(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
1 juillet 2010 (01.07.2010)

PCT

(10) Numéro de publication internationale
WO 2010/072953 A1

(51) Classification internationale des brevets : *H04L 12/46* (2006.01)

(21) Numéro de la demande internationale : PCT/FR2009/052609

(22) Date de dépôt international : 18 décembre 2009 (18.12.2009)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0859002 23 décembre 2008 (23.12.2008) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6 place d'Alleray, F-75015 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **BURGEY, Eric** [FR/FR]; 47, rue des Acacias, F-75017 Paris (FR).

(74) Mandataire : **FRANCE TELECOM R&D/PIV/BREVETS**; LEDEY Michel, 38-40 rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

[Suite sur la page suivante]

(54) **Title** : SYSTEM FOR CONVEYING AN IPV4 DATA PACKET

(54) **Titre** : SYSTEME D'ACHEMINEMENT D'UN PAQUET DE DONNEES IPv4

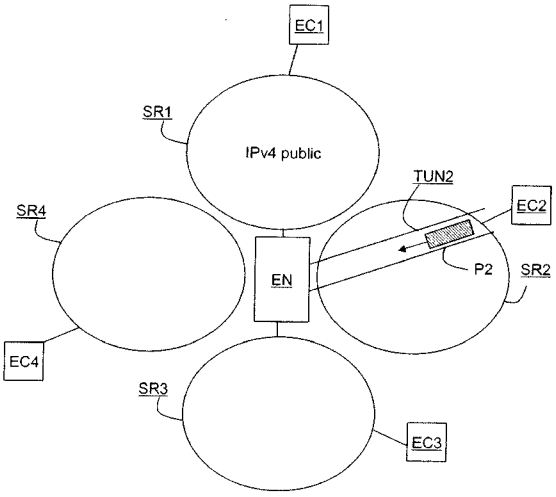

FIG.1

(57) **Abstract** : The invention relates to a system for conveying an IPv4 data packet, transmitted in the IPv4 telecommunication network of an operator, to a client device having a public IP address shared with other client devices connected to said IPv4 network. According to the invention: said IPv4 network is divided into a plurality of subnetworks; the plurality of client devices sharing said IPv4 address is linked to said plurality of subnetworks so as to connect at most one of said client devices per subnetwork; and the system is capable of sending the IPv4 data packet via a point-to-point link established between the transmitter client device and identification means of the subnetwork for linking the client device to receive the packet, said means being capable of identifying said subnetwork from the destination IPv4 address and an identifier of the IPv4 context of said communication contained in the data packet received from the source client device, and of conveying said IPv4 packet towards the identified subnetwork.

(57) **Abrégé** : L'invention concerne un système d'acheminement

[Suite sur la page suivante]

WO 2010/072953 A1

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

d'un paquet de données IPv4 émis dans un réseau de télécommunications IPv4 d'un opérateur, à destination d'un équipement client possédant une adresse publique IP partagée avec d'autres équipements clients connectés audit réseau IPv4. Selon l'invention : ledit réseau IPv4 est décomposé en une pluralité de sous-réseaux; la pluralité d'équipements clients partageant ladite adresse IPv4 est rattaché à ladite pluralité de sous-réseaux, de façon à connecter au plus un desdits équipements clients par sous-réseau; et ledit système est apte à envoyer le paquet de données IPv4 par une liaison point à point établie entre l'équipement client émetteur à des moyens d'identification du sous- réseau de rattachement de l'équipement client destinataire du paquet, lesdits moyens étant aptes à identifier ledit sous-réseau à partir de l'adresse IPv4 de destination et d'un identifiant de contexte IPv4 de ladite communication contenu dans le paquet de données reçu de l'équipement client source et à acheminer ledit paquet IPv4 vers le sous-réseau identifié.

Système d'acheminement d'un paquet de données IPv4

Domaine de l'invention

Le domaine de l'invention est celui d'un réseau de télécommunications, en particulier un réseau de télécommunications IP dans lequel sont transportés des paquets de données d'un équipement source vers un équipement de destination identifié par une adresse de destination.

Un tel réseau de télécommunications groupe une pluralité d'équipements, de liens et de fonctions dédiés au transport des données issues d'équipements terminaux connectés à ce réseau. En particulier, les fonctions de transport peuvent être implémentées grâce à l'activation de protocoles de routage et de transmission. Un réseau de télécommunications administré par un opérateur est encore appelé un domaine.

Un fournisseur de service de connectivité IP déploie une architecture dédiée pour permettre aux utilisateurs d'équipements terminaux d'être joignables. L'accès au service de connectivité IP est géré par le fournisseur de service qui s'appuie sur le réseau de télécommunications d'un opérateur pour router les paquets de données émis par les équipements terminaux vers leur destination finale. Dans certains cas, ledit fournisseur de service est aussi l'opérateur de réseau de télécommunications.

Un type adressage, public ou privé, communément utilisé dans un tel réseau IP est l'adressage défini par le protocole IPv4 (Internet Protocol version 4).

Or il est communément admis par la communauté des fournisseurs de service IP que l'épuisement des adresses IPv4 publiques est une fatalité. Pour éviter ce problème, la communauté s'est mobilisée dans le passé, ce qui a conduit à la définition d'un nouveau protocole IPv6 (*Internet Protocol version 6*), qui offre un grand nombre d'adresses IP et un mécanisme de routage hiérarchique aux performances améliorées. Néanmoins, cette solution n'est en pratique pas activée par les opérateurs, pour des raisons financières ou stratégiques. Ces mêmes fournisseurs ne sont toutefois pas indifférents aux alarmes récemment émis par l'IETF (*Internet Engineering Task Force*), notamment dans des rapports présentés au sein du groupe de travail GROW (*Global*

Routing Operations Working Group) concernant un risque d'épuisement des adresses IPv4 de l'IANA fin 2009.

Le document intitulé "Provider-Provisioned CPE: IPv4 Connectivity Access in the context of IPv4 address exhaustion" et disponible sur le site http://www.ietf.org/internet-drafts/draft-boucadair-port-range-00.txt enseigne une solution pour retarder l'épuisement d'adresses IPv4. Une telle solution consiste à partager une adresse IPv4 publique entre une pluralité d'équipements clients, les équipements clients étant différenciés entre eux lors du routage des paquets de données ayant pour adresse de destination l'adresse IPv4 partagée, par un numéro de port compris dans une plage de numéro de ports contrainte et réservée à chacun des équipements destinataires. Le paquet de données est d'abord routé vers un équipement nœud du réseau apte à traiter ce type de paquets de données. Cet équipement nœud dispose d'une table de correspondance associant au couple formé par l'adresse partagée et la plage de numéros de ports réservée, un identifiant unique de l'équipement destinataire. Cet identifiant unique, par exemple une adresse IP privée, est ajouté au paquet de données et permet le routage du paquet de données jusqu'à l'équipement client destinataire.

Un premier inconvénient de cette solution est qu'elle impose la mémorisation de la correspondance entre l'adresse partagée et l'identifiant d'équipement destinataire dans l'équipement nœud, ce qui crée un passage obligé par cet équipement nœud.

Un deuxième inconvénient est que cette solution nécessite l'ajout de cet identifiant unique au paquet de données et donc sa modification par l'équipement nœud.

Par ailleurs, l'équipement nœud apte à traiter ce type de paquet de données est généralement l'équipement dédié au traitement de tous les paquets destinés à une adresse partagée. Autrement dit, les équipements clients partageant la même adresse sont regroupés géographiquement. Un tel équipement nœud est donc situé au niveau d'un réseau d'accès au réseau de télécommunications. Un troisième inconvénient d'une telle solution est qu'elle impose la mise en œuvre d'un grand nombre

d'équipements nœuds de ce type dans le réseau de télécommunications, ce qui représente un coût important pour un opérateur.

Un quatrième inconvénient de cette solution est qu'elle ne permet pas le routage d'un paquet de données ne comprenant pas de numéro de port de destination.

Il existe donc un besoin de pallier ces inconvénients de l'art antérieur.

Plus précisément, il existe un besoin de fournir une nouvelle solution pour économiser l'usage d'adresses IPv4 publiques, qui limite les impacts sur l'architecture du réseau de télécommunications, en particulier des réseaux d'accès IPv4 existants à ce réseau.

Exposé de l'invention

L'invention répond à ce besoin à l'aide d'un système d'acheminement d'un paquet de données IPv4 émis par un équipement client source à destination d'un équipement client destinataire au cours d'une communication établie dans un réseau de télécommunications d'un opérateur, ledit équipement client destinataire possédant une adresse publique IP partagée avec d'autres équipements clients connectés audit réseau IPv4, caractérisé en ce que :

- ledit réseau IPv4 est décomposé en une pluralité de sous-réseaux;
- la pluralité d'équipements clients partageant ladite adresse IPv4 est rattaché à ladite pluralité de sous-réseaux, de façon à connecter au plus un desdits équipements clients par sous-réseau; et
- ledit système comprend :

- des moyens d'envoi de données IPv4, par une liaison point à point établie entre l'équipement client émetteur et des moyens d'identification du sous-réseau de rattachement de l'équipement destinataire;

- des moyens d'identification du sous-réseau de rattachement de l'équipement client destinataire du paquet, à partir de l'adresse IPv4 de destination et d'un identifiant de contexte IPv4 de ladite communication contenu dans le paquet de données reçu de l'équipement client source; et

des moyens d'acheminement dudit paquet IPv4 vers le sous-réseau identifié.

Selon l'invention, les équipements clients partageant la même adresse IP ne sont plus nécessairement localisés dans la même zone géographique, ni gérés par un même équipement nœud du réseau. Ils peuvent au contraire être disséminés dans le réseau de façon à être tous rattachés à des sous-réseaux différents.

Ainsi, l'acheminement du paquet de données, jusqu'au sous-réseau auquel est rattaché l'équipement client destinataire, se fait à l'aide d'un contexte qui est identifié par un identifiant de contexte.

Le contexte est lié à une adresse IPv4 partagée et permet d'identifier le sous réseau auquel est rattaché l'équipement destinataire.

Une fois le sous réseau atteint, le paquet de données peut être routé normalement, sans ajout d'adresse IP, puisque son adresse de destination est unique dans ce sous-réseau.

L'invention permet ainsi de résoudre le problème technique de la pénurie d'adresses IPv4, sans modifier les équipements de routage des réseaux d'accès au réseau de télécommunications, ni les équipements clients connectés à ces réseaux d'accès.

Un avantage est de préparer une migration du réseau vers le protocole IPv6 sans imposer que les équipements clients ni le réseau d'accès déjà en place n'aient à supporter ce protocole.

Selon un aspect de l'invention, lorsque le paquet de données IPv4 comprend une adresse de destination IPv4 partagée et un numéro de port appartenant à une plage de numéros de ports, ladite plage de numéros de ports étant affectée de façon unique au sous-réseau de l'équipement destinataire, ledit identifiant de contexte est ledit numéro de port.

Le sous-réseau de l'équipement destinataire est donc simplement identifié en déterminant la plage de numéros de ports à laquelle appartient le numéro de port de destination du paquet de données.

Selon un aspect de l'invention, le paquet de données comprenant une

deuxième adresse IPv4, l'identifiant de contexte est ladite deuxième adresse IPv4 du paquet de données. Un tel identifiant de contexte est avantageusement utilisé, lorsque le paquet de données ne comprend pas de numéro de ports. Il n'est toutefois pas suffisant pour identifier directement le sous-réseau de l'équipement destinataire et doit donc être complété par au moins une donnée de contexte qui identifie le sous-réseau et est mémorisée dans le système d'acheminement.

Selon encore un autre aspect de l'invention, le paquet de données appartenant à un datagramme et comprenant un identifiant dudit datagramme, ledit identifiant de contexte est ledit identifiant de datagramme.

Un datagramme est une séquence de données qui ne peut pas toujours être transportée dans un seul paquet. Dans ce cas, le datagramme est fragmenté sur plusieurs paquets, qui comprennent chacun l'identifiant de datagramme. Seul le premier paquet comprend un numéro de port. Un avantage de l'identifiant de datagramme est qu'il peut constituer un identifiant de contexte utilisé pour mémoriser le numéro de port lors de la réception du paquet portant le même identifiant de datagramme et le numéro de port.

Selon un premier mode de réalisation de l'invention, ledit système d'acheminement comprend un équipement nœud comprenant une interface avec chacun desdits sous-réseaux.

Un unique équipement nœud du système de routage selon l'invention est dédié au routage des paquets de données destinés à une adresse IPv4 partagée. Il comprend au moins une interface logique avec chacun des sous-réseaux constituant le réseau IPv4. C'est donc au sein de cet équipement nœud que l'identification du sous-réseau de l'équipement destinataire est réalisée. Une telle identification permet à l'équipement nœud d'aiguiller le paquet de données vers la bonne interface logique. De façon connue, une telle interface peut être basée sur une technologie de type Ethernet, ATM (Asynchronous Transport Mode, en anglais), VPN (Virtual Path Network, en anglais) ou toute autre technologie d'interface réseau.

Selon un deuxième mode de réalisation de l'invention, ledit système comprend une pluralité d'équipements nœuds aptes à communiquer entre eux par l'intermédiaire

d'un réseau de télécommunications IPv6 et tels que pour chaque sous-réseau de ladite pluralité de sous-réseaux il existe au moins un équipement nœud comprenant une interface avec ce sous-réseau.

Une fois le sous-réseau identifié, le paquet de données est routé jusqu'à un équipement nœud comprenant une interface avec ce sous-réseau. Un avantage est que l'acheminement des paquets de données destinés à une adresse partagée ne repose pas sur un seul équipement nœud.

Selon un aspect de l'invention, le système d'acheminement comprend un premier équipement nœud, apte à mettre en œuvre, sur réception d'un paquet de données en provenance du sous-réseau avec lequel il est interfacé :

des moyens de détermination d'un type de contexte de l'adresse de destination IPv4 partagée;

des moyens de conversion du paquet de données IPv4 reçu de l'équipement client émetteur en un paquet de données IPv6, ledit paquet comprenant une adresse IPv6 de destination construite à partir de l'adresse IPv4 partagée source, de l'adresse IPv4 de destination et de l'identifiant de contexte et d'un préfixe, ledit préfixe étant choisi en fonction du type de contexte déterminé; et

Des moyens d'envoi du paquet de données IPv6 obtenu dans le réseau IPv6.

On comprend que le premier équipement nœud convertit le paquet de données IPv4 en un paquet de données IPv6 qui peut comprendre l'identifiant du sous-réseau de rattachement de l'équipement émetteur dans son adresse source IPv6 et dont le préfixe de l'adresse destination IPv6 est inclus dans un des préfixes routés sur le réseau IPv6 vers le prochain équipement du système d'acheminement qui devra traiter ce paquet. Cette adresse de destination IPv6 construite est routable dans le réseau IPv6. Ainsi, ce paquet est routé de façon classique par des routeurs standards du réseau IPv6.

On comprend en outre que, l'adresse IPv6 de destination n'est pas construite de la même façon selon le type de contexte associé à l'adresse IPv4 partagée. Avantageusement, un préfixe différent peut être utilisé, selon que l'équipement nœud

adresse le paquet IPv6 qu'il a construit à l'équipement nœud du sous réseau de rattachement de l'équipement client destinataire ou à un autre équipement du système selon l'invention.

Selon un aspect de l'invention, le système d'acheminement comprend au moins un équipement de mémorisation d'une association entre ladite adresse IPv4 partagée, l'identifiant de contexte IPv4 de la communication et l'identifiant de sous-réseau de rattachement de l'équipement client possédant ladite adresse partagée, ledit équipement étant apte à fournir, sur réception d'une requête comprenant l'adresse IPv4 partagée et l'identifiant de contexte IPv4, au moins l'identifiant de sous-réseau.

L'équipement de mémorisation selon l'invention permet ainsi d'associer une donnée de contexte à l'identifiant de contexte associé à IPv4 partagée source du paquet de données IPv4. Ceci est nécessaire lorsque le paquet de données IPv4 ne porte pas lui-même d'identifiant du sous-réseau de rattachement de l'équipement source possédant l'adresse IPv4 partagée. C'est notamment le cas lorsque le paquet de données ne comprend pas de numéro de port. On comprend que la donnée de contexte mémorisée contient, soit directement l'identifiant de sous-réseau associé à l'adresse IPv4 source partagée, soit une information permettant de retrouver cet identifiant de sous-réseau. Un avantage est d'éviter que cet identifiant de sous-réseau ne soit perdu lorsque le paquet de données IPv4 quitte le sous-réseau IPv4 dont il provient pour être acheminé vers sa destination. Lorsqu'un paquet de réponse arrivera, l'identifiant de sous-réseau associée à l'adresse IPv4 partagée devenue destination pourra être récupéré auprès desdits moyens de mémorisation.

Selon encore un autre aspect de l'invention, lorsque l'adresse IPv4 source est une adresse partagée, ledit premier équipement nœud est apte à déterminer un type de contexte de l'adresse IPv4 source, et

lorsque le type de contexte déterminé est un contexte avec données, le premier équipement nœud est apte à choisir le préfixe de l'adresse de destination du paquet de données IPv6 converti de façon à ce qu'il parvienne audit équipement de mémorisation de contexte pour mémorisation d'une association entre ladite adresse source IPv4 partagée, ledit identifiant de contexte et une donnée de contexte identifiant de sous-

réseau de rattachement de l'équipement client source.

Ainsi, lorsqu'une mémorisation de donnée de contexte est nécessaire, le paquet de données passe obligatoirement par l'équipement de mémorisation de contexte selon l'invention.

Selon un autre aspect de l'invention, au moins un équipement de mémorisation de contexte est apte à mettre en œuvre, sur réception d'un paquet de données IPv6 en provenance d'un desdits équipements nœuds:

- des moyens d'extraction de l'adresse de destination IPv4 partagée et de l'identifiant de contexte,
- des moyens de détermination d'un type de contexte associé au paquet de données IPv6 reçu parmi un contexte sans données et un contexte avec données;
- si le type de contexte déterminé est un contexte avec données, des moyens de recherche dans la base de données d'une association entre ladite adresse IPv4 de destination, ledit identifiant de contexte et une donnée de contexte identifiant le sous-réseau de rattachement de l'équipement client destinataire;
- si une association a été trouvée, des moyens de remplacement de l'adresse de destination du paquet de données IPv6 par une adresse IPv6 construite à partir de l'adresse de destination partagée, de l'identifiant de sous-réseau trouvé et d'un préfixe opérateur.

Le ou les équipements de mémorisation selon l'invention permettent donc de récupérer la donnée de contexte identifiant le sous-réseau de rattachement de l'équipement destinataire du paquet de données IPv4 et de modifier l'adresse de destination IPv6 construite pour qu'elle désigne l'équipement nœud interfacé avec ce sous-réseau.

Un avantage est de limiter les opérations de mémorisation à un nombre limité d'équipements du système et donc de restreindre la vulnérabilité du système selon l'invention aux attaques de déni de service.

L'invention concerne aussi un équipement nœud d'un système d'acheminement d'un paquet de données à destination d'un équipement client destinataire et un équipement client destinataire, dans un réseau de télécommunications IPv4, l'un au

moins desdits équipements clients possédant une adresse publique IPv4 partagée avec d'autres équipements clients connectés audit réseau IPv4.

Selon l'invention, un tel équipement nœud est caractérisé en ce que :

- ledit réseau IPv4 étant décomposé en une pluralité de sous-réseaux;
- la pluralité d'équipements clients partageant ladite adresse IPv4 étant rattachée à ladite pluralité de sous-réseaux, de façon à connecter au plus un desdits équipements clients par sous réseau,

Ledit système comprenant une pluralité d'équipements nœuds aptes à communiquer entre par l'intermédiaire d'un réseau IPv6,

Ledit équipement nœud comprend :

des premiers moyens de communication avec un desdits sous réseaux IPV4;

des seconds moyens de communication avec d'autres équipements nœuds dudit système par l'intermédiaire d'un réseau de télécommunication IPv6;

des moyens de détermination d'un type de contexte de l'adresse de destination IPv4 partagée, aptes à être mis en œuvre sur réception d'un paquet de données IPv4 sur lesdits premiers moyens de communication;

des moyens de conversion du paquet de données IPv4 reçu sur lesdits premiers moyens en un paquet de données IPv6, ledit paquet comprenant une adresse IPv6 de destination construite à partir de l'adresse IPv4 partagée de destination et de l'identifiant de contexte et d'un préfixe opérateur, ledit préfixe étant choisi en fonction du type de contexte déterminé lié à l'adresse IPv4 destination ; et

des moyens d'envoi du paquet de données IPv6 obtenu sur les deuxièmes moyens de communication.

Selon un aspect de l'invention, ledit équipement nœud comprend des moyens de conversion inverse d'un paquet de données IPv6 comprenant une adresse IPv4 de destination partagée et un identifiant de contexte, en un paquet de données IPv4 comprenant ladite adresse de destination et l'identifiant de contexte, lesdits moyens de conversion inverses étant aptes à être mis en œuvre sur réception du paquet de

données sur les deuxièmes moyens de communication, et des moyens d'envoi du paquet de données IPv4 obtenu sur les premiers moyens de communication dans le sous réseau IPv4 interfacé avec ledit équipement nœud.

Selon une variante, si ledit équipement nœud est interfacé avec plusieurs sous-réseaux IPv4 de ladite pluralité de sous réseaux, l'adresse IPv6 destination du paquet reçu peut lui permettre de déterminer vers lequel de ces sous-réseaux il doit remettre le paquet IPv4.

L'équipement nœud selon l'invention permet d'émettre des paquets de données dans le réseau IPv6 le reliant aux autres équipements nœuds du système d'acheminement selon l'invention. Il permet aussi de recevoir des paquets de données IPv6 reçus en provenance des autres équipements nœuds.

L'invention concerne en outre un procédé de traitement d'un paquet de données émis par un équipement client source à destination d'un équipement client destinataire au cours d'une communication établie dans un réseau de télécommunications IPv4 d'un opérateur, ledit équipement client destinataire possédant une adresse publique IP partagée avec d'autres équipements clients connectés audit réseau IPv4, caractérisé en ce que :

- ledit réseau IPv4 est décomposé en une pluralité de sous-réseaux;
- la pluralité d'équipements clients partageant ladite adresse IPv4 est rattaché à ladite pluralité de sous-réseaux, de façon à connecter au plus un desdits équipements clients par sous-réseau;

Ledit système comprend une pluralité d'équipements nœuds aptes à communiquer entre eux par l'intermédiaire d'un réseau IPv6,

et ledit procédé étant apte à être mis en œuvre par un desdits équipements nœuds, il comprend les étapes suivantes :

- détermination d'un type de contexte de l'adresse de destination IPv4 partagée, destinée à être mise en œuvre sur réception d'un paquet de données IPv4 en provenance d'un sous-réseau IPv4;
- conversion du paquet de données IPv4 reçu en un paquet de données IPv6, ledit paquet comprenant une adresse IPv6 de destination construite à partir de

l'adresse IPv4 partagée de destination et de l'identifiant de contexte et d'un préfixe opérateur, ledit préfixe étant choisi en fonction du type de contexte déterminé lié à l'adresse IPv4 destination; et

- envoi du paquet de données IPv6 obtenu dans le réseau IPv6.

Selon un aspect de l'invention, ledit procédé de traitement comprend en outre les étapes suivantes, mises en œuvre sur réception du paquet de données en provenance du réseau IPv6 :

- conversion inverse du paquet de données IPv6 comprenant une adresse IPv4 de destination partagée et un identifiant de sous-réseau de rattachement de l'équipement client destinataire, en un paquet de données IPv4 comprenant ladite adresse de destination et l'identifiant de contexte, et

- envoi du paquet de données IPv4 obtenu dans le sous réseau IPv4 interfacé avec ledit équipement nœud.

Dans un mode particulier de réalisation, les différentes étapes du procédé de traitement d'un paquet de données selon l'invention sont déterminées par des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans un équipement nœud ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de traitement d'un paquet de données tel que décrit ci-dessus.

L'invention concerne aussi un procédé de mémorisation d'un contexte de communication associé à une adresse IPv4 source d'un paquet de données émis par un équipement client à destination d'un équipement client destinataire au cours d'une communication établie dans un réseau de télécommunication IPv4, ladite adresse étant partagée avec d'autres équipements clients connectés audit réseau IPv4 et ledit paquet comprenant un identifiant de contexte de la communication, caractérisé en ce que :

- ledit réseau IPv4 est décomposé en une pluralité de sous-réseaux;

- la pluralité d'équipements clients partageant ladite adresse IPv4 est rattaché à ladite pluralité de sous-réseaux, de façon à connecter au plus un desdits équipements clients par sous-réseau;

ledit procédé de mémorisation de contexte comprenant les étapes suivantes mises en œuvre sur réception d'un paquet de données comprenant ladite adresse IPv4 partagée:

- des moyens d'extraction de l'adresse source IPv4 partagée et de l'identifiant de contexte,

- des moyens de détermination d'un type de contexte associé, parmi un contexte sans données et un contexte avec données;

- si le type de contexte déterminé est un contexte avec données, des moyens de recherche dans la base de données d'une association entre ladite adresse IPv4 source, ledit identifiant de contexte et un identifiant du sous-réseau avec lequel ledit équipement nœud est interfacé;

- si aucune association n'a été trouvée, des moyens d'enregistrement d'une association entre ladite adresse source IPv4 partagée, l'identifiant de contexte et l'identifiant de sous-réseau;

-si une association a été trouvée comprenant l'identifiant de sous-réseau, des moyens de remplacement de l'adresse de destination du paquet de données IPv6 par une adresse IPv6 construite à partir de l'adresse de destination du paquet de données IPv4 extraite du paquet IPv6 reçu, de l'identifiant du sous-réseau destinataire et d'un préfixe opérateur adapté; et

- si une association a été trouvée comprenant un autre identifiant de sous-réseau, des moyens de remplacement de l'adresse IPv4 source partagée par une autre adresse IPv4 et des moyens d'enregistrement d'une association entre ladite autre adresse IPv4, l'identifiant de contexte, l'identifiant de sous-réseau et l'adresse IPv4 partagée.

Dans un mode particulier de réalisation, les différentes étapes du procédé de mémorisation d'un contexte d'un paquet de données selon l'invention sont déterminées par des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans un

équipement nœud ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé de mémorisation d'un contexte d'un paquet de données tel que décrit ci-dessus.

Liste des figures

D'autres avantages et caractéristiques de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation particulier de l'invention, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 présente un exemple de système d'acheminement d'un paquet de données IPv4 selon un premier mode de réalisation de l'invention;
- la figure 2 présente un exemple de système d'acheminement d'un paquet de données dans un réseau de télécommunications IPv4 selon un deuxième mode de réalisation de l'invention;
- la figure 3 présente un procédé de traitement d'un paquet de données IPv4 mis en œuvre par un équipement nœud selon l'invention;
- la figure 4 présente un procédé de traitement d'un paquet de données IPv6 mis en œuvre par un équipement nœud selon l'invention;
- la figure 5 présente la structure matérielle d'un équipement nœud selon l'invention;
- la figure 6 présente un exemple de format de conversion d'une adresse IPv4 en IPv6 selon l'invention utilisé pour former les adresses IPv6 destination des paquets envoyés vers un équipement nœud d'interface avec le réseau public IPv4;
- la figure 7 présente un exemple de format de conversion d'une adresse IPv4 en IPv6 selon l'invention utilisé par un équipement nœud d'interface avec un sous-réseau, qui n'est pas le réseau public IPv4, pour former les adresses IPv6 destination des paquets envoyés à un équipement de mémorisation des contextes;
- la figure 8 présente un exemple de format de conversion d'une adresse IPv4 en

IPv6 selon l'invention utilisé pour former les adresses IPv6 destination des paquets envoyés vers un équipement nœud d'interface avec un sous-réseau qui n'est pas le réseau public IPv4;

- la figure 9 présente la structure matérielle d'un équipement nœud selon l'invention;
- les figures 10 et 11 présentent un procédé de mémorisation d'un contexte de communication selon l'invention;
- la figure 12 présente un exemple de système d'acheminement d'un paquet de données selon l'invention, lorsque l'équipement destinataire comprend une interface compatible.

Description d'un mode de réalisation particulier de l'invention

Dans la suite de la description, nous nous placerons dans le contexte de l'accès au service de connectivité IP (Internet, Intranet, etc.) et les équipements clients considérés seront des passerelles domestiques. Il faut noter toutefois que l'invention n'est pas limitée à cet exemple et peut s'appliquer à tout réseau, service ou dispositif utilisant des adresses IPv4.

Pour rappel, les principes de l'invention sont les suivants :

- choisir un ou plusieurs ensembles d'adresses IPv4 dont les adresses seront partagées entre plusieurs équipements clients;
- décomposer le réseau de télécommunications IPv4 en une pluralité de sous-réseaux, de telle sorte que deux équipements clients partageant la même adresse IPv4 soient rattachés à des sous-réseaux différents; et
- associer à ladite adresse partagée des informations de contexte comprenant au moins un identifiant de contexte à partir duquel le routage du paquet de données pourra être effectué jusqu'au sous-réseau de l'équipement client destinataire.

1. La décomposition du réseau IPv4 en sous-réseaux

L'un de ces sous réseaux est le réseau normal ou réseau IPv4 public qui est composé d'adresses IPv4 non partagées et de toutes les adresses publiques gérées par d'autres opérateurs. Pour simplifier, on englobe aussi dans ce réseau toutes les adresses IPv4 partagées appartenant aux autres ensembles d'adresses IPv4 partagées disjoints (le plus souvent gérés par d'autres opérateurs) qui sont accessibles via le réseau IPv4 public.

Chacun des autres sous-réseaux est associé à un identifiant spécifique ou clone_sub_network_identifier. Une même adresse IPv4, appelée Shared_@IPv4 peut donc être réutilisée avec des identifiants de sous-réseaux différents. En revanche chaque couple (Shared_@IPv4, clone_sub_network_identifier) est unique.

Les sous-réseaux peuvent être soit

- *Réels* c'est-à-dire qu'à l'intérieur du sous-réseau, les adresses partagées shared_@IPv4 sont utilisées pour effectuer le routage des paquets vers leur destination.

- *Virtuels,* c'est-à-dire que ce réseau est construit en "overlay" sur un autre réseau IPv4 ou IPv6.

2. Le contexte de communication

Un contexte de communication est généralement associé à une communication. Au sens des protocoles internet, une communication est un échange de paquets entre deux interfaces donc chacune possède sa propre adresse. On désigne par interface la connexion dont dispose un équipement avec un réseau de télécommunication. Une adresse IPv4 public normale identifie habituellement une interface unique. Mais ce n'est plus le cas avec les adresses IPv4 partagées. Pour acheminer un paquet vers l'interface d'un équipement client, il faut retrouver l'identifiant de sous-réseau de rattachement de cet équipement client ou directement l'équipement client attaché à cette adresse IPv4 partagée à partir d'informations complémentaires que l'on appelle contexte de communication. Ce contexte pourra également contenir d'autres informations utiles.

On notera que la notion de communication s'applique aussi bien aux protocoles avec ou sans numéro de port.

On adopte donc la définition suivante :

Un contexte de communication est un ensemble d'informations liées à une adresse IPv4 partagée shared_@IPv4 et qui peut se composer des deux types d'éléments suivants :

- un identifiant de contexte, qui est formé d'informations échangées dans les paquets, et qui permettent de reconnaître le contexte. Ces informations peuvent être transmises soit dans l'en-tête IP du paquet, soit dans le datagramme (les données du paquet), par exemple dans un en-tête de protocole (comme les en-têtes UDP ou TCP). L'important est que dans le datagramme ou les datagrammes envoyés en réponse à un datagramme qui porte un identifiant de contexte on puisse retrouver, pas nécessairement à la même place, le même identifiant de contexte;
- des données de contexte optionnelles qui, lorsqu'elles existent, sont mémorisées dans une fonction spécifique (ce qui suppose dans ce cas un équipement "statefull") et qui peuvent être retrouvées sur la base de l'identifiant de contexte et de l'adresse IPv4 partagée shared_@IPv4 à laquelle ce contexte est lié.

Un paquet peut donc porter deux identifiants de contexte, un pour son adresse source et un autre pour son adresse destination.

Le contexte permet d'identifier le sous-réseau de rattachement de l'équipement client. On distingue deux cas :

- le cas où l'identifiant de contexte permet à lui seul d'identifier le sous-réseau; et
- le cas où l'identifiant ne permet pas d'identifier le sous-réseau. L'identifiant de sous-réseau est alors porté par les données de contexte.

Une "communication" est alors définie comme l'ensemble des paquets échangés qui ont même la même paire de couples {(adresse IPv4 source, identifiant de contexte source), (adresse IPv4 de destination, identifiant de contexte de destination)}.

Lorsqu'un contexte de communication utilise des données de contexte, il a une durée limitée dans le temps. Lorsque les données de contexte ne sont plus utiles ou lorsqu'elles ne sont plus utilisées depuis un certain temps, les données de contexte sont effacées. Le contexte est alors réinitialisé et on parlera d'un nouveau contexte lorsque les données de contexte seront de nouveau utilisées.

On ne s'intéressera donc par la suite qu'à des contextes de communication qui ont les deux propriétés suivantes :

- Les données de l'adresse IPv4 partagée shared_@IPv4 et du contexte permettent d'identifier sans ambiguïté l'interface qui est concernée par la communication parmi toutes celles qui partagent cette adresse. (par exemple, il suffit de pouvoir en déduire l'identifiant de sous-réseau ou une adresse d'interface qui n'est pas partagée);
- Un même identifiant de contexte ne peut généralement pas être associé deux fois à la même adresse partagée shared_@IPv4, même s'il existe une exception à cette règle.

Cela signifie qu'à un instant donné deux interfaces qui partagent la même adresse shared_@IPv4 ne peuvent communiquer simultanément en IPv4 que si les identifiants de contexte de ces deux communications sont différents. Sinon, pour un paquet d'une des deux communications qui porte cette adresse partagée, il ne serait plus possible de déterminer lequel de ces deux contextes est associé à cette adresse.

On peut citer deux types principaux de contextes :

- le contexte basé sur un numéro de port appartenant à une plage de numéros de ports réservée à un sous-réseau. Ce contexte comprend seulement un identifiant de contexte constitué du numéro port. Il utilise le fait que dans la réponse à un datagramme les ports source et destination sont inversés. Il ne nécessite pas de données de contexte, car il est unique. Selon l'invention, l'identifiant de sous-réseau est dérivé directement du numéro de port grâce à la limitation selon une plage de ports autorisés;

- les contextes basés sur d'autres données propres à une communication particulière, par exemple l'adresse IPv4 de l'autre équipement client avec lequel la communication est établie, qui constitue un identifiant de contexte très simple. Cet exemple de contexte utilise le fait que dans la réponse à un paquet les adresses source et destination sont inversées. Malheureusement l'identifiant de ce contexte n'est pas unique car dans ce cas deux interfaces situés sur des équipements différents qui partagent la même adresse shared_@IPv4 peuvent vouloir communiquer chacune en IPv4 avec des interfaces possédant des adresses IPv4 identiques (par exemple parce qu'elles dialoguent toutes deux avec le même équipement). Avec ce contexte, deux interfaces partageant la même adresse IPv4, ne peuvent pas communiquer au même instant avec la même interface ou avec deux interfaces partageant la même adresse IPv4. Il faudra donc changer l'adresse IPv4 source pour la deuxième communication vers la même adresse IPv4. De plus il est nécessaire de lui ajouter des données de contexte, qui peuvent être, à titre d'exemple, l'identifiant de sous-réseau. On peut également ajouter d'autres données à ce contexte.

Bien entendu, d'autres contextes peuvent être utilisés dans le cadre de l'invention. C'est le cas, en particulier, pour des paquets de type ICMP (Internet Control Message Protocol).

3. Un premier mode de réalisation d'un système d'acheminement selon l'invention

En relation avec la **Figure 1**, on présente un système d'acheminement d'un paquet de données selon un premier mode de réalisation de l'invention, dans lequel un réseau IPv4 1 est décomposé en quatre sous-réseaux SR1 à SR4. Dans cet exemple, le sous-réseau SR1 constitue le réseau IPv4 public. Le système d'acheminement selon l'invention comprend un équipement nœud EN comprenant des interfaces logiques I1 à I4 avec chacun des sous-réseaux SR1 à SR4. On considère maintenant l'équipement client EC2 connecté au sous-réseau IPv4 SR2 et on suppose que cet équipement client émet un paquet de données destiné à l'équipement client EC4, rattaché au sous-réseau SR4 et dont l'adresse de destination est une adresse IPv4 partagée

shared_@IPv4. Selon l'invention, le paquet de données comprend des informations de contexte qui constituent un identifiant de contexte permettant d'identifier le sous réseau EC4 du réseau IPv4 auquel est rattaché l'équipement client destinataire. Dans cet exemple, l'identifiant de contexte est, par exemple constitué par le numéro de port de destination, ce numéro de port appartenant à une plage de numéros de ports réservée au sous-réseau de rattachement de l'équipement destinataire.

Selon ce mode de réalisation de l'invention, le système d'acheminement comprend un équipement nœud EN comprenant une interface de communication avec chacun des sous-réseaux SR1 à SR4. Le paquet de données étant destiné à un autre sous-réseau, il doit être envoyé directement à l'équipement nœud EN en charge du traitement de ce type de paquets. On comprend en effet que, puisque l'adresse IPv4 partagée de destination shared@IPv4 du paquet de données pourrait être affectée à un équipement client du sous-réseau, les techniques de routage classiques ne permettent pas de router le paquet de données en dehors du sous-réseau. Par conséquent, le système selon l'invention comprend des moyens d'établissement d'une liaison point à point entre l'équipement client émetteur et l'équipement nœud EN. Une solution simple pour réaliser cette liaison point à point est de construire un tunnel TUN2 entre l'équipement client émetteur EC2 et l'équipement nœud EN.

De façon avantageuse, l'équipement client émetteur EC2 peut recevoir, sur requête d'un serveur DHCP, les coordonnées de l'adresse destination du tunnel TUN2 vers l'équipement nœud EN par exemple sous forme d'une adresse IPv4 partagée qui est routable sans risque de confusion sur le sous-réseau SR2. On notera que cette adresse peut être la même sur les deux autres interfaces avec les sous réseaux SR3 et SR4.

L'équipement client EC2 peut alors monter un tunnel avec cet équipement. Un tunnel GRE (Generic Routing Encapsulation) est en général suffisant mais toutes les autres formes connues de liaison point à point ou de VPN (Virtual Private Network) sont utilisables (on peut citer à titre d'exemple les tunnels IPv4 dans IPv4, les tunnels L2TP, les VLAN Ethernet, les VC ATM, Les Label Stack Path MPLS). A ce stade, l'équipement client EC2 dispose alors de deux interfaces, l'interface normale avec le

sous-réseau SR2 et le tunnel TUN2. L'adresse de l'interface normale avec le sous-réseau est son adresse partagée shared_@IPv4. Toutefois, il faut alors attribuer une adresse IPv4, au sein de l'équipement client, à l'interface constituée par le tunnel TUN2. Cette adresse servira d'adresse source pour les paquets envoyés dans le tunnel. Par dérogation aux règles usuelles qui veulent que deux interfaces différentes possèdent des adresses IPv4 différentes, on propose d'utiliser également l'adresse partagée shared_@IPv4, car ce sont plus deux composants d'une même interface que deux interfaces différentes. En variante, il est tout à fait possible de choisir une autre adresse pour l'une ou l'autre de ces deux adresses.

L'équipement nœud EN selon l'invention est apte à recevoir le paquet de données P2, à identifier le sous-réseau de destination à l'aide du numéro de port de destination qui constitue un identifiant du sous réseau de destination SR4 et à aiguiller le paquet de données sur son interface logique avec le sous réseau SR4.

Une fois dans le sous-réseau SR4, le routage du paquet de données ne pose plus de problème, car son adresse de destination shared_@IPv4 y est unique.

4. Un deuxième mode de réalisation d'un système d'acheminement selon l'invention

En relation avec la **Figure 2**, on présente maintenant un système d'acheminement selon un deuxième mode de réalisation de l'invention. Un tel système d'acheminement comprend une pluralité d'équipements nœuds EN1 à EN4, lesquels sont connectés entre eux par l'intermédiaire d'un réseau IPv6 public 10. On comprend que de tels équipements nœuds comprennent chacun au moins une interface de communication avec un sous-réseau SR_i, i entier de 1 à 4 et une interface de communication avec le réseau IPv6 10. Ils sont donc nécessairement agencés pour communiquer à la fois selon les protocoles IPv4 et IPv6.

On considère un paquet de données P3 émis par l'équipement client EC3 du sous-réseau SR3 à destination de l'équipement client EC2 possédant une adresse partagée shared_@IPv4. De la même façon que précédemment, ce paquet de données envoyé directement à l'équipement nœud EN3 en charge du routage des

paquets à destination d'adresses IPv4 partagées via une liaison point à point établie entre l'équipement client EC3 et l'équipement nœud EN3. A titre d'exemple, une telle liaison est constituée d'un tunnel TUN_3 établi entre l'équipement client émetteur EC3 et l'équipement nœud EN3.

De façon avantageuse, l'équipement client émetteur EC3 peut recevoir sur requête auprès d'un serveur DHCP les coordonnées de l'adresse destination du tunnel TUN_3 vers l'équipement nœud EN3, par exemple sous forme d'une adresse IPv4 virtuelle. Cette adresse représente l'adresse de la fonction de transcodage IPv4/IPv6 de l'équipement nœud EN3. Le terme virtuel signifie que c'est la même adresse IPv4 publique qui est utilisée par tous les équipements nœuds ENi du système de routage selon l'invention (même si plusieurs équipements nœuds différents étaient raccordés au même sous-réseau SR3, ce qui n'est pas le cas sur la figure). Vu de l'équipement nœud EN3, c'est une adresse qu'il doit intercepter pour traitement comme si c'était sa propre adresse.

L'équipement client EC3 peut alors monter le tunnel TUN_3, par exemple de type GRE ou VPN, avec l'équipement nœud EN3.

Sur réception du paquet de données P3 émis par un équipement client du sous-réseau SR3, par exemple l'équipement EC3 et destiné à un équipement client possédant une adresse IPv4 partagée shared_@IPv4, par exemple l'équipement EC2, le système d'acheminement selon l'invention est apte à envoyer le paquet de données vers l'équipement nœud EN2.

Selon l'invention, l'équipement nœud EN3 est apte à mettre en œuvre le procédé de traitement d'un paquet de données selon l'invention qui va maintenant être décrit en relation avec la **Figure 3**. Un tel procédé comprend une étape E1 de réception du paquet de données IPv4 P3 sur la liaison point à point directe TUN_3 établie avec l'équipement client source EC3. En E2, un type de contexte est déterminé à partir de l'identifiant de contexte contenu dans le paquet de données. Par exemple, si le protocole est du type TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol), l'identifiant de contexte sera le numéro de port et le contexte sera sans

données. Si le protocole est d'un type sans numéro de port alors il s'agira d'un contexte avec données.

S'il est établi qu'il s'agit d'un contexte sans données, l'identifiant de contexte est porteur d'un identifiant du sous-réseau de rattachement de l'équipement destinataire EC2. Un paquet de données IPv6 est donc construit en E3 par conversion du paquet de données IPv4 P3 en utilisant les mécanismes usuels de conversion entre IPv4 et IPv6 (dans une variante, le paquet IPv4 P3 peut être simplement encapsulé dans le paquet IPv6 ce qui facilite la conversion mais impose des en-têtes de paquets plus longs qui peuvent conduire à fragmenter davantage de paquets). L'adresse de destination IPv6 de ce paquet est construite à partir de l'adresse de destination IPv4 partagée du paquet P3, de l'identifiant de contexte et d'un préfixe opérateur désignant l'équipement nœud EN2. Ainsi, l'adresse IPv6 de destination obtenue est routable dans le réseau IPv6 à l'aide de routeurs standards.

Si au contraire, il est établi que le contexte est de type avec données (par exemple parce que le protocole IP n'utilise pas de numéro de port), un paquet de données P3_IPv6 est construit en E3 à partir du paquet IPv4 P3 avec une adresse de destination comprenant un préfixe désignant un équipement de mémorisation de contexte EM. Si, comme dans l'exemple du nœud EN3, ce nœud est interfacé avec un sous-réseau qui n'est pas le réseau public IPv4, cette adresse IPv6 de destination est construite en appliquant un format de conversion dit format de conversion commun sans numéro de port, qui sera décrit en section 5 de cette description, avec l'adresse IPv4 source du paquet IPv4. Comme indiqué dans cette section, si on a choisi de faire une conversion des paquets IPv4 en paquet IPv6 plutôt qu'une simple encapsulation, il faut alors également recopier l'adresse IPv4 destination dans les 32 bits de poids les plus faibles de cette adresse.

Dans le cas d'un équipement nœud tel que EN1 qui est interfacé avec le réseau public IPv4, cette adresse IPv6 de destination aurait été construite en appliquant un format dit format de conversion commun sans numéro de port, qui sera lui aussi décrit à la section 5 de cette description, avec l'adresse IPv4 destination du paquet IPv4.

Ensuite, le paquet de données est envoyé dans le réseau IPv6, au cours d'une étape E4.

Dans la suite de cet exemple, on suppose que le contexte est de type sans données. L'identifiant de contexte est, par exemple, un numéro de port appartenant à une plage réservée à l'équipement client destinataire.

Selon l'invention, le paquet de données IPv6 émis par l'équipement nœud EN3 est reçu par un équipement nœud EN2. Selon l'invention, cet équipement est apte à mettre en œuvre les étapes F1 à F3 du procédé de traitement d'un paquet de données selon l'invention, qui vont maintenant être décrites en relation avec la **Figure 4**. Si le contexte avait été du type avec données, le paquet aurait transité par un ou deux équipements de mémorisation de contexte, mais le traitement du paquet IPv6 reçu par le nœud serait le même. En F1, le paquet de données IPv6 est reçu par l'équipement EN2 en provenance du réseau IPv6 10. En F2, une étape de conversion IPv6/IPv4 inverse est effectuée sur le paquet de données P3-IPv6 reçu, en extrayant de l'adresse IPv6 de destination l'adresse partagée shared@IPv4 de destination, de l'adresse IPv6 source l'adresse IPv4 source et en reconstruisant le paquet de données IPv4 P3 à partir des informations extraites et des mécanismes usuels de conversion entre IPv6 et IPv4 (ou en extrayant simplement le paquet IPv4 encapsulé dans la variante avec encapsulation).

En F3, le paquet de données IPv4 P3 obtenu est envoyé dans le sous-réseau SR2 pour y être routé de façon classique à partir de son adresse de destination IPv4, qui est unique dans le sous-réseau SR2. Ce paquet n'a pas besoin d'être placé dans le tunnel $TUN_{2,1}$.

En relation avec la **Figure 5**, on présente un équipement nœud ENi, i entier de 1 à 4, 100 selon l'invention, qui comporte les éléments matériels que l'on retrouve classiquement dans un ordinateur conventionnel, à savoir un processeur 110, une mémoire vive de type RAM 120, une mémoire morte de type ROM 130 et des premiers moyens 140 de communication ou interface avec le sous-réseau IPv4 SRi et des deuxièmes moyens 150 de communication ou interface avec le réseau IPv6.

La mémoire morte 130 constitue un support d'enregistrement conforme à l'invention. Ce support mémorise le programme d'ordinateur conforme à l'invention. Ce programme comporte des instructions pour l'exécution des étapes du procédé de traitement d'un paquet de données conforme à l'invention qui vient d'être décrit en référence à la **Figure 4.**

On comprend donc que l'utilisation d'un réseau IPv6 pour les communications entre les différents équipements nœuds permet de séparer les différentes fonctions mises en œuvre par le système d'acheminement selon l'invention, de telle sorte que seules les fonctions de conversion IPv4/IPv6 et IPv6/IPv4 réalisées par les équipements nœuds soient spécifiques, les autres fonctions de routage étant effectuées par des équipements de routage standards.

Un autre avantage concerne une localisation des fonctions de conversion spécifiques précédemment évoquées, qui peuvent être mises en œuvre très en amont dans le réseau et sur un nombre d'équipements nœuds restreints, le nombre d'équipements nœuds concernés étant liés au volume de trafic à traiter, à la capacité de traitement de chaque nœud, à la topologie de routage retenue par l'opérateur et aux exigences de sécurisation de l'opérateur.

On comprend en outre que si une communication est établie entre les réseaux IPv4 de deux opérateurs qui mettent en œuvre un système d'acheminement de paquets de données selon l'invention, les paquets IPv4 échangés lors de cette communication vont être convertis une première fois en paquets IPv6, puis reconvertis en paquet IPv4 dans un équipement nœud selon l'invention pour être acheminés sur le réseau IPv4 public du premier opérateur, avant d'être reconverti en IPv6 dans un équipement nœud du deuxième opérateur et enfin à nouveau en IPv4.

Les conversions intermédiaires IPv6 vers IPv4 puis IPv4 vers IPv6 réalisées dans les deux équipements nœuds pourraient être évitées si les opérateurs se mettaient d'accord pour échanger ces paquets directement en IPv6.

En supposant qu'une communauté d'opérateur, la plus large possible, puisse s'accorder sur un mécanisme commun d'échange de paquets de données, cet accord

devra préciser comment transmettre un paquet de données IPv4 en IPv6 et, au moins comment construire les adresses IPv6 source et destination du paquet de données IPv6 obtenu par conversion du paquet de données IPv4.

On notera que le routage des paquets de données avec numéro de port venant d'un sous-réseau IPv4 selon l'invention et à destination du réseau IPV4 public peut se faire directement en IPv4 par le biais de routeurs IPv4 qui interconnecteraient le sous-réseau IPv4 selon l'invention et le réseau IPv4 public ou en IPv6 à travers le système d'acheminement décrit précédemment. Mais le routage d'un paquet de données venant du réseau IPv4 public vers un sous-réseau IPv4 selon l'invention doit utiliser le système d'acheminement via IPV6 décrit précédemment. De même le routage des paquets de données sans numéro de port venant d'un sous-réseau IPv4 selon l'invention et à destination du réseau IPV4 public doit se faire nécessairement via IPv6 et le système d'acheminement décrit précédemment.

5. Formats de conversion IPv4/IPv6

Trois formats de conversion vont maintenant être décrits, à titre d'exemple :

- **le format de conversion commun** : afin d'optimiser les communications, différents opérateurs peuvent s'accorder sur un format de conversion permettant d'associer une adresse IPV6 à un couple (adresse_IPv4, port). Dans la suite, on désignera ce format d'adresse IPv6 par common_format, dont un exemple est présenté en relation avec la **Figure 6**. Comme toute adresse IPv6 celle-ci peut se décomposer en un préfixe (dont la longueur peut être égale, supérieure ou inférieure à 64 bits) et une adresse d'interface.

Ce format est utilisé pour former les adresses IPv6 destination des paquets envoyés vers un nœud interfacé avec le réseau IPv4 public lorsque le protocole IP utilise des numéros de port. Il sera également utilisé pour former les adresses IPv6 source des paquets envoyés sur le réseau IPv6 par un nœud interfacé avec le réseau IPv4 public si le protocole IP utilise des numéros de port.

Un tel format inclut le port ce qui permet d'identifier, le sous-réseau de rattachement de l'équipement client associé à l'adresse partagée.

Il existe un algorithme qui permet d'extraire l'adresse_IPv4 à partir de l'adresse IPv6.

La partie de cette adresse marquée "IP6/IPv4 EN prefix" sur la **Figure 6** représente un préfixe IPv6 qui sera routé vers un équipement nœud qui fait l'interface avec le réseau public IPv4 ou directement vers une gateway domestique dual-stack qui utilise cette adresse IPv4 partagée.

On notera que ce préfixe peut inclure une partie variable des bits de poids fort de l'adresse IPv4, voir même toute l'adresse IPv4 et une partie du numéro de port constituant la plage de port. Cette partie de l'adresse IPv4 représente le préfixe IPv4 des paquets IPv4 qui doivent être routés en IPv6 vers cet équipement.

En jouant sur la taille de ce préfixe IPv6, l'opérateur peut décider d'inclure ou d'exclure des adresses IPv4 dans ce préfixe.

Par exemple, une passerelle dual-stack (IPv4/IPv6) qui utilise une adresse IPv4 partagée peut être considérée comme un sous-réseau IPv4 qui ne comprend qu'un seul équipement (elle-même) et pour lequel l'équipement nœud d'interface avec ce sous-réseau est inclus dans la passerelle. Dans ce cas, le préfixe aura l'extension maximale et comprendra l'adresse IPv4 de la passerelle domestique et la plage de port réservée à la passerelle.

Mais l'opérateur devra aussi veiller à ce qu'il existe une route par défaut vers toutes les adresses IPv4 qui ne sont pas gérées par le système d'acheminement selon l'invention. Pour cela, il veillera à créer une route IPv6 par défaut vers le préfixe "IP6/IPv4 EN prefix" formé avec toutes ces adresses IPv4 (par exemple il pourra utiliser la taille minimale qui n'inclut pas l'adresse IPv4 si il s'est assuré que ce format de conversion ne sera jamais utilisé avec les adresses gérées par le système d'acheminement ou si il s'est assuré que les adresses formées en appliquant ce format de conversion à des adresses gérées par le système d'acheminement seront dirigées, via une route plus courte, vers un autre équipement qui les convertira vers les autres

formats de conversion décrits ci-dessous). Cette route par défaut conduira à un équipement nœud interfacé avec le réseau public IPv4.

- **Le format de conversion commun sans numéro de port** (common_portless_format) **:** Il permet d'associer une adresse IPv6 à une adresse IPv4 pour les protocoles qui n'utilisent pas de numéro de port.

Cet algorithme est très proche du common_format mais la différence principale est qu'il n'utilise que l'adresse IPv4 et un autre préfixe.

Ce format est utilisé pour former les adresses IPv6 destination des paquets envoyés vers un nœud interfacé avec le réseau IPv4 public lorsque le protocole IP n'utilise pas de numéro de port. Il sera également utilisé pour former les adresses IPv6 source des paquets envoyés sur le réseau IPv6 par un nœud interfacé avec le réseau IPv4 public si le protocole IP n'utilise pas de numéro de port.

Ce format de conversion sera aussi utilisé pour former les adresses IPv6 destination des paquets obtenus par conversion d'un paquet IPv4 et qui doivent être envoyés à un moyen de mémorisation des contextes.

On notera qu'il existe un algorithme qui permet d'extraire l'adresse_IPv4 à partir de l'adresse IPv6.

Cet algorithme peut être très voisin de celui utilisé pour le common_format et fournir des préfixes identiques ou différents suivant les options choisies.
Certaines variantes peuvent n'utiliser que ce format, c'est-à-dire ne pas tenir compte du numéro de port pour calculer l'adresse IPv6.

Le champ port est remplacé par une valeur réservée, en général des zéros.

Il est recommandé que le préfixe formé par la concaténation des champs "Common id" , "IPv6/IPv4 EN" et du champ réservé qui précède l'adresse IPv4 ne diffère de celui du common_format que par le bit de poids faible.

Dans le cas d'un préfix commun partagé entre plusieurs opérateurs, il serait donc souhaitable que les 2 préfixes ne différent donc que par le bit 64 (si on numérote par 0 le bit de poids le plus faible et 127 celui de poids le plus fort).

La partie de cette adresse qui correspond à la partie marquée "IP6/IPv4 EN prefix" sur la **figure 6** représente un préfixe IPv6 qui sera routé vers un équipement de mémorisation des contextes.

On notera que l'adresse IPv4 est séparée en deux parties. Les bits de poids fort qui constituent le préfixe IPv4 d'un pool d'adresse IPv4 qui résulte de la répartition, par l'opérateur, en plusieurs pools, du pool d'adresses partagées attribué à cet opérateur. Les bits de poids faible permettent de différencier les différentes adresses IPv4 au sein de ce pool. La partie qui correspond à la partie marquée "IP6/IPv4 EN prefix" sur la figure 6 inclut ces bits de poids fort de l'adresse IPv4.

On notera que l'opérateur peut donc diviser le pool d'adresses IPv4 partagées en plusieurs pools attribués à des équipements de mémorisation différents. Cette division du pool d'adresses IPv4 partagées est transparente pour les nœuds d'interface avec les sous-réseaux qui utilisent toujours le même format de conversion d'adresse. Ce sont les mécanismes normaux de routage IPv6 qui gèrent cette répartition.

De plus l'opérateur veillera à ce qu'il existe au moins une route par défaut vers un ou des nœuds interfacés avec le réseau public IPv4 pour les préfixes "IPv6/IPv4 EN prefix" formés en appliquant ce format commun sans numéro de port pour les adresses IPv4 n'appartenant pas à ces pools d'adresses IPv4 partagées.

Pour les paquets IPv6 envoyés par un nœud interfacé avec le réseau IPv4 public, ou envoyés par un équipements de mémorisation des contextes, vers un équipement de mémorisation des contextes, c'est bien l'adresse IPv4 destination qui est utilisée pour former l'adresse IPv6 de destination avec ce format.

Il en est de même pour les paquets sans numéro de port envoyés vers un nœud interfacé avec le réseau public IPv4.

Cependant pour les échanges internes au système d'acheminement qui ont pour origine un nœud interfacé avec un sous réseau qui n'est pas le réseau public IPv4 et pour destination un équipement de mémorisation des contextes, l'adresse IPv4 qui est utilisée pour former l'adresse destination du paquet IPv6 est l'adresse source du paquet IPv4.

Dans ce dernier cas, et seulement dans la variante de conversion des paquets IPv4 en paquets IPv6 qui n'utilise pas une encapsulation, on peut avoir besoin des 32 bits de poids faibles, qui ne sont pas encore affectés, pour stocker l'adresse IPv4 destination. En effet, dans cette variante, l'adresse IPv4 destination d'origine serait perdue sans cela. Ce cas est représenté en relation avec la **Figure 7**.

- **le format de conversion interne** : afin de router les paquets IPv6 vers l'équipement nœud interfacé vers le bon sous-réseau IPv4 l'opérateur doit utiliser un format de conversion spécifique décrit en relation avec la **Figure 8**.

Ce format de conversion sera utilisé pour former les adresses IPv6 destination des paquets envoyés vers un nœud interfacé avec un sous réseau qui n'est ni un sous réseau réduit à une seule passerelle dual-stack, ni le réseau public IPv4.

Ce format de conversion sera aussi utilisé pour former les adresses IPv6 source des paquets IPv6 formés par conversion d'un paquet IPv4 par ces mêmes nœuds.

Par rapport au format de conversion de la figure 6 il utilise un identifiant propre à l'opérateur pour différencier ces adresses des autres adresses utilisées sur le réseau IPv6 et un identifiant "IPv6/IPv4 interne" qui est réservé aux paquets IPv6 transportant un paquet IPv4 selon ce procédé. Ensuite la partie d'un numéro de port représentant la plage de port associée à ce sous réseau est insérée dans le préfixe avant l'adresse IPv4. Cette partie est donc juste un identifiant de sous-réseau et c'est ce même identifiant qui est stocké et récupéré par les moyens de mémorisation.

On notera que l'adresse IPv4 est séparée en deux parties. Les bits de poids fort qui constituent le préfixe IPv4 du pool d'adresse IPv4 attribué à cet opérateur et qu'il a décidé de partager entre plusieurs équipements. Les bits de poids faible qui permettent de différencier les différentes adresses IPv4 au sein de ce pool.

La partie de cette adresse marquée "IP6/IPv4 interne prefix" sur la **Figure 8** représente un préfixe IPv6 qui sera routé vers un équipement nœud qui fait l'interface avec le sous-réseau IPv4 auquel est attribuée cette plage de port pour ce pool d'adresse.

6. Fonction de mémorisation d'un contexte de communication

Selon un mode de réalisation de l'invention, le système d'acheminement selon l'invention comprend des moyens de mémorisation d'un contexte de communication associé à une adresse IPv4 partagée. En relation avec la **Figure 2**, de tels moyens sont avantageusement mis en œuvre par au moins un équipement de mémorisation EM du système d'acheminement d'un paquet de données selon l'invention, qui est dédié à la mémorisation d'un tel contexte.

Le recours à un tel équipement de mémorisation de contexte est particulièrement avantageux dans le cas d'un contexte de type avec données. En effet, dans ce cas, les données du paquet IPv4 ne portent pas l'identifiant de sous-réseau de rattachement de l'équipement client associé à l'adresse IPv4 partagée. Par conséquent, il est nécessaire de lui associer une donnée de contexte identifiant ce sous-réseau. Cette mémorisation consiste à enregistrer une association entre l'adresse IPv4 partagée, l'identifiant de contexte et la donnée de contexte identifiant de sous-réseau de rattachement de l'équipement client possédant l'adresse partagée. Selon l'invention, on accède à cette association à partir du couple (adresse IPv4 partagée, identifiant de contexte).

On comprend que, lorsque l'identifiant de contexte est un numéro de port appartenant à la plage de numéros de port réservée à l'équipement client possédant l'adresse partagée, il constitue un identifiant de ce sous-réseau et la mémorisation d'une telle association n'est donc pas nécessaire.

En relation avec la **Figure 9**, l'équipement de mémorisation de contexte EM selon l'invention comporte les éléments matériels que l'on retrouve classiquement dans un ordinateur conventionnel, à savoir un processeur 210, une mémoire vive de type RAM 220, une mémoire morte de type ROM 230 et des moyens 240 de communication avec le réseau IPv6.

Conformément à l'invention, l'équipement de mémorisation de contexte EM 200 comporte une mémoire 250 comprenant une base de données dans laquelle sont stockées les associations entre l'adresse IPv4 partagée, l'identifiant de contexte et la

donnée de contexte identifiant le sous-réseau de rattachement de l'équipement client utilisant l'adresse partagée.

On notera que cette mémoire peut aussi bien être externe à l'équipement EM pourvu qu'il puisse y accéder.

La mémoire morte 230 constitue un support d'enregistrement conforme à l'invention. Ce support mémorise le programme d'ordinateur conforme à l'invention. Ce programme comporte des instructions pour l'exécution des étapes du procédé de mémorisation d'un contexte de communication d'un paquet de données conforme à l'invention qui va maintenant être décrit en référence aux **Figures 10 et 11.** Pour des questions de clarté, chacune de ces figures décrit l'une des deux branches principales du procédé. L'étape M1 et la première décision qui permet de choisir la branche ont été reproduites sur les deux figures.

Sur réception M1 d'un paquet de données IPv6 comprenant une adresse source IPv4 partagée et un identifiant de contexte, la branche de traitement est déterminée en comparant l'adresse IPv4 partagée qui a été utilisée pour former l'adresse IPv6 destination au "format de conversion commun sans numéro de port" avec l'adresse source du paquet IPv4. Il existe plusieurs variantes pour cela, on peut soit chercher l'adresse IPv4 qui a servi à former l'adresse IPv6 source, soit si on a choisi la variante avec encapsulation, regarder directement dans le paquet encapsulé, soit si on a choisi une variante sans encapsulation, regarder dans les 32 bits de poids faibles de l'adresse IPv6 destination car une valeur différente de la valeur réservée indique alors la présence d'une adresse destination et confirme que l'adresse IPv4 utilisée pour appliquer le format est bien l'adresse source.

Si l'adresse IPv4 partagée qui a été utilisée pour former l'adresse IPv6 au "format de conversion commun sans numéro de port" est bien l'adresse source du paquet IPv4, il faut suivre la branche décrite en relation avec la **Figure 10**. Sinon, il faut suivre la branche décrite en relation avec la **Figure 11**.

Dans la branche décrite en relation avec la **Figure 10**, une étape M2 d'extraction de l'adresse source IPv4 partagée et de l'identifiant de contexte est mise en œuvre.

En M3, un type de contexte associé est déterminé parmi les différents contextes avec données qui peuvent être mis en œuvre par le système. Avantageusement, cette détection s'appuie sur le numéro de protocole. Par exemple, un contexte spécifique utilisant l'identifiant de datagramme comme identifiant de contexte peut être mis en œuvre pour le protocole ICMP, alors que pour les autres protocoles sans numéro de port on utilisera plutôt l'adresse IPv4 destination comme identifiant du contexte attaché à l'adresse IPv4 source.

Une recherche dans la base de données d'une association entre ladite adresse IPv4 source, ledit identifiant de contexte et un identifiant du sous-réseau avec lequel ledit équipement nœud est interfacé, est effectuée en M4.

- si aucune association n'a été trouvée, un enregistrement d'une association entre ladite adresse source IPv4 partagée, l'identifiant de contexte et l'identifiant de sous-réseau est effectué en M5 et on passe ensuite à l'étape M6 décrite ci-dessous

-si une association a été trouvée comprenant l'identifiant de sous-réseau, l'adresse destination du paquet de données IPv6 est remplacée en M6 par une adresse IPv6 construite en appliquant le "format de conversion commun sans numéro de port" à l'adresse IPv4 de destination (cette adresse se trouve dans le paquet IPv4 encapsulé si on a choisi la variante avec encapsulation ou dans les 32 bits de poids faibles de l'adresse IPv6 destination reçue si on a choisi la variante avec conversion directe).

- si une association a été trouvée comprenant un autre identifiant de sous-réseau, l'adresse IPv4 source partagée est remplacée en M7 par une autre adresse IPv4 prise dans un pool attribué spécifiquement à l'équipement de mémorisation des contextes pour cet usage, l'adresse source paquet IPv4 est modifié si on a choisi la variante avec encapsulation et une association entre ladite autre adresse IPv4, l'identifiant de contexte, l'identifiant de sous-réseau et l'adresse IPv4 partagée est enregistrée en M8 dans la base de données.

Une nouvelle adresse IPv6 source est construite en appliquant le "format de conversion commun sans numéro de port" à la nouvelle adresse IPv4 source en M9 et on passe à l'étape M6 déjà décrite.

Après l'étape M6 il ne reste plus qu'a envoyer le paquet sur le réseau IPv6 à

l'étape M10.

Dans la branche décrite en relation avec la **Figure 11**, après la sélection de branche qui a suivi l'étape M1, une étape D1 d'extraction de l'adresse destination IPv4 partagée et de l'identifiant de contexte est mise en œuvre.

En D2, un type de contexte associé est déterminé parmi les différents contextes avec données qui peuvent être mis en œuvre par le système.

Si le type de contexte est un contexte sans données (ce qui peut se produire pour des paquets d'erreurs ICMP envoyés en réponse à un message avec numéro de port et qui contiennent ce numéro de port dans le paquet) on passe directement à l'étape D5.

Sinon une recherche dans la base de donnée d'une association entre ladite adresse destination IPv4 partagée, l'identifiant de contexte est mise en œuvre et un identifiant du sous-réseau est mise en œuvre en D3.

Si aucune association n'est trouvée, le paquet ne peut pas être acheminé et il faut retourner une erreur ICMP en D4.

Si une association est trouvée, elle permet en D5 d'en extraire l'identifiant de sous-réseau et elle peut aussi contenir l'adresse IPv4 d'origine. Dans ce dernier cas et si on a choisi la variante avec encapsulation du paquet IPv4 il faut aussi à cette étape D5 modifier l'adresse IPv4 du paquet encapsulé.

Une nouvelle adresse IPv6 destination est construite en D6 en appliquant le "format de conversion interne" avec comme paramètre l'adresse IPv4 partagée originale extraite en D5 du contexte mémorisée si il y en avait une ou sinon ladite adresse IPv4 destination partagée qui a servi pour la recherche de l'association et comme autre paramètre l'identifiant du sous-réseau qui est une plage de port représentée sur la **Figure 8** comme les bits de poids fort d'un numéro de port.

En D7 le paquet IPv6 est envoyé sur le réseau IPv6.

On notera qu'à l'étape 10 de la **Figure 10**, il est possible que l'équipement de mémorisation des contextes s'envoie lui même un paquet IPv6. Dans ce cas bien entendu les étapes M6, M10 la nouvelle étape M1 la décision et l'étape M2 peuvent être omise puisque la décision conduit forcément dans ce cas à conclure l'adresse

IPv4 partagée qui a été utilisée pour former l'adresse IPv6 au "format de conversion commun sans numéro de port" n'est pas l'adresse source du paquet IPv4, mais son adresse destination. La seule exception à cette règle serait le cas où l'adresse IPv4 partagée source est égale à l'adresse IPv4 destination. Mais dans ce cas le paquet ne sert qu'à ouvrir la communication et peut être détruit.

On comprend que le traitement des contextes de communication qui utilisent des données de contexte est plus compliqué que celui des contextes sans données de contexte. En effet l'existence de données à mémoriser entraine:

- des risques d'attaques en déni de service de l'équipement de mémorisation en augmentant artificiellement le volume de données à stocker jusqu'à ce que celui-ci dépasse la capacité de stockage,
- une complexité accrue pour la sécurisation de cet équipement car il faut alors mettre en place des mécanismes de réplication des données de contexte mémorisées entre l'équipement principal et l'équipement de secours,
- une complexité accrue lors de la gestion du passage à l'échelle, car lorsque le volume de traitement nécessite d'éclater le traitement sur plusieurs équipements il faut alors gérer la répartition des données sur plusieurs équipements,
- des temps de traitement plus importants car il faut réaliser des accès aux données de contexte mémorisées, ce qui limite les possibilités de faire directement les traitements à partir d'éléments matériels (hardware, en anglais).

L'avantage de la solution de l'invention est qu'elle permet d'isoler la fonction de mémorisation dans un seul type d'équipement spécifique, les autres équipements constitutifs du système de routage étant sans état (stateless, en anglais).

7. Cas de datagrammes fragmentés

Un paquet de données est destiné à transporter une séquence de données ou datagrammes. Dans un réseau IPv4, les datagrammes qui sont trop long peuvent être décomposés en plusieurs fragments qui sont transportés par des paquets différents.

Mais, dans ce cas, l'en-tête de la couche transport qui porte les identifiants de port du paquet de données ne figurent que dans le paquet de données IPv4 contenant le premier fragment (ou fragment d'offset 0).

Selon l'invention, le système d'acheminement d'un paquet de données comprend un équipement de mémorisation de fragmentation aptes à mémoriser le numéro de port figurant dans le paquet contenant le premier fragment et à l'associer aux paquets portant les autres fragments. Un tel équipement de mémorisation de fragmentation FM est représenté, en relation avec la **Figure 2**.

Un avantage est qu'ainsi tous les paquets du fragment disposent d'un identifiant de contexte unique pour la communication.

Toutefois, comme les paquets portant les fragments peuvent prendre des chemins différents dans le réseau et arriver dans un ordre différent de l'ordre initial, un mécanisme doit être mis en place pour permettre de :

- regrouper les différents fragments d'un même datagramme vers le même équipement de mémorisation de fragmentation,

-mémoriser les numéros de port, tant que tous les fragments issus du même datagramme ne sont pas traités,

-mémoriser tous les paquets portant un fragment tant que l'on n'a pas reçu le paquet portant le fragment d'offset 0.

Par construction de tels moyens sont donc vulnérables à des attaques en déni de service (envoi d'un ensemble incomplet de fragments). Même si des mesures existent pour limiter ces attaques (durée de conservation limitée dans le temps) il est donc préférable de séparer cette fonction des autres.

De façon avantageuse, le système d'acheminement selon l'invention comprend un équipement de mémorisation de fragmentation apte à communiquer en IPv6 avec les équipements nœuds et comprenant lesdits moyens de mémorisation de fragmentation.

Selon l'invention, on associe un mécanisme de routage IPv6 permettant de regrouper vers cet équipement les paquets contenant des datagrammes fragmentés utilisant la même adresse IPv4 partagée shared_@IPv4.

8. Un exemple de gestion d'un conflit entre deux communications parallèles par l'équipement de mémorisation de contexte

En relation avec la **Figure 2**, on présente un paquet de données P4 émis par un équipement client EC4 possédant une adresse IPv4 partagée shared_@IPv4 au cours d'une communication avec un équipement client destinataire EC1 possédant une adresse IPv4 publique non partagée. On considère que l'adresse IPv4 de l'équipement client émetteur EC4, ou adresse source, est partagée avec une pluralité d'équipements clients et que la communication IP utilise un protocole sans numéro de port. Le contexte qui est associé à cette communication est donc de type avec données. Comme décrit précédemment, le paquet de données P4 est reçu par un équipement nœud EN4 du système d'acheminement selon l'invention. Cet équipement nœud EN4 connaît le sous-réseau de rattachement SR4 de l'équipement émetteur, car il s'agit du sous-réseau avec lequel il est interfacé et il a reçu le paquet via une liaison point à point avec l'équipement client EC4 de ce sous-réseau.

Selon l'invention, il est apte à déterminer le type de contexte de communication qui sera utilisé dans un paquet de données de réponse à ce paquet de données. Pour ce faire, il met en application des règles prédéfinies par l'opérateur du réseau de télécommunications. Pour rappel, le type de contexte est un identifiant avec données.

Il doit donc faire l'objet d'une mémorisation. L'équipement nœud EN4 est apte à convertir le paquet de données IPv4 en un paquet de données P4_IPv6 dont l'adresse de destination IPv6 est construite à partir d'un préfixe spécifique à l'équipement de mémorisation de contexte EM en charge de mémoriser les contextes, et dont l'adresse source IPv6 est construite à partir d'un préfixe spécifique aux équipements nœuds qui résulte de l'application du "format de conversion interne" à l'adresse adresse IPv4 source et à la plage de port qui constitue l'identifiant du sous-réseau SR4 de rattachement de l'équipement client EC4 émetteur du paquet de données P4.

Selon l'invention, le paquet de données IPv6 obtenu est acheminé, jusqu'à un équipement de mémorisation de contexte EM. Cet équipement est apte à extraire du paquet P4_IPv6 l'adresse source IPv6, l'adresse de destination IPv6, l'adresse IPv4

source, l'identifiant de sous-réseau de l'adresse IPv4 source et l'adresse IPv4 destination.

1. il recherche dans sa base de données s'il existe une entrée correspondant au couple (adresse source shared@IPv4, identifiant de contexte), l'identifiant de contexte étant par exemple égal à l'adresse de destination IPv4.

1.2. Si cette entrée existe et fait correspondre au couple ci-dessus le même identifiant de sous-réseau ID-SR4, alors l'équipement de mémorisation de contexte a déjà mémorisé le contexte associé à cette communication entre l'équipement client EC4 et l'équipement client destinataire EC1. Il n'a donc pas de donnée de contexte supplémentaire à mémoriser pour l'adresse IPv4 source.

1.3 On considère maintenant le cas où l'entrée correspondant au couple (adresse source shared@IPv4, adresse de destination IPv4) existe, mais associe un autre identifiant de sous-réseau que l'identifiant du sous-réseau SR4, par exemple l'identifiant du sous-réseau SR3. On comprend qu'il existe déjà une première communication en cours entre les deux adresses IPv4 partagées, par exemple celle de l'équipement client EC3 et celle de l'équipement client EC4. Il y a donc un risque de conflit.

Selon un mode de réalisation de l'invention, l'équipement de mémorisation de contexte EM est apte à remplacer l'adresse IPv4 source partagée par une nouvelle adresse IPv4 New@IPv4 appartenant à un ensemble ou pool d'adresses IPv4 qui lui est réservé.

Il enregistre donc une nouvelle entrée dans sa base de données associant au couple (New@IPv4, adresse IPv4 de destination) l'identifiant de sous-réseau de rattachement ID-SR4 et l'adresse IPv4 source partagée d'origine shared@IPv4.

Il modifie en outre l'adresse source du paquet de données IPv6 en remplaçant l'adresse source shared@IPv4 par la nouvelle adresse New@IPv4.

Il reprend ensuite le traitement du paquet de données IPv6, en particulier la construction de l'adresse IPv6 de destination comme décrit sur la Figure 10.

On comprend que lorsqu'un paquet de données de réponse sera reçu par l'équipement de mémorisation de contexte EM, son adresse de destination IPv6 comprendra l'adresse IPv4 New@IPv4. L'équipement EM interrogera la base de données à partir du couple (New@IPv4, EC2@IPv4) et il obtiendra l'identifiant de sous-réseau ID-SR4 et l'adresse IPv4 shared@IPv4 de l'équipement client destinataire EC4. Il pourra ainsi modifier l'adresse de destination IPv6 du paquet en utilisant le format de conversion interne désignant les équipements nœuds, l'adresse de destination shared@IPv4 et l'identifiant de sous-réseau. Le paquet de données IPv6 obtenu pourra être acheminé jusqu'à l'équipement nœud EN4, converti en IPv4 par ce dernier et routé de façon standard jusqu'à l'équipement destinataire EC4.

On comprend que la situation de conflit qui vient d'être décrite a d'autant plus de chances de survenir que l'équipement client impliqué dans les deux communications est populaire et que lorsqu'elle survient elle consomme une nouvelle adresse IPv4 (pour l'équipement situé sur le sous-réseau SR4 dans notre exemple) ce qui va à l'encontre de notre objectif d'économiser les adresses IPv4.

9. Cas des interfaces compatibles

Selon l'invention, certains équipements clients possèdent une adresse IPv4 publique et une interface avec le réseau public IPv6 dotée d'une adresse IPv6 spécifique pour recevoir des paquets IPv4 qui ont été convertis en IPv6.

Si, de plus, ces équipements répondent à ces paquets IPv6 par d'autres paquets IPv6 qui sont la conversion en IPv6 des paquets de réponse IPv4, mais avec une adresse destination IPv6 qui est l'adresse IPv6 source des paquets reçus et si de plus ils possèdent un mécanisme qui leur permet de communiquer cette adresse IPV6 et de faire savoir qu'elle est associée à une interface destinée à recevoir des paquets IPv4 destiné à cette adresse IPv4 et convertis en paquets IPv6, on parlera de full_compatible_interface.

Une telle interface est particulièrement avantageuse pour les équipements clients populaires qui reçoivent beaucoup de communication sans numéro de port.

Un équipement client possédant une interface compatible est donc un équipement dit "dual stack IPv4/IPv6", ce qui signifie qu'il est à la fois apte à communiquer selon les protocoles IPv4 et IPv6.

Un tel équipement client possède donc :

- une adresse IPv4 publique non partagée que l'on dira associée à la full_compatible_interface;
- une interface IPv6 qui est la full_compatible_interface;
- une adresse IPv6 qui est l'adresse de la full_compatible_interface.
- un mécanisme qui lui permet de faire connaître à ses correspondants l'adresse IPv6 de la full_compatible_interface associée à son adresse IPv4.

Il est également préférable d'affecter l'adresse IPv6 obtenue en appliquant à l'adresse IPv4 publique associée à la full_compatible_interface le "format de conversion commun sans numéro de port". Il est préférable que cette adresse soit différente de l'adresse IPv6 de la full_compatible_interface. En effet l'adresse destination des paquets IPv6 envoyés en réponse à des paquets dont l'adresse IPv6 a été obtenue en appliquant le "format de conversion commun sans numéro de port" doit être l'adresse IPv6 obtenue en appliquant le "format de conversion commun sans numéro de port" à l'adresse IPv4 destination.

On notera cependant que c'est bien cette adresse IPv6 obtenue en appliquant le "format de conversion commun sans numéro de port" à l'adresse IPv4 associée à la full_compatible_interface qui sera utilisée comme adresse source des paquets IPv6 envoyés par la full_compatible_interface.

Il existe de nombreux mécanismes permettant de faire connaître l'adresse IPv6 de la full_compatible_interface associé à une adresse IPv4 tels que la publication de cette association sur un serveur. Cependant un mécanisme qui consisterait à renvoyer au correspondant un paquet IPv4 avec une caractéristique spécifique permettant de le reconnaître et contenant l'adresse IPv6 de la full_compatible_interface et converti en un paquet IPv6 dont l'adresse IPv6 destination serait l'adresse IPv6 obtenue en appliquant le "format de conversion commun sans numéro de port" appliquée à l'adresse IPv4 du correspondant serait préférable (on notera au passage que ce n'est

pas la méthode normale de réponse aux paquets envoyés à la full_compatible_interface mais c'est la méthode de réponse aux paquets envoyés à l'adresse IPv6 obtenue en appliquant le "format de conversion commun sans numéro de port" à l'adresse IPv4 associée à la full_compatile_interface).

En relation avec la **Figure 12**, on considère un équipement client EC1 du réseau IPv4 public. Cet équipement possède une full_compatible_interface. On suppose qu'un équipement client EC3 possédant l'adresse shared@IPv4 partagée établit une communication avec l'équipement client EC1. Au cours de cette communication, l'équipement client EC3 envoie un paquet de données P3 à l'équipement client EC1. On suppose que ce paquet de données ne possède pas de numéro de port.

Selon l'invention, le paquet de données est converti en un paquet IPv6 par un équipement nœud EN3 et envoyé à un équipement de mémorisation de contexte EM. On suppose qu'au moins une communication est déjà en cours entre l'équipement EC1 possédant la full_compatible_interface et un équipement client EC4 partageant la même adresse IPv4 shared@IPv4 que l'équipement client EC3.

Selon l'invention, l'équipement de mémorisation de contexte EM a appris lors de l'établissement de la communication entre les équipements clients EC3 et EC1 que l'équipement client EC1 dispose d'une full_compatible_interface dont il a appris et mémorisé l'adresse IPv6.

Cela n'a rien changé pour la communication entre EC3 et EC1.

En revanche lorsqu'il reçoit un paquet en provenance d'EC4 à destination d'EC1, et qu'il constate qu'il existe déjà une association entre l'adresse IPv4 partagée, l'adresse IPv4 d'EC1 et l'identifiant de sous réseau SR3. Au lieu d'attribuer une nouvelle adresse IPv4 source et de mémoriser un contexte il se contente d'utiliser l'adresse IPv6 de la full_compatible_interface comme adresse de destination IPv6.

On notera que l'adresse source du paquet IPv6 qui n'a pas été modifiée est toujours l'adresse IPv6 qui a été construite par l'équipement EN4. C'est donc une adresse IPv6 construite en utilisant le format de conversion interne et elle est routée

sur le réseau IPv6 vers EN4. La réponse de la full_compatible_interface sera donc routée en IPv6 vers EN4 sans jamais emprunter le réseau IPv4 public et sans avoir besoin de passer par l'équipement de mémorisation des contextes. L'objectif d'économie des adresses IPv4 est bien préservé dans ce cas.

10. L'annonce des préfixes IPv6 sur le réseau

Chaque adresse IPv6 ayant un préfixe on peut, par abus de langage, considérer qu'il existe des préfixes IPV6 associés à chaque format (ou des formats de préfixe). Ces préfixes peuvent permettre de diffuser les capacités et les modes de traitements qui doivent être appliqués aux adresses IPV4 partagées. Les informations concernant l'existence de ces préfixes et leur étendue peuvent être, tout simplement, distribuées sur le réseau IPV6 par le biais des informations de routage IPV6.

Chaque format peut exister sous deux formes:

- posséder des préfixes inclus dans un préfixe IPv6 propre à l'opérateur. Cette information de format est alors destinée à être partagée au sein du réseau IPv6 de cet opérateur, mais n'a pas vocation à être interprétée au-delà;
- avec un préfixe inclus dans un préfixe commun, à plusieurs opérateurs qui devront alors partager une politique commune de gestion de ce préfixe. Ce mode est d'autant plus intéressant que la communauté des opérateurs est étendue. L'idéal serait même que cette communauté soit celle de l'internet et que ce préfixe soit assigné par l'IANA.

Il suffit alors de vérifier que l'adresse IPV6 générée en appliquant un format à un couple (shared_@IPv4, port) ou (shared_@IPv4, identifiant de sous-réseau) ou à une shared_@IPv4 seule (suivant le format) est bien dans l'étendue d'un préfixe annoncé pour en déduire que l'adresse shared_@IPv4 possède les caractéristiques et les capacités qui caractérisent ce format. De plus si l'algorithme est bien conçu et pour les formats qui sont destinés à être échangés avec d'autres opérateurs, il n'est pas nécessaire de connaître la valeur de l'identifiant de sous-réseau pour déterminer cette information de format.

Pour éviter que les tables de routages IPv6 ne deviennent trop grandes, ces préfixes IPv6 peuvent être agrégés et englober lors de cette opération des adresses IPv6, construites en appliquant le common_format à des adresses IPv4, pour lesquelles l'opérateur, qui fait l'agrégation, n'a reçu aucun préfixe sur le réseau IPv6. Dans ce cas cette agrégation est autorisée à condition que l'opérateur qui la réalise mette en place une route pour ces adresses IPv6 vers un nœud interfacé avec le réseau public IPv4.

Les informations qui peuvent être déduites de l'annonce d'un préfixe common_format sont les suivantes :

L'inclusion d'une adresse IPv4 dans un préfixe de ce type annoncé sur le réseau IPV6 signifie que l'opérateur qui annonce ce préfixe est prêt à recevoir, via le réseau IPv6, des communications vers ces interfaces pour des protocoles utilisant un numéro de port. Il met à disposition les équipements nœuds nécessaires pour permettre d'acheminer les communications du réseau IPV6 conformes à ce format d'encapsulation vers cette adresse IPV4. On peut noter que :

L'annonce de ce préfixe ne fournit aucune indication sur la nature de l'adresse IPV4 qui peut aussi bien être une adresse IPv4 normale qu'une adresse partagée Shared_@IPv4.

L'annonce d'un format commun de type common_portless_format et l'inclusion d'une adresse IPv4 dans un préfixe de ce type annoncé sur le réseau IPV6 signifie que l'opérateur qui annonce ce préfixe est prêt à recevoir, via le réseau IPv6, des communications vers cette interfaces pour des protocoles n'utilisant pas de numéro de port. Il met à disposition les équipements nœuds nécessaires pour permettre d'acheminer les communications du réseau IPV6 et n'utilisant pas de numéro de port, conformes à ce format d'encapsulation vers cette adresse IPV4. Les autres règles, en particulier la règle d'agrégation sont identiques à celle du common_format.

11. Extension à des équipements clients "dual-stack"

Une variante possible du système d'acheminement selon l'invention qui vient d'être décrit, concerne le raccordement d'équipements clients possédant une interface

IPv4 partagée et une interface IPv6. On considère, en particulier, le cas de passerelles domestiques "dual stack" aptes à communiquer avec des équipements clients IPv6 et avec des équipements terminaux de leur réseau domestique qui peuvent être IPv4 et/ou IPv6. Dans cette variante, une telle passerelle domestique joue normalement son rôle de passerelle IPv4 privé vers IPv4 public partagé pour les équipements clients IPv4 de son réseau domestique qui souhaitent communiquer avec des équipements clients destinataires IPv4 d'un autre sous-réseau. Mais la passerelle domestique joue aussi le rôle d'équipement nœud interfacé avec le sous réseau constitué de cette seule adresse IPv4 partagée. On comprend que, dans cette variante, le client constitue à lui seul un sous-réseau IPv4 au sens de l'invention.

A titre d'exemple, on suppose que le mode de partage des adresses IPv4 se fait selon un mode de partage des numéros de ports spécifique, de façon à ce que des plages de ports spécifiques soient réservées à ce type d'équipement client.

Toutes les adresses IPv6 construites en appliquant la technique de conversion IPv4/ IPv6 common_format précédemment évoquée, à partir :
d'une adresse IPv4 partagée selon le mode de partage spécifique ;
et d'un numéro de port contenu dans la plage correspondant à un sous-réseau donné;
seront attribuées comme adresse IPv6 natives à l'interface IPv6 de la passerelle domestique du sous-réseau virtuel à laquelle cette adresse IPv4 partagée a été attribuée.

Dans ce cas les fonctions de conversion IPv4/IPv6 et conversion inverse IPv6/IPv4 d'un paquet de données sont intégrés dans la passerelle domestique.

Une telle variante constitue une évolution du système d'acheminement de paquets de données selon l'invention, qui permet de s'adapter au remplacement progressif de passerelles domestiques clientes IPv4 en passerelles domestiques IPv6 et plus généralement, à la migration progressive vers le tout IPv6.

REVENDICATIONS

1. Système d'acheminement d'un paquet de données IPv4 émis par un équipement client source à destination d'un équipement client destinataire au cours d'une communication établie dans un réseau de télécommunications IPv4 d'un opérateur, ledit équipement client destinataire possédant une adresse publique IP partagée avec d'autres équipements clients connectés audit réseau IPv4, caractérisé en ce que :

- ledit réseau IPv4 est décomposé en une pluralité de sous-réseaux;
- la pluralité d'équipements clients partageant ladite adresse IPv4 est rattaché à ladite pluralité de sous-réseaux, de façon à connecter au plus un desdits équipements clients par sous-réseau; et
- ledit système comprend :
  - des moyens d'envoi du paquet de données IPv4 par une liaison point à point établie entre l'équipement client émetteur et des moyens d'identification du sous-réseau de rattachement de l'équipement destinataire;
  - des moyens d'identification du sous-réseau de rattachement de l'équipement client destinataire du paquet, à partir de l'adresse IPv4 de destination et d'un identifiant de contexte IPv4 de ladite communication contenu dans le paquet de données reçu de l'équipement client source; et
  - des moyens d'acheminement dudit paquet IPv4 vers le sous-réseau identifié.

2. Système d'acheminement selon la revendication **1**, caractérisé en ce que, lorsque le paquet de données IPv4 comprend une adresse de destination IPv4 partagée et un numéro de port appartenant à une plage de numéros de ports, ladite plage de numéros de ports étant affectée de façon unique au sous-réseau de l'équipement destinataire, ledit identifiant de contexte est ledit numéro de port.

3. Système d'acheminement selon la revendication **1**, caractérisé en ce que le paquet de données comprenant une deuxième adresse IPv4, l'identifiant de contexte est ladite deuxième adresse IPv4 du paquet de données.

4. Système d'acheminement selon la revendication **1**, caractérisé en ce que, le paquet de données appartenant à un datagramme et comprenant un identifiant dudit

datagramme, ledit identifiant de contexte est ledit identifiant de datagramme.

5. Système d'acheminement selon la revendication **1**, caractérisé en ce qu'il comprend un équipement nœud comprenant une interface avec chacun desdits sous-réseaux.

6. Système d'acheminement selon la revendication **1**, caractérisé en ce que ledit système comprend une pluralité d'équipements nœuds aptes à communiquer entre eux par l'intermédiaire d'un réseau de télécommunications IPv6 et tel que pour chaque sous-réseau de ladite pluralité de sous-réseaux il existe au moins un équipement nœud comprenant une interface avec ce sous-réseau.

7. Système d'acheminement selon la revendication **6**, caractérisé en ce que, sur réception d'un paquet de données en provenance du sous-réseau avec lequel il est interfacé, un premier équipement nœud est apte à mettre en œuvre :

- des moyens de détermination d'un type de contexte de l'adresse de destination IPv4 partagée;
- des moyens de conversion du paquet de données IPv4 reçu de l'équipement client émetteur en un paquet de données IPv6, ledit paquet comprenant une adresse IPv6 de destination construite à partir de l'adresse IPv4 partagée source, de l'adresse IPv4 de destination et de l'identifiant de contexte et d'un préfixe opérateur, ledit préfixe étant choisi en fonction du type de contexte déterminé; et
- des moyens d'envoi du paquet de données IPv6 obtenu dans le réseau IPv6.

8. Système d'acheminement selon la revendication **6**, caractérisé en ce qu'il comprend au moins un équipement de mémorisation d'une association entre ladite adresse IPv4 partagée, l'identifiant de contexte IPv4 de la communication et l'identifiant de sous-réseau de rattachement de l'équipement client possédant ladite adresse partagée, ledit équipement étant apte à fournir, sur réception d'une requête comprenant l'adresse IPv4 partagée et l'identifiant de contexte IPv4, au moins l'identifiant de sous-réseau.

9. Système d'acheminement selon les revendications **7** et **8**, caractérisé en ce que: Lorsque l'adresse IPv4 source est une adresse partagée, ledit premier équipement

nœud est apte à déterminer un type de contexte de l'adresse IPv4 source, et

lorsque le type de contexte déterminé est un contexte avec données, le premier équipement nœud est apte à choisir le préfixe de l'adresse de destination du paquet de données IPv6 converti de façon à ce qu'il parvienne audit équipement de mémorisation de contexte pour mémorisation d'une association entre ladite adresse source IPv4 partagée, ledit identifiant de contexte et une donnée de contexte identifiant de sous-réseau de rattachement de l'équipement client source.

10. Système d'acheminement selon la revendication **8**, caractérisé en ce que au moins un équipement de mémorisation de contexte est apte, sur réception d'un paquet de données IPv6 en provenance d'un desdits équipements nœuds, à mettre en œuvre :

- des moyens d'extraction de l'adresse de destination IPv4 partagée et de l'identifiant de contexte,
- des moyens de détermination d'un type de contexte associé au paquet de données IPv6 reçu parmi un contexte sans données et un contexte avec données;
- si le type de contexte déterminé est un contexte avec données, des moyens de recherche dans la base de données d'une association entre ladite adresse IPv4 de destination, ledit identifiant de contexte et un identifiant du sous-réseau de rattachement de l'équipement client destinataire;
- si une association a été trouvée, des moyens de remplacement de l'adresse de destination du paquet de données IPv6 par une adresse IPv6 construite à partir de l'adresse de destination partagée, de l'identifiant de sous-réseau trouvé et d'un préfixe opérateur.

11. Système d'acheminement selon la revendication **10**, caractérisé en ce que, sur réception d'un paquet de données IPv6 en provenance d'un desdits équipements nœuds et comprenant une adresse IPv4 source partagée, ledit équipement de mémorisation de contexte est apte à mettre en œuvre :

- des moyens d'extraction de l'adresse source IPv4 partagée et de l'identifiant de contexte,
- des moyens de détermination d'un type de contexte associé, parmi un contexte sans

données et un contexte avec données;

- si le type de contexte déterminé est un contexte avec données, des moyens de recherche dans la base de données d'une association entre ladite adresse IPv4 source, ledit identifiant de contexte et un identifiant du sous-réseau avec lequel ledit équipement nœud est interfacé;

- si aucune association n'a été trouvée, des moyens d'enregistrement d'une association entre ladite adresse source IPv4 partagée, l'identifiant de contexte et l'identifiant de sous-réseau;

-si une association a été trouvée comprenant l'identifiant de sous-réseau, des moyens de remplacement de l'adresse destination du paquet de données IPv6 par une adresse IPv6 construite à partir de l'adresse IPv4 de destination, et d'un préfixe opérateur adapté; et

- si une association a été trouvée comprenant un autre identifiant de sous-réseau, des moyens de remplacement de l'adresse IPv4 source partagée par une autre adresse IPv4 et des moyens d'enregistrement d'une association entre ladite autre adresse IPv4, l'identifiant de contexte, l'identifiant de sous-réseau et l'adresse IPv4 partagée.

12. Equipement nœud d'un système d'acheminement d'un paquet de données à destination d'un équipement client destinataire et un équipement client destinataire, dans un réseau de télécommunications IPv4, l'un au moins desdits équipements clients possédant une adresse publique IPv4 partagée avec d'autres équipements clients connectés audit réseau IPv4, caractérisé en ce que :

- ledit réseau IPv4 est décomposé en une pluralité de sous-réseaux;

- la pluralité d'équipements clients partageant ladite adresse IPv4 est rattaché à ladite pluralité de sous-réseaux, de façon à connecter au plus un desdits équipements clients par sous réseau,

Ledit système comprend une pluralité d'équipements nœuds aptes à communiquer entre par l'intermédiaire d'un réseau IPv6,

Ledit équipement nœud comprend :

des premiers moyens de communication avec un desdits sous réseaux IPV4;

des seconds moyens de communication avec d'autres équipements nœuds

dudit système par l'intermédiaire d'un réseau de télécommunication IPv6;

Des moyens de détermination d'un type de contexte de l'adresse de destination IPv4 partagée, aptes à être mis en œuvre sur réception d'un paquet de données IPv4 sur lesdits premiers moyens de communication;

des moyens de conversion du paquet de données IPv4 reçu sur lesdits premiers moyens en un paquet de données IPv6, ledit paquet comprenant une adresse IPv6 de destination construite à partir de l'adresse IPv4 partagée source, l'adresse IPv4 de destination et de l'identifiant de contexte et d'un préfixe opérateur, ledit préfixe étant choisi en fonction du type de contexte déterminé; et

Des moyens d'envoi du paquet de données IPv6 obtenu sur les deuxièmes moyens de communication.

13. Equipement nœud selon la revendication **12**, caractérisé en ce qu'il comprend des moyens de conversion inverse d'un paquet de données IPv6 comprenant une adresse IPv4 de destination partagée et un identifiant de contexte, en un paquet de données IPv4 comprenant ladite adresse de destination et l'identifiant de contexte, lesdits moyens de conversion inverses étant aptes à être mis en œuvre sur réception du paquet de données sur les deuxièmes moyens de communication, et des moyens d'envoi du paquet de données IPv4 obtenu sur les premiers moyens de communication dans le sous réseau IPv4 interfacé avec ledit équipement nœud.

14. Procédé de traitement d'un paquet de données IPv4 émis par un équipement client source à destination d'un équipement client destinataire au cours d'une communication établie dans un réseau de télécommunications IPv4 d'un opérateur, ledit équipement client destinataire possédant une adresse publique IP partagée avec d'autres équipements clients connectés audit réseau IPv4, caractérisé en ce que :

- ledit réseau IPv4 est décomposé en une pluralité de sous-réseaux;
- la pluralité d'équipements clients partageant ladite adresse IPv4 est rattaché à ladite pluralité de sous-réseaux, de façon à connecter au plus un desdits équipements clients par sous-réseau;

Ledit système comprend une pluralité d'équipements nœuds aptes à communiquer entre par l'intermédiaire d'un réseau IPv6,

et

Ledit procédé étant apte à être mis en œuvre par un desdits équipements nœuds et comprenant les étapes suivantes :

- détermination d'un type de contexte de l'adresse de destination IPv4 partagée, destinée à être mise en œuvre sur réception d'un paquet de données IPv4 en provenance d'un sous-réseau IPv4;
- conversion du paquet de données IPv4 reçu en un paquet de données IPv6, ledit paquet comprenant une adresse IPv6 de destination construite à partir de l'adresse IPv4 partagée source, de l'adresse IPv4 de destination et d'un préfixe opérateur, ledit préfixe étant choisi en fonction du type de contexte déterminé; et
- envoi du paquet de données IPv6 obtenu dans le réseau IPv6.

15. Procédé de traitement selon la revendication **14**, caractérisé en ce qu'il comprend en outre les étapes suivantes, mises en œuvre sur réception d'un paquet de données IPv6 en provenance du réseau IPv6 :

- conversion inverse du paquet de données IPv6 comprenant une adresse IPv4 de destination partagée et un identifiant de sous-réseau de rattachement de l'équipement client destinataire, en un paquet de données IPv4 comprenant ladite adresse de destination et l'identifiant de contexte, et
- envoi du paquet de données IPv4 obtenu dans le sous réseau IPv4 interfacé avec ledit équipement nœud.

16. Procédé de mémorisation d'un contexte de communication associé à une adresse IPv4 source d'un paquet de données émis par un équipement client à destination d'un équipement client destinataire au cours d'une communication établie dans un réseau de télécommunication IPv4, ladite adresse étant partagée avec d'autres équipements clients connectés audit réseau IPv4 et ledit paquet comprenant un identifiant de contexte de la communication, caractérisé en ce que :

- ledit réseau IPv4 est décomposé en une pluralité de sous-réseaux;

- la pluralité d'équipements clients partageant ladite adresse IPv4 est rattaché à ladite pluralité de sous-réseaux, de façon à connecter au plus un desdits équipements clients par sous-réseau;

ledit procédé de mémorisation de contexte comprenant les étapes suivantes mises en œuvre sur réception d'un paquet de données comprenant ladite adresse IPv4 partagée:

- des moyens d'extraction de l'adresse source IPv4 partagée et de l'identifiant de contexte,

- des moyens de détermination d'un type de contexte associé, parmi un contexte sans données et un contexte avec données;

- si le type de contexte déterminé est un contexte avec données, des moyens de recherche dans la base de données d'une association entre ladite adresse IPv4 source, ledit identifiant de contexte et un identifiant du sous-réseau avec lequel ledit équipement nœud est interfacé;

- si aucune association n'a été trouvée, des moyens d'enregistrement d'une association entre ladite adresse source IPv4 partagée, l'identifiant de contexte et l'identifiant de sous-réseau;

-si une association a été trouvée comprenant l'identifiant de sous-réseau, des moyens de remplacement de l'adresse destination du paquet de données IPv6 par une adresse IPv6 construite à partir de l'adresse IPv4 de destination, et d'un préfixe opérateur adapté; et

- si une association a été trouvée comprenant un autre identifiant de sous-réseau, des moyens de remplacement de l'adresse IPv4 source partagée par une autre adresse IPv4 et des moyens d'enregistrement d'une association entre ladite autre adresse IPv4, l'identifiant de contexte, l'identifiant de sous-réseau et l'adresse IPv4 partagée.

17. Produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution du procédé d'émission d'un paquet de données selon la revendication **14**.

18. Produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution du procédé de mémorisation d'un contexte d'un paquet de données selon la revendication **16**.

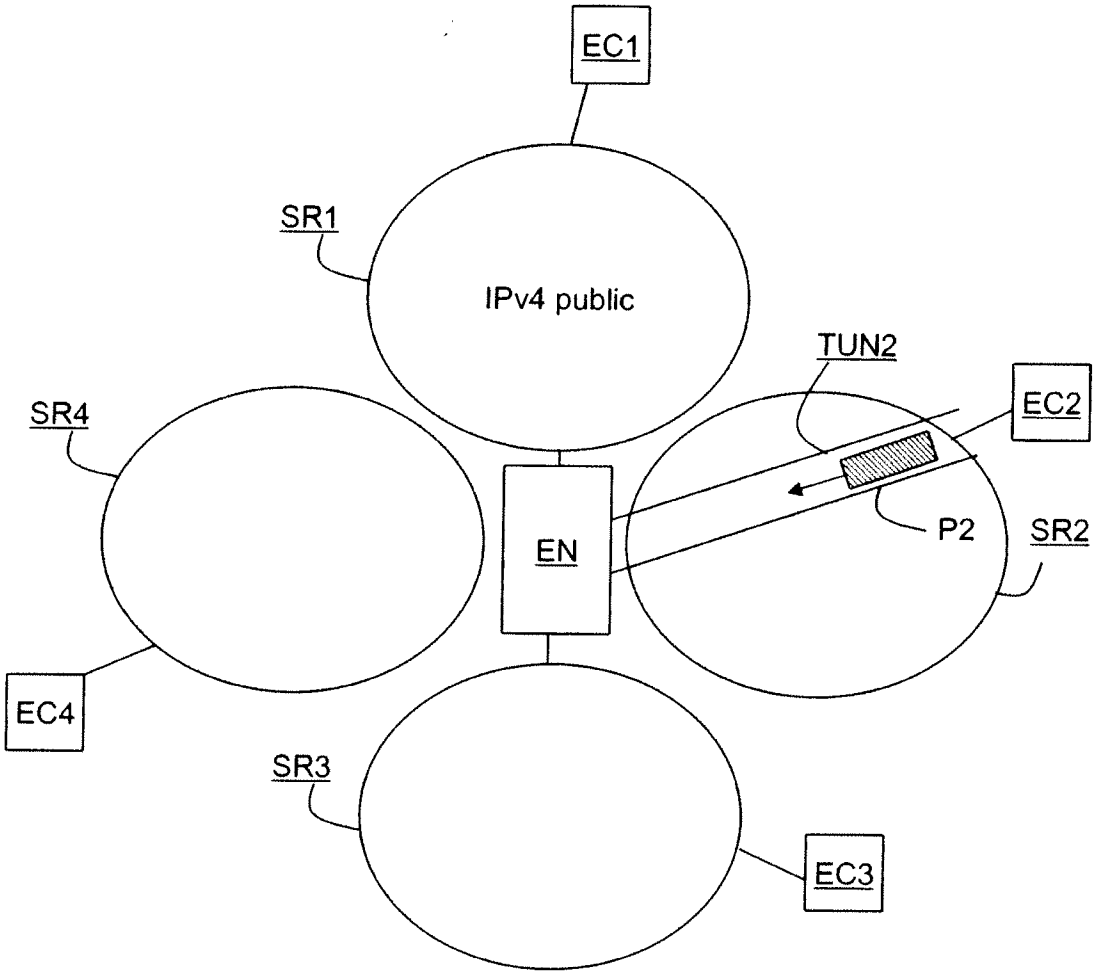

FIG.1

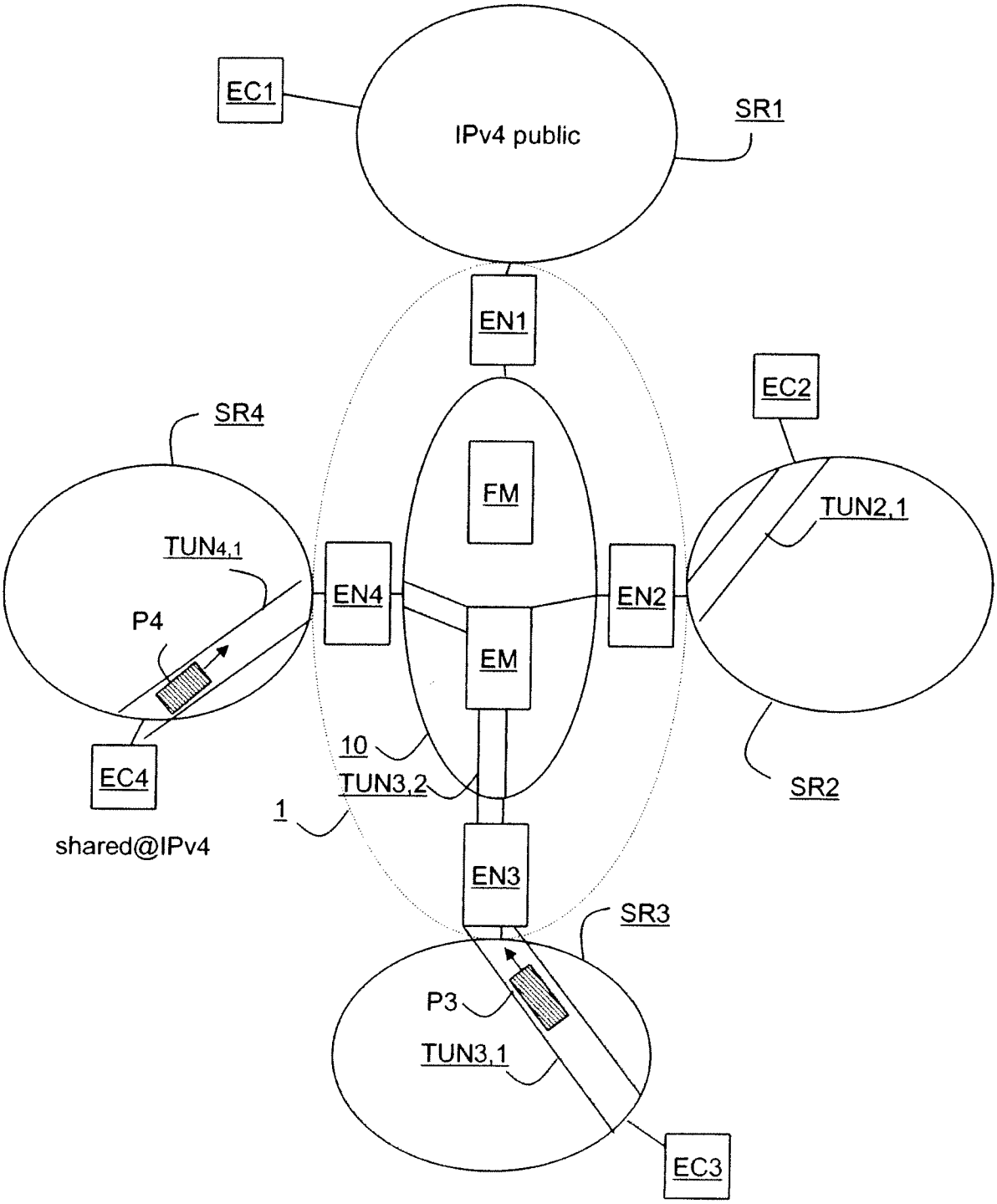
EC1
IPv4 public
SR1
EN1
EC2
SR4
FM
TUN2,1
TUN4,1
EN4
EN2
P4
EM
EC4
10
TUN3,2
SR2
1
shared@IPv4
EN3
SR3
P3
TUN3,1
EC3

FIG.2

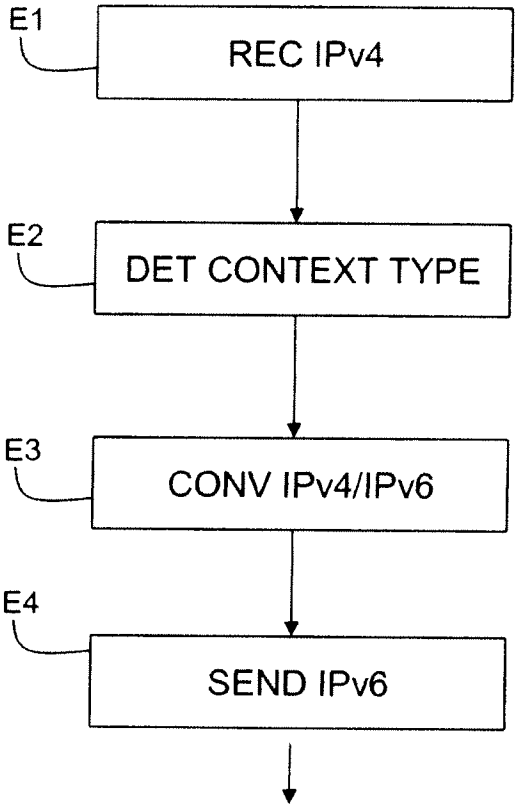
E1
REC IPv4
E2
DET CONTEXT TYPE
E3
CONV IPv4/IPv6
E4
SEND IPv6

FIG.3

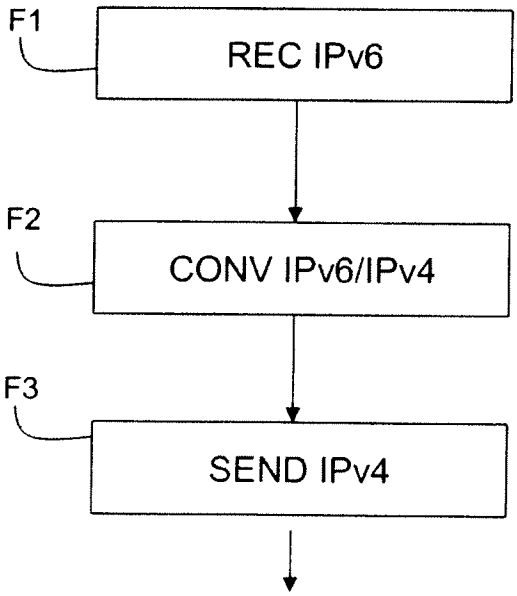
F1
REC IPv6
F2
CONV IPv6/IPv4
F3
SEND IPv4

FIG.4

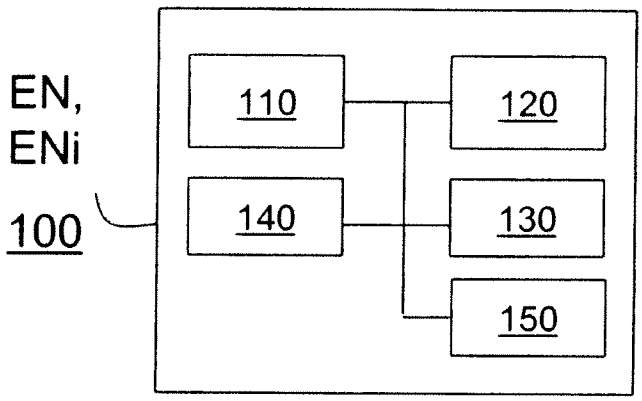
EN,
ENi
100
110
120
140
130
150

FIG.5

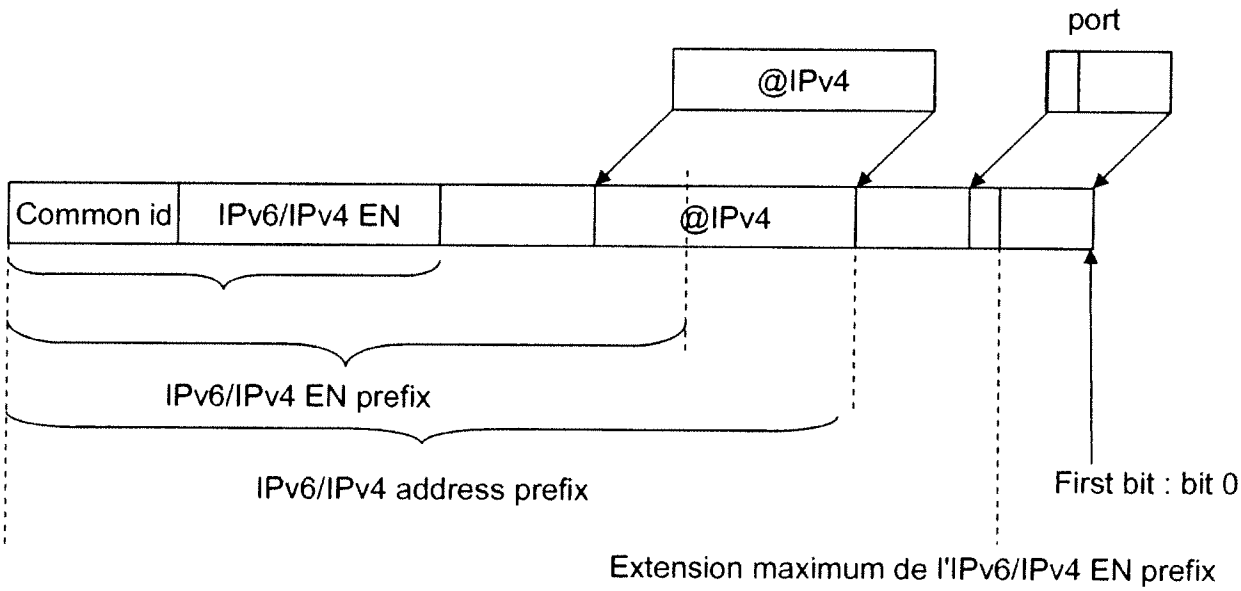
port
@IPv4
Common id
IPv6/IPv4 EN
@IPv4
IPv6/IPv4 EN prefix
IPv6/IPv4 address prefix
First bit : bit 0
Extension maximum de l'IPv6/IPv4 EN prefix

FIG. 6

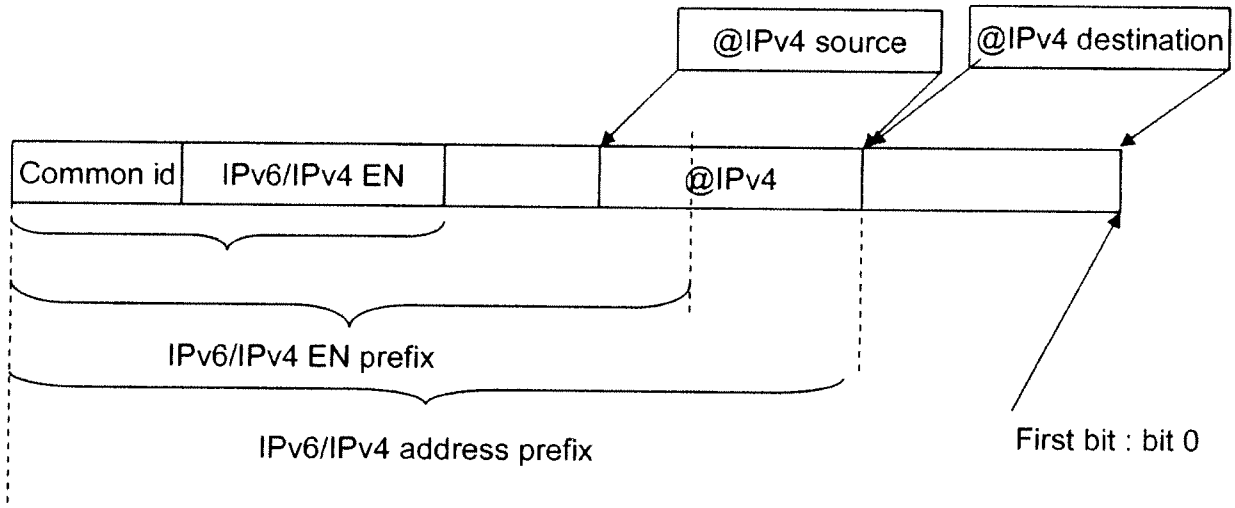
@IPv4 source
@IPv4 destination
Common id
IPv6/IPv4 EN
@IPv4
IPv6/IPv4 EN prefix
IPv6/IPv4 address prefix
First bit : bit 0

FIG. 7

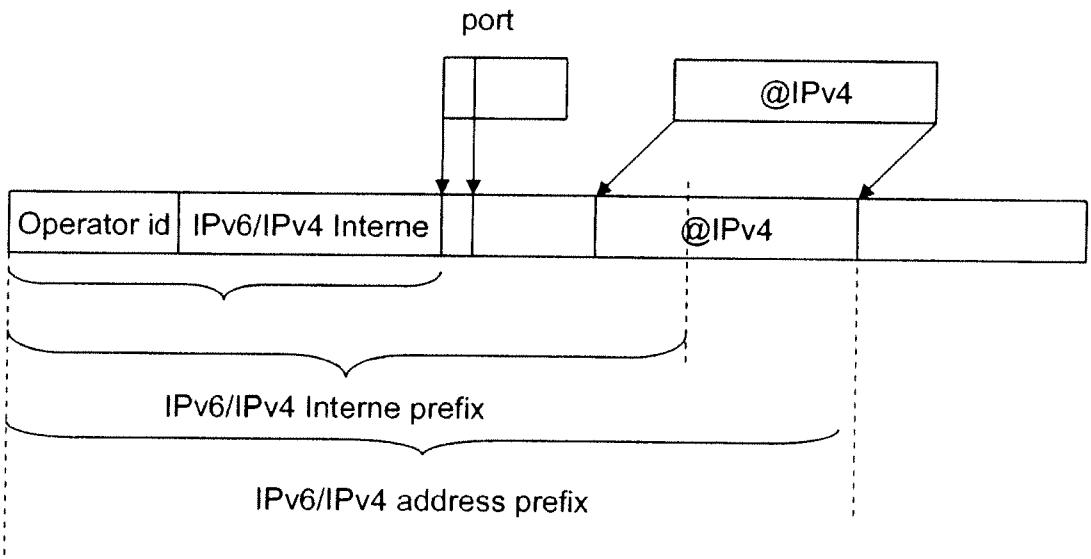
port
@IPv4
Operator id
IPv6/IPv4 Interne
@IPv4
IPv6/IPv4 Interne prefix
IPv6/IPv4 address prefix

FIG. 8

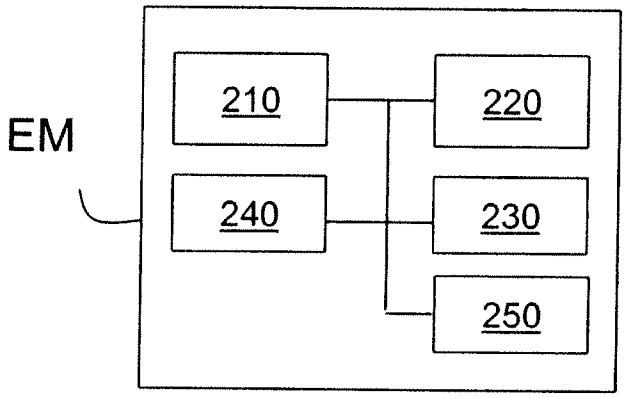

FIG. 9

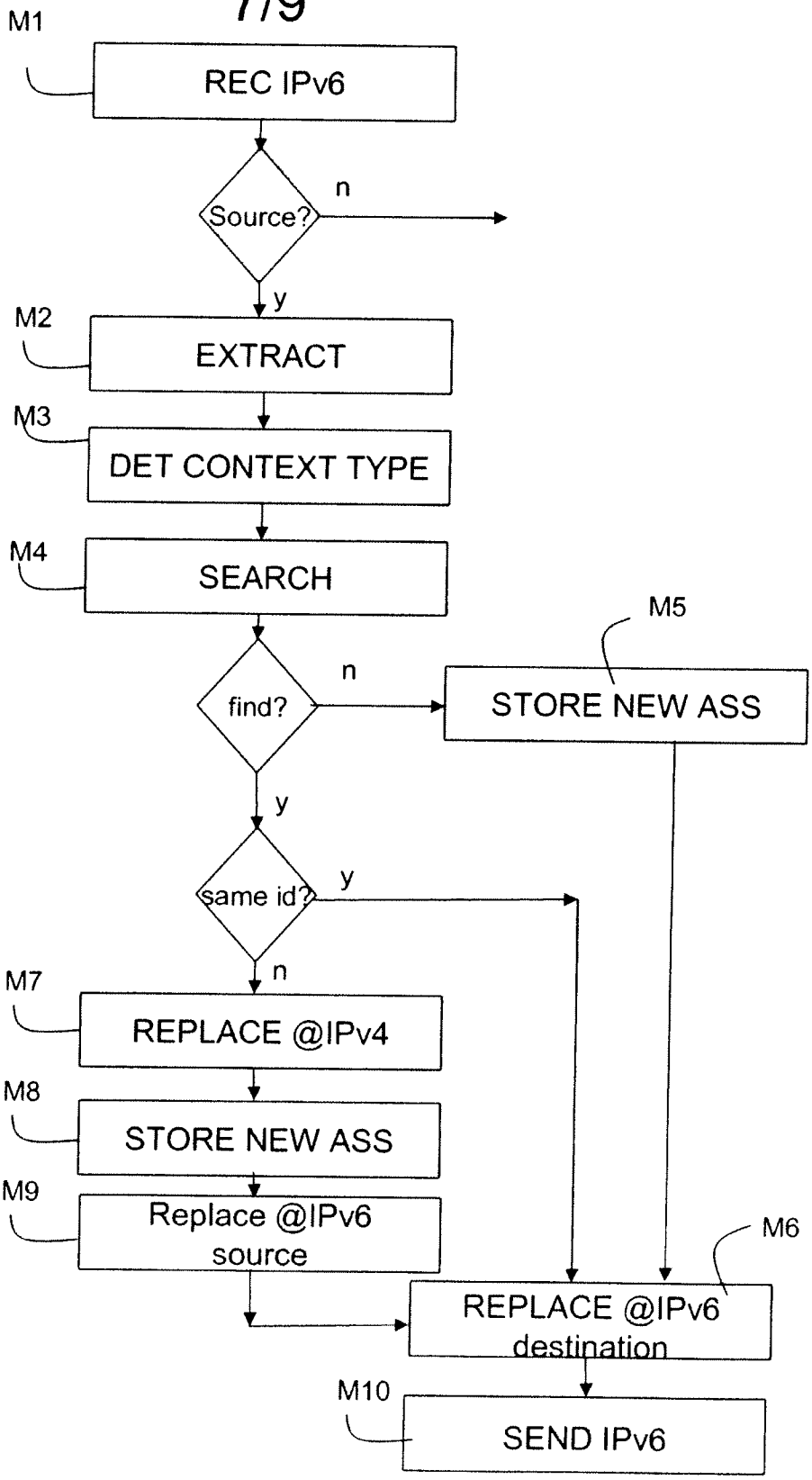
M1
REC IPv6
Source?
n
y
M2
EXTRACT
M3
DET CONTEXT TYPE
M4
SEARCH
M5
find?
n
STORE NEW ASS
y
same id?
y
n
M7
REPLACE @IPv4
M8
STORE NEW ASS
M9
Replace @IPv6 source
M6
REPLACE @IPv6 destination
M10
SEND IPv6

FIG. 10

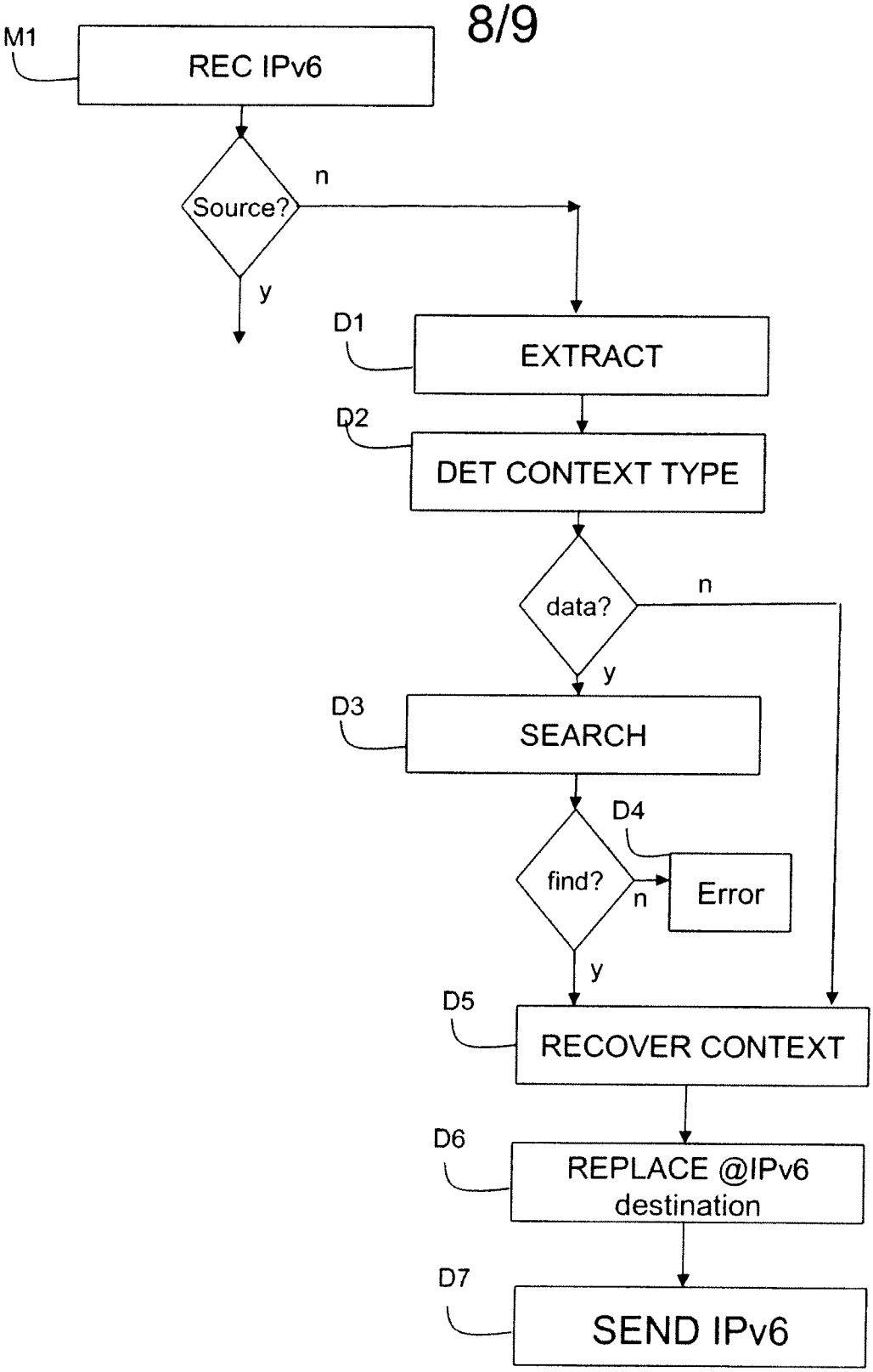
M1
REC IPv6
Source?
n
y
D1
EXTRACT
D2
DET CONTEXT TYPE
data?
n
y
D3
SEARCH
D4
find?
n
Error
y
D5
RECOVER CONTEXT
D6
REPLACE @IPv6 destination
D7
SEND IPv6

FIG. 11

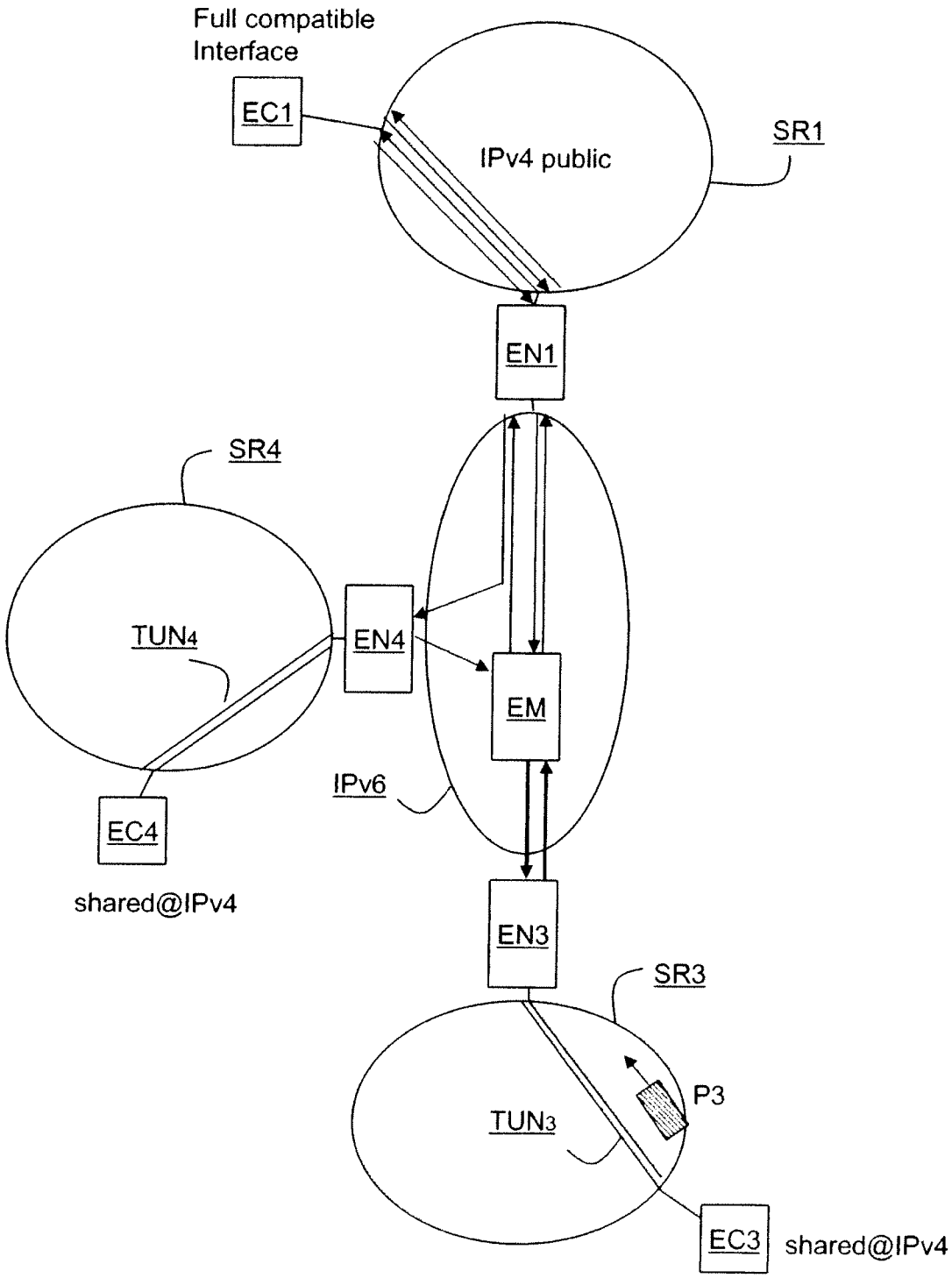
Full compatible
Interface
EC1
IPv4 public
SR1
EN1
SR4
TUN4
EN4
EM
IPv6
EC4
shared@IPv4
EN3
SR3
P3
TUN3
EC3
shared@IPv4

FIG. 12

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/052609

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CÉDRIC DE LAUNOIS ET AL: "Connection of Extruded Subnets: A Solution Based on RSIP" NETWORKING 2002: NETWORKING TECHNOLOGIES, SERVICES, AND PROTOCOLS; PERFORMANCE OF COMPUTER AND COMMUNICATION NETWORKS; MOBILE AND WIRELESS COMMUNICATIONS; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, vol. 2345, 19 May 2002 (2002-05-19), pages 685-696, XP019054116 ISBN: 978-3-540-43709-3	1-6,8
A	page 689 - page 692	7,9-18

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 February 2010	25/02/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Eraso Helguera, J

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/052609

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	LANDFELDT B ET AL: "Providing scalable and deployable addressing in third-generation cellular-networks" IEEE WIRELESS COMMUNICATIONS, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 10, no. 1, 1 February 2003 (2003-02-01), pages 36-42, XP011095589 ISSN: 1536-1284	1-6,8
A	page 38, right-hand column, paragraph 2 - page 40, right-hand column, paragraph 4	7,9-18
A	WO 01/93540 A (NOKIA NETWORKS OY [FI]; HIPPELAEINEN LASSI [FI]; SAIRANEN JUSSI PEKKA) 6 December 2001 (2001-12-06) page 15, line 8 - page 16, line 12; figure 2	1-18
A	WO 01/31888 A (3COM CORP [US]; BORELLA MICHAEL S [US]; GRABELSKY DAVID A [US]) 3 May 2001 (2001-05-03) abstract page 22, line 13 - page 23, line 2; figure 7	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2009/052609

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0193540 A	06-12-2001	AT 429770 T	15-05-2009
		AU 5074300 A	11-12-2001
		CA 2413879 A1	06-12-2001
		EP 1290858 A1	12-03-2003
		JP 3805255 B2	02-08-2006
		JP 2003535507 T	25-11-2003
		US 7289504 B1	30-10-2007
WO 0131888 A	03-05-2001	AU 1967301 A	08-05-2001
		US 6708219 B1	16-03-2004

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/052609

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L12/46

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	CÉDRIC DE LAUNOIS ET AL: "Connection of Extruded Subnets: A Solution Based on RSIP" NETWORKING 2002: NETWORKING TECHNOLOGIES, SERVICES, AND PROTOCOLS; PERFORMANCE OF COMPUTER AND COMMUNICATION NETWORKS; MOBILE AND WIRELESS COMMUNICATIONS; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, vol. 2345, 19 mai 2002 (2002-05-19), pages 685-696, XP019054116 ISBN: 978-3-540-43709-3	1-6,8
A	page 689 - page 692	7,9-18

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
18 février 2010	25/02/2010

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Eraso Helguera, J

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/052609

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	LANDFELDT B ET AL: "Providing scalable and deployable addressing in third-generation cellular-networks" IEEE WIRELESS COMMUNICATIONS, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 10, no. 1, 1 février 2003 (2003-02-01), pages 36-42, XP011095589 ISSN: 1536-1284	1-6,8
A	page 38, colonne de droite, alinéa 2 - page 40, colonne de droite, alinéa 4	7,9-18
A	WO 01/93540 A (NOKIA NETWORKS OY [FI]; HIPPELAEINEN LASSI [FI]; SAIRANEN JUSSI PEKKA) 6 décembre 2001 (2001-12-06) page 15, ligne 8 - page 16, ligne 12; figure 2	1-18
A	WO 01/31888 A (3COM CORP [US]; BORELLA MICHAEL S [US]; GRABELSKY DAVID A [US]) 3 mai 2001 (2001-05-03) abrégé page 22, ligne 13 - page 23, ligne 2; figure 7	1-18

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2009/052609

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0193540	A	06-12-2001	AT	429770 T	15-05-2009
			AU	5074300 A	11-12-2001
			CA	2413879 A1	06-12-2001
			EP	1290858 A1	12-03-2003
			JP	3805255 B2	02-08-2006
			JP	2003535507 T	25-11-2003
			US	7289504 B1	30-10-2007
WO 0131888	A	03-05-2001	AU	1967301 A	08-05-2001
			US	6708219 B1	16-03-2004