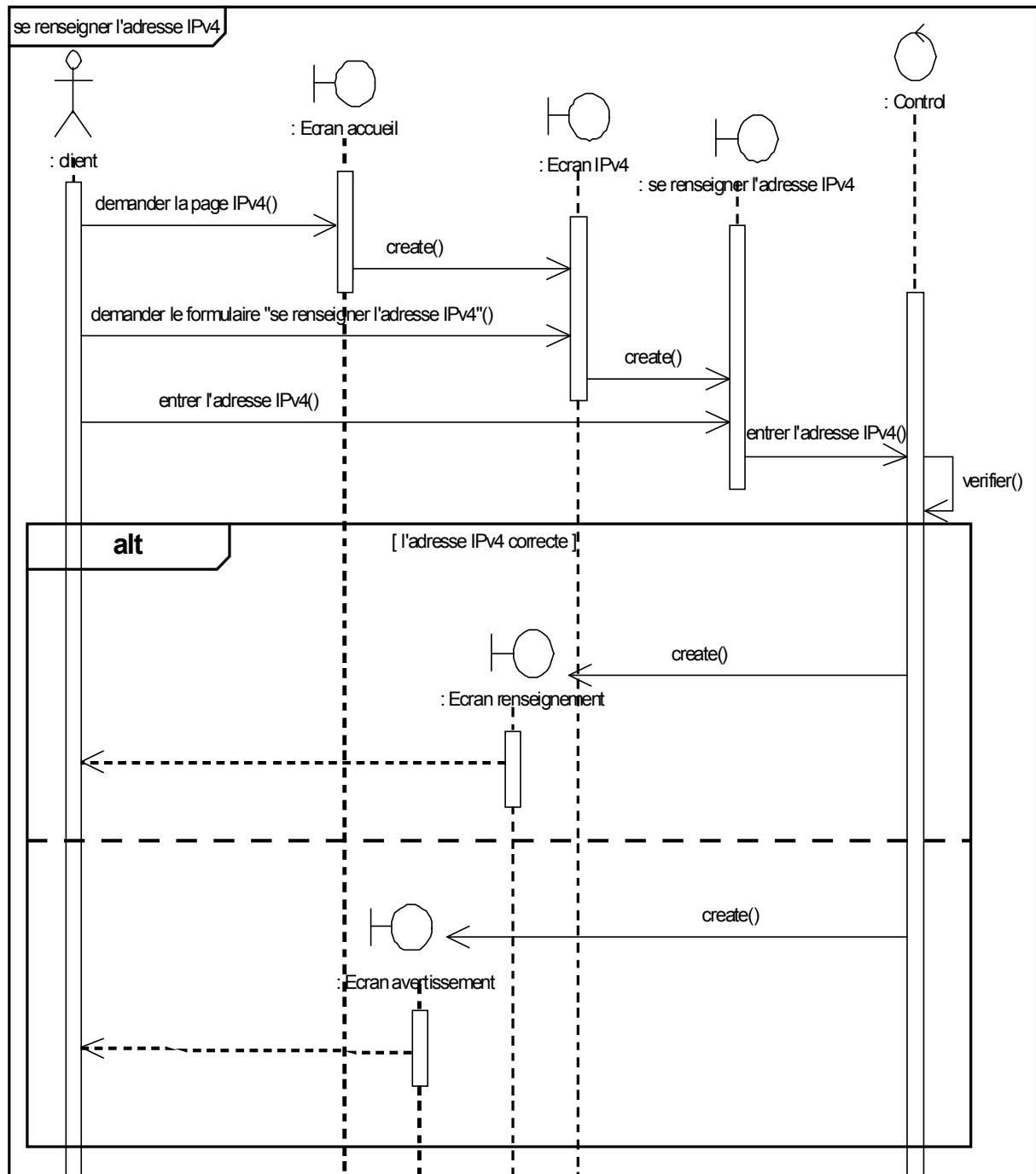


Figure 3.3. Diagramme d'interaction du cas d'utilisation

« Se renseigner sur une adresse IPv4 ».

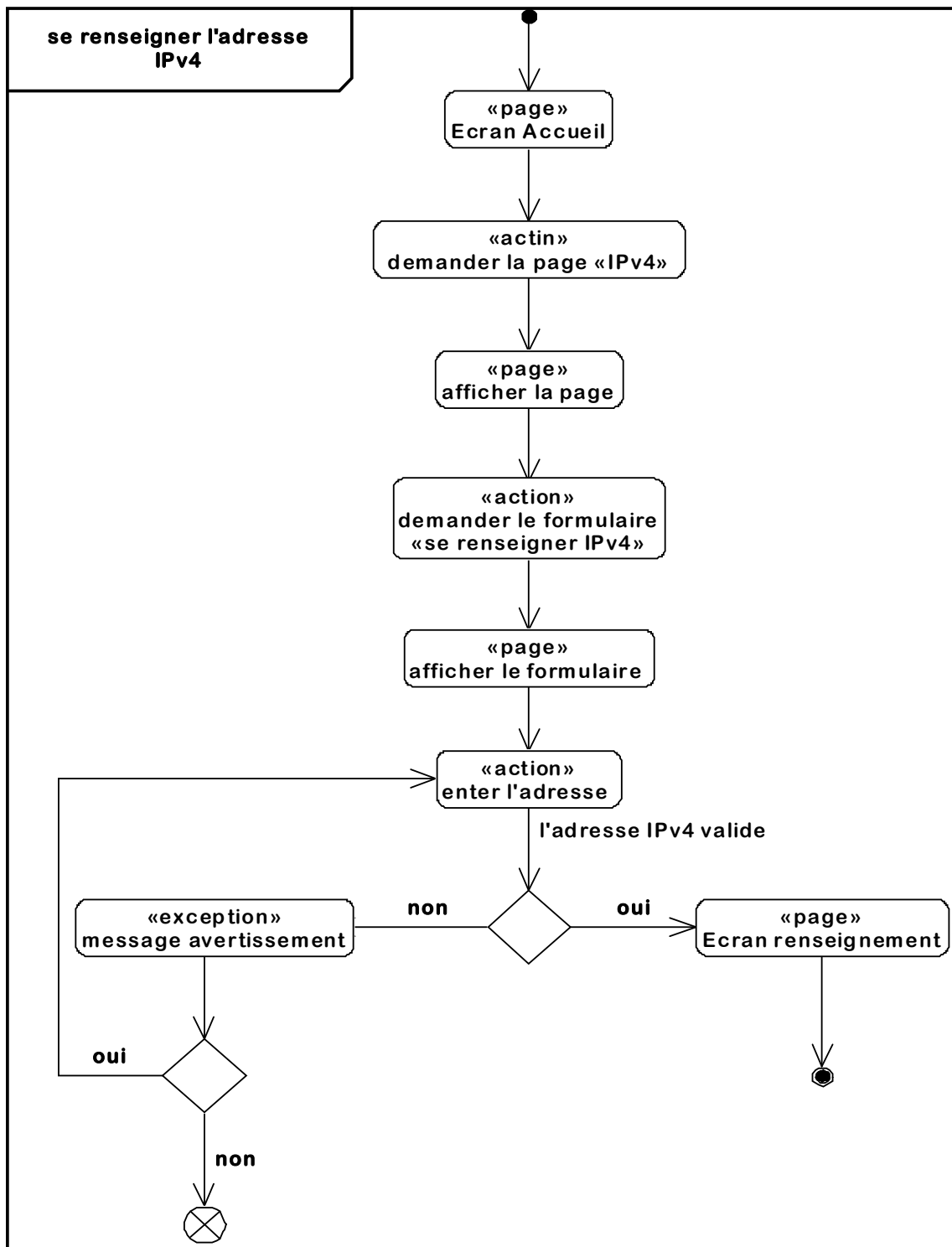


Figure 3.4. Diagramme de navigation du cas d'utilisation
« Se renseigner sur une adresse IPv4 ».

III.2.2. Cas d'utilisation « Segmenter des réseaux IPv4 »

Cas utilisation	Segmenter des réseaux IPv4
Acteur	Client
Objectif	Segmenter une adresse réseau IPV4 en un nombre de sous réseaux tout en calculant l'adresse de diffusion, la première et la dernière adresse IP utilisable pour chaque sous réseau.
Pré condition	Validité de l'adresse IPV4 introduite ainsi que la conformité du nombre de sous-réseaux voulus.
Post condition	Les sous-réseaux sont calculés
Scenario nominal	1. Le client demande la page « IPv4 ». 2. Le système affiche la page. 3. Le client demande le formulaire « segmentation des réseaux ». 4. Le système affiche le formulaire. 5. Le client saisit l'adresse IPv4 et le nombre de sous-réseaux voulus ensuite valide. 6. Le système calcule et affiche les résultats.
Scenario alternatif1	1. L'adresse IPV4 ou le nombre de sous-réseaux introduits sont invalides. Système afficher un message d'avertissement.

Tableau 3.2. La fiche descriptive du cas d'utilisation

«Segmenter des réseaux IPv4 ».

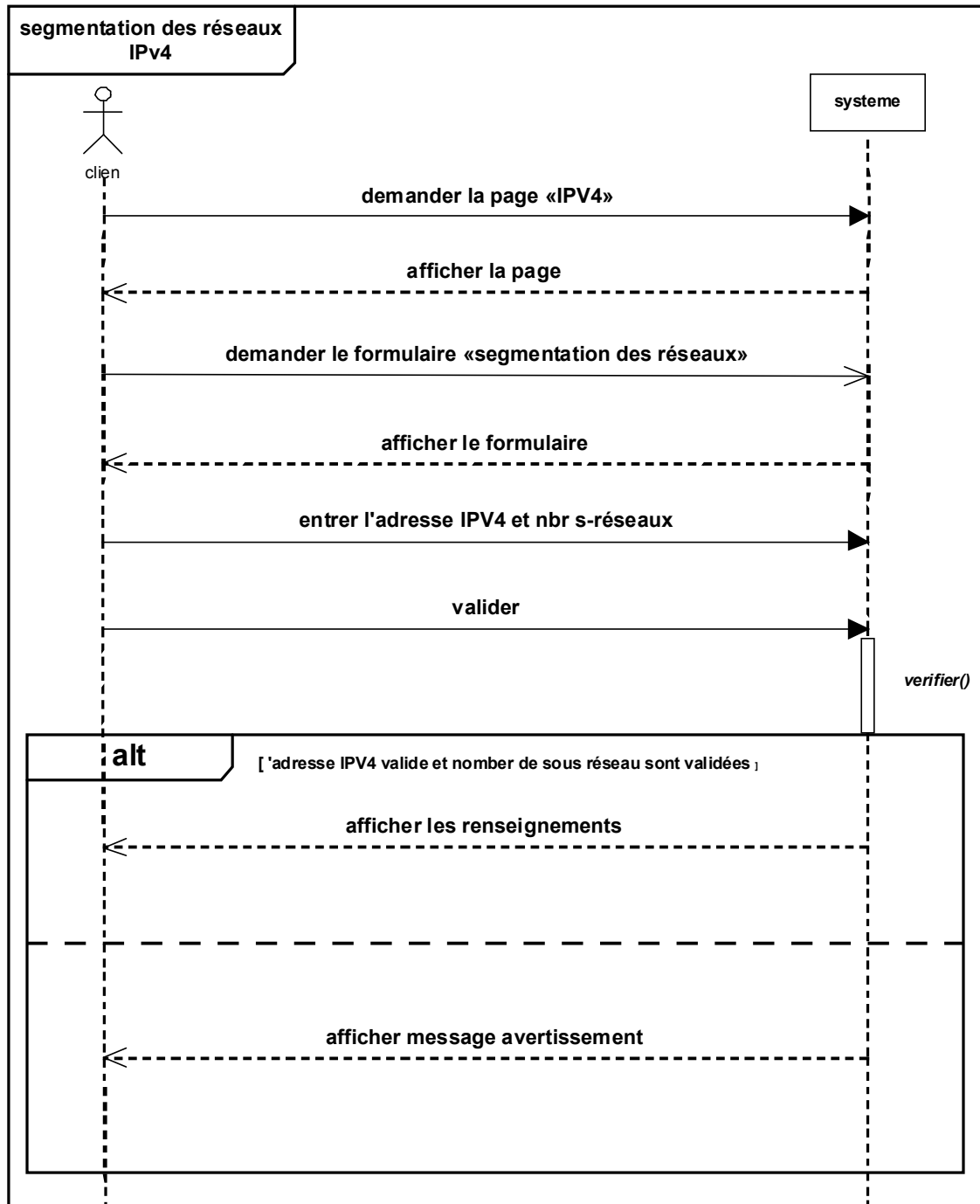


Figure 3.5. Diagramme de séquence système du cas d'utilisation
« Segmenter des réseaux IPv4 ».

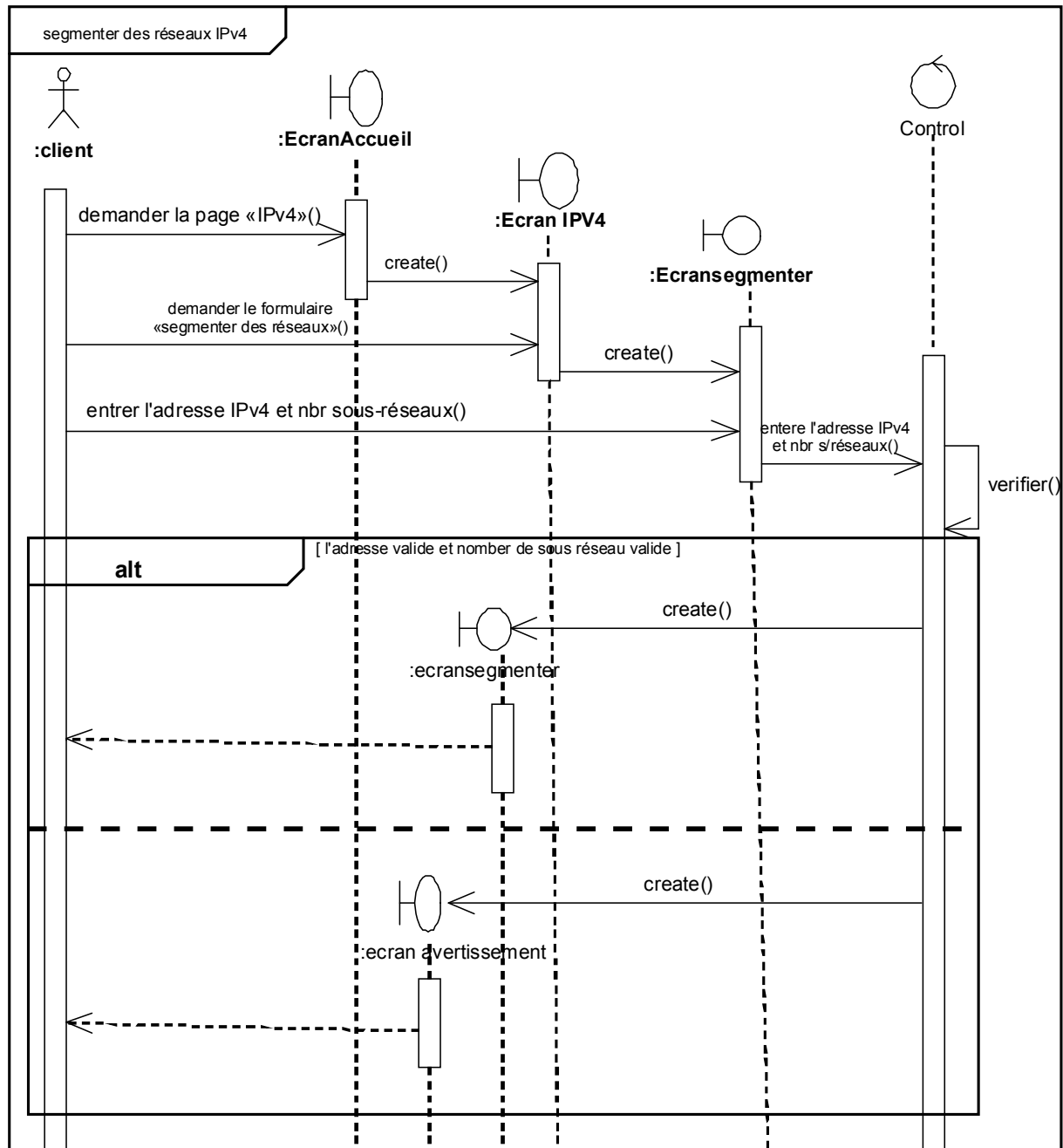
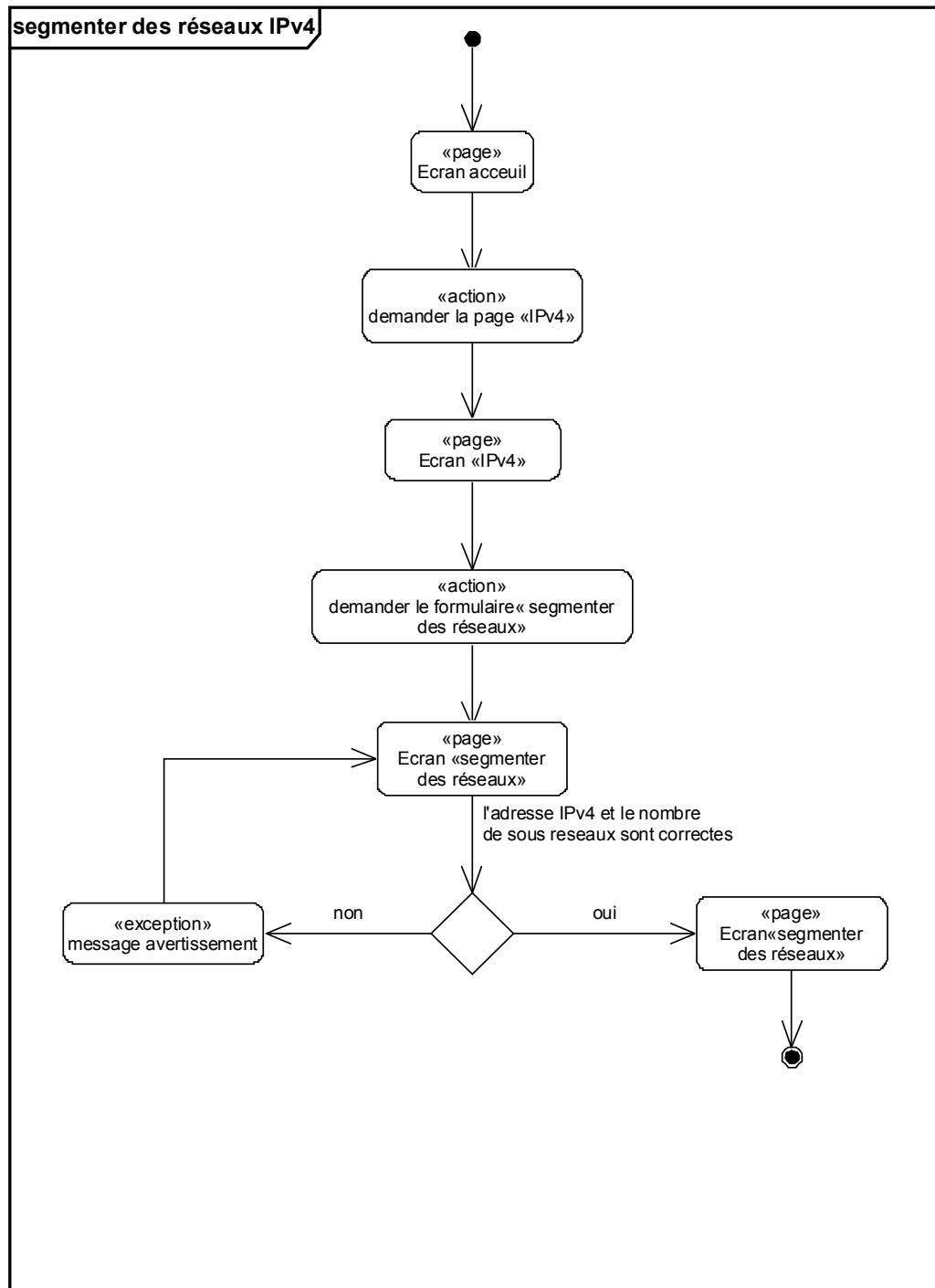


Figure 3.6. Diagramme d'interaction du cas d'utilisation

« Segmenter des réseaux IPv4 ».



**Figure 3.7. Diagramme de navigation du cas d'utilisation
« Segmenter des réseaux IPv4 ».**

III.2.3. Cas d'utilisation « *Se renseigner sur une adresse IPv6* »

Cas utilisation	<i>Se renseigner sur une adresse IPv6</i>
Acteur	Client
Objectif	Se renseigner sur une adresse IPV6.
Pré condition	Validité de l'adresse IPV6 introduite.
Post condition	Afficher les renseignements sur l'adresse IPv6 saisi.
Scenario nominal	1. Client demande la page « IPv6 ». 2. Système affiche la page. 3. Client demande le formulaire « Se renseigner sur une adresse IPv6 ». 4. Système affiche le formulaire. 5. Client saisit l'adresse IPv6 et valide. 6. Le système affiche les renseignements.
Scenario alternatif1	1. L'adresse IPV6 n'est pas valide. Système afficher le message d'avertissement. 2. Retour a scenario nominal.
Exception	Néant

Tableau 3.3. La fiche descriptive du cas d'utilisation
« *Se renseigner sur une adresse IPv6* ».

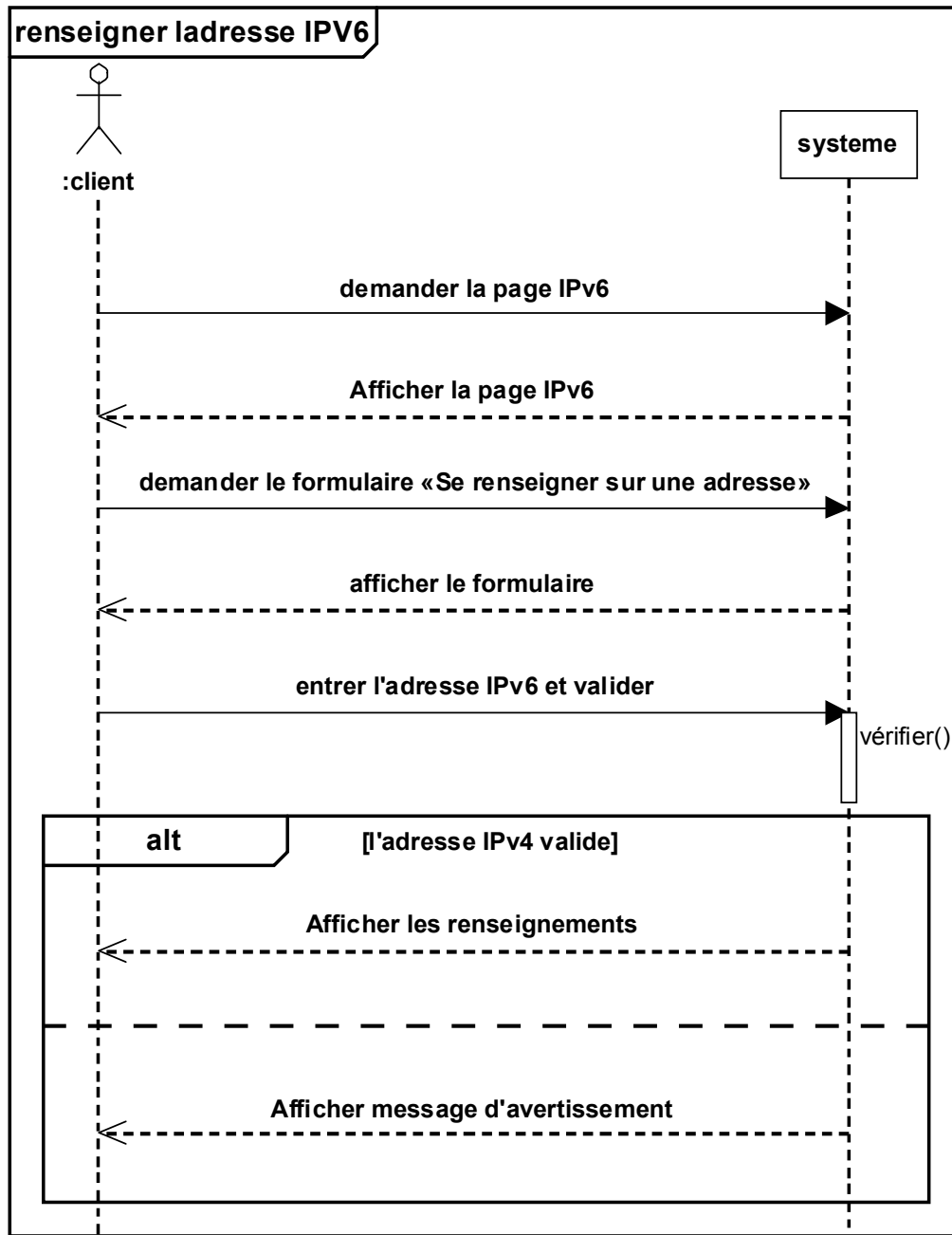


Figure 3.8. Diagramme de séquence système du cas d'utilisation

« Se renseigner sur une adresse IPv6 ».

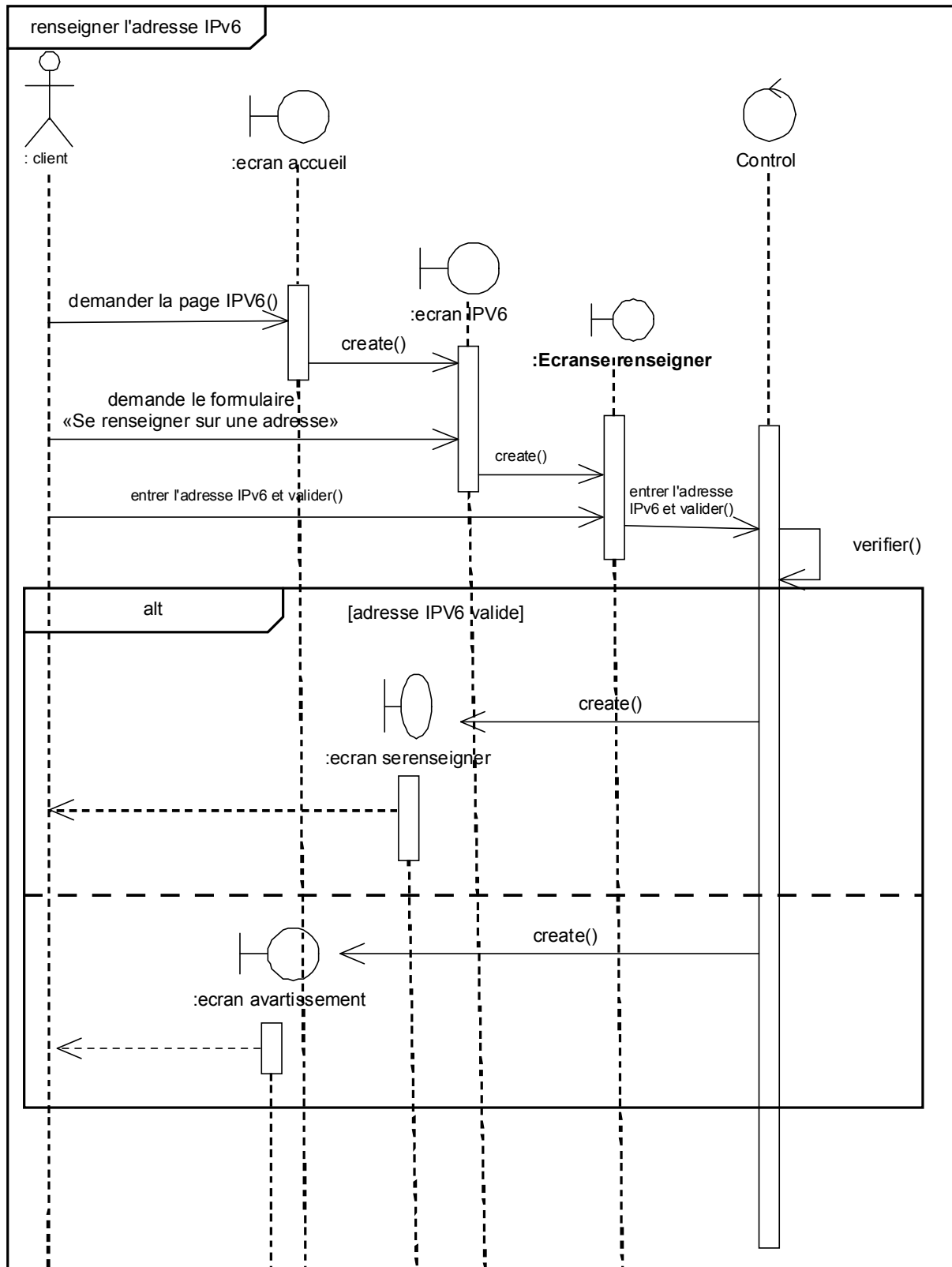


Figure 3.9. Diagramme d'interaction du cas d'utilisation

« Se renseigner sur une adresse IPv6 ».

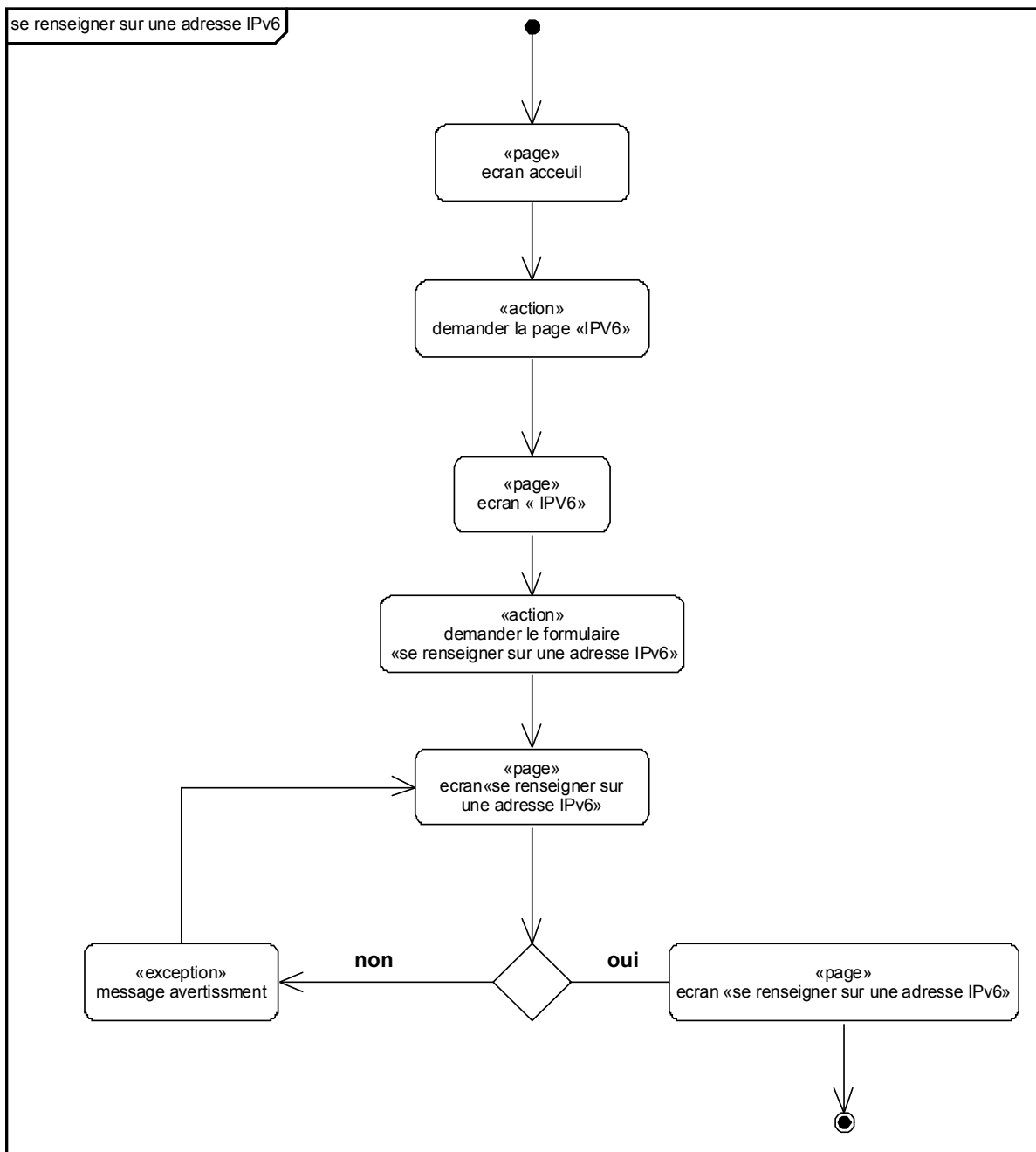


Figure 3.10. Diagramme de navigation du cas d'utilisation

« Se renseigner sur une adresse IPv6 ».

III.2.4. Cas d'utilisation « compresser / décompresser »

Cas d'utilisation	Compresser/décompresser
Acteur	Client
Objectif	Compresser (ou décompresser) un adresse IPV6 .
Pré condition	Validité de l'adresse IPV6 introduite.
Post condition	Affichage de l'adresse IPV6 compressée (ou décompresser).
Scenario nominal	1. Client demande la page « IPV6 ». 2. Système affiche la page. 3. Client demande le formulaire « compresser/décompresser ». 4. Système affiche le formulaire. 5. client saisit l'adresse IPV6 ensuite choisit une des options compression / décompression. 6. Système afficher l'adresse IPV6 compressée (ou décompressée).
Scenario alternatif1	1. Client saisit une adresse IPV6 non valide. 2. Système afficher un message d'avertissement. 3. Retour à scenario nominal
Exception	Néant

**Tableau 3. 4. La fiche descriptive du cas d'utilisation
« Compresser/décompresser».**

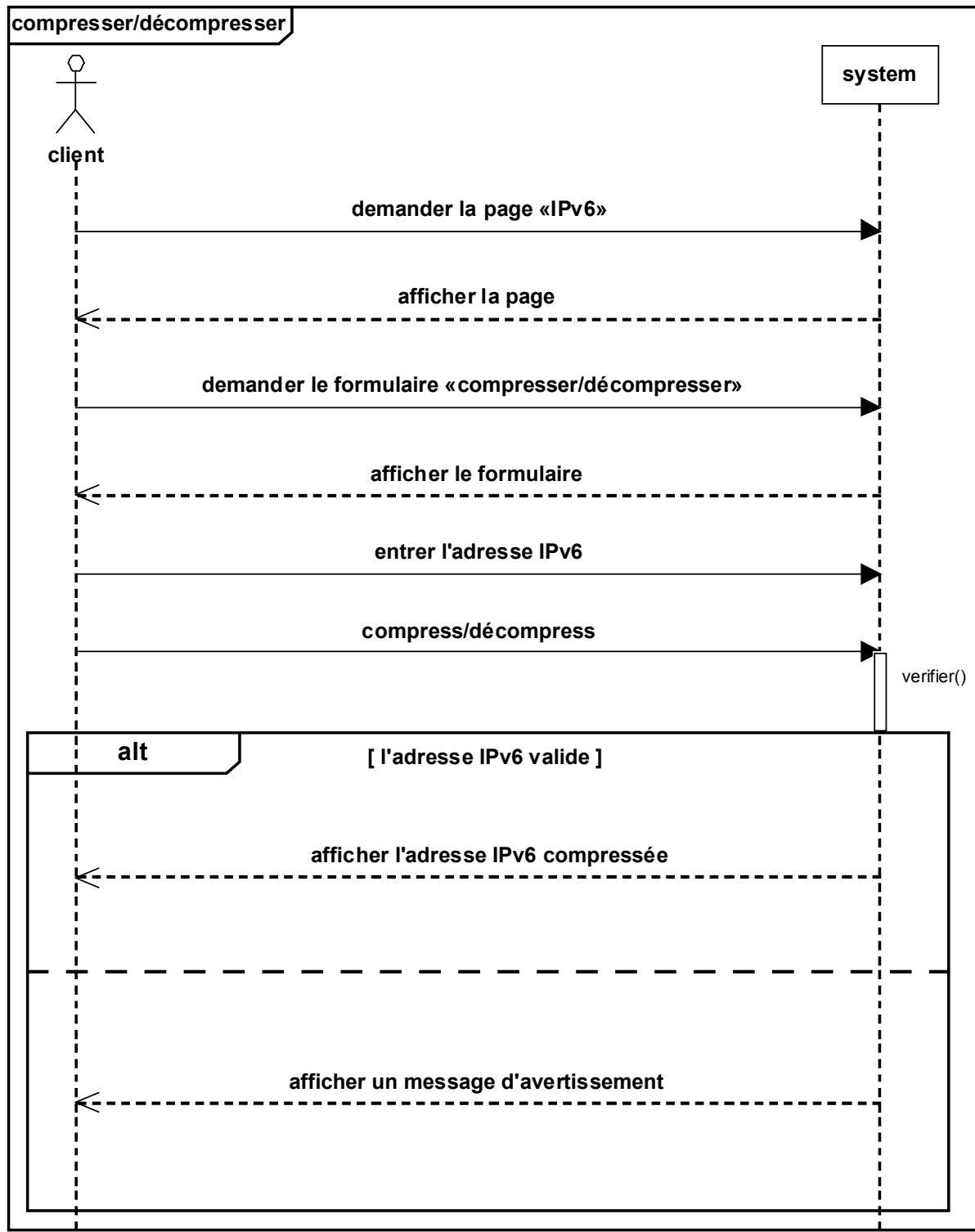


Figure 3.11. Diagramme de séquence système du cas d'utilisation « compresser/décompresser ».

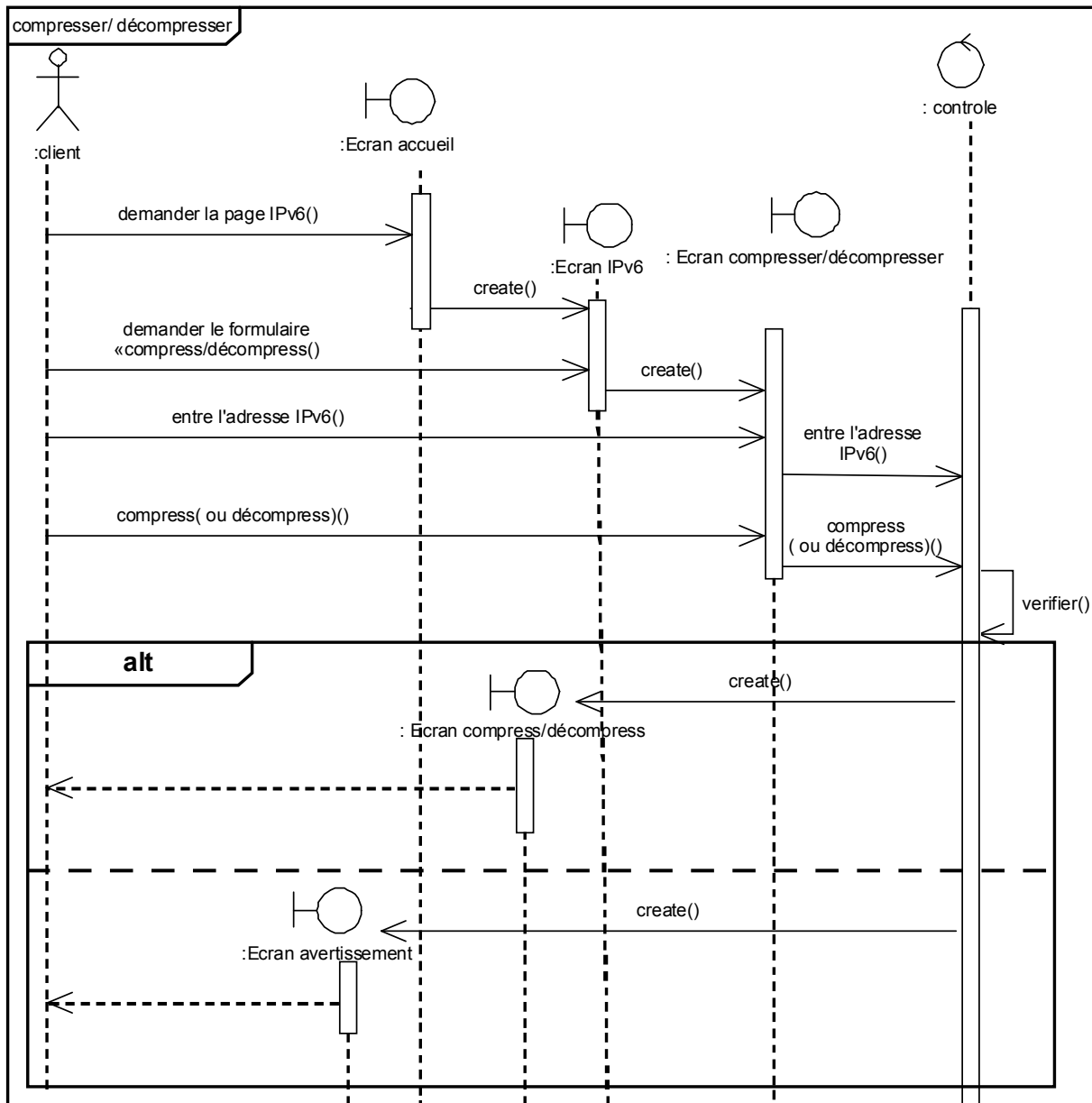


Figure 3.12. Diagramme d'interaction du cas d'utilisation
« compresser/décompresser».

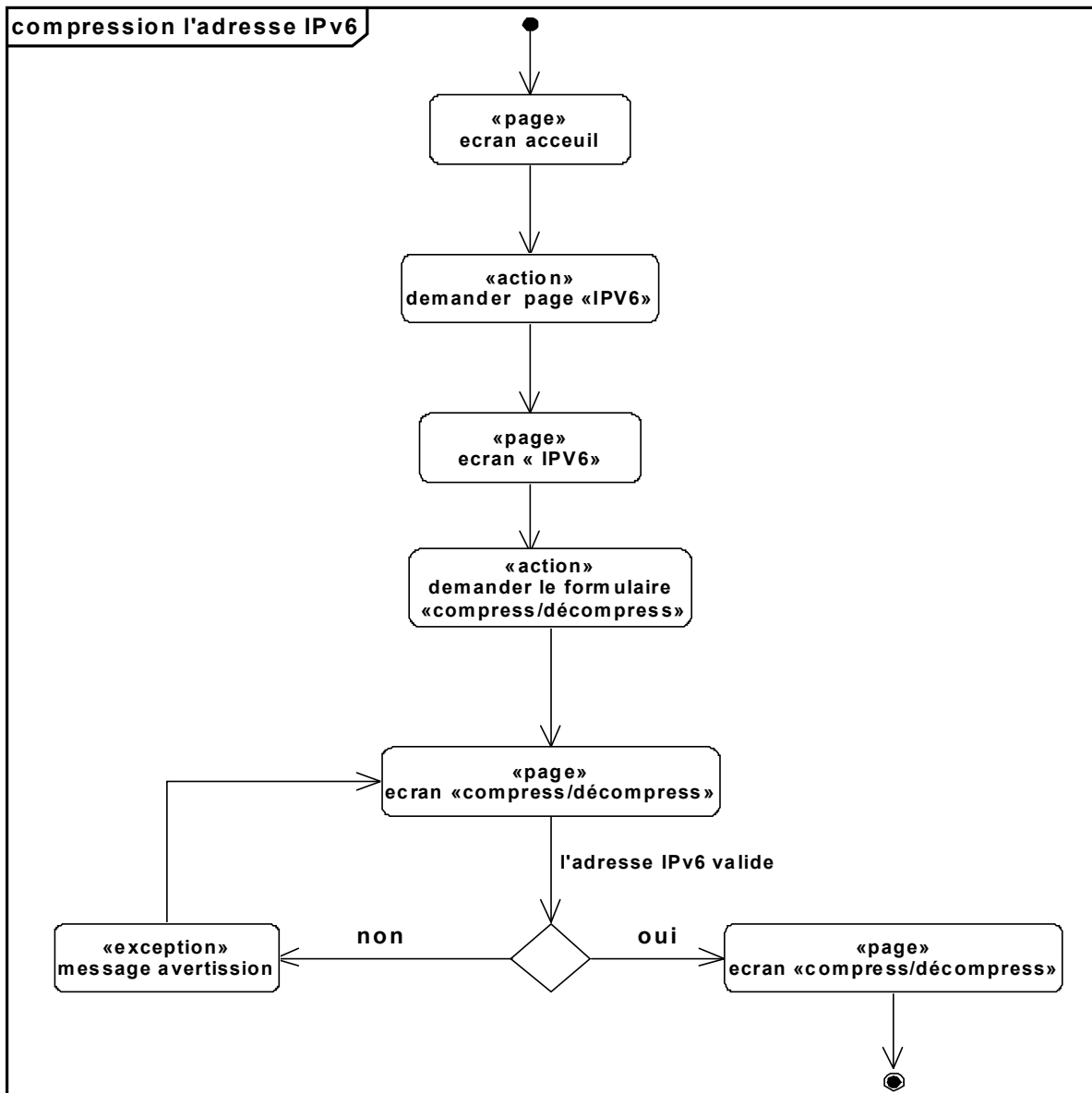


Figure 3.13. Diagramme de navigation du cas d'utilisation
« compresser/décompresser ».

III.2.5. cas d'utilisation « Assister le choix du tunnel »

Cas utilisation	Assister le choix du tunnel
Acteur	Client
Objectif	Choisir le tunnel le plus adapté aux besoins du client.
Pré condition	Remplissage du formulaire.
Post condition	Annoncer le tunnel recommandé pour la topologie.
Scenario nominal	1. Client demande la page « tunneling ». 2. Système affiche la page. 3. Client demande le formulaire « assistant choix du tunnel ». 4. Système affiche le formulaire. 5. Client choisir le besoin et valider. 6. Le système afficher les tunnels recommandée et petite définition sur cette tunnel.
Exception	Néant

Tableau 3.5. La fiche descriptive du cas d'utilisation

« Assister le choix du tunnel».

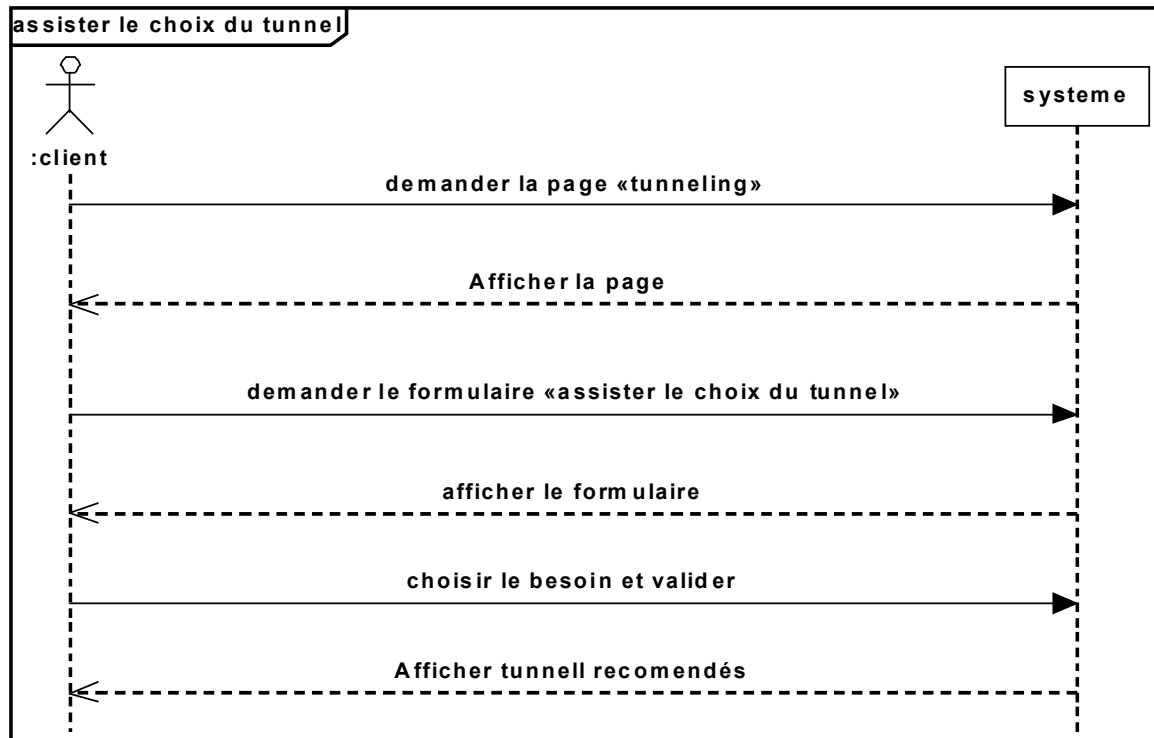


Figure 3.14. Diagramme de séquence du cas d'utilisation

« Assister le choix du tunnel ».

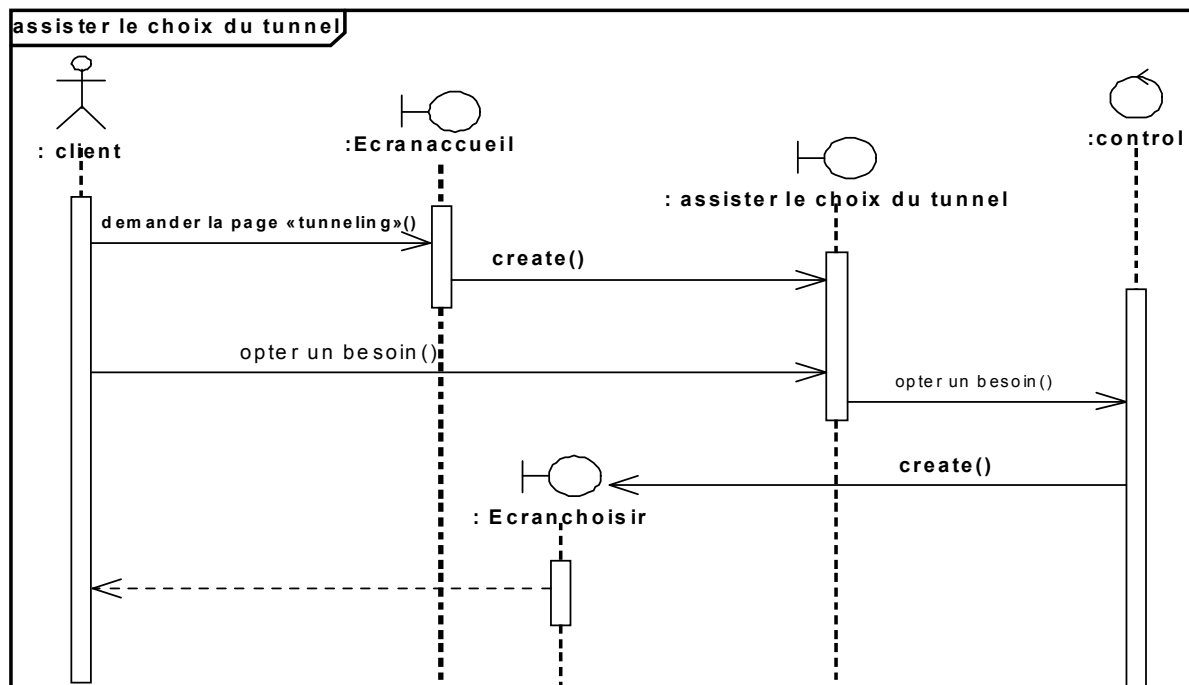


Figure 3.15. Diagramme d'interaction du cas d'utilisation

« Assister le choix du tunnel ».

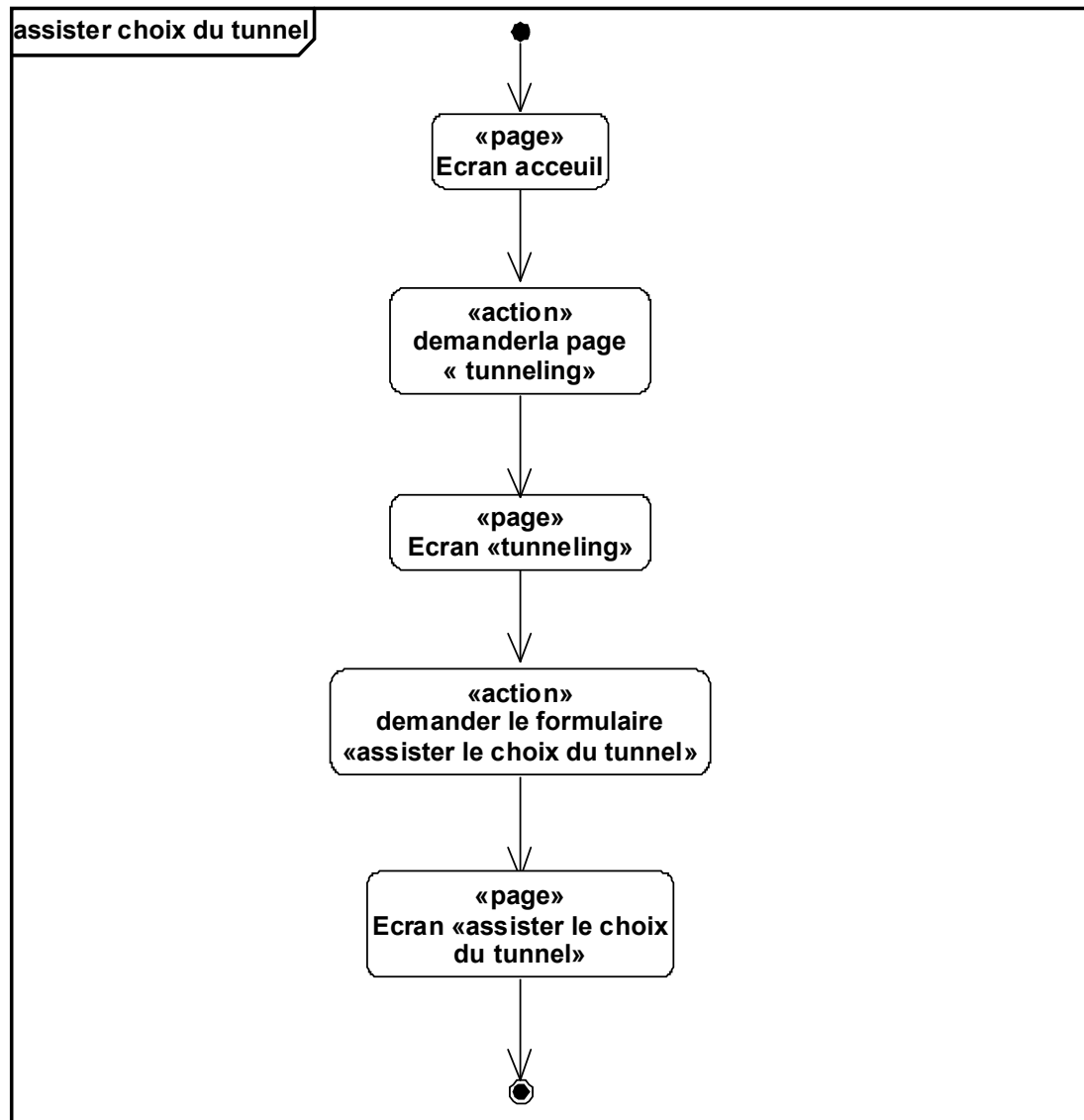


Figure 3.16. Diagramme de navigation du cas d'utilisation

« Assister le choix du tunnel ».

IV. Conclusion

Dans ce chapitre, nous avons présenté les diagrammes nécessaires à la conception de notre site WEB utilisant le langage UML qui nous a permis de bien définir tous les concepts participants à la réalisation de la dernière phase de ce projet.

CHAPITRE 04

Implémentation



Le chapitre 04 couvre les points suivants :

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

I. Introduction

La phase de conception que nous avons détaillée dans le chapitre précédent a été concrétisée par le développement de notre solution WEB.

Dans ce chapitre, nous allons présenter les langages de programmation utilisés 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. HTML (*HyperText Markup Language*)

C'est le langage universel utilisé sur les pages Web lisibles par tous les navigateurs Web (Internet Explorer, Mozilla, etc....). Ce langage fonctionne suivant l'assemblage et la combinaison des balises permettant de structurer et donner l'apparence voulue aux données textes, images et multimédias suivant la mise en page voulue.

II.2. CSS (*Cascading Style Sheets*, aussi appelées *Feuilles de style*)

Le rôle du CSS est de gérer l'apparence de la page web (agencement, positionnement, décoration, couleurs, taille du texte...). Ce langage est venu compléter le HTML en 1996 [13].

II.3. 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 propriétés [13].

II.4.Langage PHP

Plus connu sous son sigle PHP (Personal Home Page), est un langage de programmation compilé à la volée libre principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP (hyper text transfer protocole), mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale.

PHP est considéré par certains comme une plate-forme de développement en raison de l'étendue et de la richesse de sa bibliothèque [].

III. Outils de développement

III.1 Sublime Text

est un éditeur de texte générique codé en C++ et Python, disponible sur Windows, Mac et Linux. Le logiciel a été conçu tout d'abord comme une extension pour Vim, riche en fonctionnalités.

Depuis la version 2.0, sortie le 26 juin 2012, l'éditeur prend en charge 44 langages de programmation majeurs, tandis que des plugins sont souvent disponibles pour les langages plus rares [13].

• Fonctionnalités

Sublime Text intègre la plupart des fonctionnalités de base d'un éditeur de texte, dont la coloration syntaxique personnalisable, l'auto complétion, un système de plugins... L'éditeur propose cependant des fonctions plus avancées, dont:

- Minimap : prévisualisation de tout le fichier dans une barre latérale
- Sélection et édition dans plusieurs sections de code en parallèle
- Marque-page au sein même des fichiers
- Sauvegarder automatique
- Recherche et remplacement par expressions régulières
- Support des macros et de plugins en Python
- Personnalisation des raccourcis clavier [13].

III. 2. WampServer

Est une plate-forme de développement Web sous Windows pour des applications Web dynamiques à l'aide du serveur Apache2, du langage de scripts PHP. Il possède également PHPMyAdmin pour gérer plus facilement les bases de données [13].

IV. Conclusion

La phase d'implémentation nous a permis de découvrir la puissance du WEB qui représente actuellement un backbone pour la technologie de l'information.

Les tests effectués au cours de la dernière étape, confirment que la solution proposée répond aux besoins des acteurs, avec la possibilité d'enrichir l'ensemble des services offerts par notre site WEB avec des fonctionnalités avancées, toujours dans le but d'offrir un excellent support pour le domaine professionnel ainsi que le domaine d'enseignement supérieur.

Conclusion Générale

La recherche effectuée durant ce travail nous a montrée que le domaine des réseaux informatiques, est un grand labyrinthe qui ne cesse de s'accroître et de se développer à une vitesse impressionnante, au point où certains protocoles n'ont pu voir le jour. Cette évolution exige à tout administrateur réseau d'être à jour dans le but d'exploiter les avantages des nouvelles technologies.

Dans ce mémoire, nous avons essayé de couvrir toutes les techniques utilisées dans le système d'adressage du protocole IP avec ses deux versions. La complexité ainsi que les problèmes liés à la planification des réseaux informatiques ont fait l'objet de notre projet, à savoir un site web offrant un ensemble de services gratuits, destiné aux étudiants universitaires ou bien aux administrateurs réseau ayant peu d'expérience, dans le but de les assister au cours de leurs études, formations ou projets, simplifiant des tâches complexes avec moins d'erreurs et plus de fiabilité.

Nous projetons dans le futur à développer une solution plus intelligente, permettant de proposer une planification complète (adressage IP et protocoles de routage) pour une topologie réseau WAN, à partir des besoins de client exprimés par des simples clics de bouton.

Références Bibliographiques

<i>Code</i>	<i>Référence</i>
[1]	Réseaux & télécoms 3 ^{eme} edition 2008
[2]	TCP/IP Illustrated: the protocols”, by W. Richard Stevens
[3]	Transmission de paquet
[4]	www.cisco.com
[5]	www.oracle.com
[6]	www.g6.asso.fr
[7]	www.univ-ubs.fr
[8]	www.ietf.org
[9]	www.ipv6tf.org
[10]	www.inetdoc.net

[11]	www.u-bourgogne.fr/o.togni
[12]	www.ipv6.org
[13]	www.Wikipedia.com
[14]	TCP/IP Illustrated: the protocols”, by W. Richard Stevens

ANNEXE

Simulation de notre solution WEB

- La Page d'accueil

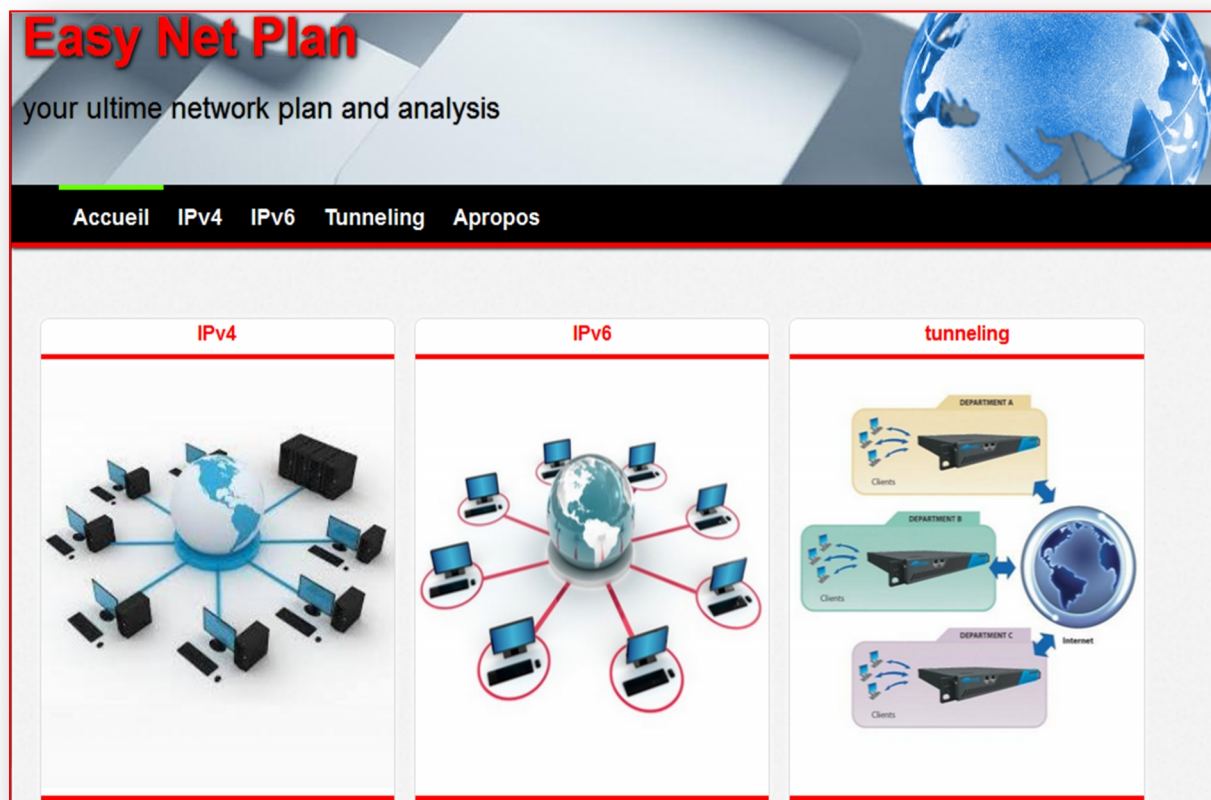


Figure A.1 : page d'accueil.

- La page : services IPv4



Figure A.2 : Page services IPv4.

- La page : se renseigner sur une adresse IPv4
- Cas N°1 : adresse IPv4 valide

Easy Net Plan
your ultime network plan and analysis

Accueil IPv4 IPv6 Tunneling A propos

Se renseigner sur une adresse IPv4

Entrez votre adresse IP:

Adresse IP:	10.20.30.10
Classe:	A
Type d' adresse:	Adresses privées
Adresse réseau:	10.0.0.0
Le masque réseau:	255.0.0.0
Adresse du broadcast:	10.255.255.255

Figure A.3 : Page adresse IPv6 valide.

- **Cas N°2 : adresse IPv4 non valide**

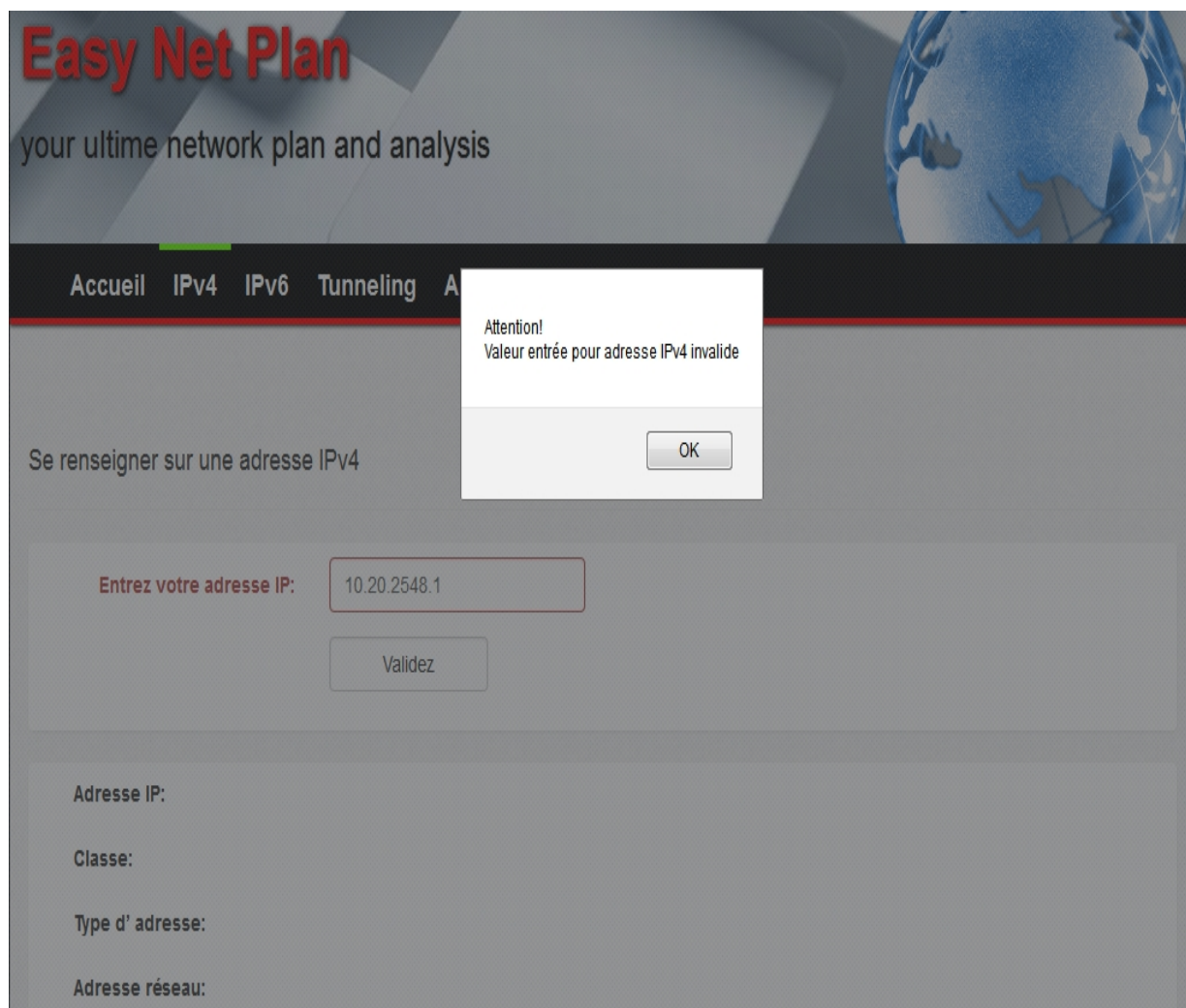


Figure A.4 : adresse IPv4 non valide.

- Page segmentation des réseaux IPv4

Saisir l'adresse IPv4 et conforme un champs adresse IPv4.

adresses S/Réseau	Premier Hôte	Dernier Hôte	Adresse de diffusion
192.168.50.0	192.168.50.1	192.168.50.62	192.168.50.63
192.168.50.64	192.168.50.65	192.168.50.126	192.168.50.127
192.168.50.128	192.168.50.129	192.168.50.190	192.168.50.191
192.168.50.192	192.168.50.193	192.168.50.254	192.168.50.255

Figure A.5 : page segmentation de réseaux IPv4.

- Page de documentation

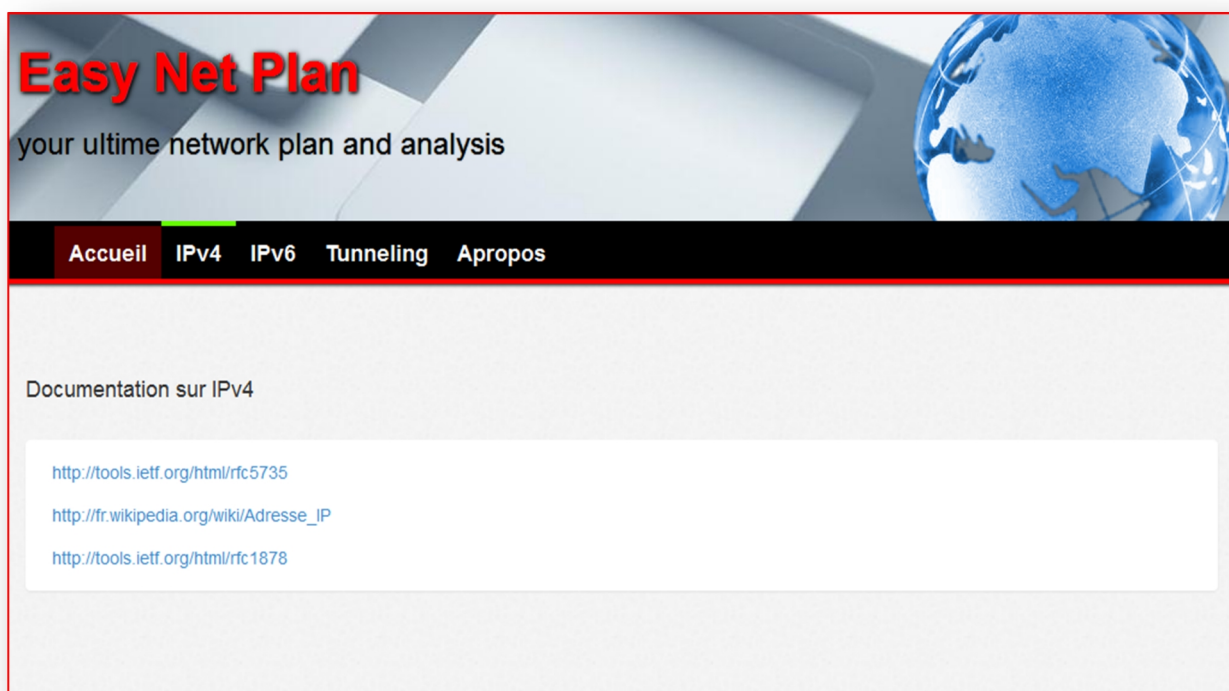


Figure A.6 : page de documentation.

- Page IPv6

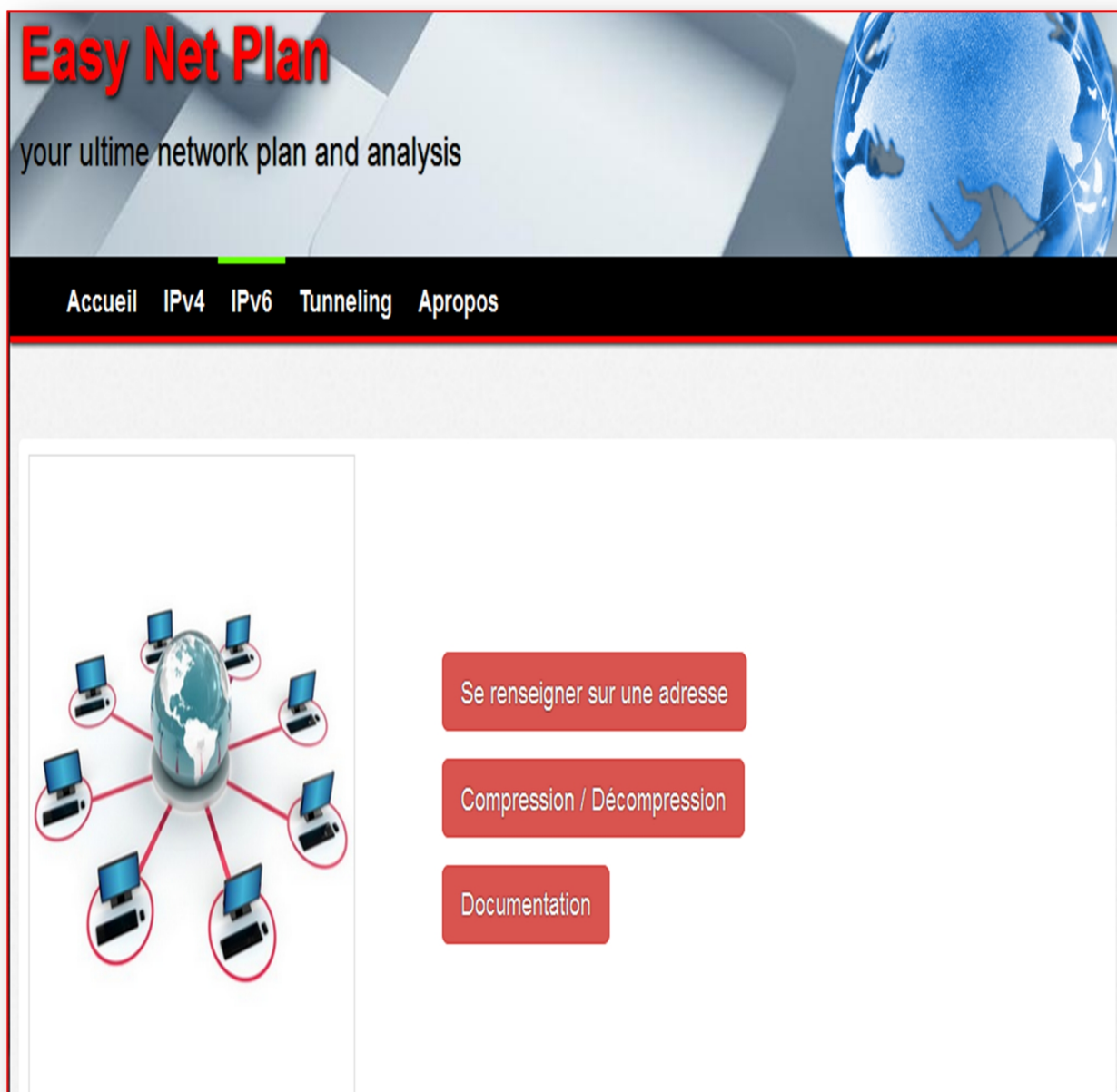
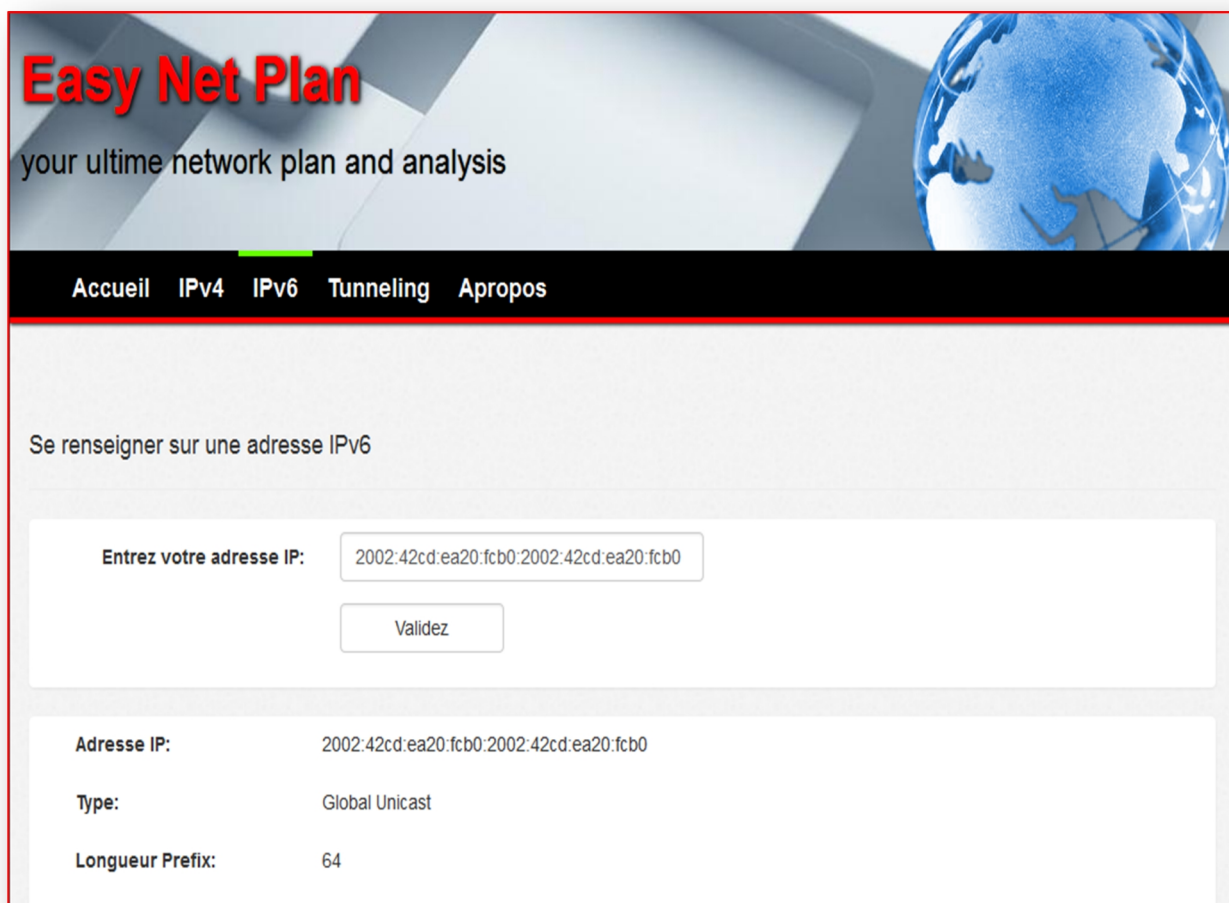


Figure A.1 : Page services IPv6.

- Page se renseigner sur adresse une IPv6
- Cas N°1 : l'adresse IPv6 valide



The screenshot shows the 'Easy Net Plan' website interface. The header includes the logo 'Easy Net Plan' and the tagline 'your ultime network plan and analysis'. A navigation bar contains links for 'Accueil', 'IPv4', 'IPv6', 'Tunneling', and 'Apropos'. The main content area is titled 'Se renseigner sur une adresse IPv6'. It features a form with the label 'Entrez votre adresse IP:' and a text input field containing the address '2002:42cd:ea20:fc0:2002:42cd:ea20:fc0'. Below the input field is a 'Validez' button. At the bottom, a table displays the validation results.

Adresse IP:	2002:42cd:ea20:fc0:2002:42cd:ea20:fc0
Type:	Global Unicast
Longueur Prefix:	64

Figure A.2 : page se renseigner sur une adresse IPv6.

- **Cas N°1 : l'adresse IPv6 non valide**

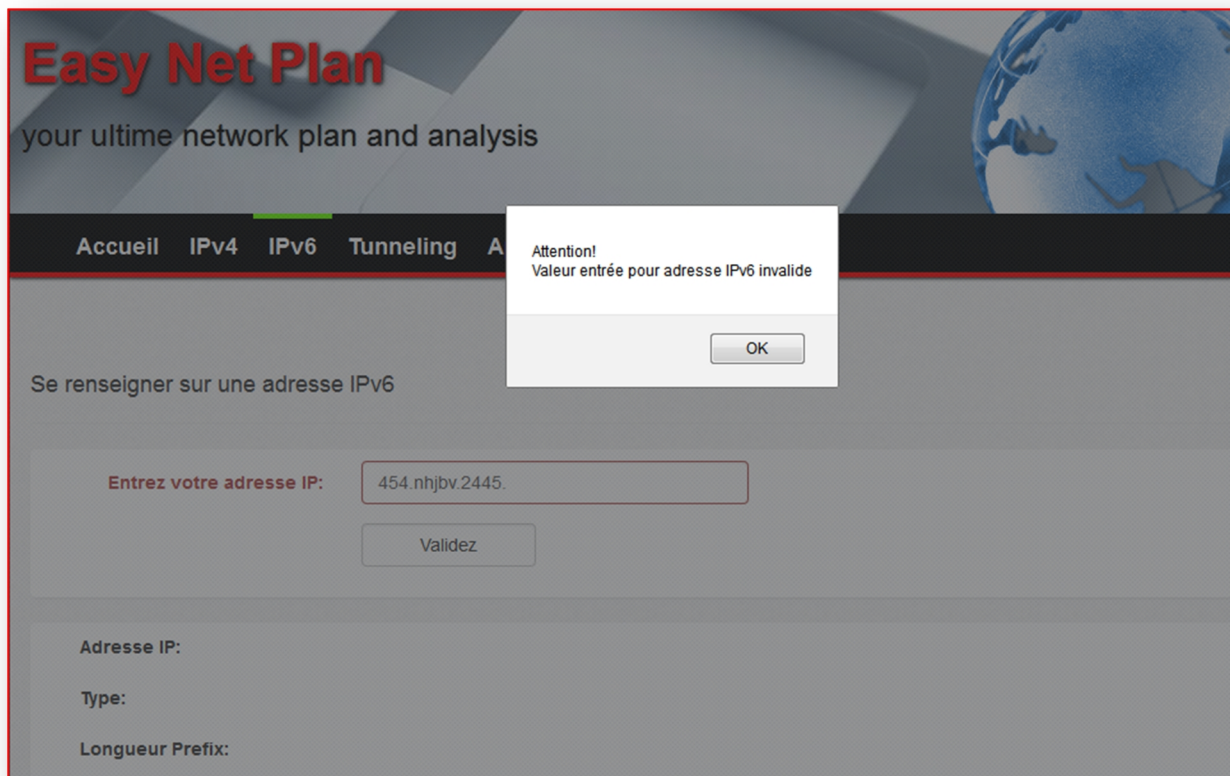
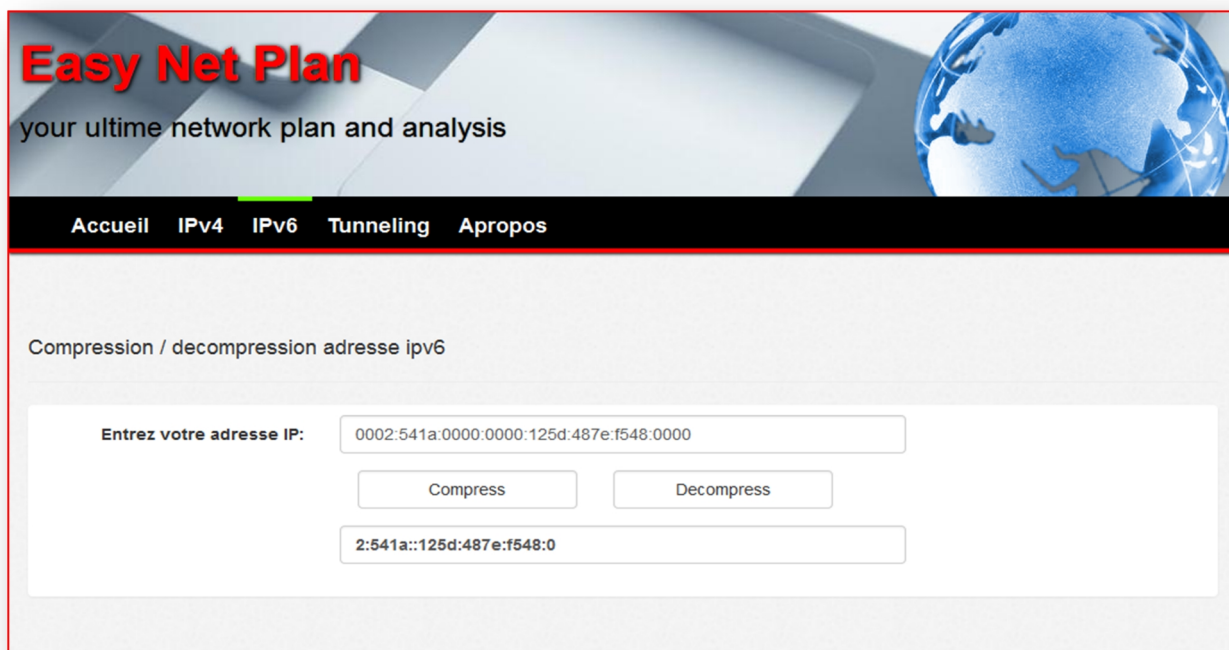


Figure A.3 : page avertissement adresse IPv6.

- Page compression/décompression



Easy Net Plan
your ultime network plan and analysis

Accueil IPv4 **IPv6** Tunneling A propos

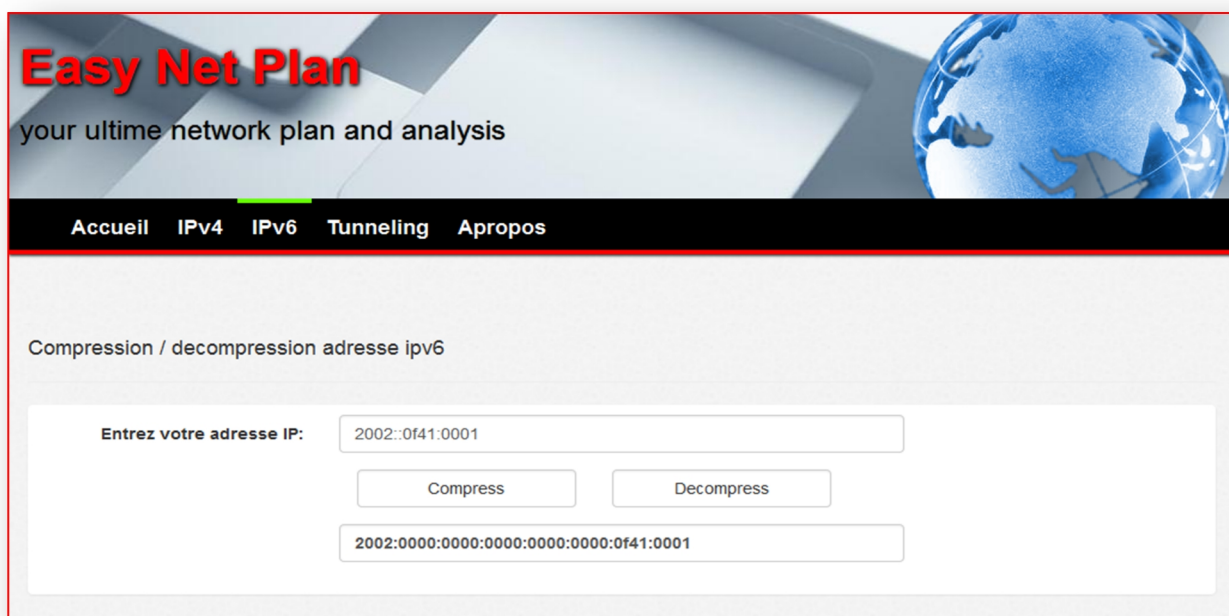
Compression / décompression adresse ipv6

Entrez votre adresse IP: 0002:541a:0000:0000:125d:487e:f548:0000

Compress Decompress

2:541a::125d:487e:f548:0

Figure A.4 : résultat de compression d'une adresse IPv6.



Easy Net Plan
your ultime network plan and analysis

Accueil IPv4 **IPv6** Tunneling A propos

Compression / décompression adresse ipv6

Entrez votre adresse IP: 2002::0f41:0001

Compress Decompress

2002:0000:0000:0000:0000:0000:0f41:0001

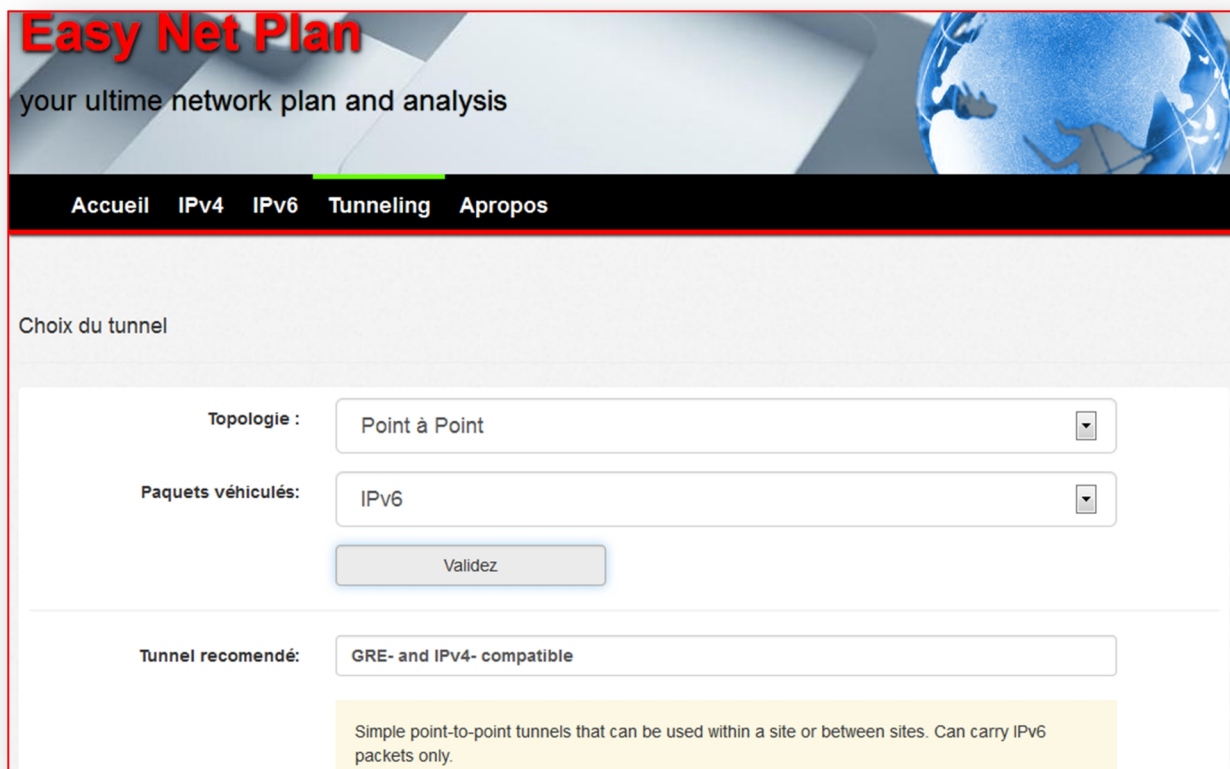
Figure A.5 : résultat de décompression d'une adresse IPv6.

- Page tunneling



Figure A.6 :page tunneling.

- Page assistant le choix du tunnel



Easy Net Plan
your ultime network plan and analysis

Accueil IPv4 IPv6 Tunneling A propos

Choix du tunnel

Topologie : Point à Point

Paquets véhiculés: IPv6

Validez

Tunnel recomandé: GRE- and IPv4- compatible

Simple point-to-point tunnels that can be used within a site or between sites. Can carry IPv6 packets only.

Figure A.7 : page choix du tunnel.

- Page tableau comparatif des tunnels



Easy Net Plan
your ultime network plan and analysis

Accueil IPv4 IPv6 Tunneling A propos

Tableau comparatif des tunnels

Tunnel	Topologie et adressage	Application
Automatic 6to4	☐ Point à Multi-Points ☐ Utilise la plage 2002::/16	Connexion des réseaux IPv6 isolés.
IPv6 over IPv4 GRE	☐ Point à Point ☐ Adressage Unicast ☐ Nécessite la double pile (IPv4-IPv6)	Véhicule les paquets IPv6 , CLNS et d'autre trafic.
ISATAP	☐ Point à Multi-Points ☐ Utilise l'adressage suivant : [Préfixe Unicast :0000:5EFE:@IPv4]	Destiné à la connexion des hôtes IPv6 situés dans le même site.
Automatic IPv4-compatible	☐ Point à Multi-Points ☐ Adressage : (::/96) ☐ Nécessite la double pile (IPv4-IPv6)	Il n'est pas largement utilisé . Il est recommandé d'utiliser ISATAP à sa place.
Configuration manuelle	☐ Point à Point ☐ N'importe quelle plage d'adressage ☐ Nécessite la double pile (IPv4-IPv6)	Véhicule les paquets IPv6 à travers les réseaux IPv4.

Figure A.8: page tableau comparatif du tunnel.

- Page documentation du tunnel

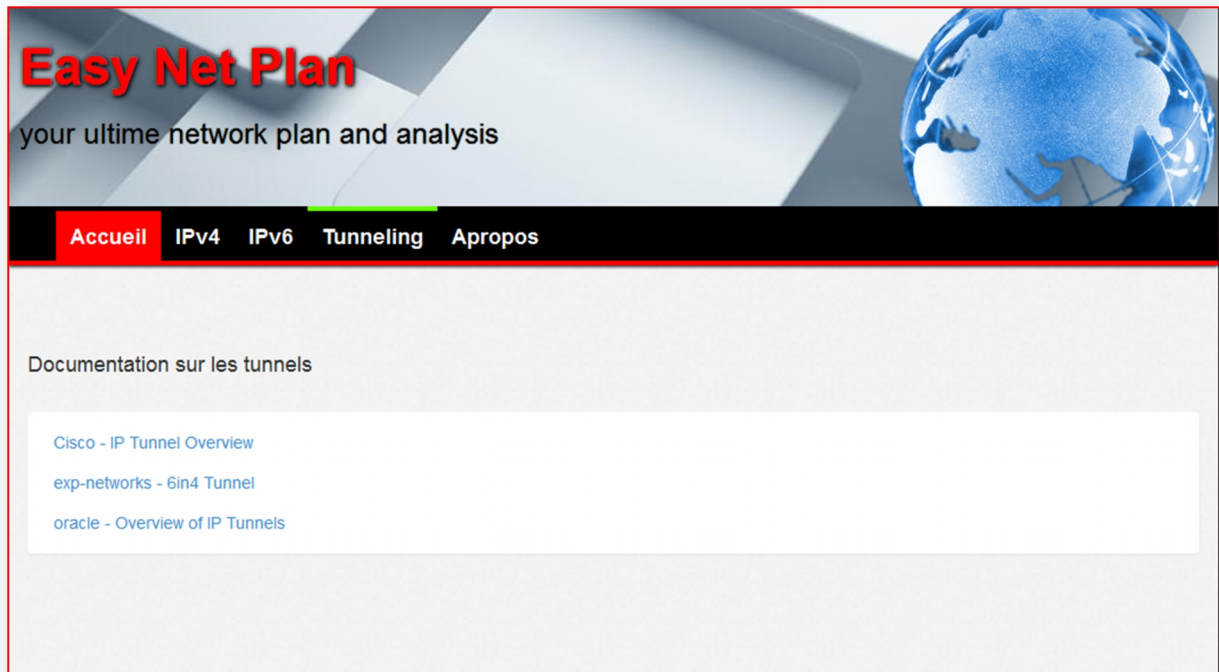


Figure A.9 : page documentation du tunnels.

- Page A propos



Figure A.10 : page A-propos.