

(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
6 décembre 2007 (06.12.2007)

PCT

(10) Numéro de publication internationale
WO 2007/138228 A2

(51) Classification internationale des brevets :
H04L 29/12 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2007/051347

(22) Date de dépôt international : 29 mai 2007 (29.05.2007)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
06 51989 31 mai 2006 (31.05.2006) FR

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

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : **MIGAULT,**

Daniel [FR/FR]; 52 rue Hoche, F-92130 Issy Les Moulin-
eaux (FR). **HOUSIER, Loïc** [FR/FR]; 25 avenue de
l'Europe, F-92310 Sevres (FR). **FOUQUART, Philippe**
[FR/FR]; 161 avenue de Suffren, F-75015 Paris (FR).

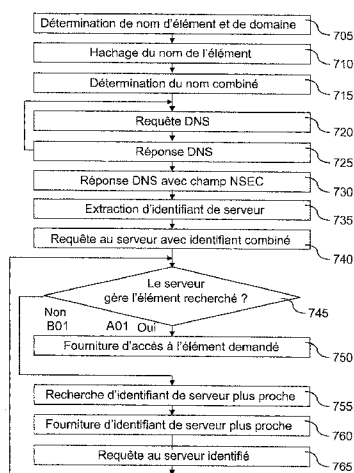
(74) Mandataire : **SIMON Viviane**, FRANCE TELECOM/R
& D/PIV/BREVETS, 38/40 rue du Général Leclerc,
F-92794 Issy Moulineaux Cedex 9 (FR).

(81) États désignés (sauf indication contraire, pour tout titre de
protection nationale disponible) : AE, AG, AL, AM, AT,
AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO,
RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD, DEVICE AND NAMING SYSTEM, METHOD AND TERMINAL FOR ACCESSING A RESOURCE, METHOD FOR RESPONDING TO A QUERY AND RESOLVING SERVER

(54) Titre : PROCEDE, DISPOSITIF ET SYSTEME DE NOMMAGE, PROCEDE ET TERMINAL D'ACCES A UNE RES-
SOURCE, PROCEDE DE REPONSE A UNE INTERROGATION ET SERVEUR DE RESOLUTION



705 Determine element and domain name
710 Hash element name
715 Determine combined name
720 DNS query
725 DNS response
730 DNS response with NSEC field
735 Retrieve server identifier
740 Query server with combined identifier
745 Is the server administering the search element?
B01 No
A01 Yes
750 Provide access to the requested element
755 Search for closest server identifier
760 Provide identifier of closer server
765 Query identified server

(57) Abstract: The method for accessing an element having an identifier comprises: at least one querying step (720) for querying a name resolution server of a hierarchic naming system responsible for a domain represented by said identifier, which query comprises the identifier, a step (730) of receiving a response from a name resolution server, which response is representative of at least one server name that differs from the identifier and is hierarchically on the same level as the identifier, and a querying step (740) for querying a server which has a name that is different from the said identifier. In particular embodiments, in the course of the response reception step (730), the response is representative of at least one server name which is located, in lexicographical order and in the memory of the name resolution server, immediately above or immediately below the identifier.

(57) Abrégé : Le procédé d'accès à un élément possédant un identifiant comporte : au moins une étape d'interrogation (720) d'un serveur de résolution de noms d'un système de nommage hiérarchique, responsable d'un domaine représenté par ledit identifiant, l'interrogation comportant l'identifiant, une étape de réception (730) d'une réponse provenant d'un serveur de résolution de noms, représentative d'au moins un nom de serveur différent de l'identifiant et hiérarchiquement au même niveau que l'identifiant et une étape d'interrogation (740) d'un serveur possédant un tel nom différent dudit identifiant. Dans des modes de réalisation particuliers, au cours de l'étape de réception d'une réponse (730), la réponse est représentative d'au moins un nom de serveur qui se trouve, dans l'ordre lexicographique et dans la mémoire du serveur de résolution de noms, immédiatement supérieur ou immédiatement inférieur à l'identifiant.

WO 2007/138228 A2



(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), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

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

Publiée :

— sans rapport de recherche internationale, sera republiée dès réception de ce rapport

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE, DISPOSITIF ET SYSTEME DE NOMMAGE, PROCEDE ET TERMINAL D'ACCES A UNE RESSOURCE, PROCEDE DE REPONSE A UNE INTERROGATION ET SERVEUR DE RESOLUTION

La présente invention concerne un procédé et un système de nommage de
5 ressources sur un réseau informatique, ainsi qu'un dispositif et un procédé d'accès à une ressource sur un réseau informatique, et un procédé et un dispositif de réponse à une interrogation. Elle s'applique, en particulier, à permettre l'accès, sur le réseau internet, à des données non référencées par le système de nommage de noms de domaines DNS.

10 Les systèmes informatiques reliés au réseau Internet communiquent entre eux en utilisant une adresse IP (sigle de « internet protocol » pour protocole internet), telle que « 10.192.123.234 », par exemple. Le système DNS (sigle de « domain name system » pour système de noms de domaines) est un système de nommage, c'est-à-dire d'association d'un identifiant alphanumérique à une
15 adresse IP, hiérarchique. L'objectif de cette architecture de nommage est de permettre d'établir un lien entre un identifiant, ici un nom de domaine, par exemple www.wanadoo.fr (Wanadoo est une marque déposée), et une adresse IP. Ce système a été établi de manière à donner aux divers systèmes informatiques accessibles sur le réseau internet des noms « humainement compréhensibles ». En
20 effet, il est plus simple de retenir « www.wanadoo.fr » qu'une adresse IP. Il s'agit, en quelque sorte, d'un annuaire mondial faisant la correspondance entre un nom et un numéro. Par la suite, cette architecture s'est généralisée et est utilisée pour effectuer le lien entre un nom de domaine et une information différente d'un site. Le système DNS est donc à considérer, dans sa généralité, comme une
25 architecture hiérarchique permettant d'effectuer un lien entre un nom de domaine et une information de connectivité.

On désigne par « root domain » la racine commune à tous les noms de domaine. Elle se note « . ». Cette racine possède un nombre restreint de sous domaines appelés domaines de plus haut niveau, « top level domain », « TLD ».
30 On distingue trois catégories de TLD. La première contient les TLD qui désignent des noms de pays (par exemple « uk », « jp »). On les nomme « Country Code TLD » (ccTLDs). La deuxième est un TLD réservé à des expérimentations techniques, nommé « .arpa ». Enfin les autres TLD (par exemple, « .com »,

« .org », « .edu ») sont appelées « generic TLD » ou domaines de plus haut niveau génériques (gTLD).

Les noms de domaines sont donc repartis, à partir de la racine, en TLD. Ce schéma se reproduit itérativement à partir de chaque TLD et ce jusqu'à ce que l'on arrive à la feuille de l'arborescence. Cette hiérarchisation permet à chaque entité possédant un nom de domaine d'être répertoriée universellement et d'administrer son domaine de manière hiérarchique et indépendante.

En ce qui concerne l'organisation des serveurs de résolution de noms de domaine, la structure hiérarchique est subdivisée en domaines et sous domaines permettant la mise en place d'un service distribué et hiérarchisé. Au niveau de la structure de nommage, les serveurs de nom gèrent chacun leur domaine et redirigent les clients vers les sous domaines auxquels la gestion est déléguée. Ainsi, en reprenant le nom de domaine `www.opera-de-paris.fr`, le domaine root ou racine ne connaît pas directement la réponse, par contre il connaît les références du serveur gérant le sous domaine « .fr ». Il redirige donc la requête vers ce serveur et ainsi de suite jusqu'à la résolution complète du nom.

On distingue les serveurs hébergeant réellement les données DNS, des serveurs ayant obtenu les données au cours d'une interrogation précédente. Les serveurs hébergeant réellement les données d'une zone sont appelés les serveurs « primaires ». Les serveurs DNS ayant la réponse à une requête car ils ont déjà émis cette requête et conservent la réponse sont appelés serveurs « cache ».

Au niveau des données, une durée de validité est associée à chaque donnée DNS. Tant que la date de validité n'est pas expirée, la donnée reste dans le réseau grâce à la présence de caches. Les caches sont des fichiers qui contiennent des données ayant déjà fait l'objet de requêtes DNS. Elles sont conservées tant que la date de validité n'est pas expirée. Un client émettant une requête vers un cache pourra recevoir la réponse de ce dernier, ce qui peut ainsi éviter l'interrogation des serveurs DNS.

La figure 1 illustre le fonctionnement du DNS au sein du réseau, dans le cas d'une résolution récursive. Dans l'exemple illustré, un terminal utilisateur souhaite connaître l'adresse IP du serveur Web `www.orange.fr` (Orange est une marque déposée). Il adresse d'abord une requête 101 à un serveur de résolution locale 115 (en anglais « local resolver ») aussi appelé serveur « cache récursif »,

« cache » car il conserve les résultats qu'il reçoit, pendant leur durée de validité et « récursif » parce qu'il effectue une succession de requêtes pour le compte du terminal utilisateur. Le serveur de résolution locale 115 émet, alors, une requête 102 à destination du serveur maître 120 du domaine « . » et reçoit, en retour, un message 103 lui indiquant une adresse IP du serveur maître du domaine « .fr » 125. Le serveur de résolution locale 115 émet, alors, une requête 104 à destination du serveur 125 et reçoit, en retour, un message 105 lui indiquant une adresse IP du serveur du domaine « orange.fr » 130. Le serveur de résolution locale 115 émet, alors, une requête 106 à destination du serveur 130 et reçoit, en retour, un message 107 lui indiquant une adresse IP du serveur 135 comportant le contenu du domaine www.orange.fr 135. Le terminal 110 peut alors utiliser cette adresse IP pour accéder au domaine « www.orange.fr ».

Ainsi, le nom de domaine « www.orange.fr. » désigne un nom de domaine sur quatre niveaux :

- 15 - « . » désigne le root domain,
- « fr » désigne le TLD, et plus précisément le ccTLD
- « orange » désigne le domaine géré par la société Orange (marque déposée) et
- « www » désigne le nom donné au serveur de la toile.

20 Le nom de domaine constitue l'entrée unique de la base, et les noms doivent remplir certaines règles, notamment ils doivent respecter une hiérarchie. Ainsi «www» est un sous domaine de «orange» qui lui-même est un sous domaine de «fr» qui lui-même est un sous domaine de «root» ou «.».

Cependant, si l'architecture DNS convient à une structure de nommage hiérarchisée comme celle qui régit les noms de domaine classique sur l'internet, le DNS n'est, en revanche, pas conçu pour répondre à une structure de nommage sans hiérarchie, ou encore appelée structure de nommage « à plat ». Par exemple, le système DNS ne peut gérer le cas où chaque machine ou entité du réseau possède un identifiant sans structure, comme un nombre aléatoire. En effet, il faudrait qu'il possède un fichier de zone contenant tous les identifiants, ce qui dans le cas d'identifiants d'une longueur, par exemple, de 12 bits, c'est-à-dire la même longueur que les adresses IPv6, semble irréaliste du fait du nombre d'adresses considérées. Or, l'utilisation des identifiants non hiérarchiques se

développe car il permet d'intégrer des fonctionnalités, comme la sécurité, directement dans le système de nommage.

Par exemple, à la base du protocole HIP (acronyme de « host identity protocol » pour protocole d'identité hôte), la séquence de bits désignant l'identifiant est constituée à partir du condensât ou hachage (en anglais « hash ») d'une clé publique. On parle alors d'identifiants « cryptographiques ». L'utilisation de tels identifiants permet d'intégrer des fonctionnalités comme des procédures d'attachement sécurisé, une preuve d'appartenance, des données relatives à la confidentialité des informations. Les protocoles HIP, et des projets comme « Ambient Network » (pour réseau ambiant), partent du principe que l'identité d'un nœud ou de n'importe quel élément accessible sur le réseau est désigné par son couple de clé publique / clé privée.

Plus généralement, l'utilisation d'un système de nommage sans hiérarchie facilite les configurations automatiques au sein d'un réseau. En effet si 234543267098765 et 039543266098705 sont deux identifiants binaires écrits en base décimale, sans lien apparent. Ils peuvent appartenir à deux machines n'ayant aucun lien entre elles ou, au contraire, être associés à deux nœuds très proches comme deux terminaux appartenant à un même sous réseau.

Les avantages que l'on trouve, au niveau réseau, à un système de nommage sans hiérarchie, notamment en ce qui concerne la simplification des opérations de configuration automatique rencontrent, au niveau du système de nommage, une nouvelle problématique : Comment gérer l'ensemble des identifiants binaires ? En effet, comme exposé plus haut, il n'est pas envisageable de mettre en place une base de données centralisée possédant tous les identifiants possibles.

L'utilisation d'un système de nommage non hiérarchisé dans l'architecture DNS est particulièrement complexe puisque l'on a à faire à deux conceptions différentes de systèmes de nommage, l'un non hiérarchisé, l'autre centralisé, l'un orienté contenu (fichier ou données), l'autre orienté information de connexion.

La présente invention propose de permettre à la structure DNS d'intégrer au moins un espace de nommage non hiérarchisé.

A cet effet, la présente invention vise, selon un premier aspect, un procédé d'accès à un élément possédant un identifiant, qui comporte :

- au moins une étape d'interrogation d'un serveur de résolution de noms d'un système de nommage hiérarchique, responsable d'un domaine représenté par ledit identifiant, ladite interrogation comportant ledit identifiant,
- 5 - une étape de réception d'une réponse provenant d'un dit serveur de résolution de noms, ladite réponse étant représentative d'au moins un nom de serveur différent dudit identifiant et hiérarchiquement au même niveau que ledit identifiant et
- 10 - une étape d'interrogation d'un serveur possédant un dit nom différent dudit identifiant.

Grâce à ces dispositions, un élément possédant un identifiant inconnu du système de résolution d'adresse, par exemple DNS, peut être retrouvé par l'intermédiaire du serveur dont le nom est différent de l'identifiant de l'élément, en particulier lorsque cet autre serveur est lié à un réseau comportant ledit élément.

- 15 La présente invention vise ainsi à intégrer deux systèmes de nommage, hiérarchique et non hiérarchique, de manière à utiliser, dans le système DNS, des identifiants possédant, en partie, un identifiant non-hiérarchique propre à un domaine.

- 20 La mise en œuvre de la présente invention présente donc les avantages suivants :

- d'une part, le système de nommage hiérarchisé, par exemple DNS, n'est pas encombré par des noms associés à chaque élément accessible et
- d'autre part, les systèmes de nommage non hiérarchiques n'ont pas à gérer des éléments extérieurs au domaine.

- 25 Selon des caractéristiques particulières, au cours de l'étape de réception d'une réponse, ladite réponse est représentative d'au moins un nom de serveur qui se trouve, dans l'ordre lexicographique et dans la mémoire dudit serveur de résolution de noms, immédiatement supérieur ou immédiatement inférieur audit identifiant.

- 30 Grâce à ces dispositions, le procédé d'accès bénéficie, à la fois des avantages du système DNS et des avantages des systèmes de nommage non hiérarchisés, qui permettent, par exemple, l'ajout ou le retrait aisé et rapide de fichiers ou de nœuds. En effet, dans les systèmes de nommage non hiérarchisés,

les éléments sont gérés par les serveurs qui possèdent l'identifiant le plus proche, étant entendu que la notion de proximité dépendant d'une fonction de distance définie pour le système de nommage non hiérarchisé.

5 Selon des caractéristiques particulières, au cours de l'étape de réception d'une réponse, ladite réponse est représentative, d'une part, de ce que ledit identifiant est inconnu dudit serveur de résolution de noms et, d'autre part, de chaque dit nom différent dudit identifiant.

Grâce à ces dispositions, l'extension DNSSEC du système de nommage DNS peut être mise en œuvre pour implémenter la présente invention.

10 Selon des caractéristiques particulières, le procédé d'accès tel que succinctement exposé ci-dessus comporte, en outre, une étape de détermination d'obtention d'un accès audit élément de la part d'un dit serveur possédant un nom différent dudit identifiant et, en l'absence d'obtention dudit accès audit élément, une étape d'interrogation d'un autre serveur possédant un dit nom différent dudit
15 identifiant.

Grâce à ces dispositions, si l'accès à l'élément recherché ne peut être obtenu de la part d'un serveur possédant un nom qui suit, dans l'ordre lexicographique, l'identifiant de l'élément recherché, on l'obtient de la part d'un serveur possédant un nom qui précède, dans l'ordre lexicographique, l'identifiant
20 combiné.

Selon des caractéristiques particulières, au cours de chaque étape d'interrogation, ledit identifiant est un identifiant dit « combiné » représentatif, d'une part, du nom dudit domaine et, d'autre part, d'un identifiant d'élément sur un réseau dit « non hiérarchisé » qui comporte ledit serveur possédant ledit nom
25 différent dudit identifiant et ledit élément.

Grâce à ces dispositions, le système de nommage DNS peut utiliser le nom de domaine concerné et le réseau non hiérarchisé peut, ensuite, utiliser l'identifiant d'élément.

30 Selon des caractéristiques particulières, ledit réseau non hiérarchisé met en œuvre un système de nommage non hiérarchisé dans lequel les identifiants sont gérés par intervalles juxtaposés.

Grâce à ces dispositions, on peut retrouver le gestionnaire de l'élément recherché sans avoir à rechercher tous les éléments du réseau non hiérarchisé.

Selon des caractéristiques particulières, le procédé tel que succinctement exposé ci-dessus comporte, de manière itérative, une étape de détermination, par un serveur possédant un nom différent dudit identifiant, s'il est responsable dudit élément et

- 5 - si oui, une étape de fourniture d'un accès audit élément et
 - si non, une étape de sélection, par ledit serveur possédant un nom différent dudit identifiant, d'un autre nom de serveur du réseau non hiérarchisé différent dudit identifiant et plus proche dudit identifiant que l'identifiant du serveur effectuant ladite étape de détermination.

- 10 Grâce à ces dispositions, on converge progressivement vers le gestionnaire de l'élément recherché.

Selon des caractéristiques particulières, au cours des étapes itératives, on met en œuvre une table mettant en correspondance chaque identifiant d'élément dudit réseau non hiérarchisé et un nom de serveur dudit réseau non hiérarchisé.

- 15 Selon des caractéristiques particulières, ladite table contient des identifiants d'éléments qui sont représentatifs de résultats d'une fonction de hachage d'au moins une partie du nom et/ou du contenu desdits éléments.

- Selon des caractéristiques particulières, au cours des étapes itératives, on met en œuvre un système de nommage à tables de hachages distribuées sur les
20 serveurs du réseau non hiérarchisé.

Grâce à chacune de ces dispositions, la présente invention peut être implémentée avec les systèmes de nommage à distribution de tables de hachage, nommés DHT.

- Selon des caractéristiques particulières, le procédé tel que succinctement
25 exposé ci-dessus comporte une étape de référencement, auprès d'un serveur de résolution de noms du système de nommage hiérarchique, du serveur possédant le nom différent dudit identifiant, nom représentant d'une part, ledit domaine et, d'autre part, un identifiant non hiérarchisé.

- Selon un deuxième aspect, la présente invention vise un système de
30 nommage qui attribue, pour au moins un élément, un identifiant combiné représentatif, d'une part, d'un nom selon un système de nommage hiérarchisé et, d'autre part, d'un identifiant d'élément d'un système de nommage non hiérarchisé, l'identifiant du système de nommage hiérarchisé permettant l'accès à un serveur

et l'identifiant du système de nommage non hiérarchisé permettant l'accès aux éléments accessibles audit serveur, en mettant en œuvre le système de nommage non hiérarchisé.

5 Selon des caractéristiques particulières, le système de nommage attribue un identifiant combiné à un serveur dont l'identifiant non hiérarchisé est le dernier identifiant de l'ensemble des identifiants non hiérarchisés.

10 Selon des caractéristiques particulières, le système de nommage tel que succinctement exposé ci-dessus détermine l'identifiant d'un système de nommage non hiérarchisé par hachage d'au moins une partie du nom et/ou du contenu dudit élément.

Les avantages, buts et caractéristiques particulières de ce système de nommage étant similaires à ceux du procédé d'accès à un élément tel que succinctement exposé ci-dessus, ils ne sont pas rappelés ici.

15 Selon un troisième aspect, la présente invention vise un procédé de nommage d'un élément d'un réseau non hiérarchisé sur lequel les identifiants sont gérés par intervalle, qui comporte une étape d'attribution, audit élément, d'un nom hiérarchisé d'un domaine possédant un serveur dudit réseau non hiérarchisé et une étape d'attribution, audit élément, d'un complément de nom représentant son identifiant sur le réseau non hiérarchisé.

20 Selon des caractéristiques particulières, le procédé de nommage tel que succinctement exposé ci-dessus comporte, en outre, une étape de mise à jour d'une table distribuée dans laquelle chaque élément du réseau non hiérarchisé est mis en relation avec un identifiant de serveur responsable dudit élément.

25 Selon des caractéristiques particulières, le procédé de nommage tel que succinctement exposé ci-dessus comporte, en outre, une étape de référencement d'au moins un serveur dudit réseau non hiérarchisé sur au moins un serveur de résolution de nom de domaine.

30 Selon des caractéristiques particulières, le procédé de nommage tel que succinctement exposé ci-dessus comporte une étape d'attribution d'un identifiant combiné à un serveur dont l'identifiant non hiérarchisé est le dernier identifiant de l'ensemble des identifiants non hiérarchisés.

Les avantages, buts et caractéristiques particulières de ce procédé de nommage étant similaires à ceux du procédé d'accès à un élément tel que

succinctement exposé ci-dessus, ils ne sont pas rappelés ici.

Selon un quatrième aspect, la présente invention vise un procédé de réponse, par un serveur, à une interrogation de résolution de nom comportant un identifiant, qui comporte :

- 5 - lorsque ledit serveur conserve, en mémoire, une adresse correspondant audit identifiant, une étape de réponse au cours de laquelle ledit serveur fournit ladite adresse et
- lorsque ledit serveur ne conserve pas, en mémoire, une adresse correspondant audit identifiant, une étape de réponse au cours de
- 10 laquelle ledit serveur fournit une réponse représentative d'au moins un nom de serveur différent dudit identifiant et hiérarchiquement au même niveau que ledit identifiant, sans indication de ce que ledit nom est différent dudit identifiant.

15 Selon des caractéristiques particulières, lorsque ledit serveur ne conserve pas, en mémoire, une adresse correspondant audit identifiant, au cours de l'étape de réponse, ladite réponse est représentative d'un nom de serveur qui se trouve, dans l'ordre lexicographique et dans la mémoire dudit serveur, immédiatement supérieur ou immédiatement inférieur audit identifiant.

20 Les avantages, buts et caractéristiques particulières de ce procédé de réponse étant similaires à ceux du procédé d'accès à un élément tel que succinctement exposé ci-dessus, ils ne sont pas rappelés ici.

Selon un cinquième aspect, la présente invention vise un terminal d'accès à un élément possédant un identifiant, qui comporte :

- 25 - un moyen d'interrogation adapté à interroger au moins un serveur de résolution de noms d'un système de nommage hiérarchique, responsable d'un domaine représenté par ledit identifiant, ladite interrogation comportant ledit identifiant et
- un moyen de réception d'une réponse provenant d'un dit serveur de résolution de noms, ladite réponse étant représentative d'au moins un
- 30 nom de serveur différent dudit identifiant et hiérarchiquement au même niveau que ledit identifiant,
- ledit moyen d'interrogation étant adapté à interroger un serveur possédant un dit nom différent dudit identifiant.

Selon des caractéristiques particulières, le moyen de réception de réponse est adapté à ce que ladite réponse soit représentative, d'une part, de ce que ledit identifiant est inconnu dudit serveur de résolution de noms et, d'autre part, de chaque dit nom différent dudit identifiant.

5 Selon des caractéristiques particulières, ledit moyen d'interrogation est adapté à ce que ledit identifiant soit un identifiant dit « combiné » représentatif, d'une part, du nom dudit domaine et, d'autre part, d'un identifiant d'élément sur un réseau qui comporte ledit serveur possédant ledit nom différent dudit identifiant et ledit élément.

10 Selon des caractéristiques particulières, le moyen d'interrogation est adapté à déterminer si un accès audit élément a été obtenu de la part d'un dit serveur possédant un nom différent dudit identifiant et, dans la négative, à interroger un autre serveur possédant un dit nom différent dudit identifiant.

 Selon des caractéristiques particulières, le moyen d'interrogation est adapté
15 à mettre en œuvre un identifiant d'un système de nommage non hiérarchisé dans lequel les identifiants sont gérés par intervalles.

 Les avantages, buts et caractéristiques particulières de ce terminal d'accès à un élément étant similaires à ceux du procédé d'accès à un élément tel que succinctement exposé ci-dessus, ils ne sont pas rappelés ici.

20 Selon un sixième aspect, la présente invention vise un dispositif de nommage d'un élément d'un réseau non hiérarchisé sur lequel les identifiants sont gérés par intervalle, qui comporte une moyen d'attribution, audit élément, d'un nom hiérarchisé d'un domaine possédant un serveur dudit réseau non hiérarchisé et un moyen d'attribution, audit élément, d'un complément de nom représentant
25 son identifiant sur le réseau non hiérarchisé.

 Selon des caractéristiques particulières, le dispositif de nommage tel que succinctement exposé ci-dessus comporte, en outre, un dispositif de mise à jour d'une table distribuée dans laquelle chaque élément du réseau non hiérarchisé est mis en relation avec un identifiant de serveur responsable dudit élément.

30 Selon des caractéristiques particulières, le dispositif de nommage tel que succinctement exposé ci-dessus comporte, en outre, un moyen de référencement d'au moins un serveur dudit réseau non hiérarchisé sur au moins un serveur de résolution de nom de domaine.

Selon des caractéristiques particulières, le dispositif de nommage tel que succinctement exposé ci-dessus comporte, en outre, un moyen de référencement d'un serveur dudit réseau non hiérarchisé possédant le dernier des identifiants utilisés sur le réseau non hiérarchisé, sur au moins un serveur de résolution de nom de domaine.

Les avantages, buts et caractéristiques particulières de ce dispositif de nommage étant similaires à ceux du procédé de nommage tel que succinctement exposé ci-dessus, ils ne sont pas rappelés ici.

Selon un septième aspect, la présente invention vise un serveur de résolution de nom comportant un identifiant comportant une mémoire dans laquelle des identifiants sont associés à des adresses en réponse à une interrogation, caractérisé en ce qu'il comporte un moyen de réponse adapté

- lorsque ladite mémoire conserve une adresse correspondant audit identifiant, à fournir une réponse représentative de ladite adresse et
- lorsque ladite mémoire ne conserve pas une adresse correspondant audit identifiant, à fournir une réponse représentative d'au moins un nom de serveur différent dudit identifiant et hiérarchiquement au même niveau que ledit identifiant, sans indication de ce que ledit nom est différent dudit identifiant.

Les avantages, buts et caractéristiques particulières de ce serveur étant similaires à ceux du procédé de réponse à une interrogation tel que succinctement exposé ci-dessus, ils ne sont pas rappelés ici.

Grâce aux caractéristiques de chacun des aspects de la présente invention, le système DNS n'est pas encombré par des adresses ou noms d'éléments accessibles par des nœuds d'un réseau non hiérarchisé mais ne gère que les adresses des nœuds possédant un nom DNS. De plus, les avantages des systèmes de nommage non hiérarchisés, qui permettent, par exemple, l'ajout ou le retrait aisé et rapide d'éléments, données, fichiers ou nœuds, sont des avantages de chacun des aspects de la présente invention.

La présente invention vise aussi un programme d'ordinateur chargeable dans un système informatique, ledit programme contenant des instructions permettant la mise en œuvre du procédé de procédé d'accès à un élément possédant un identifiant tel que succinctement exposé ci-dessus, lorsque ce

programme est chargé et exécuté par un système informatique.

La présente invention vise aussi un programme d'ordinateur chargeable dans un système informatique, ledit programme contenant des instructions permettant la mise en œuvre du procédé de procédé de nommage d'un élément
5 tel que succinctement exposé ci-dessus, lorsque ce programme est chargé et exécuté par un système informatique.

La présente invention vise aussi un programme d'ordinateur chargeable dans un système informatique, ledit programme contenant des instructions permettant la mise en œuvre du procédé de procédé de réponse à une
10 interrogation tel que succinctement exposé ci-dessus, lorsque ce programme est chargé et exécuté par un système informatique.

Les avantages, buts et caractéristiques de ces programmes d'ordinateur étant similaires à ceux des procédés qu'ils implémentent, tels que succinctement exposés ci-dessus, ils ne sont pas rappelés ici.

15 Les différents aspects de la présente invention et leurs caractéristiques particulières sont destinés à être combinés pour cumuler les avantages de ces caractéristiques.

D'autres avantages, buts et caractéristiques de la présente invention ressortiront de la description qui va suivre, faite, dans un but explicatif et nullement
20 limitatif en regard des dessins annexés, dans lesquels :

- la figure 1 représente, schématiquement, des échanges de requêtes et de réponses pour obtenir une adresse IP dans le système DNS,
- la figure 2 représente, schématiquement, un réseau mettant en œuvre un système de nommage DHT,
- 25 - la figure 3 représente, schématiquement, un premier mode de réalisation d'un système de nommage conforme à la présente invention,
- la figure 4 représente, schématiquement, un deuxième mode de réalisation d'un système de nommage conforme à la présente invention,
- la figure 5 représente, schématiquement, des échanges de requêtes et
30 réponses pour la mise en œuvre de la présente invention,
- les figures 6A à 6C représentent, respectivement, des logigrammes d'étapes mises en œuvre pour des ajouts et des retraits de ressources

accessibles sur un réseau informatique mondial et pour répondre à une requête,

- la figure 7 représente, sous forme d'un logigramme, des étapes mises en œuvre par un système informatique tentant d'accéder à un élément d'un réseau non hiérarchisé, en mettant en œuvre un premier mode de réalisation du procédé d'accès à un élément objet de la présente invention et
- la figure 8 représente, sous forme d'un logigramme, des étapes mises en œuvre par un système informatique tentant d'accéder à un élément d'un réseau non hiérarchisé, en mettant en œuvre un deuxième mode de réalisation du procédé d'accès à un élément objet de la présente invention.

Avant de décrire des modes de réalisation particuliers de la présente invention, en regard des figures, on donne, ci-dessous, des éléments utiles pour sa compréhension.

Dans toute la description, les termes d'« identifiant » et de « nom » sont utilisés indifféremment et les « clés » sont des identifiants particuliers.

Dans toute la description, les termes de « nœud » ou de « serveur » sont utilisés indifféremment.

Dans toute la description, les termes d'« élément » ou de « ressources » sont utilisés indifféremment.

Selon la présente invention, pour pouvoir accéder aux ressources associées à ces identifiants d'un réseau non hiérarchisé, à partir d'un système informatique extérieur au réseau non hiérarchisé, conformément à la présente invention, on associe à l'identifiant de ces ressources sur le réseau non hiérarchisé, des informations de connectivité, sous forme d'un nom de domaine hiérarchisé, au moins un nœud du réseau non hiérarchisé faisant partie dudit domaine.

Grâce à ce système de nommage, le nom combiné d'un élément auquel on cherche à accéder depuis l'extérieur du réseau non hiérarchisé peut être traité, d'abord, par les serveurs de résolution de noms de domaines DNS, de manière connue en soi, à l'exception du dernier serveur DNS mis en œuvre, comme exposé plus bas, puis l'identifiant non hiérarchisé de l'élément peut être traité par le réseau non hiérarchisé de manière connue en soi.

Par exemple, pour intégrer les identifiants cryptographiques à un domaine DNS, on définit un ensemble de nœuds Chord qui composent une architecture de nommage Chord de ce domaine. Ainsi, par exemple, un nom de domaine tel que « wanadoo.fr » peut définir un ensemble d'éléments (par exemple, serveurs, données ou fichiers) Chord, par exemple, dont les noms combinés sont formés de l'ajout d'un identifiant cryptographique au nom de domaine, par exemple « 201.wanadoo.fr », « 207.wanadoo.fr », « 203.wanadoo.fr », etc. Ces noms combinés constituent ainsi le système de nommage objet de la présente invention, qui permet d'établir un lien entre un identifiant cryptographique et une information de connectivité, au moins l'un des nœuds possédant un nom combiné étant connu du système DNS et donnant ainsi accès aux autres ressources Chord.

Parmi les méthodes de nommage non hiérarchisées, la présente invention met préférentiellement en œuvre celles appelées « DHT » (sigle de « distributed hash tables » pour tables de condensâts, ou hachages, distribuées) qui classent, sans hiérarchie, les données accessibles et réparties sur le réseau auxquelles on doit pouvoir accéder. Différents protocoles DHT ont été élaborés afin, d'une part, de pouvoir ajouter des données sur le réseau et, d'autre part, de pouvoir trouver les données en question.

Parmi ceux-ci, le mécanisme nommé Chord, un système de nommage non hiérarchique, a pour objectif de permettre une classification de clés. Dans le système de nommage Chord, chaque nœud du réseau possède un identifiant. L'identifiant des fichiers ou données à référencer est généré grâce à une fonction de hachage qui produit un condensât. Ainsi Chord est un système adapté à gérer un ensemble de fichiers.

L'intégration des systèmes de nommage DNS et DHT objet de la présente invention est effectuée dans le cadre de l'utilisation d'identifiants ordonnés sur le réseau non hiérarchisé, c'est-à-dire possédant, entre eux, une relation d'ordre, par exemple d'identifiants cryptographiques dans le protocole HIP, chaque nœud étant représenté par un identifiant formé à partir du condensât, ou hachage, d'une clé publique associée à ce nœud.

Une table de noms est une structure qui associe un nom à chaque élément accessible par cette structure, l'ensemble des noms possédant une relation d'ordre, au sens mathématique du terme.

Une table de hachage est une table qui associe à un élément un identifiant constituée d'une clé cryptographique obtenue par une fonction de hachage, par exemple mise en œuvre au cours d'une signature électronique, d'au moins une partie du nom et/ou du contenu de cet élément.

5 Une table distribuée est une table qui est répartie, par morceaux, entre différents nœuds d'un réseau. Dans une structure non hiérarchisée, chaque nœud est responsable de quelques unes des associations entre des noms et des éléments, typiquement d'un intervalle de noms. La partie de la table distribuée qu'il conserve comporte donc, au moins, les associations noms-éléments dont il a
10 la responsabilité.

A chaque nœud est associé un identifiant Chord qui lui indique l'intervalle de noms dont il a la responsabilité. Par exemple, dans le système Chord, l'identifiant du nœud est un nom qui suit le dernier nom d'élément dont il a la responsabilité. Suivant la nature de l'application, les noms et les éléments
15 représentent différentes choses. Dans le cas d'une application d'échanges de fichiers, un nom est un identifiant de fichier, et l'élément correspondant est la liste des adresses IP des nœuds qui possèdent le fichier, c'est-à-dire le conserve en mémoire.

Dans une table de hachage distribuée DHT, rechercher un élément revient,
20 dans un premier temps, à retrouver le nœud responsable de sa clé, puis, dans un deuxième temps, à l'interroger sur la valeur de l'élément correspondant, le terme de « valeur » pouvant signifier aussi bien le contenu de l'élément recherché, par exemple des données, et l'adresse IP où ce contenu est accessible. Le nœud peut ainsi avoir la donnée, ou bien comporter une indirection, et indiquer où télécharger
25 la donnée, par exemple. De même, la publication d'un élément revient à trouver le nœud responsable de sa clé avant de lui envoyer l'association clé-élément.

Pour que la recherche d'un élément par un nœud soit efficace, les nœuds forment un réseau structuré où chaque nœud possède des connaissances partielles sur les autres nœuds. A cet effet, on peut mettre en œuvre une table
30 d'index qui associe à certains éléments du réseau, les nœuds qui en sont responsables. Préférentiellement, chaque nœud du réseau possède plus d'information sur les éléments dont les noms sont les plus proches du nom de ce nœud que sur les éléments dont les noms sont les plus lointains, la notion de

distance étant ici celle qui est définie par une topologie associée au système de nommage. Différentes topologies peuvent être utilisées. Les topologies adoptées peuvent, par exemple, être l'hypercube, le tore ou le graphe de Bruijn. Ces différentes topologies définissent, entre autres, les algorithmes de routage pour
5 chercher le nœud responsable d'une clé.

Une table de hachage distribuée (ou DHT) associe un élément à une clé cryptographique, dans une table distribuée où les associations clé-élément sont réparties sur les nœuds du réseau. On accède ainsi à chaque élément de la table via sa clé cryptographique. Les deux opérations élémentaires effectuées sur une
10 table de hachage sont la création d'une association entre un élément et une clé cryptographique, par hachage de son contenu, et la récupération d'un élément par utilisation de sa clé, comme exposé en regard de la figure 2.

La figure 2 est une représentation d'un espace des responsabilités de nœuds dans un système DHT, ici le système Chord. En figure 2, les nœuds 200,
15 203, 206, 210 et 211 sont représentés par des disques noirs et les éléments 201, 202, 204, 205, 207, 208, 209 et 211 à 215 par des carrés noirs. La topologie utilisée dans Chord est l'hypercube. Chaque nœud possède un identifiant unique appartenant à l'intervalle $[0, 2^b - 1]$ qui définit sa position dans l'anneau représenté, avec la valeur du nombre « b » suffisamment élevée pour que
20 l'intervalle puisse accueillir tous les nœuds du système Chord. Typiquement, « b » = 64 ou 128, voire 256. En figure 2, « b » est égal à 4. Pour constituer les références numériques utilisées en figure 2, on a ajouté 200 à l'identifiant Chord de chaque nœud. Ainsi, par exemple, la référence 203 désigne le nœud dont l'identifiant Chord est « 3 » et la référence 207 désigne l'élément dont l'identifiant
25 Chord est « 7 ».

L'identifiant du nœud définit l'intervalle des clés d'éléments dont le nœud est responsable, cet espace de clés étant délimité par l'identifiant du nœud et par celui du nœud qui possède l'identifiant immédiatement inférieur. Ainsi, le nœud 210 est responsable des éléments dont les identifiants vont de 207 à 210. Les
30 nœuds voisins sont renseignés de telle sorte que chaque nœud ait plus de connaissances des nœuds ayant un identifiant proche du sien que des nœuds ayant un identifiant éloigné du sien. Dans la table de hachage distribuée, chaque nœud d'identifiant « i » connaît, pour chaque valeur $i+2^k$

(modulo 2^b), avec « k » dans l'intervalle $[0, b-1]$, le nœud ayant l'identifiant immédiatement supérieur à $i+2^k$, c'est-à-dire le nœud responsable de l'élément ayant comme identifiant $i+2^k$. Ces identifiants de nœuds constituent la table d'index du nœud en question.

5 Par exemple, le nœud 200, d'identifiant « 0 » possède la table d'index suivante :

	1	3
	2	3
	4	6
10	8	10

et le nœud 210, d'identifiant « 10 » possède la table d'index suivante :

	1	11
	2	0
	4	0
15	8	3

Pour trouver le nœud responsable d'un identifiant « j », c'est-à-dire le nœud dont l'identifiant est immédiatement supérieur ou égal à « j », un nœud cherche dans sa table d'index, l'identifiant du nœud ayant l'identifiant immédiatement inférieur à « j ». Il adresse une requête à ce nœud ayant, dans sa table d'index, l'identifiant immédiatement inférieur à « j » et celui-ci répète ces étapes jusqu'à ce que le dernier nœud interrogé, possède, dans sa table d'index, comme successeur immédiat, c'est-à-dire en première ligne de sa table d'index, un nœud d'identifiant « m » supérieur à « j ». Dans ce cas, le nœud recherché est le nœud d'identifiant « m » et, pour accéder à l'élément d'identifiant « j », on adresse une requête au nœud d'identifiant « m », celui-ci pouvant conserver l'élément « j » en mémoire ou savoir, par sa table de hachage distribuée, quel nœud conserve en mémoire l'élément « j » recherché.

Par exemple, si le nœud 203 recherche l'identifiant du nœud responsable de l'élément 215, il interroge le nœud 211 et celui-ci, ayant pour successeur immédiat le nœud 200, détermine que le nœud 200 est responsable de l'élément 215.

La manière dont les intervalles sont choisis fait que la recherche est effectuée de manière dichotomique et possède une complexité de l'ordre de

$\log(n)$, formule dans laquelle « n » est le nombre de nœuds connectés au système.

On peut aussi noter qu'un nœud peut être référencé par plusieurs nœuds qui possèdent, dans leur table d'index, des pointeurs qui le désignent, ce qui
5 améliore la tolérance aux fautes ou pannes, par exemple en cas de déconnexion de nœuds.

Pour se joindre à la topologie DHT, un nœud remplit sa table d'index et se signale auprès des nœuds qui pourraient l'avoir dans leur table d'index. Il doit également récupérer les associations clé-élément dont il devient responsable.
10 Réciproquement, avant de partir, un nœud doit signaler son départ aux nœuds qui l'ont dans leur table d'index et envoyer les associations au nœud qui possède l'identifiant immédiatement supérieur au sien et qui va devenir responsable de ces associations.

Pour implémenter la présente invention, en réponse à une requête
15 identifiant un élément recherché, par son nom combiné, le serveur de nom de domaine responsable du domaine comportant les éléments d'un réseau non hiérarchisé et qui ne reconnaît pas l'identifiant recherché transmet au moins le nom du nœud «le plus proche» de l'identifiant en question.

Le client, qui recherche l'accès à l'élément considéré peut alors utiliser le
20 nom de ce nœud « le plus proche » de l'identifiant en question et, grâce à la structure du réseau non hiérarchisé, accède ainsi à un nœud du réseau non hiérarchisé qui le dirige, directement ou indirectement, vers l'élément recherché.

Deux principaux modes de réalisation de la présente invention sont représentés dans les figures :

- 25
- un espace de nommage DHT-chord au niveau mondial et
 - un espace de nommage DHT-chord au niveau privé, c'est-à-dire pour un domaine précis, comme par exemple « wanadoo.fr ».

Dans le premier mode de réalisation particulier, illustré en figure 3, l'invention comprend la désignation d'un nom de domaine «.chord» par exemple,
30 qui sera considéré comme un TLD (sigle de « Top Level Domain » pour domaine de plus haut niveau) dans l'architecture DNS, domaine où sont disposés l'ensemble des identifiants des nœuds qui gèrent un intervalle de clés, dans un système de nommage non hiérarchisé. Dans ce premier mode de réalisation, il est

ainsi prévu un TLD spécifique, dédié à l'hébergement des données de type DHT-chord. Cet espace est préférentiellement géré, tout comme l'est le DNS actuel, par un consortium mondial. Les nœuds hébergeant les données sont gérés comme les différents « root » serveurs par ce consortium international.

- 5 Dans le second mode de réalisation, illustré en figure 4, l'ensemble des nœuds hébergeant les identifiants binaires sont gérés par l'organisation à qui appartient ce nom de domaine. Ceci correspond au cas où une entité décide d'administrer sa propre zone.

On observe que, dans la figure 3, le domaine public et mondial destiné à devenir un TLD illustré en figure 3 correspond, d'abord, au domaine Chord.arpa. En effet, c'est la fonction du domaine « .arpa » d'héberger, du moins dans une première mise en place, ce genre d'extension à l'architecture DNS mondiale.

Dans la figure 4, le domaine réservé pour les identifiants binaires de l'université de Berkeley est représenté.

- 15 Dans les deux cas, au sein d'un domaine, un ensemble de nœuds définissent l'architecture DHT-chord appartenant à ce domaine. Chaque nœud du réseau non hiérarchisé référencé dans le système DNS est défini par un nouveau type d'enregistrement DNS, appelé « ChordNODE ».

Une fois le domaine identifié par ce nouveau type d'enregistrement, on définit les différents nœuds de l'architecture DHT-Chord. Ces nœuds possèdent les informations suivantes:

- le nom de domaine auquel ils sont rattachés (dans les cas représentés en figure 3, il s'agit du domaine « Chord.arpa » et, en figure 4, du domaine « berkeley.edu »)
- 25 - les localisateurs (en anglais « locators ») qui lui sont rattachés (dans le cas représenté, il s'agit d'une adresse IP).

La figure 2 représente la structure DHT chord implémentée à Berkeley. Cette architecture possède trois nœuds de type ChordNODE, dont les caractéristiques sont les suivantes :

- 30 - Nœud 0 :
- identifiant non hiérarchisé : 0
 - adresse IP : 192.234.98.98
 - nom de domaine : chord.berkeley.edu

- identifiant combiné : 0.chord.berkeley.edu
- Nœud 1 :
 - identifiant non hiérarchisé : 1
 - adresse IP : 192.234.98.99
- 5 - nom de domaine : chord.berkeley.edu
- identifiant combiné : 1.chord.berkeley.edu
- Nœud 3 :
 - identifiant non hiérarchisé : 3
 - adresse IP : 192.234.98.100
- 10 - nom de domaine : chord.berkeley.edu
- identifiant combiné : 3.chord.berkeley.edu

L'implémentation, au niveau du fichier DNS, est la suivante (les données en caractères droits sont celles dues à l'utilisation du protocole DNS, les données d'implémentation de la présente l'invention étant en italiques) :

```

15 $ORIGIN chord.berkeley.edu.
   $TTL 8640
   @ IN SOA ns      bogdan\marinoiu.rd.francetelecom.com.(
                                2005112301; YY/MM/DD/version
                                200      ; update delay
20                                100      ; retry
                                604800   ; give up
                                100      )

                                IN      NS      ns
25      ns      IN      A      10.193.171.53

                                0      IN      ChordNODE « 192.234.98.98 » « chord.berkeley.edu. »
                                1      IN      ChordNODE « 192.234.98.99 » « chord.berkeley.edu. »
                                3      IN      ChordNODE « 192.234.98.100 »
30 « chord.berkeley.edu. »

```

On observe que les champs « SOA » et « ns » sont des champs du protocole DNS.

Ainsi, si on cherche l'information correspondant à l'identifiant « 2 » du réseau Chord, qui n'est pas référencé dans le système DNS, on commence par interroger le nœud dont l'identifiant est « 3 » sur ce réseau, qui est référencé dans le système DNS. En effet, les identifiants des éléments sont hébergés par le nœud
5 qui suit, c'est-à-dire que c'est le nœud qui suit qui en a la responsabilité.

Aussi, dans des modes de réalisation de la présente invention adaptés aux réseaux non hiérarchisés de type « Chord », la résolution de l'identifiant « 2 » utilise des mécanismes permettant de donner à l'émetteur de la requête l'accès au nœud le plus proche du réseau non hiérarchisé qui est référencé dans le système
10 DNS et qui suit l'identifiant recherché.

A cet effet, dans des modes de réalisation particuliers de la présente invention, on utilise une propriété de l'extension DNSSEC. En effet, les champs DNS de type NSEC permettent de donner à l'émetteur d'une requête sur un nom de domaine n'appartenant pas à la zone (en l'occurrence le nœud dont l'identifiant
15 est « 2 ») l'identifiant de nœud le plus proche et qui suit l'identifiant recherché qui n'a pas été trouvé.

Un fichier DNSSEC s'obtient d'après un fichier DNS. Dans un but didactique, on décrit, ci-dessous, l'extension sécurisée du DNS appelée « DNSSEC », étant cependant observé que la mise en œuvre de la présente
20 invention ne requiert pas l'utilisation du champ NSEC de ce protocole.

Décrite pour la première fois par l'organisation de normalisation IETF (sigle de « internet engineering task force » pour force de travail d'ingénierie de l'internet) dans le document RFC (sigle de « request for comments » pour requête de commentaires) 2535, cette extension est maintenant décrite dans les
25 documents RFC 4033, RFC 4034 et RFC 4035. DNSSEC a été essentiellement conçu afin d'assurer l'authentification de l'origine des messages DNS et de garantir leur intégrité durant leur transport.

Pour authentifier les réponses négatives (par exemple, le nom ou l'enregistrement demandé n'existe pas), les enregistrements NSEC
30 (anciennement nommés « NXT ») ont été rajoutés. Ils lient de façon cyclique les enregistrements d'une zone en indiquant, pour chaque nom, quels sont les types d'enregistrement qui y sont associés et quel est le prochain nom (en ordre lexicographique) situé dans le fichier de zone. On obtient la certitude qu'il n'y a

pas d'enregistrement correspondant à une requête si on vérifie l'enregistrement NSEC du nom qui est, du point de vue lexicographique, le plus proche prédécesseur du nom concerné par la requête.

L'enregistrement « SOA » spécifie le nom du serveur primaire de la zone,
 5 « dnssec1 », mais sans suffixe. Le suffixe, par exemple « .mabanquea.fr », est rajouté à tous les noms qui ne finissent pas par « . ». Cet enregistrement donne également l'adresse électronique (ou « adresse email ») de l'administrateur de la zone ainsi que des délais concernant la mise à jour des serveurs esclaves.

L'enregistrement « NS » spécifie un serveur de noms pour le domaine. Les
 10 enregistrements « A » donnent des adresses « IPv4 » pour le serveur de noms et pour un serveur de la toile, ou web, qui appartient au domaine.

Les enregistrements d'un nom de type NSEC indiquent le nom DNS suivant dans la zone, en ordre lexicographique, et la liste des types de ses enregistrements font la clôture cyclique de la zone (« mabanquea.fr » vers
 15 « dnssec1.mabanquea.fr » vers www.mabanquea.fr vers « mabanquea.fr »).

Ainsi, dans des modes particuliers de réalisation de la présente invention, le fichier DNSSEC prend la forme suivante, dans laquelle les données d'implémentation de la présente invention sont en italiques, les autres données étant dues à l'utilisation du protocole DNS/DNSSEC :

20 ; dnssec_signzone version 9.3.1

\$ORIGIN chord.berkeley.edu

@. 8640 IN SOA ns.berkeley.edu. bogdan\marinoiu.rd.francetelecom.com.

(

2005112301 ; serial

25 200 ; refresh (1 minute 40 seconds)

100 ; retry (3 minutes 20 seconds)

604800 ; expire (1 week)

100 ; minimum (1 minute 40 seconds)

)

30 8640 RRSIG SOA 5 2 8640 20060104100453 (

20051205100453 48254 chord.berkeley.edu

5VIIFIUdNmJvVZfpiHKYbRW4LePhRIWAdopf

gcizUoYZ+PFg6FtM9RU1AXUViJS7UYH189p8

```

      ttyQMXAFm1CADeddJoNT3ZXLx9quxzCYC3g2
      2ACvLbjmljlvexV4OMWb8VHLICcc45ubYjP8
      8RQt0F3juNMCBW+OVXDwy15u/H4= )
5      8640 NS      ns.berkeley.edu.
      8640 RRSIG NS 5 2 8640 20060104100453 (
      20051205100453 48254 chord.berkeley.edu.
      db2Tsfm/cnFyaSkHaYWiBon2r2HYtBrwQsYC
      BR2A300WuCk1ejMOP0464RkKDIKWJSz4JF6r
      OttW/TCwUy5OyrXq+WMfZMjQ7GR5VTAs5UJQ
10     b4WVOqfLYLxQ4sPaiozolzWld1Y+J8WUbdj
      nzj1hFPp+Bx82dxJCdty06eAVAI= )
      100 NSEC 0.chord.berkeley.edu. NS SOA RRSIG NSEC DNSKEY
      100 RRSIG NSEC 5 2 100 20060104100453 (
      20051205100453 48254 chord.berkeley.edu.
15     scYwzOQihvasXeXUX1u3QwWbnH/mzkvuOQdc
      MpD+BJzn7LSHF28kbiuizdua3ukNI8IVjqcC
      m4MhmaVvxJpBtXbxMoOQG6eE0Wf6lvV/Gsbd
      bh8DSfudtU2Zu1J7VObpkQRodlgidyhnPbAZ
      BGC3KWbBplz9TuDprmGWm6CUIJ8= )
20     8640 DNSKEY      256 3 5 (
      AQPvG9Z4OwGpYryJeQ5oDGRJYc45hvLiLE99
      MzLwJ3Coix/FtidVexBqHRC9Js+fg/iJVWSm
      ue6VMluEteShtEohlc418/K9qAQcwyCS8ZNx
      scBKc1W1sw5RmCkCprGkltSUCUeP10SP/cPK
25     yN/Z6/qSgvXxAVjh7IMauhVelv2iw==
      ) ; key id = 48254
      8640 DNSKEY      257 3 5 (
      AQOzHIM1NL7E5fuA3hpddBdXcHq3deTPHkLK

```

nt3N3QPRc8XrXJ6WgHp9dreqS8uvp8bF76sB
 pen/XP8bn9ybOJBz9++w0ScugKzIYbF6E/zE
 vGrKitky5iz1pZ+VsHwy78QKbDSMlsqT25T
 L8Sx2VthbWJF1IRLuuTAMo7sGnNERw==
 5) ; key id = 27075
 8640 RRSIG DNSKEY 5 2 8640 20060104100453 (
 20051205100453 27075 chord.berkeley.edu.
 G063olGAPTN0fUr4KK2xqAAiexfd9PTa1IU4
 dl6NMrU8FfOhXKQemh/QGp+GCxa2bindz/lf
 10 RRYvIcOWu2BDAGPNHVFD0ZD5LxJ8PiHDWaTL
 h7FpnJt0XQ44SFadA0Vt9Zi0GFJgAasewfnK
 9uhx+Q0HM60GXorQxS/RU8jIMB4=)
 8640 RRSIG DNSKEY 5 2 8640 20060104100453 (
 20051205100453 48254 chord.berkeley.edu.
 15 e5IYx0f/jT0z/tFa2wRt2NRZTOYO2zoxwiq
 7zoQhj2IR5IGHQkzvndqg54XmUdg8V+SwPf1
 UqeX+G+wnuAejLfGrqt2TkQSsVvZ3mVgJt+j
 EExuuWBFUxwg07GDsM+WZvQ67HQbshUC2NkC
 UCGt00V6ddyIEPbW2UVhyi6AyLQ=)
 20 0.chord.berkeley.edu. 8640 IN ChordNODE «192.234.98.98»
 «chord.berkeley.edu.»
 8640 RRSIG ChordNODE 5 3 8640 20060104100453 (
 20051205100453 48254 chord.berkeley.edu.
 25 zJsbRND8YziK26rYbABkYT07+IC+gdjsvea
 9oOjitL+NYFxE/ZVqdfhdID2PaX2WoKax0Vq
 IjvvxllC2759C1MG2WqzGFwf1yyoNbcLtRNI
 qqq4l9kXm4Mgj+JHLEv6z2cJbZoulJU5e62l
 7d6IU2MYg+KYsY+DQMq/XLv3gOA=)
 30 100 NSEC 1.chord.berkeley.edu. ChordNODE RRSIG NSEC
 100 RRSIG NSEC 5 3 100 20060104100453 (
 20051205100453 48254 chord.berkeley.edu.
 jXLkQJJUDz3me0n4L8is3MJIHxaCkkEh1OV

ZSdICLXx2A6Y7H0w0xKKJp+1zdMlc4mB0uZG
 1H8bdSaG6Do7R8s1K5j0T8gOAuoGVho5PPob
 Z2WTLfRqDcYBAxr9hSL4GMi0FGYTq2V6h8zg
 AbWOyCcZm+6hknQVTiKgf6nZTel=)

5

1.chord.berkeley.edu. 8640 IN ChordNODE «192.234.98.99»
 «chord.berkeley.edu.»

10

8640 RRSIG ChordNODE 5 3 8640 20060104100453 (
 20051205100453 48254 chord.berkeley.edu.
 zjJsbRND8YziK26rYbABkYT07+IC+gdjsvea
 9oOjitL+NYFxE/ZVqdfhdID2PaX2WoKax0Vq
 lJvvxllC2759C1MG2WqzGFwf1yyoNbcLtRNI
 qq4l9kXm4Mgj+JHLEv6z2cJbZoulJU5e62l
 7d6IU2MYg+KYsY+DQMq/XLv3gOA=)

15

100 NSEC 3.chord.berkeley.edu. ChordNODE RRSIG NSEC
 100 RRSIG NSEC 5 3 100 20060104100453 (

20

20051205100453 48254 chord.berkeley.edu.
 jXLikQJJUDz3me0n4L8is3MJHxaCkEh1OV
 ZSdICLXx2A6Y7H0w0xKKJp+1zdMlc4mB0uZG
 1H8bdSaG6Do7R8s1K5j0T8gOAuoGVho5PPob
 Z2WTLfRqDcYBAxr9hSL4GMi0FGYTq2V6h8zg
 AbWOyCcZm+6hknQVTiKgf6nZTel=)

3.chord.berkeley.edu. 8640 IN ChordNODE «192.234.98.100»
 «chord.berkeley.edu.»

25

8640 RRSIG ChordNODE 5 3 8640 20060104100453 (
 20051205100453 48254 chhord.berkeley.edu.
 zjJsbRND8YziK26rYbABkYT07+IC+gdjsvea
 9oOjitL+NYFxE/ZVqdfhdID2PaX2WoKax0Vq
 lJvvxllC2759C1MG2WqzGFwf1yyoNbcLtRNI
 qq4l9kXm4Mgj+JHLEv6z2cJbZoulJU5e62l
 7d6IU2MYg+KYsY+DQMq/XLv3gOA=)

30

100 NSEC chord.berkeley.edu. ChordNODE RRSIG NSEC

100 RRSIG NSEC 5 3 100 20060104100453 (
 20051205100453 48254 chord.berkeley.edu.
 jXLikQJJUDz3me0n4L8is3MJHxaCkkEh1OV
 ZSdlCLXx2A6Y7H0w0xKKJp+1zdMlc4mB0uZG
 5 1H8bdSaG6Do7R8s1K5j0T8gOAuoGVho5PPob
 Z2WTLfRqDcYBAxr9hSL4GMi0FGYTq2V6h8zg
 AbWOyCcZm+6hknQVTiKgf6nZTel=)

Une version plus allégée, sans les valeurs associées aux champs de type
 10 signatures donne le fichier suivant :
 ; *dnssec_signzone version 9.3.1*
 \$ORIGIN *chord.berkeley.edu*

@. 8640 IN SOA ns.berkeley.edu. bogdan\marinoiu.rd.francetelecom.com.
 15 (
 2005112301 ; *serial*
 200 ; *refresh (1 minute 40 seconds)*
 100 ; *retry (3 minutes 20 seconds)*
 604800 ; *expire (1 week)*
 20 100 ; *minimum (1 minute 40 seconds)*
)
 8640 RRSIG SOA [...]
 8640 NS ns.berkeley.edu.
 8640 RRSIG NS [...]
 25 100 NSEC 0.chord.berkeley.edu. NS SOA RRSIG NSEC DNSKEY
 100 RRSIG NSEC [...]
 8640 DNSKEY 256 3 5 (

```

5      AQPvG9Z4OwGpYryJeQ5oDGRJYc45hvLiLE99
      MzLwJ3Coix/FtidVexBqHRC9Js+fg/iJVWSm
      ue6VMluEteShtEohlc418/K9qAQcwyCS8ZNx
      scBKc1W1sw5RmCkCprGklfSUCUeP10SP/cPK
      yN/Z6/qSgvXxAVjh7IMauhVeltv2iw==
      ) ; key id = 48254
8640  DNSKEY 257 3 5 (
      AQOzHIM1NL7E5fuA3hpddBdXcHq3deTPHkLK
      nt3N3QPRc8XrXJ6WgHp9dreqS8uvp8bF76sB
10     pen/XP8bn9ybOJBz9++w0ScugKzIYbF6E/zE
      vGrKitky5iz1pZ+VsHwy78QKbDSMIsIqT25T
      L8Sx2VthbWJF1IRLuuTAMo7sGnNERw==
      ) ; key id = 27075
8640  RRSIG DNSKEY [...]
15     8640  RRSIG DNSKEY [...]

0.chord.berkeley.edu. 8640 IN ChordNODE «192.234.98.98»
      «chord.berkeley.edu.»
8640  RRSIG ChordNODE [...]
20     100  NSEC 1.chord.berkeley.edu. A RRSIG NSEC
      100  RRSIG NSEC [...]

1.chord.berkeley.edu. 8640 IN ChordNODE «192.234.98.99»
      «chord.berkeley.edu.»
25     8640  RRSIG ChordNODE [...]
      100  NSEC 3.chord.berkeley.edu. ChordNODE RRSIG NSEC
      100  RRSIG NSEC [...]

3.chord.berkeley.edu. 8640 IN ChordNODE
      «192.234.98.100»«chord.berkeley.edu.»
30     8640  RRSIG ChordNODE [...]
      100  NSEC chord.berkeley.edu. ChordNODE RRSIG NSEC
      100  RRSIG NSEC [...].

```

Dans ce dernier fichier, on constate que les champs NSEC indiquent

5 systématiquement le champ le plus proche qui suit. En cas d'interrogation pour le champ « 2.chord.berkeley.edu », le serveur implémentant DNSSEC retourne un message de type « NXDOMAIN » indiquant que le champ n'existe pas mais, grâce au champ de type NSEC, il indique que l'identifiant « 1.chord.berkeley.edu » est juste suivi par l'identifiant « 3.chord.berkeley.edu ».

10 Le client qui cherche à accéder à l'élément « 2.chord.berkeley.edu » reçoit alors une réponse qui, bien que ne permettant pas l'accès direct à l'élément recherché, lui permet d'accéder au réseau non hiérarchisé et, de manière indirecte, au nœud hébergeant les données relatives à l'identifiant « 2.chord.berkeley.edu ».

15 On décrit, ci-dessous, en regard de la figure 5, le fonctionnement d'une résolution d'un identifiant combiné mis en œuvre dans des modes de réalisation particuliers de la présente invention, en partant de l'exemple donné décrit ci-dessus dans le cas de la résolution de l'identifiant « 2 » dans le domaine « chord.berkeley.edu ».

20 Un client 500, par exemple de type ordinateur à usage général ou serveur, comporte des moyens de traitement 550, des moyens d'interrogation 555 et des moyens de réception 560 de réponse, de type connu mais adaptés à mettre en œuvre la présente invention. On considère que le client 500 souhaite accéder à l'élément d'identifiant « 2 » du domaine « chord.berkeley.edu ». Il a donc besoin de résoudre l'identifiant combiné « 2.chord.berkeley.edu », c'est-à-dire obtenir les locators (en français, localisateurs) relatifs à cet identifiant, comme, par exemple, l'adresse IP. L'identifiant combiné « 2.chord.berkeley.edu » est représentatif, d'une part, du nom de domaine, hiérarchisé, auquel est lié le réseau Chord, non hiérarchisé, et, d'autre part, de l'identifiant de l'élément de ce réseau Chord auquel le client 500 souhaite accéder, le nom « 2.chord.berkeley.edu » étant inconnu des serveurs de résolution de nom de domaine, par exemple les serveurs DNS.

30 Les moyens d'interrogation 555 émettent donc une requête 505 indiquant l'identifiant combiné aux serveurs DNS successivement responsables des domaines et sous-domaines représentés hiérarchiquement par l'identifiant combiné. Après trois interrogations auprès des serveurs gérant les domaines « . », « .edu » et « berkeley.edu », la requête arrive sur le serveur DNS 510 responsable du domaine « chord.berkeley.edu ». Le serveur DNS 510 comporte une mémoire

580 conservant une base de données de noms de domaine et d'adresses IP de serveurs responsables desdits sous-domaines, des moyens de traitement 565, des moyens de réception de requêtes 570 et des moyens d'émission de réponse 575, de type connu mais adaptés à mettre en œuvre la présente invention.

5 Le nom de domaine combiné n'existe pas dans la base de données du serveur DNS 510. Le message d'erreur renvoyé alors par le serveur DNS 510 est de type « NXDOMAINE ». En effet, puisque le serveur DNS 510 implémente l'option DNSSEC, le message d'erreur 515 est complété par le champ « NSEC » indiquant le nom de domaine qui précède le nom de domaine faisant l'objet de la
10 requête, et le nom de domaine qui suit le nom de domaine faisant l'objet de la requête, c'est-à-dire, dans l'exemple, respectivement « 3.chord.berkeley.edu. » et « 1.chord.berkeley.edu ». En effet, les noms de domaine étant classés par ordre lexicographique au sein de la zone, les noms de domaine qui encadrent l'identifiant recherché constituent des preuves de non existence du nom de
15 domaine recherché.

Préférentiellement, le client 500 indique, pour les identifiants combinés, comme type de requête, le type ChordNode et le serveur DNS 510 n'effectue une réponse comportant le champ « NSEC » que pour ce type de requête. Cela évite que le serveur DNS 510 effectue, pour tout type de requête, une réponse
20 comportant le champ « NSEC » et encombre, ainsi, le réseau hiérarchisé.

Le champ additionnel « NSEC » de la réponse adressée, par le serveur DNS 510 au client 500, comporte également les adresses IP des noms de domaine mentionnés par le champ de type « NSEC ».

Une fois la réponse reçue par les moyens de réception 560, le client 500
25 interprète la réponse 515 qu'il reçoit, c'est-à-dire un message d'erreur « NXDOMAIN » indiquant que le nom de domaine n'existe pas, et continue la recherche de l'élément en utilisant la réponse du serveur DNS et en suivant le protocole Chord. Les moyens d'interrogation 555 émettent alors la requête 520 vers le nom de domaine 525 qui suit, dans l'ordre lexicographique, celui faisant
30 l'objet de la requête, c'est-à-dire, ici, le nœud chord ayant l'identifiant binaire « 3 », et l'identifiant combiné « 3.chord.berkeley.edu. », selon le protocole Chord.

Le nœud 525 d'identifiant « 3 » étant capable, selon le protocole Chord exposé plus haut, de guider le client vers l'élément recherché, s'il ne possède pas

directement l'accès à cet élément, il communique au client 500 l'identifiant d'un serveur du réseau Chord plus proche de l'élément recherché, en mettant en œuvre sa table d'index. Ainsi, s'il ne possède pas la réponse, il permet au client de l'obtenir par itérations d'interrogations de serveurs du réseau Chord, mêmes si ces
5 serveurs possèdent un identifiant inconnu du système de nommage hiérarchisé, jusqu'à ce que le client obtienne l'accès à l'élément recherché, par exemple sous forme d'une adresse IP du serveur possédant l'élément recherché et la retourne au client 500, dans une réponse 530.

L'architecture décrite pour des modes particuliers de réalisation de la
10 présente invention permet d'insérer, au sein d'une architecture de nommage unique, ici le DNS, un espace de nommage dédié aux identifiants binaires.

L'invention permet, par exemple, d'intégrer le système Chord au système DNS par l'intermédiaire d'un nouveau champ DNS de type « ChordNODE ».

La figure 6 concerne la gestion des identifiants lors de la création, l'ajout, le
15 retrait et le référencement dans le système DNS, de serveurs sur ce réseau Chord.

On observe, en figure 6, une étape 605 d'ajout de création d'un réseau Chord avec au moins un serveur, comportant une étape 606 d'affectation du dernier identifiant non hiérarchisé à un serveur, dans la relation d'ordre, selon des
20 techniques connues en soi, une étape 607 d'affectation à chaque serveur du réseau Chord, de la responsabilité d'éléments dudit réseau Chord, par exemple dans une table de hachage distribuée et une étape 608 de création d'une table d'index pour chaque dit serveur.

Puis, au cours d'une étape 610, on attribue un identifiant combiné à au
25 moins un serveur du réseau Chord, dont au moins le serveur possédant le dernier identifiant non hiérarchisé, en complétant l'identifiant de chaque dit serveur sur le réseau Chord par le nom de domaine auquel appartient ce réseau et, éventuellement, par une information indiquant qu'il s'agit d'un identifiant combiné.

Au cours d'une étape 615, on met à jour la base de données du serveur
30 responsable dudit domaine et, au cours d'une étape 620, on propage l'identifiant combiné sur les serveurs caches dudit domaine.

Au cours d'une étape 625, on détermine si un serveur est ajouté dans le réseau Chord. Sinon, on passe à l'étape 650. Si oui, au cours d'une étape 626, on

affecte un identifiant non hiérarchisé audit serveur, au cours d'une étape 627, on affecte audit serveur la responsabilité d'éléments dudit réseau Chord possédant un identifiant non hiérarchisé, par exemple dans une table de hachage distribuée, au cours d'une étape 628, on crée une table d'index dudit serveur et au cours
5 d'une étape 629, on met à jour chaque table d'index de chaque autre serveur dudit réseau Chord. Puis, au cours d'une étape 630, on détermine si ledit serveur doit être référencé dans le serveur de résolution de nom DNS du domaine auquel appartient le réseau Chord. Si non, on passe à l'étape 650. Si oui, au cours d'une étape 635, on attribue un identifiant combiné audit serveur, en complétant son
10 identifiant sur le réseau Chord par le nom de domaine auquel appartient ce réseau et, éventuellement, par une information indiquant que cet identifiant est de type identifiant combiné, au sens de la présente invention. Au cours d'une étape 640, on met à jour la base de données du serveur responsable dudit domaine et, au cours d'une étape 645, on propage l'identifiant combiné sur les serveurs caches
15 dudit domaine.

Au cours d'une étape 650, on détermine si un serveur est retiré du réseau Chord. Sinon, on retourne à l'étape 625. Si oui, au cours d'une étape 655, on affecte à au moins un autre serveur du réseau Chord, la responsabilité d'éléments dudit réseau Chord qui étaient sous la responsabilité du serveur sortant. Puis, au
20 cours d'une étape 660, on met à jour chaque table d'index de chaque autre serveur dudit réseau Chord. Puis, au cours d'une étape 665, on détermine si ce serveur possède le dernier identifiant du réseau Chord. Si non, on passe à l'étape 685. Si oui, au cours d'une étape 670, on sélectionne un autre serveur du réseau Chord dont le nom combiné est référencé dans la base de données du serveur de
25 résolution de nom du domaine auquel appartient le réseau Chord. Au cours d'une étape 675, on attribue le dernier identifiant du réseau Chord au serveur sélectionné. Puis, au cours d'une étape 680, on modifie les affectations des éléments du réseau Chord entre les serveurs de ce réseau afin de respecter les règles d'affectation de ce type de réseau et on met à jour les tables d'index des
30 serveurs du réseau Chord.

Puis, au cours d'une étape 685, on détermine si ce serveur est référencé dans la base de données du serveur de résolution de nom du domaine auquel appartient le réseau Chord. Sinon, on passe à l'étape 625. Si oui, au cours d'une

étape 690, on met à jour la base de données du serveur responsable dudit domaine et, au cours d'une étape 695, on propage l'identifiant combiné sur les serveurs caches dudit domaine et on retourne à l'étape 625.

5 La figure 7 représente, sous forme d'un logigramme, des étapes mises en œuvre par un système informatique tentant d'accéder à un élément d'un réseau non hiérarchisé, en mettant en œuvre un premier mode de réalisation du procédé d'accès à un élément objet de la présente invention.

Au cours d'une étape 705, le client détermine le nom d'un élément auquel il doit accéder ainsi que le nom du domaine auquel appartient cet élément.

10 Au cours d'une étape 710, le client applique une fonction de hachage à au moins une partie dudit nom de l'élément pour déterminer l'identifiant de l'élément sur un réseau non hiérarchisé.

15 Au cours d'une étape 715, le client détermine le nom combiné de l'élément en complétant le résultat de la fonction de hachage avec le nom de domaine auquel appartient ledit élément.

Au cours d'une étape 720, le client effectue une requête concernant l'élément auquel l'accès est recherché, en indiquant que le type de requête est un type « ChordNode ».

20 Au cours d'une étape 725, le serveur DNS interrogé répond à la requête en fournissant l'adresse IP du serveur DNS responsable du sous-domaine suivant dans l'ordre hiérarchique des sous-domaines représentés par la partie hiérarchisée de l'identifiant combiné. On retourne alors à l'étape 720, les étapes 720 et 725 se répétant jusqu'au dernier serveur DNS, responsable du dernier sous-domaine représenté par la partie hiérarchisée de l'identifiant combiné.

25 Au cours d'une étape 730, ce dernier serveur DNS répond à la requête en indiquant, dans un champ « NSEC » :

- qu'il ne connaît pas le nom d'élément objet de la requête,
- le nom de l'élément qui succède, dans sa base de données, à l'identifiant demandé,
- 30 - l'adresse IP correspondant à ce nom,
- le nom de l'élément qui précède, dans sa base de données, l'identifiant demandé,
- l'adresse IP correspondant à ce nom.

La réponse du serveur DNS est ainsi, préférentiellement, représentative d'au moins un nom de serveur qui se trouve, dans l'ordre lexicographique et dans la mémoire dudit serveur de résolution de noms, immédiatement supérieur ou immédiatement inférieur audit identifiant.

- 5 On observe que la mise en œuvre des étapes 700 à 730 présente, à la fois les avantages du système DNS et les avantages des systèmes de nommage non hiérarchisés, par exemple, l'ajout ou le retrait aisé et rapide de fichiers ou de nœuds. En effet, dans les systèmes de nommage non hiérarchisés, les éléments sont gérés par les serveurs qui possèdent l'identifiant le plus proche, étant
10 entendu que la notion de proximité dépendant d'une fonction de distance définie pour le système de nommage non hiérarchisé.

Au cours d'une étape 735, le client détermine que la réponse comporte un champ « NSEC » et en extrait l'adresse IP du serveur possédant le nom qui succède à l'identifiant demandé.

- 15 Au cours d'une étape 740, le client adresse une requête identique à celle émise au cours des étapes 710 au serveur possédant le nom qui succède à l'identifiant demandé.

- Au cours d'une étape 745, le serveur qui reçoit cette requête détermine s'il gère l'élément demandé. Si oui, au cours d'une étape 750, il fournit au client,
20 l'accès à l'élément demandé, par exemple sous la forme d'un fichier, de données ou d'une adresse IP où le client peut télécharger l'élément demandé. Sinon, le serveur détermine, en mettant en œuvre la table de hachage distribuée DHT, le nom et l'adresse IP d'un serveur du réseau non hiérarchisé qui est plus proche du nom de l'élément demandé et qui lui succède, au cours d'une étape 755 et
25 retourne ce nom et cette adresse IP au client, au cours d'une étape 760.

Au cours d'une étape 765, le client adresse une requête identique à celle émise au cours des étapes 710 au serveur possédant le nom identifié au cours de l'étape 755. Puis, on retourne à l'étape 740.

- Le premier mode de réalisation du procédé d'accès objet de la présente
30 invention, illustré en figure 7, correspond au cas où le réseau non hiérarchisé est structuré comme exposé en regard de la figure 6, c'est-à-dire avec, en permanence, un serveur possédant un identifiant sur le réseau non hiérarchisé

supérieur aux identifiants de tous les autres éléments de ce réseau non hiérarchisé, ce serveur étant référencé dans le système DNS.

Le deuxième mode de réalisation du procédé objet de la présente invention, illustré en figure 8 correspond au cas où les éléments peuvent avoir un
5 identifiant sur le réseau non hiérarchisé qui soit supérieur à chaque identifiant de serveur de ce réseau référencé dans le système DNS.

La figure 8 représente, sous forme d'un logigramme, des étapes mises en œuvre par un système informatique tentant d'accéder à un élément d'un réseau non hiérarchisé, en mettant en œuvre un premier mode de réalisation du procédé
10 d'accès à un élément objet de la présente invention.

Au cours d'une étape 805, le client détermine le nom d'un élément auquel il doit accéder ainsi que le nom du domaine auquel appartient cet élément.

Au cours d'une étape 810, le client applique une fonction de hachage à au moins une partie dudit nom de l'élément pour déterminer l'identifiant de l'élément
15 sur un réseau non hiérarchisé.

Au cours d'une étape 815, le client détermine le nom combiné de l'élément en complétant le résultat de la fonction de hachage avec le nom de domaine auquel appartient ledit élément.

Au cours d'une étape 820, le client effectue une requête concernant
20 l'élément auquel l'accès est recherché, en indiquant que le type de requête est un type « ChordNode ».

Au cours d'une étape 825, le serveur DNS interrogé répond à la requête en fournissant l'adresse IP du serveur DNS responsable du sous-domaine suivant dans l'ordre hiérarchique des sous-domaines représentés par la partie
25 hiérarchisée de l'identifiant combiné. On retourne alors à l'étape 820, les étapes 820 et 825 se répétant jusqu'au dernier serveur DNS, responsable du dernier sous-domaine représenté par la partie hiérarchisée de l'identifiant combiné.

Au cours d'une étape 830, ce dernier serveur DNS répond à la requête en indiquant, dans un champ « NSEC » :

- 30
- qu'il ne connaît pas le nom d'élément objet de la requête,
 - le nom de l'élément qui succède, dans sa base de données, à l'identifiant demandé,
 - l'adresse IP correspondant à ce nom,

- le nom de l'élément qui précède, dans sa base de données, l'identifiant demandé,
- l'adresse IP correspondant à ce nom.

5 Au cours d'une étape 835, le client détermine que la réponse comporte un champ « NSEC » et en extrait les adresses IP des serveurs possédant, pour l'un, le nom qui succède à l'identifiant demandé et, pour l'autre, le nom qui précède l'identifiant demandé.

10 Au cours d'une étape 840, le client adresse une requête identique à celle émise au cours des étapes 810 au serveur possédant le nom qui succède à l'identifiant demandé, c'est-à-dire au serveur ayant le dernier des deux noms du champ « NSEC ».

15 Le client détermine alors si la réponse qu'il reçoit est un message d'erreur, ce qui indiquerait que le serveur qui a reçu cette requête ne fait pas partie du réseau non hiérarchisé, au cours d'une étape 845. Si oui, le client adresse, au cours d'une étape 850, une requête identique à celle émise au cours des étapes 840 au serveur possédant le nom qui précède l'identifiant demandé, c'est-à-dire au serveur ayant le premier des deux noms du champ « NSEC ».

20 Le procédé d'accès comporte, ainsi, une étape de détermination d'obtention d'un accès à l'élément recherché, de la part d'un serveur possédant un nom différent de l'identifiant recherché et, en l'absence d'obtention de cet accès, une étape d'interrogation d'un autre serveur possédant un dit nom différent dudit identifiant. Ainsi, si l'accès à l'élément recherché ne peut être obtenu de la part d'un serveur possédant un nom qui suit, dans l'ordre lexicographique, l'identifiant de l'élément recherché, on l'obtient de la part d'un serveur possédant un nom qui
25 précède, dans l'ordre lexicographique, l'identifiant combiné.

Le serveur qui a reçu la requête émise au cours de l'étape 850 ou le serveur qui a reçu la requête émise au cours de l'étape 840 et fait partie du réseau non hiérarchisé, détermine, au cours d'une étape 855, s'il gère l'élément demandé. Si oui, au cours d'une étape 860, il fournit au client, l'accès à l'élément
30 demandé, par exemple sous la forme d'un fichier, de données ou d'une adresse IP où le client peut télécharger l'élément demandé. Sinon, le serveur considéré détermine, en mettant en œuvre la table de hachage distribuée DHT, le nom et l'adresse IP d'un serveur du réseau non hiérarchisé qui est plus proche du nom de

l'élément demandé et qui lui succède, au cours d'une étape 865 et retourne ce nom et cette adresse IP au client, au cours d'une étape 870.

Au cours d'une étape 875, le client adresse une requête identique à celle émise au cours des étapes 810 au serveur possédant le nom identifié au cours de
5 l'étape 865. Puis, on retourne alors à l'étape 855.

Comme on le voit en regard des figures 3 à 8, conformément à la présente invention, pour obtenir l'accès à un élément possédant un identifiant, le client effectue l'interrogation des serveurs de résolution de noms d'un système de nommage hiérarchique, ici DNS, en leur fournissant l'identifiant combiné. L'un de
10 ces serveurs répond en fournissant au moins un nom de serveur différent dudit identifiant et hiérarchiquement au même niveau que ledit identifiant, serveur du réseau non hiérarchisé référencé dans le système DNS. Puis, le client interroge au moins un tel serveur.

Ainsi, quelle que soit la complexité et les modifications dynamiques du
15 réseau non hiérarchisés, un élément possédant un identifiant inconnu du système de résolution d'adresse peut être retrouvé par l'intermédiaire du serveur du réseau non hiérarchisé référencé dans le système DNS, bien que son nom soit différent de l'identifiant de l'élément recherché.

La mise en œuvre de la présente invention permet ainsi d'intégrer deux
20 systèmes de nommage, hiérarchique et non hiérarchique, de manière à utiliser, dans le système DNS, des identifiants possédant, en partie, un identifiant non-hiérarchique propre à un domaine.

La présente invention ne se limite pas aux modes de réalisation décrits et représentés. Elle s'applique, bien au contraire, à tout procédé et dispositif dans
25 lequel, en réponse à une requête spécifiant un identifiant d'élément sur un réseau, identifiant inconnu d'un système informatique, celui-ci répond en fournissant un identifiant (nom ou adresse IP, par exemple) qui est connue de lui et, préférentiellement, l'identifiant ainsi fourni est le plus proche, parmi tous les identifiants connus du système informatique, dans l'ordre lexicographique, de
30 l'identifiant objet de la requête.

Ainsi, dans certains modes de réalisation de la présente invention appliqués aux réseaux de type Chord, le client ne met en œuvre aucune étape nouvelle. Par exemple, le dernier serveur DNS interrogé répond à la requête qui lui est adressée

en fournissant l'identifiant qu'il connaît le plus proche et immédiatement supérieur, dans l'ordre lexicographique, à l'identifiant spécifié dans la requête adressée par le client, sans indiquer qu'il ne s'agit pas du serveur possédant l'identifiant spécifié dans la requête. Ainsi, à la différence des modes de réalisation illustrés en figures 5 7 et 8, le client n'est pas informé de cette différence entre l'identifiant fourni et l'identifiant requis. On observe, néanmoins, que ces deux identifiants sont alors, préférentiellement, au même niveau hiérarchique dans le système de nommage hiérarchique puisqu'ils représentent le même nom de domaine et deux identifiants de réseau non hiérarchisés différents.

10 En utilisant l'identifiant qui lui est retourné dans une nouvelle requête, comme s'il s'agissait de l'adresse correspondant à l'identifiant spécifié dans la requête, le client accède alors à un serveur du réseau non hiérarchisé et obtient, de sa part, directement ou indirectement, comme exposé en regard de la figure 7, l'accès à l'élément possédant ledit identifiant.

15 Ce mode de réalisation particulier présente l'avantage de ne pas nécessiter de modification, matérielle ou logicielle, au niveau des clients.

REVENDEICATIONS

- 1 - Procédé d'accès à un élément possédant un identifiant, caractérisé en ce qu'il comporte :
- 5 - au moins une étape d'interrogation (720, 820) d'un serveur de résolution de noms d'un système de nommage hiérarchique, responsable d'un domaine représenté par ledit identifiant, ladite interrogation comportant ledit identifiant,
 - une étape de réception (730, 830) d'une réponse provenant d'un dit
10 serveur de résolution de noms, ladite réponse étant représentative d'au moins un nom de serveur différent dudit identifiant et hiérarchiquement au même niveau que ledit identifiant et
 - une étape d'interrogation (740, 840, 850) d'un serveur possédant un dit nom différent dudit identifiant.
- 15 2 – Procédé selon la revendication 1, caractérisé en ce que, au cours de l'étape de réception d'une réponse (730 830), ladite réponse est représentative, d'une part, de ce que ledit identifiant est inconnu dudit serveur de résolution de noms et, d'autre part, de chaque dit nom différent dudit identifiant.
- 3 - Système de nommage caractérisé en ce qu'il attribue, pour au moins un
20 élément (200 à 215), un identifiant combiné représentatif, d'une part, d'un nom selon un système de nommage hiérarchisé et, d'autre part, d'un identifiant d'élément d'un système de nommage non hiérarchisé, l'identifiant du système de nommage hiérarchisé permettant l'accès à un serveur et l'identifiant du système de nommage non hiérarchisé permettant l'accès aux éléments accessibles audit
25 serveur, en mettant en œuvre le système de nommage non hiérarchisé.
- 4 - Procédé de nommage d'un élément d'un réseau non hiérarchisé sur lequel les identifiants sont gérés par intervalle, caractérisé en ce qu'il comporte une étape d'attribution (610 à 620), audit élément, d'un nom hiérarchisé d'un domaine possédant un serveur dudit réseau non hiérarchisé et une étape d'attribution
30 (610), audit élément, d'un complément de nom représentant son identifiant sur le réseau non hiérarchisé.
- 5 - Procédé selon la revendication 4, caractérisé en ce qu'il comporte, en outre, une étape de mise à jour d'une table distribuée dans laquelle chaque élément du

réseau non hiérarchisé est mis en relation avec un identifiant de serveur responsable dudit élément.

- 6 - Procédé selon l'une quelconque des revendications 4 ou 5, caractérisé en ce qu'il comporte, en outre, une étape de référencement (615, 620, 630 à 645) d'au moins un serveur dudit réseau non hiérarchisé sur au moins un serveur de résolution de nom de domaine (510).
hiérarchisés.

7 – Procédé de réponse, par un serveur, à une interrogation de résolution de nom comportant un identifiant, caractérisé en ce qu'il comporte :

- 10 - lorsque ledit serveur conserve, en mémoire, une adresse correspondant audit identifiant, une étape de réponse au cours de laquelle ledit serveur fournit ladite adresse (725) et
- lorsque ledit serveur ne conserve pas, en mémoire, une adresse correspondant audit identifiant, une étape de réponse au cours de laquelle ledit serveur fournit une réponse représentative d'au moins un nom de serveur différent dudit identifiant et hiérarchiquement au même niveau que ledit identifiant, sans indication de ce que ledit nom est différent dudit identifiant (730).

- 8 – Procédé selon la revendication 7, caractérisé en ce que, lorsque ledit serveur ne conserve pas, en mémoire, une adresse correspondant audit identifiant, au cours de l'étape de réponse (730), ladite réponse est représentative d'au moins un nom de serveur qui se trouve, dans l'ordre lexicographique et dans la mémoire dudit serveur, immédiatement supérieur ou immédiatement inférieur audit identifiant.

- 9 - Terminal (500) d'accès à un élément possédant un identifiant, caractérisé en ce qu'il comporte :

- un moyen d'interrogation (555) adapté à interroger au moins un serveur de résolution de noms d'un système de nommage hiérarchique, responsable d'un domaine représenté par ledit identifiant, ladite interrogation comportant ledit identifiant et
- un moyen de réception (560) d'une réponse provenant d'un dit serveur de résolution de noms, ladite réponse étant représentative d'au moins

un nom de serveur (525) différent dudit identifiant et hiérarchiquement au même niveau que ledit identifiant,

ledit moyen d'interrogation étant adapté à interroger un serveur possédant un dit nom différent dudit identifiant.

5 10 – Terminal selon la revendication 9, caractérisé en ce que ledit moyen d'interrogation (555) est adapté à ce que ledit identifiant soit un identifiant dit « combiné » représentatif, d'une part, du nom dudit domaine et, d'autre part, d'un identifiant d'élément sur un réseau dit « non hiérarchisé » (200 à 215) qui comporte ledit serveur possédant ledit nom différent dudit identifiant et ledit
10 élément.

11 – Terminal selon l'une quelconque des revendications 9 à 10, caractérisé en ce que le moyen d'interrogation (555) est adapté à déterminer si un accès audit élément a été obtenu de la part d'un dit serveur (525) possédant un nom différent dudit identifiant et, dans la négative, à interroger un autre serveur possédant un dit
15 nom différent dudit identifiant.

12 – Serveur (510) de résolution de nom comportant un identifiant comportant une mémoire (580) dans laquelle des identifiants sont associés à des adresses en une interrogation, caractérisé en ce qu'il comporte un moyen de réponse adapté

- lorsque ladite mémoire conserve une adresse correspondant audit
20 identifiant, à fournir une réponse représentative de ladite adresse et
- lorsque ladite mémoire ne conserve pas une adresse correspondant audit identifiant, à fournir une réponse représentative d'au moins un nom de serveur différent dudit identifiant et hiérarchiquement au même niveau que ledit identifiant, sans indication de ce que ledit nom est
25 différent dudit identifiant.

13 - Programme d'ordinateur chargeable dans un système informatique, ledit programme contenant des instructions permettant la mise en œuvre du procédé de procédé d'accès à un élément possédant un identifiant selon l'une quelconque des revendications 1 à 2, lorsque ce programme est chargé et exécuté par un
30 système informatique.

14 - Programme d'ordinateur chargeable dans un système informatique, ledit programme contenant des instructions permettant la mise en œuvre du procédé de procédé de nommage d'un élément selon l'une quelconque des revendications

4 à 6, lorsque ce programme est chargé et exécuté par un système informatique.

- 15 - Programme d'ordinateur chargeable dans un système informatique, ledit programme contenant des instructions permettant la mise en œuvre du procédé de procédé de réponse à une interrogation selon l'une quelconque des
- 5 revendications 7 ou 8, lorsque ce programme est chargé et exécuté par un système informatique.

1/7

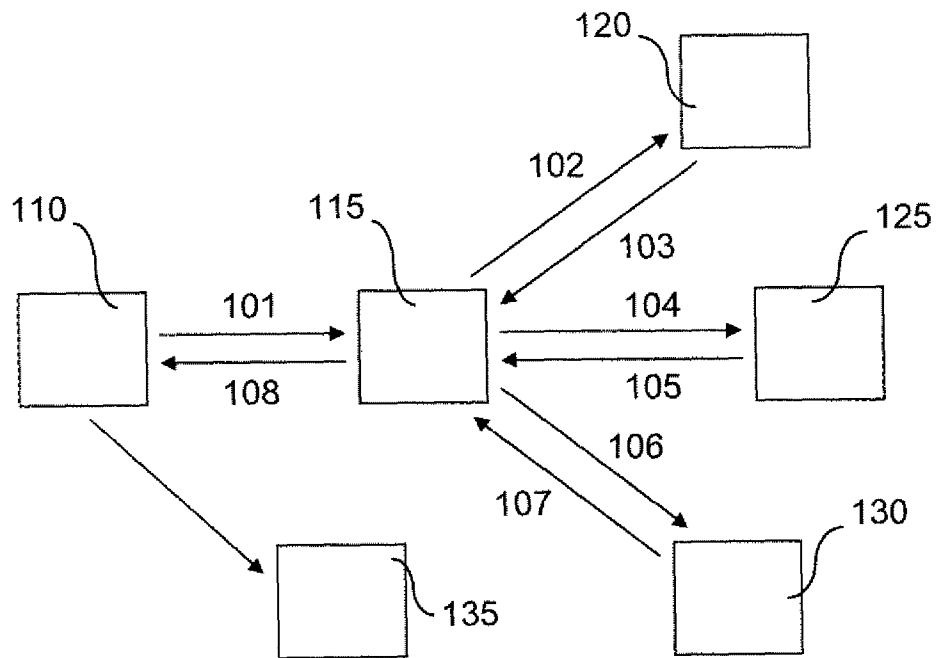


Figure 1

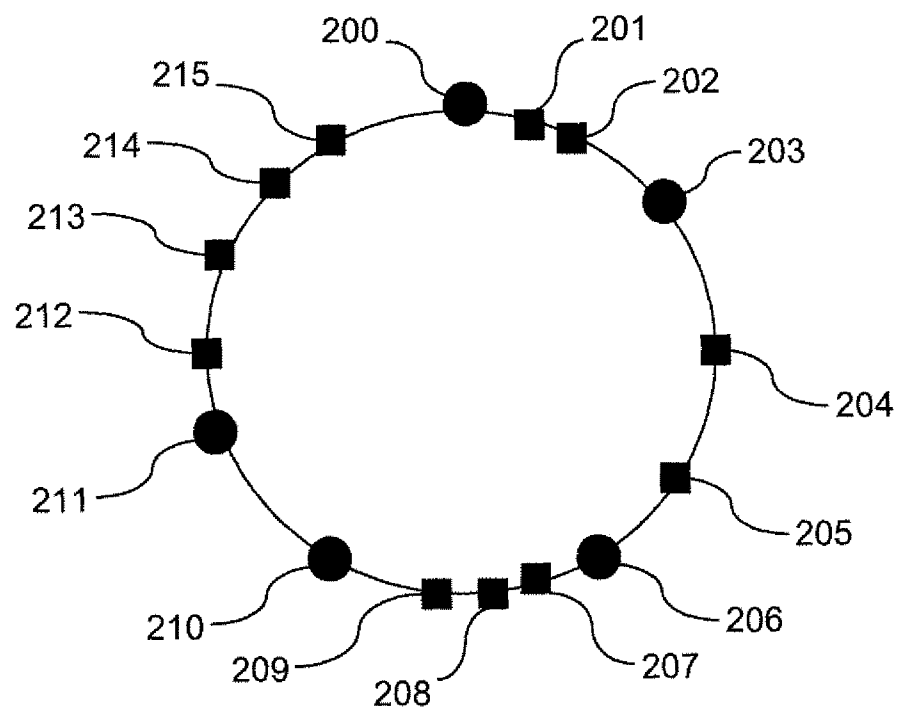


Figure 2

2/7

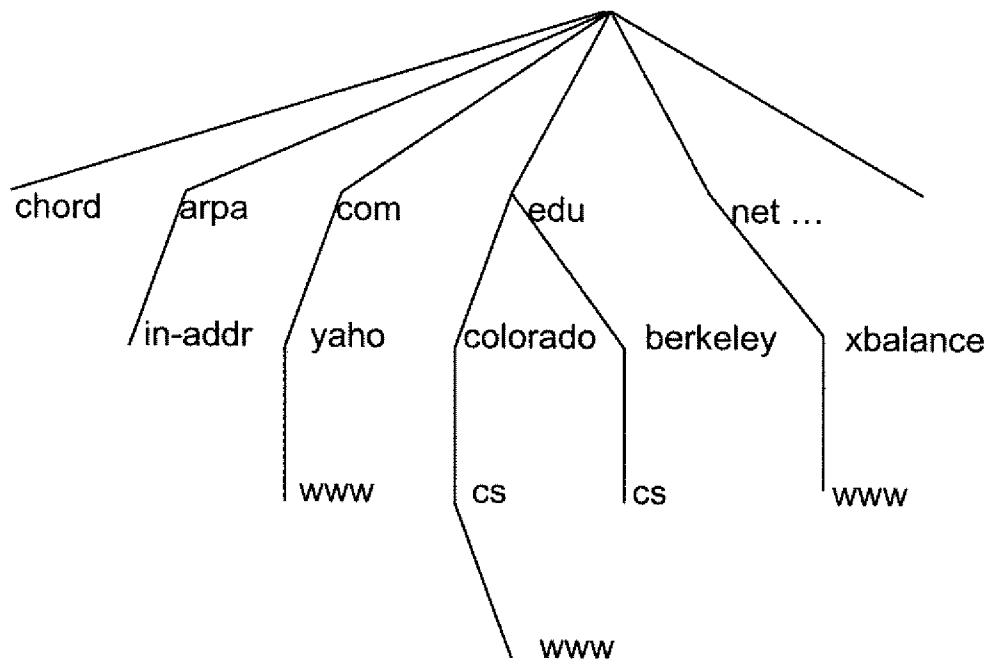


Figure 3

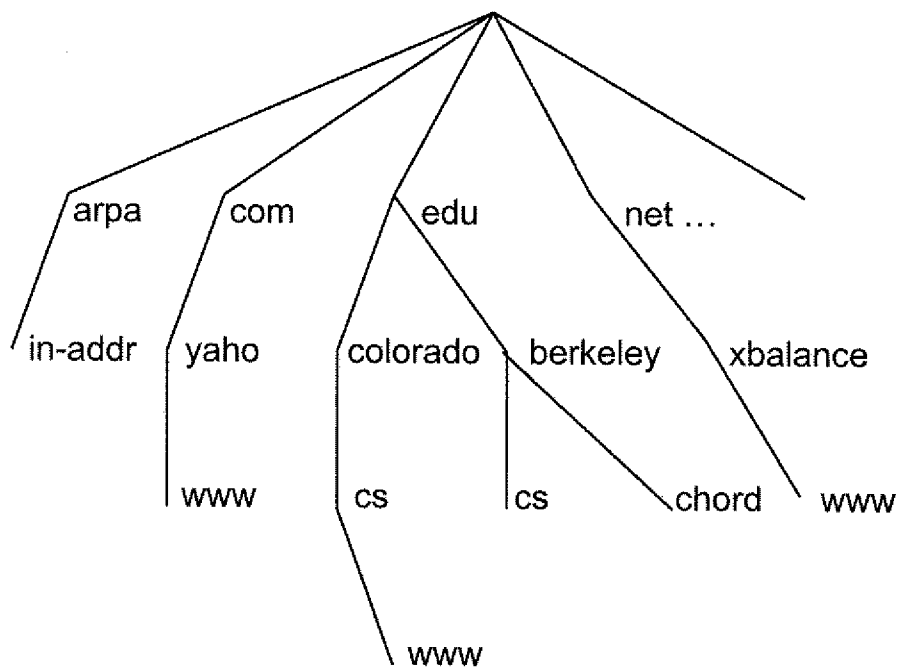


Figure 4

3/7

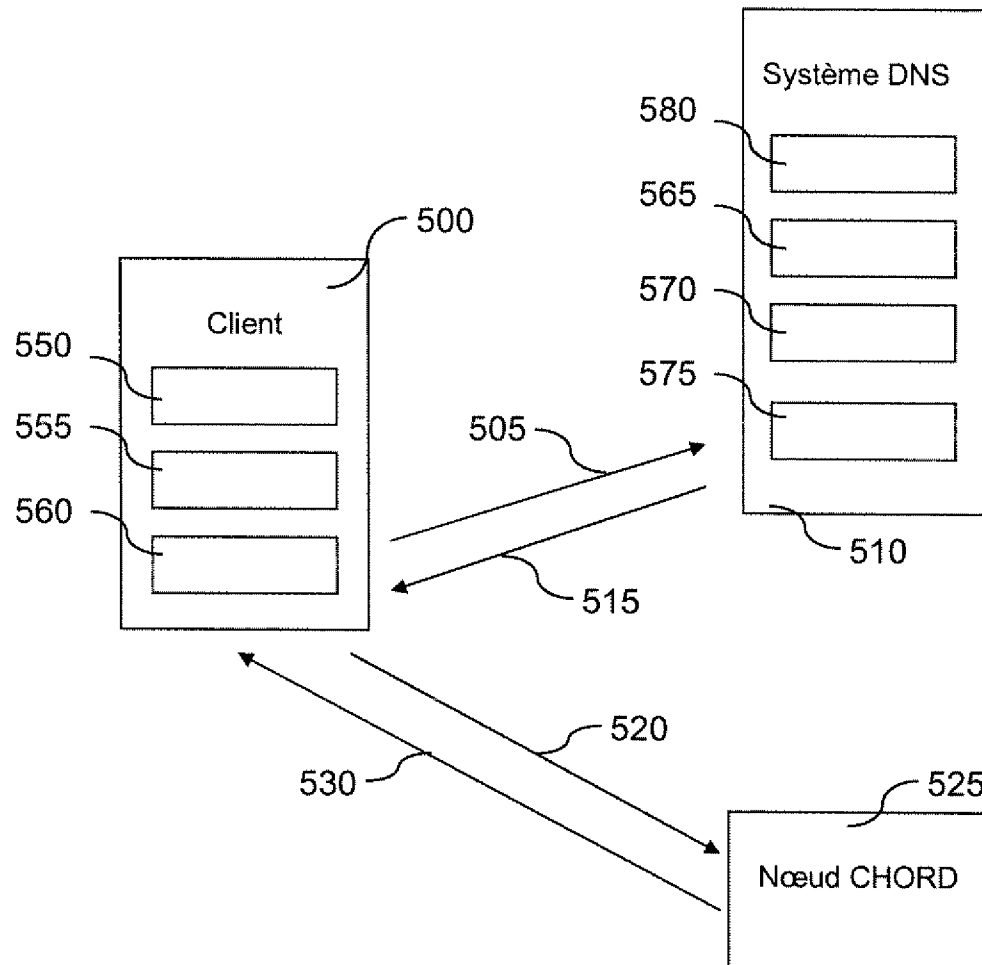


Figure 5

4/7

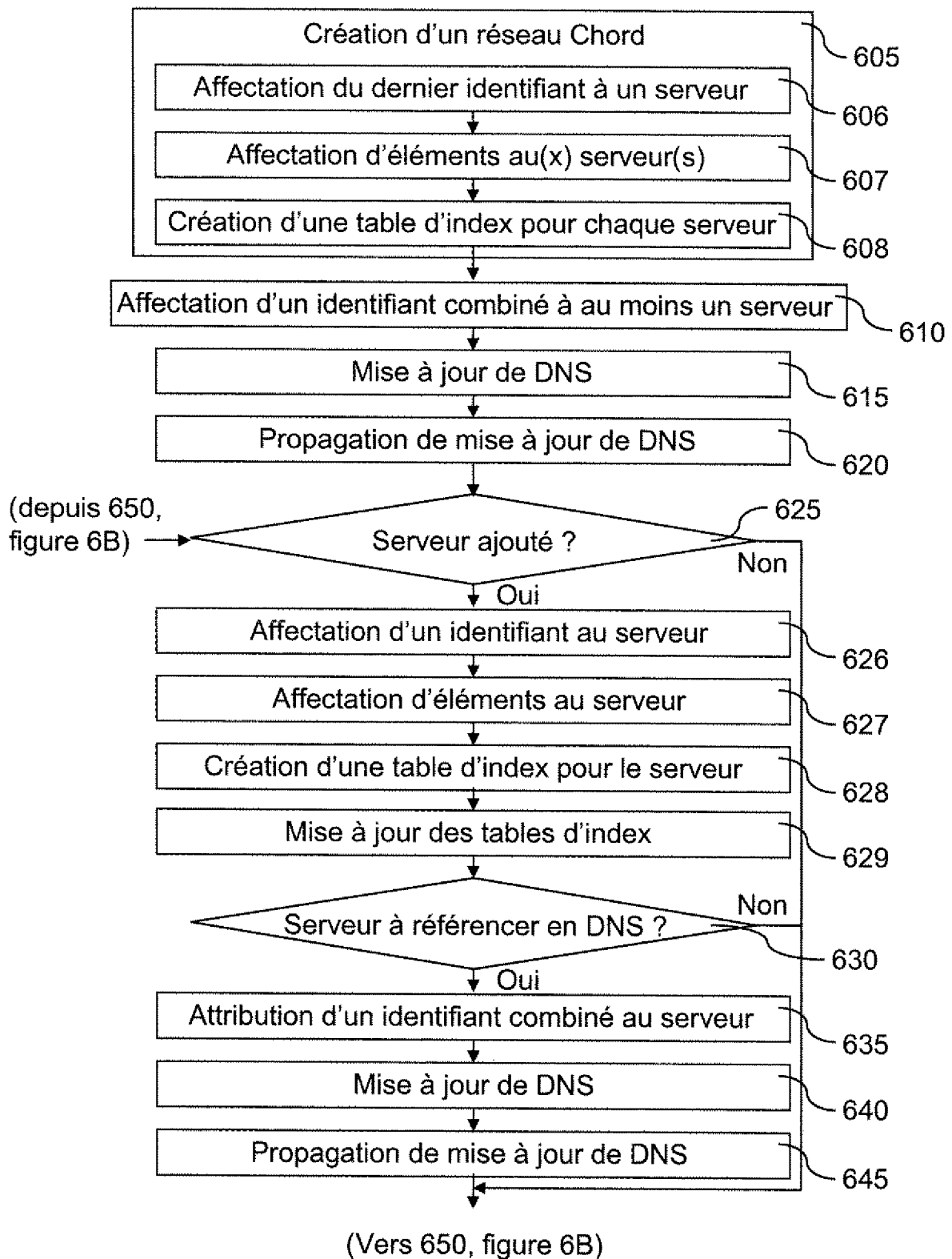


Figure 6A

5/7

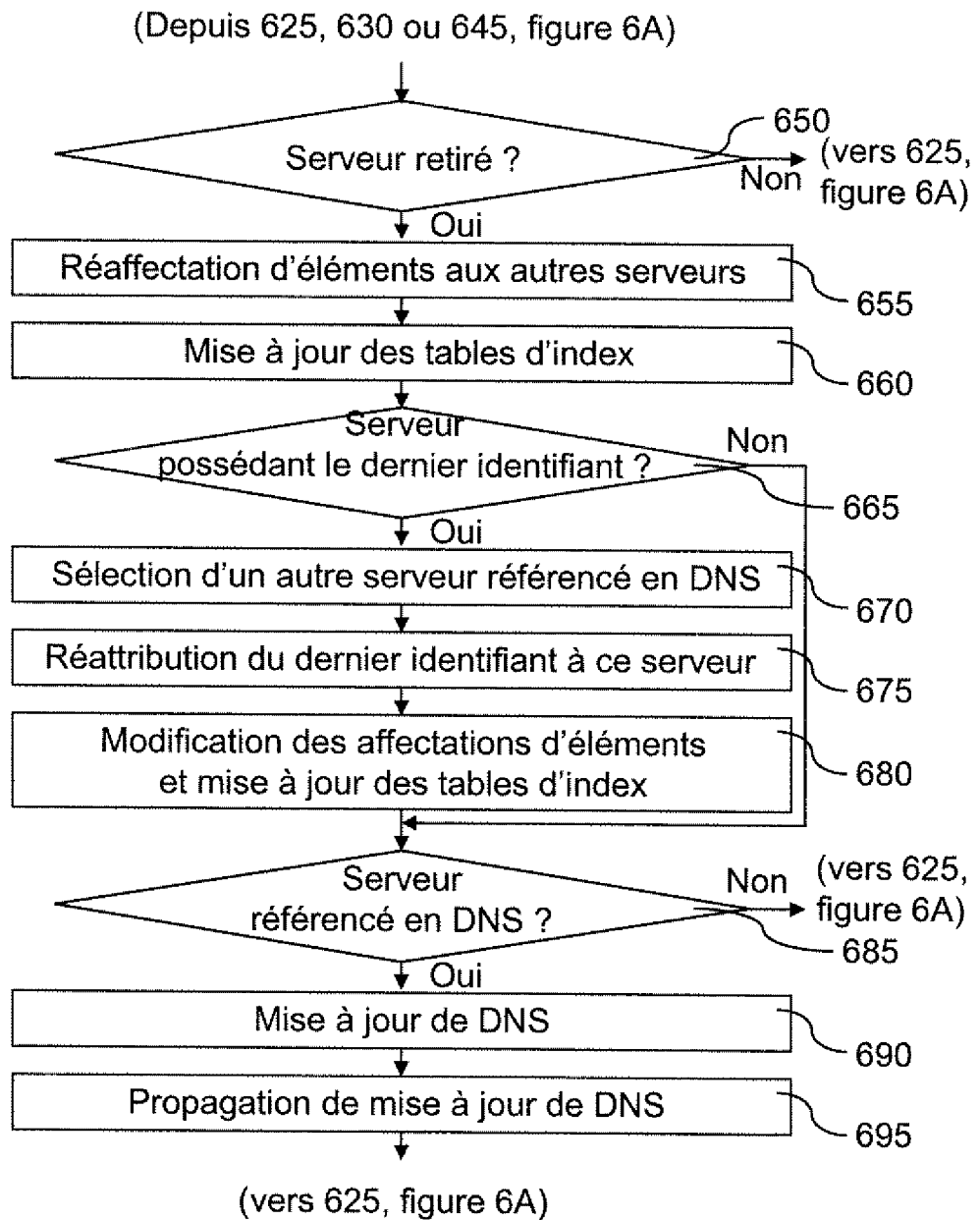


Figure 6B

6/7

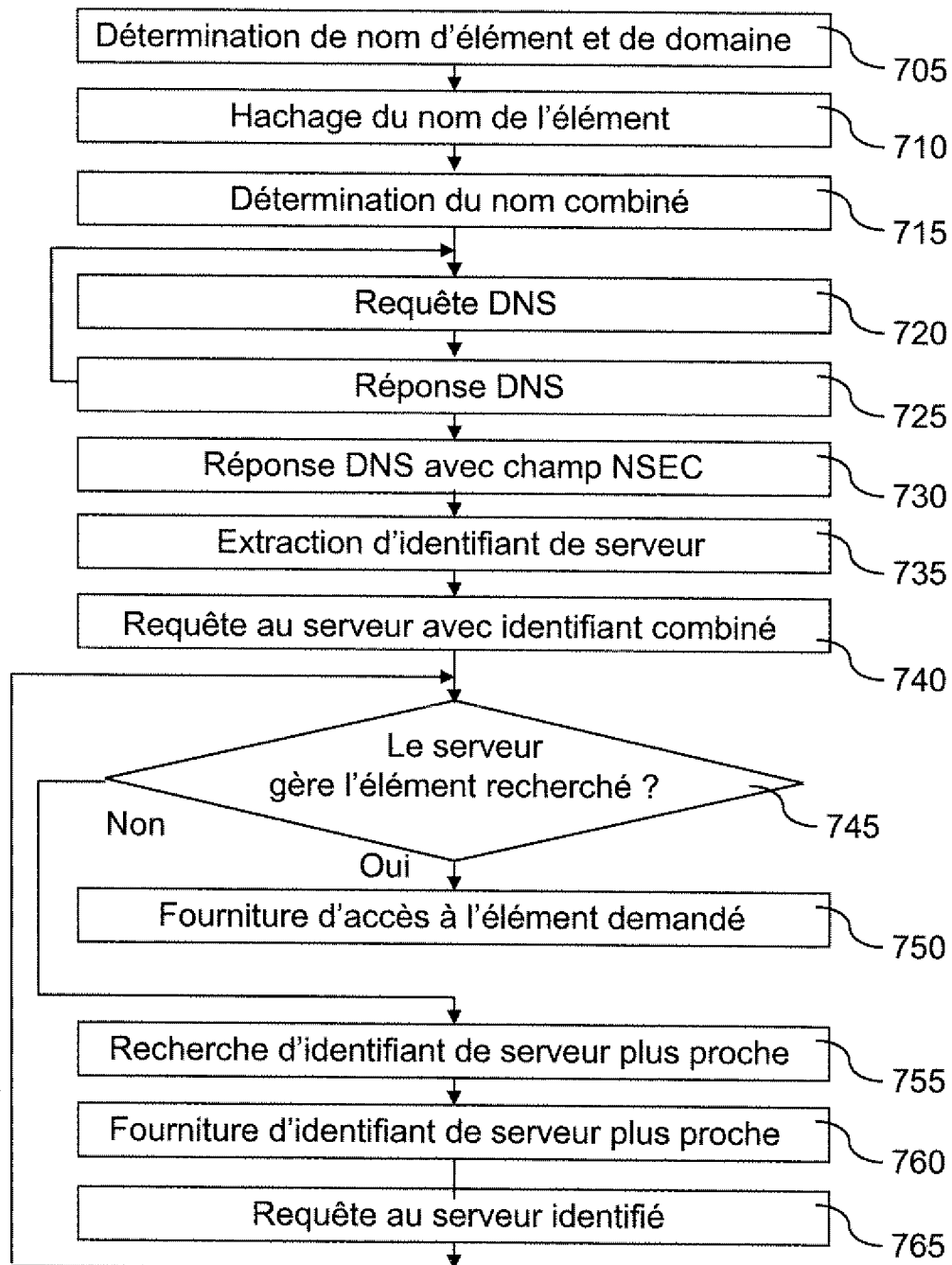


Figure 7

7/7

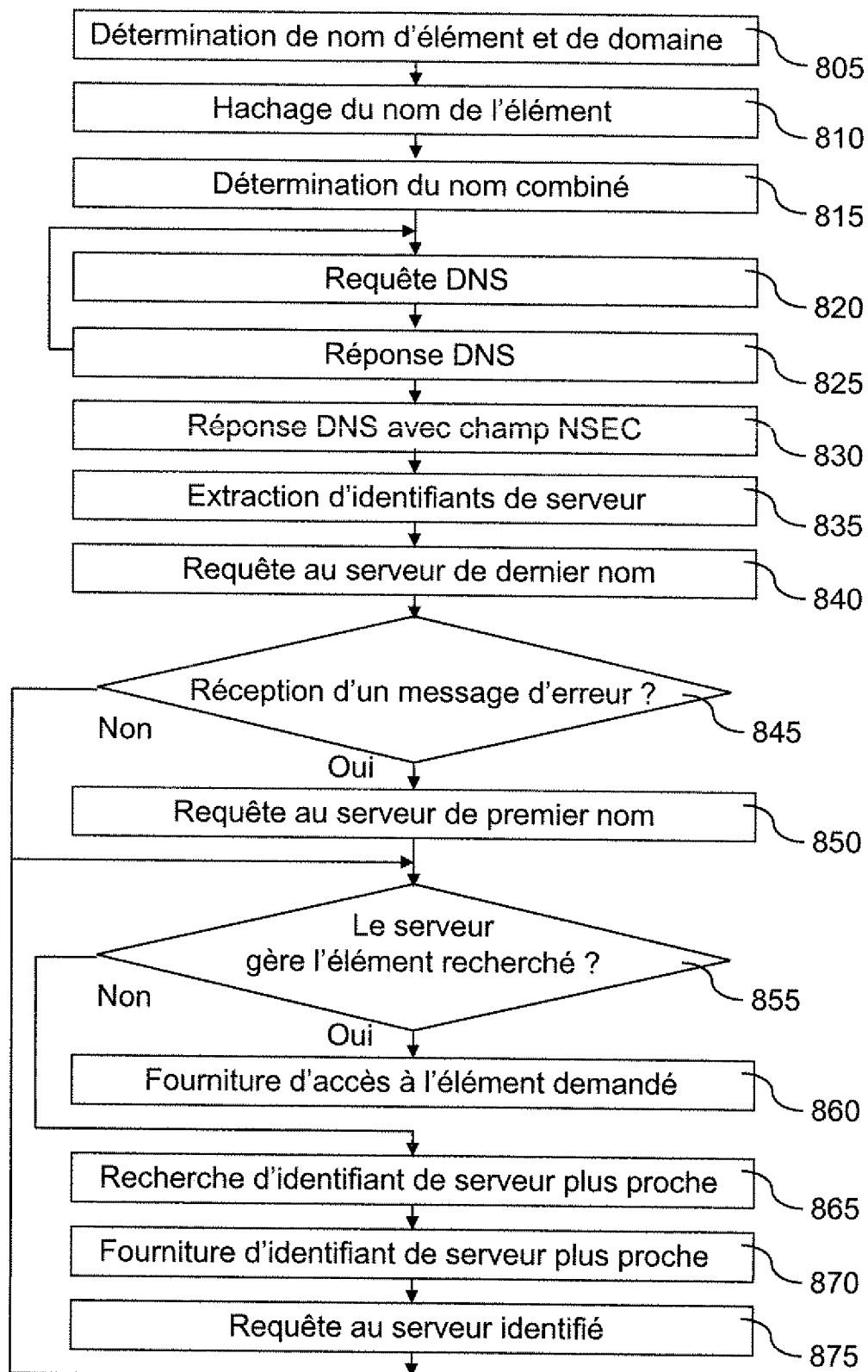


Figure 8