

(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  
4 janvier 2007 (04.01.2007)

PCT

(10) Numéro de publication internationale  
**WO 2007/000552 A2**

(51) Classification internationale des brevets : **Non classée**

(21) Numéro de la demande internationale :  
PCT/FR2006/050621

(22) Date de dépôt international : 22 juin 2006 (22.06.2006)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :  
0506572 28 juin 2005 (28.06.2005) 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) : **TUFFIN,**  
**Stéphane** [FR/FR]; 5 Residence Des Chênes, F-22700  
Louannec (FR). **BOURDAIS, François** [FR/FR]; Res-  
idence Baccara, 327 Chemin Du Petit Four, F-06600  
Antibes (FR).

(74) Mandataire : **CASPAR, Catherine**; FRANCE TELE-  
COM R & D/PIV/BREVETS, 38-40 Rue Du Général  
Leclerc, F-92794 Issy Les 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, BR, BW, BY, BZ, CA, CH, CN, CO,  
CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,  
GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE,  
KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU,  
LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG,  
NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD,  
SE, SG, SK, SL, SM, 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, HU, IE, IS, IT, LT, LU, LV, MC, 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).

**Publiée :**

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

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

(54) Title: METHOD FOR OBTAINING CONFIGURATION DATA FOR A TERMINAL BY USING THE DHCP PROTOCOL

(54) Titre : PROCEDE D'OBTENTION DE DONNEES DE CONFIGURATION POUR UN TERMINAL PAR UTILISATION  
DU PROTOCOLE DHCP

(57) Abstract: The method comprises a step consisting of inserting, into a predefined option field, a DHCP query emitted by a  
DHCP client module for obtaining configuration data, optional data containing an identifier, directly or indirectly, to a single user  
of said terminal with the aim of obtaining configuration data personalized for said user.

(57) Abrégé : Le procédé comprend une étape consistant à insérer dans un champ d'option prédéfini d'une requête DHCP émise par  
module client DHCP pour l'obtention de 10 données de configuration, des données optionnelles comprenant un identifiant, directe-  
ment ou indirectement, à un seul utilisateur dudit terminal, en vue de l'obtention de données de configuration personnalisées pour  
ledit utilisateur.



WO 2007/000552 A2

Procédé d'obtention de données de configuration pour un terminal  
par utilisation du protocole DHCP

L'invention concerne un procédé d'obtention de données de configuration pour un terminal par utilisation du protocole DHCP. Plus précisément, l'invention a pour objet un procédé d'obtention de données de configuration d'un terminal ainsi qu'un procédé de traitement par un serveur d'une ou plusieurs requêtes DHCP émises par un module client DHCP d'un terminal pour l'obtention de données de configuration dudit terminal.

Le protocole DHCP (Dynamic Host Configuration Protocol) permet à un terminal connecté à un réseau d'obtenir des données de configuration, notamment une adresse IP (Internet Protocol), auprès d'un serveur de traitement connecté à ce même réseau. Ce protocole définit un ensemble de requêtes permettant d'établir un dialogue entre, d'une part, un module client mis en œuvre dans le terminal et, d'autre part, un module serveur mis en œuvre dans le serveur. Ces requêtes sont envoyées soit directement du module client au module serveur et vice versa, soit par le biais d'un relais DHCP.

Le protocole DHCP peut être utilisé pour différents types de terminaux: PC, routeur, téléphones IP, SetTopBox, visiophones, caméra vidéo, etc, dès lors qu'un tel terminal comprend un module client DHCP apte à dialoguer avec un module serveur DHCP. De tels terminaux sont dénommés ici de manière simplifiée terminaux IP.

Pour prendre en compte cette grande diversité de terminaux IP lors du traitement des requêtes DHCP, le protocole DHCP spécifie que les requêtes DHCP émises à partir d'un terminal donné doivent contenir l'adresse MAC du terminal. Cette adresse MAC permet d'identifier de manière univoque l'interface réseau du terminal, mais elle est insuffisante pour déterminer la nature du terminal.

Le protocole DHCP prévoit par ailleurs que les requêtes DHCP peuvent contenir des données optionnelles permettant de gérer la diversité des terminaux ou la diversité des besoins des utilisateurs de ces terminaux. Ces données optionnelles sont insérées dans un champ d'option de la requête et comprennent par exemple:

- des données qui identifient le type de terminal, ces données étant envoyées en utilisant l'option 60 du protocole DHCP ("Vendor Class Identifier");
- des données qui identifient un groupe d'utilisateurs ou un ensemble d'applications associé à ce groupe d'utilisateur, ces données étant envoyées en utilisant l'option 77 du protocole DHCP ("User Class");

- des données qui identifient la ligne réseau d'arrivée de la requête, lorsque les requêtes sont interceptées par un relais DHC interconnectant au moins deux réseaux, ces données étant envoyées en utilisant l'option 82 du protocole DHCP.

Ces différentes données permettent de traiter de manière appropriée la requête DHCP qui les contient. En effet, il est notamment possible de générer une réponse qui est fonction soit du type de terminal émetteur, soit du groupe d'utilisateur, soit encore du réseau d'arrivée de la requête. En particulier, l'adresse IP générée peut être fonction de ces données. L'affectation dynamique d'adresse IP aux terminaux d'un réseau peut ainsi être exécutée de manière automatique, à partir de telles données.

Toutefois, il existe des cas particuliers dans lesquels certains utilisateurs, appartenant à un groupe d'utilisateur donné, peuvent avoir des besoins spécifiques en terme de configuration réseau. Certains utilisateurs peuvent ainsi avoir besoin d'une adresse IP statique - et non pas d'une adresse IP dynamique - qui leur permette d'accéder à un service particulier, par exemple à une base de données qui procède à une identification de l'utilisateur à partir de son adresse IP et détermine en conséquence les droits d'accès aux données de la base.

Une solution connue à ce type de problème est d'attribuer manuellement une adresse IP statique au terminal. L'inconvénient est que cette solution suppose une intervention du personnel de maintenance informatique pour chaque cas de figure. En outre, elle ne fonctionne que dans le cas où le besoin est celui d'une adresse IP statique.

Un des buts de l'invention est de fournir un procédé d'obtention de données de configuration d'un terminal au moyen de requêtes DHCP ainsi qu'un procédé de traitement de telles requêtes, qui ne présentent pas les inconvénients évoqués plus haut pour les solutions antérieures, qui soient compatibles avec le protocole DHCP et permettent notamment une gestion des données de configurations des différents terminaux d'un réseau qui soit entièrement automatisable et adaptable aux besoins spécifiques de certains utilisateurs.

Dans ce but l'invention a pour objet un procédé d'obtention de données de configuration d'un terminal, le terminal comprenant un module client DHCP apte à communiquer via un réseau avec au moins un module serveur DHCP conformément au protocole DHCP, le procédé comprenant les étapes suivantes:

- génération par ledit module client DHCP d'une ou plusieurs requêtes DHCP pour l'obtention de données de configuration dudit terminal,

- transmission desdites une ou plusieurs requêtes DHCP via ledit réseau par ledit module client DHCP audit au moins un module serveur DHCP,

- réception des données de configuration reçues par ledit module client DHCP en réponse à au moins une desdites une ou plusieurs requêtes DHCP,

5        le procédé comprenant en outre une étape consistant à insérer, dans un champ d'option prédéfini d'au moins une des requêtes DHCP, des données optionnelles comprenant un identifiant associé, directement ou indirectement, à un seul utilisateur dudit terminal, les données de configuration reçues étant personnalisées pour ledit utilisateur.

10       L'insertion dans une des requêtes d'un identifiant, associé à un et un seul utilisateur du terminal, permet la génération d'une réponse à cette requête qui est personnalisée pour un utilisateur donné, identifié, indirectement ou indirectement par l'identifiant inséré. De la sorte, les données de configuration peuvent être générées de manière à répondre aux besoins spécifiques d'un utilisateur donné.

15       De plus, le procédé permet d'envisager un contrôle sur la génération de données de configuration, et notamment, d'effectuer une identification de l'utilisateur dès sa connexion au réseau, voire de refuser l'attribution de données de configuration de manière à empêcher un utilisateur d'accéder au réseau. La sécurisation de l'accès au réseau intervient de ce fait dès la demande de  
20       configuration, et est ainsi renforcée.

Le procédé apporte de surcroît une réponse pratique aux situations de nomadisme dans lesquelles un même utilisateur peut se connecter à un réseau en utilisant chaque fois un terminal différent, par exemple en utilisant un terminal parmi une pluralité de terminaux accessibles en libre service.

25       Enfin, le procédé est en outre compatible avec le protocole DHCP et ne nécessite pas de modification des principes de base de ce protocole.

Selon un mode de réalisation avantageux, le procédé comprend une étape consistant à lire tout ou partie des données optionnelles dans un support personnel d'enregistrement accessible à partir du terminal. Un tel support d'enregistrement est  
30       typiquement une carte à puce. Ce mode de réalisation permet de faciliter l'étape d'insertion de l'identifiant dans la requête DHCP, un simple dispositif de lecture de carte à puce étant nécessaire.

Selon une variante de ce mode de réalisation, le support personnel d'enregistrement est un support dont l'accès est sécurisé par un code d'identification.  
35       Ceci permet de sécuriser l'accès à cet identifiant et son introduction dans la requête

et réduit les chances de succès d'une utilisation frauduleuse du support personnel d'enregistrement.

Selon une autre variante de ce mode de réalisation, le support personnel d'enregistrement est de type support amovible. Un utilisateur en situation de mobilité  
5 peut ainsi se munir de son support amovible pour retrouver une configuration adaptée et personnalisée quel que soit le terminal qu'il utilise.

Selon une autre variante de ce mode de réalisation, le support personnel d'enregistrement est intégré dans un terminal mobile et est accessible à partir dudit terminal par un lien local de communication établi entre ledit terminal et ledit terminal  
10 mobile. Cette variante évite à l'utilisateur d'un terminal mobile, par exemple d'un téléphone mobile, de se munir d'un support supplémentaire pour le stockage de l'identifiant.

L'identifiant peut être par exemple:

- un identifiant dudit utilisateur,
- 15 - un identifiant d'immatriculation d'un support personnel d'enregistrement associé audit utilisateur,
- un identifiant d'un objet associé audit utilisateur,
- un identifiant d'un service associé audit utilisateur,
- un identifiant de profil utilisateur associé audit utilisateur.

20 Tout type d'identifiant peut ainsi être utilisé pour la mise en œuvre du procédé selon l'invention, il n'est pas nécessaire de disposer d'un identifiant de l'utilisateur lui-même. Par exemple, l'utilisation d'un identifiant d'immatriculation d'un support personnel d'enregistrement comme identifiant facilite la mise en oeuvre du procédé, puisque qu'un tel identifiant est préexistant et qu'on dispose de bases de données et  
25 de mécanismes connus permettant de traiter de tels identifiants, et permettant si besoin, de déterminer l'identité de l'utilisateur à partir de tels identifiants.

Selon un mode de réalisation avantageux, tout ou partie des données optionnelles sont insérées dans la requête sous forme chiffrée. Ceci permet de renforcer la confidentialité des échanges et limite les chances de succès de tentatives  
30 de connexion frauduleuses.

L'invention a également pour objet un terminal comprenant un module client DHCP, convenant à la mise en œuvre du procédé de selon l'invention et comprenant

- un module pour provoquer l'insertion desdites données optionnelles dans ledit champ d'option prédéfini,
- 35 - un module pour provoquer la lecture de tout ou partie desdites données

optionnelles dans un support personnel d'enregistrement appartenant audit utilisateur et accessible à partir du terminal.

De manière complémentaire, l'invention a également pour objet un procédé de traitement par un serveur d'une ou plusieurs requêtes DHCP émises par un module client DHCP d'un terminal pour l'obtention de données de configuration dudit terminal, le serveur comprenant un module serveur DHCP apte à communiquer avec le module client DHCP via un réseau conformément au protocole DHCP, au moins une desdites une ou plusieurs requêtes DHCP reçues comprenant, dans un champ d'option prédéfini, des données optionnelles comprenant un identifiant associé, directement ou indirectement, à un seul utilisateur dudit terminal, le procédé comprenant les étapes consistant à

- générer les données de configuration demandées, les données de configuration étant personnalisées pour ledit utilisateur,
- transmettre audit module client DHCP les données de configuration en réponse à au moins une desdites une ou plusieurs requêtes DHCP.

Selon un mode de réalisation avantageux, les données de configuration générées comprennent une adresse IP, dont le type statique ou dynamique est fonction dudit identifiant. Le procédé permet ainsi la mise en place d'un processus automatique de gestion des adresses statiques à partir de la connaissance de chacun des identifiants associés aux utilisateurs ayant besoin d'une adresse statique.

Selon un mode de réalisation avantageux, le procédé comprend une étape consistant à enregistrer pour chaque requête comprenant ledit champ d'option prédéfini des données de suivi comprenant des informations de date et/ou heure de réception de ladite requête. Dans ce mode de réalisation, il est possible de suivre un utilisateur donné grâce à l'identifiant ou aux identifiants qui lui sont associés et d'envisager la mise en place de fonction de facturations ou de suivi des connexions.

Selon un mode de réalisation avantageux, le procédé comprend des étapes consistant à déterminer l'identité dudit utilisateur à partir dudit identifiant, à générer les données de configuration demandées en fonction de l'identité dudit utilisateur en cas d'identification de l'utilisateur, à refuser la génération des données de configuration demandées dans le cas où ledit utilisateur n'est pas identifié. Ce mode de réalisation permet de renforcer la sécurisation de l'accès au réseau dès l'étape de traitement des demandes de configuration.

L'invention a également pour objet un serveur comprenant un module serveur DHCP, convenant à la mise en œuvre du procédé de traitement selon l'invention, et

comprenant un module pour générer lesdites données de configuration demandées en fonction dudit identifiant.

Selon un mode de réalisation avantageux, le serveur comprend une base de données comprenant une liste d'identifiants, et pour chaque identifiant des données  
5 correspondant à une description des besoins en configuration de l'utilisateur associé à cet identifiant.

D'autres buts, caractéristiques et avantages de l'invention apparaîtront à travers la description qui va suivre, donnée uniquement à titre d'exemple non limitatif, et faite par référence aux dessins annexés dans lesquels

10 - la figure 1 représente de manière simplifiée l'architecture d'un système pour la mise en œuvre de l'invention,

- la figure 2 illustre de manière schématique différentes phases du procédé selon l'invention ainsi que les échanges de données entre les entités concernées par ces différentes phases.

15 L'invention est décrite dans le cadre de son application à une situation dans laquelle un client d'un prestataire de service souhaite accéder à des services mis à disposition par le biais de terminaux accédant à un réseau. Les terminaux sont, dans cet exemple, des terminaux accessibles en libre service.

Le client commence par s'inscrire auprès du prestataire de service pour  
20 certains services prédéfinis. En échange, le prestataire de service lui remet une carte à puce. Cette carte à puce contient des informations sur le client lui-même (identifiant Y), des informations de type service (le client a souscrit au service X, le client a souscrit à un abonnement de 12 mois) ou des informations mixtes (le client Y a souscrit au service X pour 12 mois).

25 Le client achète ou obtient du prestataire de service un terminal pour accéder aux services souscrits. Ce terminal possède une configuration standard, qui est par exemple une configuration permettant uniquement un usage en local, sans connexion réseau, de ce terminal. Pour permettre l'accès aux services souscrits par un utilisateur donné, il doit être configuré de manière appropriée, et notamment disposer  
30 d'une adresse DHCP lui permettant d'accéder aux services mis en œuvre via le réseau. Grâce à l'invention, ce terminal peut être configuré chaque fois en fonction de l'identité de l'utilisateur qui se connecte au réseau via ce terminal, et ce dès l'établissement de la connexion au réseau du terminal.

La figure 1 représente de manière simplifiée les principaux éléments coopérant  
35 dans un système d'un tel terminal. Dans le système représenté, le terminal 100 est en

communication via un réseau 50 de communication avec un serveur 200 de traitement de données accédant à une base de données 300.

Le terminal 100 est dans cet exemple un micro-ordinateur. De manière générale, ce terminal peut être tout type de terminal comprenant un module client  
5 DHCP permettant l'accès au réseau 50.

Le terminal 100 comprend une carte réseau 115 compatible avec le réseau 50 de communication. Il comprend également un lecteur 125 de carte à puce. En variante, le lecteur 125 de carte à puce peut être, non pas intégré dans le terminal 100, mais raccordé à ce terminal 100 via un port de communication externe ou  
10 encore en liaison de communication avec le terminal 100.

Le terminal 100 comprend différents modules logiciels:

- un module 110 client DHCP,
- un pilote 140 adapté au lecteur de carte à puce,
- un module 150 de lecture accédant via le pilote 140 aux données de la  
15 carte à puce,
- un module 170 d'insertion de données utilisé en combinaison avec le module client DHCP 110,
- une interface 160 de communication de type middleware permettant la communication entre le module 150 de lecture et le module 170 d'insertion.

20 Le module 110 client DHCP du terminal est adapté pour s'interfacer avec le module 170 d'insertion de données. Soit le module 110 client DHCP comprend une interface logicielle pour communiquer ou s'interfacer avec le module 170 d'insertion, soit il intègre complètement le module 170 d'insertion de données.

La carte à puce joue le rôle de support personnel d'enregistrement. Tout autre  
25 forme de support personnel d'enregistrement capable de stocker des données est également envisageable: une clé électronique USB connectée via un port USB, carte SIM d'un téléphone portable accessible via une liaison Bluetooth entre le terminal et le téléphone, etc. Les moyens d'accès au support d'enregistrement (dans l'exemple décrit, le pilote 140) sont chaque fois adaptés au support d'enregistrement utilisé.

30 De préférence l'accès au support d'enregistrement est sécurisé de manière à éviter un accès frauduleux aux données qu'il contient ou une usurpation d'identité. Cette sécurisation d'accès consiste usuellement à n'autoriser l'accès aux données de la carte à puce qu'après fourniture d'un code confidentiel.

De préférence, le support d'enregistrement est un support amovible de type  
35 carte à puce de façon à ce qu'un utilisateur donné puisse facilement, même lorsqu'il

est en déplacement fréquent, se connecter à partir de n'importe quel terminal tout en retrouvant une configuration appropriée à ses besoins.

De retour à la figure 1, le serveur 200 de traitement de données comprend une carte d'interface réseau 215 compatible avec le réseau 50 de communication. Il  
5 comprend également un module logiciel dit module serveur DHCP 210.

Le module client DHCP et le module serveur DHCP sont conçus pour dialoguer entre eux selon le protocole DHCP tel que défini par l'IETF ("Internet Engineering Task Force") dans la norme RFC 2131. Ce protocole définit notamment comment un terminal client comprenant un module client DHCP obtient sa configuration réseau  
10 (son adresse IP, en général) auprès d'un serveur DHCP comprenant un module serveur DHCP.

Les requêtes envoyées par le module client au module serveur sont par exemple:

- une requête "DHCP DISCOVER" par laquelle le module client teste la  
15 présence d'un ou de plusieurs serveurs DHCP sur le réseau et demande l'établissement d'un dialogue avec un de ces serveurs;
- une requête "DHCP REQUEST" par laquelle le module client demande des données de configuration au serveur ayant répondu à sa précédente requête "DHCP DISCOVER";
- 20 - une requête "DHCP REQUEST RENEWAL" par laquelle le module client renouvelle sa précédente requête "DHCP REQUEST".

Les requêtes DHCP émises par un module client DHCP peuvent contenir des données optionnelles. Ces données sont identifiées dans une requête DHCP par un code d'option. Par exemple, un code d'option 60 indique la présence de données  
25 identifiant le type de terminal.

Selon l'invention, on utilise un champ d'option prévu dans le protocole DHCP pour insérer, dans la requête DHCP émise par le module client DHCP, un code d'option et des données associées à ce code d'option.

- L'option DHCP insérée est conforme à la norme RFC 2489. Elle est définie par:
- 30 - un code d'option, par exemple le code 180,
  - un paramètre indiquant le format des données associées à l'option, par exemple "string",
  - un paramètre indiquant la quantité de données associées à l'option, par exemple sous forme de nombre de caractères.

35 Dans la suite de la description, une telle option sera nommée "option 180" ou

"option utilisateur". Ce code d'option prédéfini identifie le champ d'option dans lequel est inséré l'identifiant et est indicatif que les données de configuration demandées par le module client sont à générer en fonction dudit identifiant, et plus précisément, qu'elles sont à personnaliser pour l'utilisateur associé à cet identifiant.

- 5            Selon l'invention, les données associées au code d'option 180 comprennent un identifiant associé, directement ou indirectement, à un et un seul utilisateur du terminal 110. Un tel identifiant permet de déterminer sans ambiguïté l'identité de l'utilisateur associé à cet identifiant.

Un tel identifiant peut être, au choix:

- 10           - un identifiant de l'utilisateur lui-même, par exemple son nom, prénom;  
             - un identifiant de l'utilisateur lui-même sous forme de codée, qui est attribué à cet utilisateur et permet de l'identifier parmi d'autres utilisateurs au sein d'une organisation donnée; il peut s'agir par exemple un identifiant de salarié attribué à l'utilisateur dans l'entreprise pour laquelle il travaille ou encore un identifiant de client  
15           attribué à l'utilisateur par un organisme prestataire de service dont cet utilisateur est client;  
             - un identifiant d'immatriculation de carte à puce, à partir duquel l'identité de l'utilisateur peut être déterminée, l'utilisateur associé à cet identifiant étant dans ce cas le propriétaire de la carte à puce;  
20           - un identifiant de type numéro de téléphone à partir duquel l'identité de l'utilisateur peut être déterminée, l'utilisateur associé à cet identifiant étant dans ce cas l'abonné à la ligne téléphonique identifiée par ce numéro,  
             - un identifiant d'un objet ou d'un service associé à un seul utilisateur,  
             - un identifiant d'une entité abstraite associée à un unique utilisateur, par  
25           exemple un identifiant de profil utilisateur associé à cet utilisateur, etc.

Un code d'option prédéfini identifiant ledit champ d'option est de préférence utilisé pour indiquer la présence d'un tel identifiant et préciser au module de traitement de la requête, que les données de configuration demandées sont à personnaliser pour l'utilisateur associé à cet identifiant.

- 30           D'autres données peuvent également être insérées dans la requête. Celles-ci peuvent ou non être extraites de la carte à puce. Il peut notamment être utile d'insérer des données identifiant ou décrivant un profil utilisateur. On peut en effet envisager qu'un utilisateur ait besoin de se connecter avec différents types de profils au terminal. Un profil utilisateur comprend par exemple des informations d'identification  
35           des services accessibles à partir du terminal auxquels a souscrit cet utilisateur. Un

profil utilisateur peut comprendre également des informations sur les conditions d'accès à ces services: plage horaire, nombre d'accès, etc.

En variante, seul un identifiant de profil est inséré dans la requête, le serveur 200 étant dans ce cas en mesure de restituer les informations relatives aux services  
5 associés à ce profil à partir de la base de données 300.

En outre, comme indiqué plus haut, l'identifiant de profil peut être la seule et unique donnée intégrée dans le champ d'option 180 car il peut être utilisé pour identifier l'utilisateur du terminal si cet identifiant de profil est associé à un utilisateur et un seul.

10 Dans ce but, la base de données comprenant de préférence une liste d'identifiants, et pour chaque identifiant des données correspondant, soit des informations relatives aux services souscrits par l'utilisateur associé à cet identifiant, soit à une description des besoins en configuration de l'utilisateur associé à cet identifiant (type d'adresse, droits d'accès, etc), soit aux données de configuration  
15 elles-mêmes (dans le cas d'une adresse statique, il est nécessaire de mémoriser celle-ci). De cette manière, le serveur est ainsi en mesure, sans même connaître l'identité de l'utilisateur, de générer des données de configuration personnalisées.

Les données insérées dans la requête et associées au code d'option 180 sont de préférence extraites de la carte à puce. En supplément, des données de  
20 provenance différente, par exemple des données non confidentielles, peuvent également être insérées dans la requête.

Tout ou partie des données associées à l'option 180 peut être chiffré. Le chiffrement de ces données peut s'effectuer, soit avant insertion des données dans la requête, soit avant enregistrement des données sur la carte à puce. Dans cette  
25 deuxième variante, les risques d'usurpation d'identité sont très réduits, surtout si l'accès au support d'information est de surcroît sécurisé.

La figure 2 illustre les différentes phases du procédé selon l'invention ainsi que les échanges de données effectués lors de ces différentes phases entre le terminal 100, le serveur 200, le lecteur 120 et la base de données 300.

30 Après démarrage du terminal 100 et insertion de la carte à puce 130 dans le lecteur 120, les étapes S10 à S160 se déroulent comme suit:

- S10 : le terminal 100 génère une requête "DHCP DISCOVER" et demande l'insertion d'une option 180 comprenant des données présentes dans la carte à puce 130; ces données comprennent notamment un identifiant associé à un utilisateur du  
35 terminal 100;

- S20 : le lecteur 120 reçoit une instruction de lecture de données;
- S30 : le lecteur 120 lit les données demandées dans la carte à puce 130 et les renvoie au terminal;
- S40 : le terminal 100 reçoit les données lues dans la carte à puce 130;
- 5       - S50 : le terminal 100 insère les données reçues dans la requête "DHCP DISCOVER", puis envoie cette requête au serveur 200;
- S60 : le serveur 200 reçoit la requête "DHCP DISCOVER";
- S70 : le serveur 200 traite la requête "DHCP DISCOVER" en accédant S75 si besoin à la base de données 300; ce traitement est effectué en prenant en compte
- 10       tout ou partie des données lues dans la carte et insérées dans la requête; le serveur 200 génère une réponse qui, de préférence, est fonction de l'identifiant inséré dans la requête;
- S80 : le serveur 200 envoie une réponse à la requête "DHCP DISCOVER" sous forme d'une requête "DHCP OFFER";
- 15       - S90 : le terminal 100 reçoit la réponse "DHCP OFFER";
- S100 : le terminal 100 génère une requête "DHCP REQUEST" et y insère tout ou partie des données précédemment lues dans la carte;
- S110 : le terminal 100 envoie cette requête "DHCP REQUEST" au serveur 200;
- 20       - S120 : le serveur 200 reçoit la requête "DHCP REQUEST ";
- S130 : le serveur 200 traite la requête "DHCP REQUEST " en accédant S135 si besoin à la base de données 300;
- S140 : le serveur 200 envoie une réponse à la requête "DHCP REQUEST " sous forme d'une requête "DHCP ACK" comprenant une adresse IP destinée à la
- 25       configuration du terminal 100;
- S150 : le terminal 100 reçoit la réponse "DHCP ACK";
- S160 : le terminal 100 procède à sa configuration IP à partir de l'adresse IP renvoyée par le serveur 200.
- La constitution d'une requête DHCP par le terminal 100 comprend elle-même
- 30       les étapes suivantes:
  - le module 110 client DHCP crée une requête DHCP;
  - le module 110 client DHCP transfère cette requête au module 170 d'insertion;
  - le module 170 d'insertion envoie une requête au module 150 de lecture via
  - 35       le middleware 160 pour l'extraction des données de la carte à puce;

- le module 150 de lecture obtient les données demandées du pilote 140 du lecteur 120 de carte;
- le module 150 de lecture renvoie les données demandées au module 170 d'insertion via le middleware 160;
- 5       - le module 170 d'insertion insère les données dans la requête DHCP créée et la transfère au module 110 client DHCP;
- le module 110 client DHCP envoie la requête DHCP au module 210 serveur DHCP et attend sa réponse.

10       Dans chaque requête DHCP générée peut comprendre une option 180 et des données associées. Dans l'exemple décrit, ce sont les requêtes "DHCP DISCOVER" et "DHCP REQUEST" qui contiennent une information sur l'identité de l'utilisateur du terminal. Toutes les requêtes émises par le module client DHCP ("DHCP REQUEST RENEWAL", "DHCP INFORM" et "DHCP RELEASE") peuvent selon le besoin contenir cette information.

15       Selon les variantes de réalisation, il y aura ou non accès à la carte à puce à chaque génération de requête DHCP cliente pour y lire les données à insérer. Ainsi l'étape S100 de génération d'une requête "DHCP REQUEST" peut nécessiter des sous-étapes S102 et S103 d'accès à la carte à puce et de lecture de données dans la carte à puce.

20       Le serveur DHCP est configuré pour se servir de l'information positionnée dans l'option DHCP choisie de différentes manières:

- pour effectuer des opérations de type contrôle d'accès en fonction de l'identité de l'utilisateur et ne répondre qu'aux terminaux envoyant une information associée à un utilisateur connu; dans ce cas, la sécurité du service DHCP est améliorée puisque
- 25       l'on ne configure que les terminaux autorisés; dans cette situation des données d'authentification (mot de passe, certificat, etc) peuvent être insérées dans la requête DHCP avec les données permettant d'identifier l'utilisateur et permettre au serveur d'authentifier l'utilisateur courant du terminal émetteur de la requête;

- pour enregistrer des données de suivi (notamment les date et/ou heure de
- 30       réception de la requête) relatives aux connexions demandées par un utilisateur donné, c'est-à-dire pour les requêtes comprenant le champ d'option 180; dans ce cas, le prestataire de service peut mettre en oeuvre une facturation par utilisateur, par exemple en fonction du nombre de connexions ou de la durée de chaque connexion, les données de suivi étant croisées avec les informations liant un client à une carte à
- 35       puce;

- pour émettre une réponse qui est personnalisée en fonction de l'identité de l'utilisateur ou en fonction des services auxquels cet utilisateur a souscrit; par exemple en générant des données de configuration en fonction de l'identifiant et/ou de l'identité de l'utilisateur.

5 Ces différentes opérations sont effectuées de préférence lors du traitement de la requête DHCP cliente et avant l'élaboration de la réponse à cette requête. Lorsque l'opération considérée est un simple enregistrement de données de suivi, celle-ci peut optionnellement être exécutée postérieurement à l'envoi de la réponse à la requête cliente.

10 En généralisant, le traitement par le serveur 200 de la requête DHCP émise par le terminal 100 est effectué en fonction des données du champ optionnel de données. Ces données comprennent un identifiant associé, de manière univoque, à l'utilisateur du terminal 100. Il s'agit en particulier d'un identifiant permettant une identification univoque de l'utilisateur du terminal 100.

15 A partir des données associées à l'option DHCP, le serveur DHCP détermine, préalablement au traitement de la requête DHCP, l'identité de l'utilisateur du terminal 100 et traite la requête en fonction de l'identité de l'utilisateur. Ainsi des opérations telles que l'enregistrement de données de suivi, le traitement des données associées à la requête, le contrôle d'accès à partir des données associées à la requête ou la  
20 génération de la réponse à la requête, pourront être effectuées en fonction de l'identité de l'utilisateur courant du terminal 100.

En variante, l'étape de détermination de l'identité de l'utilisateur du terminal peut être évitée, si le serveur est conçu pour répondre à la requête sur la seule base de l'identifiant, notamment si le serveur comprend une base de données enregistrant les  
25 besoins en configuration de l'utilisateur en association avec l'identifiant.

Par exemple, si la base de donnée 300 comprend une table des services souscrits par les différents utilisateurs, table qui est indexée par un identifiant d'utilisateur, le serveur DHCP identifie à partir de l'identifiant associé à l'utilisateur les services souscrits par cet utilisateur et retourne une réponse (des données de  
30 configuration) qui est adaptée par rapport aux services souscrits.

En particulier, la configuration DHCP retournée par le serveur en réponse à une requête "DHCP REQUEST" pourra être fonction de l'identifiant, et donc de l'identité de cet utilisateur. Il est ainsi possible de faire en sorte que le type, statique ou dynamique, de l'adresse retournée, soit lui aussi fonction de l'identité de cet  
35 utilisateur. Dans le cas d'exemple où l'utilisateur a besoin d'une adresse statique, le

serveur retournera en permanence une adresse statique prédéfinie adaptée aux besoins de cet utilisateur.

## REVENDICATIONS

1. Procédé d'obtention de données de configuration d'un terminal (100), le terminal comprenant un module client DHCP (110) apte à communiquer via un réseau (50) avec au moins un module serveur DHCP (210) conformément au protocole DHCP, le procédé comprenant les étapes suivantes:
  - 5 - génération par ledit module client DHCP d'une ou plusieurs requêtes DHCP pour l'obtention de données de configuration dudit terminal,
  - transmission desdites une ou plusieurs requêtes DHCP via ledit réseau par ledit module client DHCP audit au moins un module serveur DHCP,
  - réception des données de configuration reçues par ledit module client DHCP
- 10 en réponse à au moins une desdites une ou plusieurs requêtes DHCP,  
le procédé étant caractérisé en ce qu'il comprend une étape consistant à insérer, dans un champ d'option prédéfini d'au moins une desdites une ou plusieurs requêtes DHCP, des données optionnelles comprenant un identifiant associé, directement ou indirectement, à un seul utilisateur dudit terminal, et en ce que
- 15 lesdites données de configuration reçues sont personnalisées pour ledit utilisateur.
2. Procédé selon la revendication 1, caractérisé en ce que le procédé comprend une étape consistant à lire tout ou partie des données optionnelles dans un support personnel d'enregistrement accessible à partir du terminal.
3. Procédé selon la revendication 2, caractérisé en ce que ledit support personnel
- 20 d'enregistrement est un support dont l'accès est sécurisé par un code d'identification.
4. Procédé selon la revendication 2 ou 3, caractérisé en ce que ledit support personnel d'enregistrement est de type support amovible.
5. Procédé selon l'une quelconque des revendications 2 à 4, caractérisé en ce
- 25 que ledit support personnel d'enregistrement est intégré dans un terminal mobile et est accessible à partir dudit terminal par un lien local de communication établi entre ledit terminal et ledit terminal mobile.
6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que ledit identifiant fait partie du groupe comprenant:
  - 30 - un identifiant dudit utilisateur,
  - un identifiant d'immatriculation d'un support personnel d'enregistrement associé audit utilisateur,
  - un identifiant d'un objet associé audit utilisateur,

- un identifiant d'un service associé audit utilisateur,
  - un identifiant de profil utilisateur associé audit utilisateur.
7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que lesdites données optionnelles comprennent en outre des données
- 5 comprenant une identification d'au moins un service auquel l'utilisateur a souscrit.
8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que tout ou partie des données optionnelles sont insérées dans la requête sous forme chiffrée.
- 10 9. Procédé de traitement par un serveur (200) d'une ou plusieurs requêtes DHCP émises par un module client DHCP (110) d'un terminal (100) pour l'obtention de données de configuration dudit terminal (100),
- ledit serveur comprenant un module serveur DHCP (210) apte à communiquer avec ledit module client DHCP (110) via un réseau (50) conformément au protocole
- 15 DHCP, ledit procédé comprenant les étapes consistant à
- générer les données de configuration demandées,
  - transmettre audit module client DHCP les données de configuration en réponse à au moins une desdites une ou plusieurs requêtes DHCP,
- le procédé étant caractérisé en ce qu'au moins une desdites une ou plusieurs
- 20 requêtes DHCP reçues comprend, dans un champ d'option prédéfini, des données optionnelles comprenant un identifiant associé, directement ou indirectement, à un seul utilisateur dudit terminal et en ce que les données de configuration générées sont personnalisées pour ledit utilisateur.
10. Procédé selon la revendication 9 caractérisé en ce que les données de configuration générées comprennent une adresse IP, dont le type statique ou
- 25 dynamique est fonction dudit identifiant.
11. Procédé selon la revendication 9 ou 10 caractérisé en ce que le procédé comprend les étapes consistant
- à déterminer l'identité dudit utilisateur à partir dudit identifiant,
- 30 - à générer les données de configuration demandées en fonction de l'identité dudit utilisateur en cas d'identification de l'utilisateur,
- à refuser la génération des données de configuration demandées dans le cas où ledit utilisateur n'est pas identifié.
12. Procédé selon l'une quelconque des revendications 9 à 11 caractérisé en ce
- 35 que le procédé comprend une étape consistant à enregistrer pour chaque

requête comprenant ledit champ d'option prédéfini des données de suivi comprenant des informations de date et/ou heure de réception de ladite requête.

- 5 13. Terminal comprenant un module client DHCP, convenant à la mise en œuvre du procédé selon l'une quelconque des revendications 1 à 8 et comprenant
- un module pour provoquer l'insertion desdites données optionnelles dans ledit champ d'option prédéfini,
  - un module pour provoquer la lecture de tout ou partie desdites données optionnelles dans un support personnel d'enregistrement associé audit utilisateur et
- 10 accessible à partir du terminal.
14. Serveur comprenant un module serveur DHCP, convenant à la mise en œuvre du procédé selon l'une quelconque des revendications 9 à 12, et comprenant un module pour générer lesdites données de configuration demandées en fonction dudit identifiant.
- 15 15. Serveur selon la revendication 14, caractérisé en ce qu'il comprend une base de données comprenant une liste d'identifiants, et pour chaque identifiant des données correspondant à une description des besoins en configuration de l'utilisateur associé à cet identifiant.

1 / 2

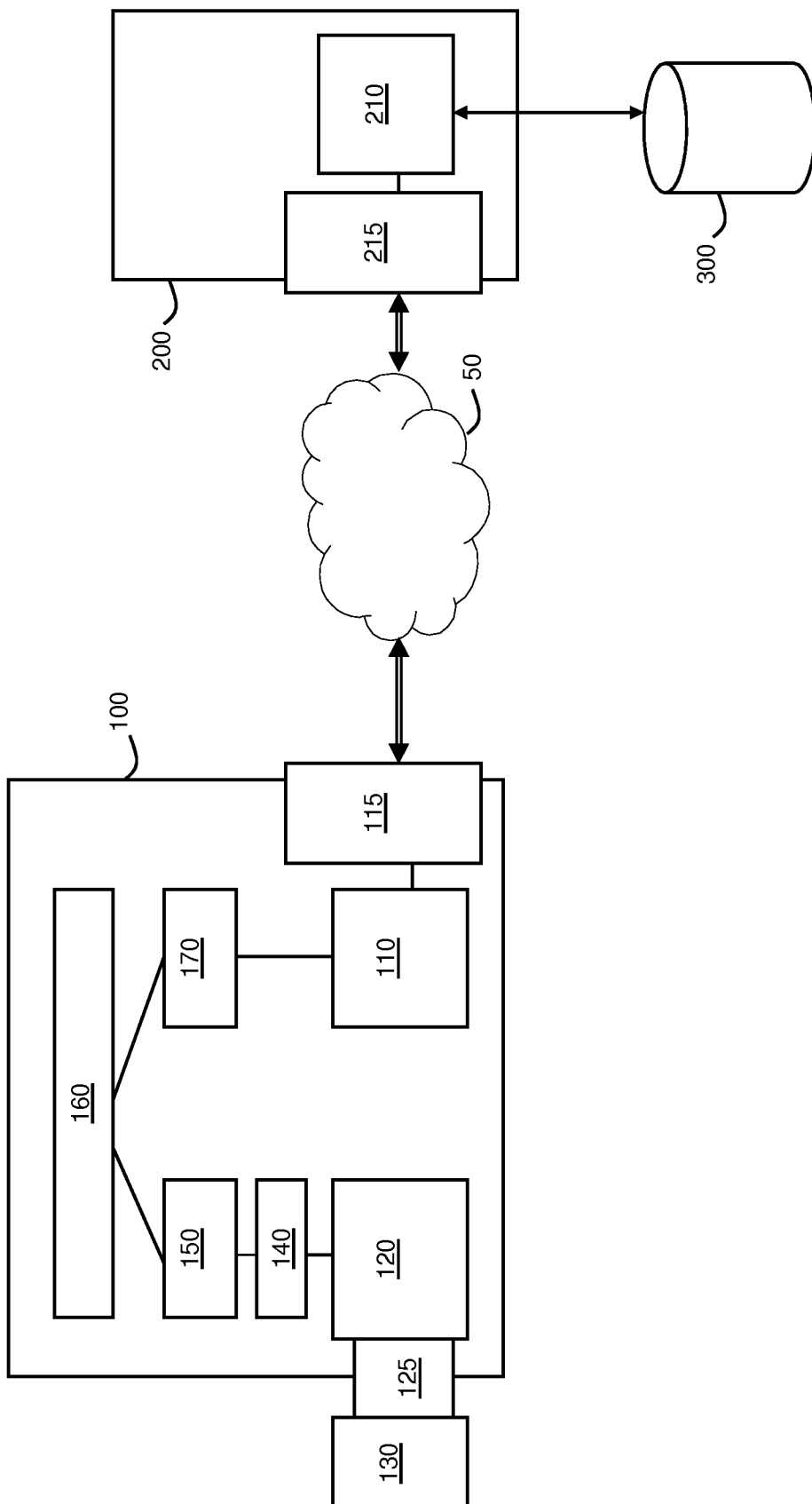


Fig. 1

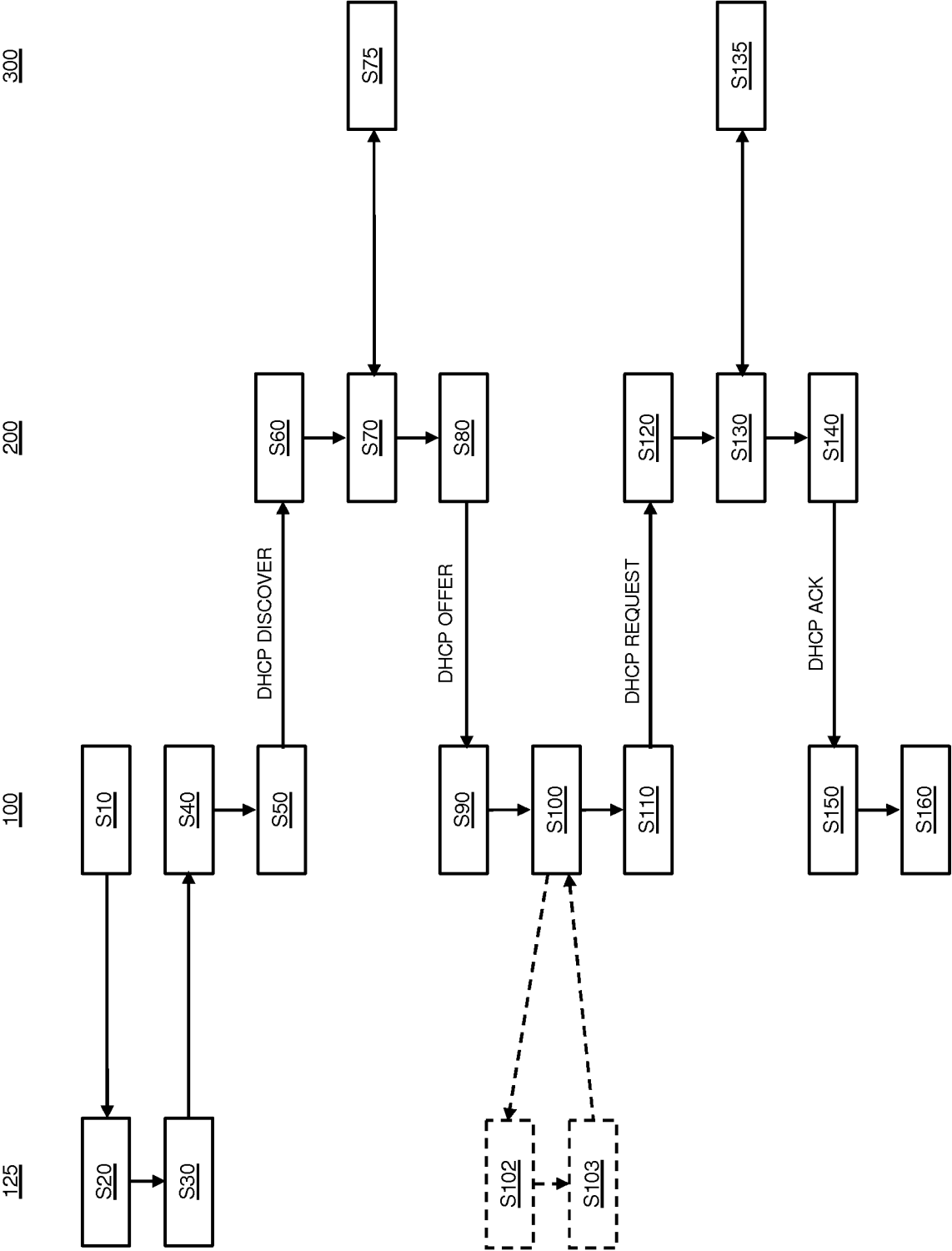


Fig. 2