(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 904 503**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **06 53161**

(51) Int Cl[8] : **H 04 L 29/06** (2006.01)

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 28.07.06.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 01.02.08 Bulletin 08/05.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *FRANCE TELECOM Société anonyme* — FR.

(72) **Inventeur(s) :** EL KHOURY RAMZI, LEJKIN THIERRY et BLANC JEAN PAUL.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** FRANCE TELECOM.

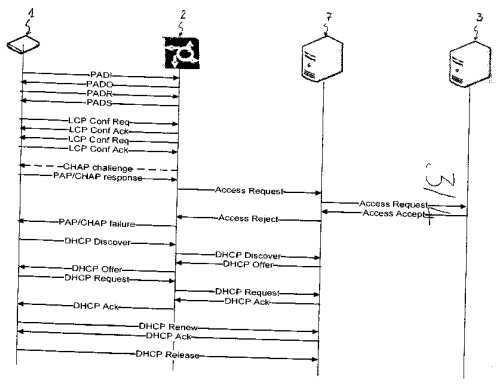
(54) PROCEDE D'ACCES PAR UN CLIENT A UN SERVICE AU TRAVERS D'UN RESEAU, PAR UTILISATION COMBINEE D'UN PROTOCOLE DE CONFIGURATION DYNAMIQUE ET D'UN PROTOCOLE POINT A POINT, EQUIPEMENT ET PROGRAMME D'ORDINATEUR CORRESPONDANTS.

(57) Procédé d'accès par un client à un service au travers d'un réseau, par utilisation combinée d'un protocole de configuration dynamique et d'un protocole point à point, équipement et programme d'ordinateur correspondants.

L'invention concerne un procédé d'accès par un client (1) à un service au travers d'un réseau, ledit client étant apte à mettre en oeuvre, pour l'établissement d'une session d'accès audit service, un protocole de connexion de type PPP et un protocole de type DHCP.

Selon l'invention, un tel procédé comprend des étapes de:

- réception d'une requête d'établissement d'une session PPP, émise à la demande dudit client et destinée à un serveur d'authentification (3);
- en cas d'authentification dudit client par le serveur d'authentification, réception d'une autorisation émise par ledit serveur d'authentification à destination dudit client, et mémorisation d'au moins un paramètre de configuration de ladite session point à point extrait de ladite autorisation;
- réception d'une requête d'établissement d'une session DHCP, émise par ledit client après rupture d'établissement de ladite session PPP;
- après vérification de l'authentification dudit client, envoi audit client dudit paramètre de configuration mémorisé, pour établissement d'une session DHCP.



FR 2 904 503 - A1

Procédé d'accès par un client à un service au travers d'un réseau, par utilisation combinée d'un protocole de configuration dynamique et d'un protocole point à point, équipement et programme d'ordinateur correspondants.

1. Domaine de l'invention

Le domaine de l'invention est celui des télécommunications, et plus particulièrement des réseaux d'accès fixes. Plus précisément, l'invention concerne un procédé d'accès à un service par un client connecté à un réseau de type IP (pour "Internet Protocol").

Elle s'applique notamment, mais non exclusivement, à l'accès de clients disposant de passerelles résidentielles aux réseaux d'opérateurs et/ou de fournisseurs d'accès Internet, notamment dans le cadre de connexions large bande telles que l'ADSL (de l'abréviation anglaise "Asymmetric Digital Subscriber Line", ou en français "Ligne d'Abonné Numérique Asymétrique").

2. Art antérieur et ses inconvénients

Un premier protocole connu et largement répandu pour l'accès à Internet au moyen d'une connexion large bande est le protocole de type point à point, appelé PPP (Point-to-Point Protocol ou "Protocole point à point" en français).

Un tel protocole PPP est un protocole de connexion qui propose une méthode pour le transport de datagrammes multi-protocoles sur une liaison point à point entre deux éléments distants. Il comprend trois composantes principales :

- une méthode pour encapsuler des datagrammes issus de plusieurs protocoles différents;
- une phase de contrôle du lien appelée "*Link Control Protocol*" (LCP) pour l'établissement, la configuration et le test de la connexion de lien de données;
- enfin, une phase pour l'établissement et la configuration de plusieurs protocoles de la couche réseau, telle que définie dans le modèle OSI (*Open Systems Interconnection* ou en français "Interconnexion de Systèmes Ouverts"), appelée "*Network Control Protocols*" (NCPs). En particulier, un protocole appelé IPCP ("*Internet Protocol Control Protocol*") est utilisé afin d'établir et de configurer la couche IP et d'attribuer et gérer des adresses IP.

Un tel protocole PPP est utilisé sur des liaisons transportant des paquets de données entre deux éléments distants et permettant une communication simultanée bidirectionnelle. Ce protocole propose une solution commune pour un raccordement

aisé d'une grande variété d'hôtes, de ponts et de routeurs. L'ensemble de protocoles contenus dans le protocole PPP permet entre autres, le contrôle d'accès, dont l'authentification des utilisateurs est une composante, et l'attribution d'adresses IP aux terminaux clients, et inclut la notion d'établissement et de terminaison de sessions entre un client et un serveur. Un tel protocole PPP est défini dans le document référencé RFC 1661 (RFC signifiant "requête pour commentaires", ou en anglais *Request For Comments*) établi par l'IETF (groupe pour la participation à la standardisation de l'Internet, abréviation des termes anglais *Internet Engineering Task Force*) (RFC 1661: "The Point-to-Point Protocol (PPP)" - IETF Network Working Group – Editor: W. Simpson – Date: July 1994).

On distingue deux types de protocole PPP à savoir PPPoA pour "PPP over ATM" et PPPoE pour "PPP over Ethernet".

En référence à la figure 1, lors de l'établissement d'une session conforme au protocole PPP, dite session PPP, une liaison point-à-point est établie entre un client PPP 1 et un serveur PPP appelé BAS 2 situé dans le réseau (BAS signifiant *Broadband Remote Access Server*, ou en français, "serveur d'accès large bande à distance").

Un tel client 1 peut consister par exemple en une passerelle résidentielle, ou en un modem d'utilisateur.

Le serveur BAS 2, également appelé de manière plus générale serveur RAS (RAS signifiant *Remote Access Server* ou en français, "serveur d'accès à distance") remplit une fonction d'identification du client PPP 1 au moyen de mécanismes d'authentification. Le serveur BAS 2 exerce aussi une fonction d'allocation d'adresses IP et de paramètres DNS (*Domain Name Server* ou en français, "serveur de nom de domaine"), ainsi qu'une fonction d'établissement et de terminaison de sessions PPP.

Le serveur BAS 2 peut également coopérer avec un serveur d'authentification 3 en charge de l'authentification du client 1. Ainsi, le serveur BAS 2 peut inclure un client RADIUS qui établit un dialogue avec un serveur RADIUS 3 (*Remote Authentification Dial-In User Service* ou en français "service d'authentification à distance d'un utilisateur entrant") qui fournit des paramètres de configuration de chaque client PPP 1 sur la base des paramètres d'authentification ou d'identification qui leurs sont associés. Ainsi, lors de l'établissement d'une session PPP, le serveur BAS 2 interroge le serveur RADIUS 3 afin d'authentifier le client PPP 1 et, le cas échéant, d'ouvrir une session

PPP. Cette phase d'authentification met en œuvre, entre le client 1 et le BAS 2, un protocole de type PAP (*Password Authentication Protocol* pour "protocole d'authentification par mot de passe") ou CHAP (*Challenge Handshake Authentication Protocol* pour "protocole d'authentification par défi réponse").

On notera que RADIUS, décrit dans le document RFC 2865 établi par l'IETF, constitue un exemple parmi d'autres de protocoles d'authentification pouvant être mis en œuvre dans le serveur d'authentification 3.

Les données échangées entre le client 1 et le BAS 2 transitent au travers d'un nœud 4, appelé DSLAM (*Digital Subscriber Line Access Multiplexor,* soit en français "Multiplexeur de Ligne d'Abonné Numérique" ou plus simplement "Multiplexeur d'accès DSL"), constituant un nœud d'accès au réseau R auquel est connecté le BAS 2.

La clôture d'une session PPP se traduit par la rupture de la liaison établie entre le client PPP 1 et le serveur BAS 2.

Les protocoles de type point à point tels que PPP présentent donc l'avantage de permettre l'authentification du client, ce qui permet par exemple à un fournisseur d'accès à Internet de personnaliser le type d'accès fourni en fonction de l'identité du client considéré (par exemple en fournissant un débit spécifique ou des services de nomadisme).

Le manque de souplesse du protocole PPP, notamment pour les applications diffusées en multicast et/ou demandant des qualités de services distinctes constitue cependant l'un de ses principaux inconvénients.

En outre, l'utilisation de serveurs RAS centralisés ne permet pas la diffusion en mode multicast de nouveaux contenus ou de nouveaux services car la bande passante disponible sur le réseau de collecte IP n'est pas suffisante. En effet, par construction, le protocole PPP fonctionne en point à point entre le client et l'équipement de terminaison PPP constitué par le serveur BAS. Dans ce segment, les flux de données ne peuvent donc être diffusés qu'en mode unicast.

Enfin, les protocoles point à point tels que PPP nécessitent une gestion des contextes des connexions ouvertes chez les clients. Il est donc nécessaire de disposer d'un équipement (à savoir le BAS) dans le réseau qui conserve toutes les informations (identification de session, durée de connexion, etc.) relatives aux sessions ouvertes par les clients. Ces fonctions sont particulièrement lourdes à gérer et pénalisent de façon très significative les performances des serveurs BAS, et ce d'autant plus que la

durée des sessions des clients a tendance à s'accroître de plus en plus. Il est donc nécessaire d'accroître le nombre de serveurs BAS dans le réseau, pour faire face à la demande croissante des clients, ce qui s'avère problématique, les serveurs BAS étant des équipements onéreux.

Une alternative aux protocoles de type point à point tels que PPP réside dans l'utilisation de protocoles de fourniture dynamique de paramètres de configuration, tels que le protocole DHCP (abréviation de *Dynamic Host Configuration Protocol*, ou en français, "protocole de configuration dynamique d'un hôte"). Un tel protocole DHCP est largement utilisé et déployé dans les réseaux locaux et privés. Il est notamment utilisé par certains opérateurs en télécommunications pour le déploiement de services tels que la télévision par ADSL, ou la visiophonie.

Le protocole DHCP est un protocole client-serveur qui permet à un équipement qui se connecte sur un réseau d'obtenir des paramètres de configuration tels qu'une adresse IP allouée pour une durée de bail donnée. Un tel protocole DHCP est défini dans le document référencé RFC 2131 établi par l'IETF (RFC 2131: "Dynamic Host Configuration Protocol" - IETF Network Working Group – Editor: R. Droms).

En référence à la figure 2, lorsqu'un équipement se connecte à un réseau une liaison est établie entre un client DHCP 1, embarqué dans l'équipement, et un serveur DHCP 6 présent dans le réseau.

Lors de la mise en œuvre du protocole DHCP, les paramètres de configuration d'un client DHCP 1, tels que son adresse IP, sont attribués pour une durée déterminée appelée "bail", à l'issue de laquelle ils sont libérés et redeviennent accessibles aux autres usagers, ce qui permet d'optimiser les ressources du réseau. Cependant, un client DHCP 1 qui voit son bail arriver à expiration peut en demander le renouvellement au serveur DHCP 6. Si le serveur DHCP 6 ne reçoit pas de requête de renouvellement du bail de la part du client DHCP 1 avant l'expiration du bail, ou si le bail n'est pas prolongeable, il rend disponible, à expiration du bail, l'adresse IP qu'il avait attribuée à ce client DHCP 1.

Afin d'initialiser un bail DHCP entre un client DHCP 1 et un serveur DHCP 6, ce dernier doit procéder à l'affectation de paramètres de configuration au client DHCP 1. Après affectation, le serveur DHCP 6 mémorise les paramètres de configuration de chaque client DHCP 1, pour toute la durée du bail, voire au delà.

Comme dans le cas de la figure 1, les données échangées entre le client DHCP 1 et le serveur DHCP 6 transitent au travers d'un nœud 4, appelé DSLAM, constituant un nœud d'accès au réseau R auquel est connecté le serveur DHCP 6.

Les protocoles de configuration dynamique tels que DHCP ont donc pour avantage d'être plus légers à implémenter, en ce sens qu'ils ne nécessitent pas l'introduction dans le réseau d'équipements (de type BAS) destinés à gérer les contextes des connexions ouvertes et à mémoriser les informations associées.

En contrepartie, ce type de protocole présente l'inconvénient de ne pas gérer les aspects d'authentification, de comptage et d'autorisation des connexions des clients, ce qui peut s'avérer pénalisant.

Pour pallier cet inconvénient, l'IETF a publié dans le document référencé RFC3118 une extension du protocole DHCP permettant à ce protocole d'offrir des services d'authentification à travers une option DHCP 90 (RFC 3118: "Authentication for DHCP messages" - IETF Network Working Group – Editors: R. Droms, W. Arbaugh). Cette extension de protocole se fonde sur l'utilisation de clefs cryptographiques symétriques "déjà partagées" et connues par le client DHCP et le serveur DHCP.

Cependant, le mécanisme de distribution de ces clefs s'avère très compliqué puisqu'il nécessite la fourniture d'une clef par client. Dans le cas d'un réseau d'opérateur rassemblant plusieurs millions de clients, la gestion de ces clefs s'avère très compliquée. Ainsi, si cette option DHCP 90 s'avère intéressante dans le cadre d'un simple réseau LAN privé, dans lequel on gère un nombre relativement limité de clients, elle n'est pas du tout adapté pour un réseau d'opérateur rassemblant un nombre élevé de clients.

Certains équipementiers, conscients des inconvénients du protocole DHCP liés à l'absence d'authentification, proposent des équipements permettant aux clients de se connecter au réseau au moyen du protocole DHCP, tout en bénéficiant d'une authentification RADIUS. Pour ce faire, un serveur d'accès crée une requête RADIUS dès qu'il détecte qu'un utilisateur s'est connecté en DHCP. Cette requête RADIUS, qui contient un ensemble d'attributs configurables, est transmise à un serveur d'authentification RADIUS pour authentification du client.

Un inconvénient de cette technique réside dans son manque de sécurité, car le nom de l'utilisateur et son mot de passe transitent en clair sur le réseau entre le client et le réseau pour qu'une telle authentification soit rendue possible.

De plus, cette technique nécessite des coûts de licence non négligeables sur les équipements BAS (sollicités pour générer les requêtes RADIUS) et souvent rédhibitoires dans le cadre d'une généralisation de ce type de solutions à un réseau d'opérateur comptant un grand nombre de clients.

Il existe donc un besoin d'une technique qui permette de pallier ces inconvénients de l'art antérieur. Notamment, il existe un besoin d'une technique qui allie les performances d'un protocole de configuration dynamique tel que DHCP et les fonctions d'authentification d'un protocole point à point tel que PPP, tout en présentant un niveau de sécurité élevé. Une telle technique doit être adaptée pour un déploiement sur un réseau auquel sont connectés de très nombreux usagers.

3. Exposé de l'invention

L'invention répond à ce besoin en proposant un procédé d'accès par un client à un service au travers d'un réseau, ledit client étant apte à mettre en œuvre, pour l'établissement d'une session d'accès audit service, un protocole de connexion de type point à point (PPP) et un protocole de fourniture dynamique d'au moins un paramètre de configuration, dit protocole de configuration dynamique (DHCP).

Selon l'invention, un tel procédé comprend des étapes de:

- réception d'une première requête d'établissement d'une session d'accès conforme audit protocole de type point à point (PPP), dite session point à point, émise à la demande dudit client et destinée à un serveur d'authentification (RADIUS);
- en cas d'authentification dudit client par ledit serveur d'authentification, réception d'une autorisation émise par ledit serveur d'authentification à destination dudit client, et mémorisation d'au moins un paramètre de configuration (@ IP) de ladite session point à point extrait de ladite autorisation;
- réception d'une deuxième requête d'établissement d'une session d'accès conforme audit protocole de configuration dynamique (DHCP), émise par ledit client après rupture d'établissement de ladite session point à point;
- après vérification de l'authentification dudit client, envoi audit client dudit au moins un paramètre de configuration mémorisé, pour établissement d'une session d'accès conforme audit protocole de configuration dynamique (DHCP).

Ainsi, l'invention repose sur une approche tout à fait nouvelle et inventive de la connexion d'un client à un réseau, notamment à un réseau de type IP. En effet, alors

que dans l'art antérieur il était toujours nécessaire de faire un choix entre l'une des deux méthodes d'accès, à savoir un accès au réseau à travers une connectivité de type PPP ou un accès au réseau à travers une connectivité de type DHCP, l'invention propose de combiner astucieusement ces deux méthodes, de façon à permettre au client de bénéficier des avantages de chacune.

Pour ce faire, l'invention propose de permettre au client de tenter d'établir une session d'accès en mode point à point, et donc de se faire authentifier par un serveur d'authentification, qui délivre un ensemble de paramètres de configuration de la session point à point en cas d'authentification réussie. Le client bénéficie ainsi de tous les avantages de la connectivité de type PPP, liés à l'authentification initiale du client.

Après rupture de l'établissement de la session point à point, l'invention offre la possibilité au client de tenter d'établir une connexion selon un protocole de configuration dynamique (par exemple de type DHCP), en réutilisant avantageusement les paramètres de configuration préalablement obtenus du serveur d'authentification dans le cadre de l'établissement de la session point à point. Cette réutilisation est bien sûr conditionnée par la vérification de l'authentification du client, c'est-à-dire qu'il est vérifié que le client qui se connecte en mode DHCP est bien le même que celui qui a été préalablement authentifié lors de la tentative d'établissement d'une session PPP.

L'établissement de la session point à point ayant préalablement échoué, le contexte ouvert pour ce client dans un équipement de type BAS a donc été refermé, libérant ainsi les ressources du serveur d'accès BAS, qui n'est donc pas surchargé inutilement.

L'invention permet donc de bénéficier également des avantages d'une connectivité de type DHCP, qui ne nécessite pas de gestion des contextes des connexions ouvertes.

En outre, le procédé de l'invention présente une sécurité élevée, dans la mesure où les nom d'utilisateur (ou *login*) et mot de passe du client ne transitent pas en clair entre le client et le réseau (en effet, dans le cas particulier du protocole PPP, le serveur d'accès peut imposer aux clients l'utilisation du protocole d'authentification CHAP, comme on le verra plus en détail par la suite).

Un tel procédé conforme à l'invention est préférentiellement mis en œuvre dans un équipement intermédiaire du réseau, situé entre un serveur d'accès de type BAS et un serveur d'authentification, comme on le verra plus en détail dans la suite de ce

document.

On notera que les protocoles PPP et DHCP sont cités à titre de simple exemple illustratif et non limitatif. L'invention pourrait également s'appliquer à tout autre type de protocoles présentant des caractéristiques proches ou similaires de celles de PPP et de DHCP. L'invention s'applique notamment à tout protocole de type point à point présentant des caractéristiques d'authentification du client et à tout protocole de configuration dynamique ne nécessitant pas de gestion des contextes des connexions ouvertes par les clients.

Avantageusement, la vérification de l'authentification dudit client met en œuvre une comparaison d'un premier identifiant dudit client, extrait de ladite première requête et mémorisé en relation avec ledit au moins un paramètre de configuration, et d'un deuxième identifiant dudit client, extrait de ladite deuxième requête.

Ainsi, lorsque l'équipement intermédiaire dans lequel est mis en œuvre le procédé de l'invention reçoit la première requête d'accès destinée au serveur d'authentification (par exemple une requête *Access Request* destinée à un serveur RADIUS), il en extrait un identifiant du client qu'elle contient. De même, lorsqu'il reçoit l'autorisation émise par le serveur d'authentification en cas de succès de l'authentification du client, il en extrait le ou les paramètres de configuration de la session alloués par le serveur d'authentification au client. L'identifiant et les paramètres de configuration sont mémorisés dans un contexte ouvert pour ce client par l'équipement intermédiaire de l'invention.

Sur réception de la deuxième requête d'accès, par exemple de type DHCP, l'équipement intermédiaire en extrait à nouveau l'identifiant client qu'elle contient (qui est contenu par exemple dans l'option 82 du protocole DHCP contenue dans la requête). Il le compare alors à l'identifiant préalablement mémorisé dans le contexte ouvert pour ce client.

En cas de conformité, l'équipement intermédiaire est alors assuré que la deuxième requête a bien été émise par le client précédemment authentifié par le serveur d'authentification, et il peut donc lui transmettre le ou les paramètres de configuration mémorisés dans le contexte ouvert, et accepter la deuxième requête.

Selon une caractéristique avantageuse de l'invention, lesdits premier et deuxième identifiants appartiennent au groupe comprenant:

- un identifiant de ligne du client (CLID pour *Calling Line Identifier*);

- un nom d'utilisateur.

En effet, le CLID peut être aisément utilisé dans le cadre de l'invention car il est inséré dans les requêtes d'accès transmises par un serveur d'accès de type BAS vers un serveur d'authentification lors de l'établissement d'une session PPP. De même, il est aussi inséré dans l'option 82 du protocole DHCP dans les requêtes DHCP transmises d'un client DHCP vers un serveur DHCP.

De manière avantageuse, le procédé de l'invention comprend une étape d'ouverture d'un contexte associé audit client comprenant au moins ledit premier identifiant et ledit au moins un paramètre de configuration, et une étape d'armement d'un temporisateur associé audit contexte, à l'expiration duquel ledit contexte cesse d'être actif.

L'équipement intermédiaire dans lequel est mis en œuvre le procédé de l'invention ouvre donc un contexte contenant le premier identifiant (par exemple le CLID), le ou les paramètres de configuration (par exemple une adresse IP), et éventuellement le nom d'utilisateur (ou *login*) et son mot de passe. Il se prépare alors à recevoir une deuxième requête de type DHCP. Ce contexte reste actif pendant une durée prédéterminée, de sorte qu'il est nécessaire que la deuxième requête parvienne à l'équipement intermédiaire avant la fin de cette durée prédéterminée.

Une telle temporisation permet d'éviter une surcharge inutile de l'équipement intermédiaire, en évitant que des contextes inutilisés ne restent ouverts trop longtemps.

Avantageusement, le procédé de l'invention comprend également une étape de filtrage de ladite autorisation et une étape d'envoi vers ledit client d'un refus d'établissement de ladite session point à point, permettant de déclencher l'émission par ledit client de ladite deuxième requête.

Ainsi, lorsqu'il reçoit l'autorisation du serveur d'authentification (par exemple de type *Access Accept*), l'équipement intermédiaire dans lequel est mis en œuvre le procédé de l'invention bloque cette autorisation, et la remplace par un message de refus (par exemple de type *Access Reject*) qu'il envoie vers le serveur d'accès de type BAS. Ce dernier informe le client de l'échec de l'établissement de la session PPP, de sorte que le client, leurré par l'équipement intermédiaire, prend alors l'initiative de lancer une tentative de connexion DHCP. En outre, le serveur BAS supprime le contexte PPP associé au client, ce qui permet de le décharger.

On notera qu'à titre de variantes, la rupture d'établissement de la session point

à point pourrait aussi être initiée volontairement par le client, ou détectée par le client après un certain nombre de tentatives de connexion PPP restées sans réponse, ou après expiration d'une temporisation de durée prédéterminée.

De manière préférentielle, ledit au moins un paramètre de configuration est une adresse IP allouée audit client pour ladite session d'accès. C'est alors cette adresse IP, fournie par le serveur RADIUS lors de l'établissement de la session PPP, qui est allouée au client pour toute la durée du bail DHCP initié par la suite. Ces paramètres de configuration peuvent également comprendre une adresse du serveur DNS, ou tout autre paramètre prévu dans les échanges DHCP, tel que les données relatives au bail par exemple.

L'invention concerne aussi un équipement d'un réseau d'accès à un service par un client apte à mettre en œuvre, pour l'établissement d'une session d'accès audit service, un protocole de connexion de type point à point (PPP) et un protocole de fourniture dynamique d'au moins un paramètre de configuration, dit protocole de configuration dynamique (DHCP).

Selon l'invention, un tel équipement comprend:

- des moyens de réception d'une première requête d'établissement d'une session d'accès conforme audit protocole de type point à point, dite session point à point, émise à la demande dudit client et destinée à un serveur d'authentification (RADIUS);
- des moyens de réception d'une autorisation émise par ledit serveur d'authentification à destination dudit client, en cas d'authentification dudit client par ledit serveur d'authentification;
- des moyens de mémorisation d'au moins un paramètre de configuration (@ IP) de ladite session point à point extrait de ladite autorisation;
- des moyens de réception d'une deuxième requête d'établissement d'une session d'accès conforme audit protocole de configuration dynamique, émise par ledit client après rupture d'établissement de ladite session point à point;
- des moyens de vérification de l'authentification dudit client;
- des moyens d'envoi audit client dudit au moins un paramètre de configuration mémorisé, pour établissement d'une session d'accès conforme audit protocole de configuration dynamique (DHCP).

Dans le cas particulier d'application de l'invention aux protocoles PPP et DHCP,

un tel équipement joue donc le double rôle de proxy RADIUS et de serveur DHCP. On l'appelle donc dans la suite de ce document PRSD (pour Proxy RADIUS Serveur DHCP). Il est situé entre un serveur d'accès de type point à point (BAS) et le serveur d'authentification (RADIUS).

Selon une caractéristique avantageuse, lesdits moyens de vérification de l'authentification dudit client comprennent des moyens de comparaison d'un premier identifiant dudit client, extrait de ladite première requête et mémorisé en relation avec ledit au moins un paramètre de configuration, et d'un deuxième identifiant dudit client, extrait de ladite deuxième requête.

L'invention concerne également une passerelle résidentielle permettant à un client d'accéder à un service d'un réseau, ladite passerelle résidentielle comprenant des moyens de mise en œuvre d'un protocole de connexion de type point à point et d'un protocole de fourniture dynamique d'au moins un paramètre de configuration, dit protocole de configuration dynamique, pour l'établissement d'une session d'accès audit service.

Selon l'invention, une telle passerelle résidentielle comprend également:

- des moyens d'émission d'une première requête d'établissement d'une session d'accès conforme audit protocole de type point à point, dite session point à point;
- des moyens, activés après rupture d'établissement de ladite session point à point, d'émission d'une deuxième requête d'établissement d'une session d'accès conforme audit protocole de configuration dynamique;
- des moyens de réception d'au moins un paramètre de configuration fourni par un serveur d'authentification lors de l'établissement de ladite session point à point, pour établissement d'une session d'accès conforme audit protocole de configuration dynamique.

La passerelle résidentielle est donc configurée pour tenter tout d'abord de se connecter en mode PPP puis, en cas d'échec de cette tentative (sur réception d'un message d'échec, ou après plusieurs tentatives infructueuses par exemple), pour tenter de se connecter en mode DHCP. Une telle passerelle résidentielle est donc nouvelle et inventive par rapport aux passerelles de l'art antérieur qui utilisaient toujours uniquement l'une ou l'autre des deux méthodes d'accès PPP et DHCP. Grâce à cette nouvelle passerelle, le client peut donc bénéficier des avantages combinés de

chacun de ces deux protocoles.

On notera qu'une telle passerelle résidentielle peut consister en un simple modem client.

L'invention concerne enfin un programme d'ordinateur comprenant des instructions de code de programme pour l'exécution des étapes du procédé décrit précédemment lorsque ledit programme est exécuté sur un ordinateur, ainsi qu'un support d'enregistrement lisible par un ordinateur sur lequel est enregistré un tel programme.

4. Liste des figures

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

- la figure 1, déjà commentée en relation avec l'art antérieur, présente les différents équipements intervenant dans l'établissement d'une session d'accès de type PPP;
- la figure 2, déjà commentée en relation avec l'art antérieur, illustre les différents équipements intervenant dans l'établissement d'une session d'accès de type DHCP;
- la figure 3 illustre les différents flux de données échangés entre les équipements intervenant dans la mise en œuvre du procédé de l'invention;
- la figure 4 illustre plus précisément les échanges de messages constituant les flux de la figure 3;
- la figure 5 présente sous forme schématique un équipement intermédiaire de type PRSD conforme à l'invention.

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

Le principe général de l'invention repose sur l'utilisation séquentielle, par un client souhaitant établir une session d'accès à un service, de deux protocoles, à savoir un protocole de type point à point (PPP) puis un protocole de configuration dynamique (DHCP), et sur la réutilisation de paramètres de configuration (@ IP), obtenus lors de l'établissement de la session point à point, pour l'établissement de la connexion conforme au protocole de configuration dynamique.

Bien que l'invention ne soit pas limitée aux deux seuls protocoles PPP et DHCP,

on se limite, dans la suite de ce document, à la description d'un mode de réalisation particulier de l'invention dans le cadre de ces deux protocoles, par souci de simplification. On considère en outre le cas particulier où l'authentification d'un client est réalisée au moyen du protocole RADIUS.

En relation avec la figure 3, l'invention repose donc sur l'introduction d'un nouvel équipement 7 dans le réseau, que l'on baptise PRSD, et qui remplit une double fonction de Proxy RADIUS et de serveur DHCP. Un tel équipement 7 se trouve entre le serveur d'accès large bande BAS 2 (qui joue également le rôle de relais DHCP) et le serveur RADIUS 3, qui interviennent dans l'établissement de la session PPP.

Contrairement à certaines solutions dites "propriétaires" proposées par des équipementiers, la technique de l'invention peut donc s'intégrer dans n'importe quel réseau existant, sans qu'il soit nécessaire de modifier les équipements déjà en place, et notamment les serveurs d'accès de type BAS 2 ou les serveurs d'authentification 3 de type RADIUS. En effet, la technique de l'invention repose uniquement sur l'adjonction d'une plate-forme PRSD 7, qui est indépendante des équipements industriels du réseau, et sur l'adaptation du kit de connexion client 1, qui est configuré pour se connecter d'abord en PPP, puis, en cas d'échec, en DHCP.

Le procédé de l'invention peut être résumé par le diagramme de flux de la figure 3. Le client 1 (modem ou passerelle résidentielle) initie 30 un dialogue PPP avec le serveur d'accès BAS 2, au moyen des protocoles PPP et PAP/CHAP. On notera que le BAS 2 utilise de préférence le protocole CHAP, pour des raisons de sécurité, afin d'éviter la transmission d'informations sensibles en clair sur le réseau. Le BAS 2 amorce alors un dialogue RADIUS 31, et envoie une demande d'authentification destinée au serveur RADIUS 3.

Cette demande d'authentification 31 est interceptée par le PRSD, qui en extrait l'identifiant de la ligne client CLID pour le sauvegarder dans un contexte qu'il ouvre 32 pour ce client. Ce contexte est destiné à contenir au moins les éléments suivants: *login,* mot de passe, CLID et @IP. Le PRSD 7 se prépare alors à traiter une requête DHCP de ce même client. Le contexte reste actif pendant une durée prédéterminée, par exemple de l'ordre de 60 secondes. Le PRSD 7 fait suivre 33 la demande d'authentification, sous forme d'une requête RADIUS, vers le serveur RADIUS 3.

Après authentification du client 1, le serveur RADIUS 3 envoie 34 une requête RADIUS d'autorisation vers le PRSD 7. A réception de l'autorisation, le PRSD 7

sauvegarde 35 l'adresse IP proposée par le serveur RADIUS 3 dans le contexte précédemment ouvert pour le client 1. Il bloque alors l'autorisation (*Access Accept*) et la remplace 36 par une requête RADIUS de rejet (*Access Reject*) qu'il émet alors vers le BAS 2, pour lui signifier un échec de la tentative de connexion PPP.

Le BAS 2, qui joue le rôle de serveur PPP, transmet cette notification d'échec au client 1 sous forme d'un message PPP 37 de type "PAP/CHAP failure". Il supprime alors le contexte PPP qu'il avait précédemment ouvert pour ce client, se déchargeant ainsi de cette tâche.

Lors d'une étape référencée 38, le client 1 est donc informé du soi-disant échec de la connexion PPP, et décide de lancer une tentative de connexion DHCP. Il émet alors une requête DHCP 39 vers le BAS 2, qui joue désormais le rôle de relais DHCP. Cette phase DHCP doit commencer au plus tard 60 secondes après l'échec de sa première connexion PPP, pour que le contexte du client 1 soit encore ouvert dans le PRSD 7.

Le BAS 2 se contente de faire suivre cette requête DHCP 310 vers le PRSD 7, qui vérifie 311 l'identité de ligne du client 1, en comparant le CLID sauvegardé 32 dans le contexte précédemment ouvert et les éléments identifiant la ligne du client 1 figurant dans l'option 82 de la requête DHCP reçue.

En cas de succès de la comparaison, le PRSD 7 attribue 312 l'adresse IP sauvegardée 35 dans le contexte précédemment ouvert. Il envoie un message 313 d'acquittement DHCP, qui est relayé 314 par le BAS 2 jusqu'au client 1.

Une connexion DHCP peut donc être établie pour le client 1, sur la base de l'adresse IP allouée 34 par le serveur RADIUS 3.

La figure 4 illustre plus en détail les différents messages qui peuvent être échangés entre le client 1, le BAS 2, le PRSD 7 et le serveur RADIUS 3 dans le cadre du procédé de l'invention. Ces différents messages sont classiques des protocoles PPP, DHCP ou RADIUS et ne seront donc pas décrits ici plus en détail.

Selon une implémentation, illustrée en figure 5, les étapes du procédé de l'invention sont déterminées par les instructions d'un programme d'ordinateur 74 incorporé dans le PRSD 7. Le programme 74 comporte des instructions de programme qui, lorsque le programme est exécuté par le processeur 73 du PRSD 7 dont le fonctionnement est alors commandé par l'exécution du programme 74, réalisent les étapes du procédé selon l'invention.

En conséquence, l'invention s'applique également à un programme d'ordinateur 74, notamment un programme d'ordinateur enregistré sur ou dans un support d'informations lisible par un ordinateur et tout dispositif de traitements de données, adapté à mettre en œuvre l'invention. Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable pour implémenter le procédé selon l'invention.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage ou support d'enregistrement 75 sur lequel est enregistré le programme d'ordinateur 74 selon l'invention, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore une clé USB, ou un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type internet.

Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé selon l'invention.

A l'initialisation, les instructions de code du programme d'ordinateur 74 sont par exemple chargées dans une mémoire RAM 75 avant d'être exécutées par le processeur de l'unité de traitement 73. Ce dernier pilote les modules 71 de proxy radius et 72 de serveur DHCP. Comme indiqué précédemment, le module 71 de proxy radius reçoit et émet des données vers le serveur BAS 2, et échange également des données avec un serveur d'authentification 3. Le module 72 de serveur DHCP échange quant à lui des données avec le client 1, par le biais du relais DHCP constitué par le BAS 2.

La mémoire 75 est également utilisée pour la sauvegarde du contexte associé au client 1.

REVENDICATIONS

1. Procédé d'accès par un client (1) à un service au travers d'un réseau, ledit client étant apte à mettre en œuvre, pour l'établissement d'une session d'accès audit service, un protocole de connexion de type point à point et un protocole de fourniture dynamique d'au moins un paramètre de configuration, dit protocole de configuration dynamique,

caractérisé en ce qu'il comprend des étapes de:

- réception d'une première requête (31) d'établissement d'une session d'accès conforme audit protocole de type point à point, dite session point à point, émise à la demande dudit client (1) et destinée à un serveur d'authentification (3);
- en cas d'authentification dudit client (1) par ledit serveur d'authentification (3), réception d'une autorisation (34) émise par ledit serveur d'authentification à destination dudit client, et mémorisation (35) d'au moins un paramètre de configuration (@ IP) de ladite session point à point extrait de ladite autorisation;
- réception d'une deuxième requête (310) d'établissement d'une session d'accès conforme audit protocole de configuration dynamique, émise par ledit client après rupture d'établissement de ladite session point à point;
- après vérification (311) de l'authentification dudit client, envoi (313, 314) audit client dudit au moins un paramètre de configuration mémorisé, pour établissement d'une session d'accès conforme audit protocole de configuration dynamique (DHCP).

2. Procédé d'accès selon la revendication 1, caractérisé en ce que la vérification de l'authentification dudit client met en œuvre une comparaison d'un premier identifiant dudit client, extrait de ladite première requête et mémorisé en relation avec ledit au moins un paramètre de configuration, et d'un deuxième identifiant dudit client, extrait de ladite deuxième requête.

3. Procédé d'accès selon la revendication 2, caractérisé en ce que lesdits premier et deuxième identifiants appartiennent au groupe comprenant:

- un identifiant de ligne du client (CLID);
- un nom d'utilisateur.

4. Procédé selon l'une quelconque des revendications 2 et 3, caractérisé en ce qu'il comprend une étape d'ouverture d'un contexte associé audit client comprenant au moins ledit premier identifiant et ledit au moins un paramètre de configuration, et une

étape d'armement d'un temporisateur associé audit contexte, à l'expiration duquel ledit contexte cesse d'être actif.

5. Procédé d'accès selon l'une quelconque des revendications 1 à 3, caractérisé en ce qu'il comprend également une étape de filtrage de ladite autorisation et une étape d'envoi (36) vers ledit client d'un refus d'établissement de ladite session point à point, permettant de déclencher l'émission par ledit client de ladite deuxième requête.

6. Procédé d'accès selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ledit au moins un paramètre de configuration est une adresse IP allouée audit client pour ladite session d'accès.

7. Equipement (7) d'un réseau d'accès à un service par un client (1) apte à mettre en œuvre, pour l'établissement d'une session d'accès audit service, un protocole de connexion de type point à point (PPP) et un protocole de fourniture dynamique d'au moins un paramètre de configuration, dit protocole de configuration dynamique (DHCP), caractérisé en ce qu'il comprend:

- des moyens de réception d'une première requête d'établissement d'une session d'accès conforme audit protocole de type point à point, dite session point à point, émise à la demande dudit client et destinée à un serveur d'authentification (RADIUS);
- des moyens de réception d'une autorisation émise par ledit serveur d'authentification à destination dudit client, en cas d'authentification dudit client par ledit serveur d'authentification;
- des moyens de mémorisation d'au moins un paramètre de configuration (@ IP) de ladite session point à point extrait de ladite autorisation;
- des moyens de réception d'une deuxième requête d'établissement d'une session d'accès conforme audit protocole de configuration dynamique, émise par ledit client après rupture d'établissement de ladite session point à point;
- des moyens de vérification de l'authentification dudit client;
- des moyens d'envoi audit client dudit au moins un paramètre de configuration mémorisé, pour établissement d'une session d'accès conforme audit protocole de configuration dynamique (DHCP).

8. Equipement selon la revendication 7, caractérisé en ce lesdits moyens de vérification de l'authentification dudit client comprennent des moyens de comparaison d'un premier identifiant dudit client, extrait de ladite première requête et mémorisé en

relation avec ledit au moins un paramètre de configuration, et d'un deuxième identifiant dudit client, extrait de ladite deuxième requête.

9. Passerelle résidentielle (1) permettant à un client d'accéder à un service d'un réseau, ladite passerelle résidentielle comprenant des moyens de mise en œuvre d'un protocole de connexion de type point à point et d'un protocole de fourniture dynamique d'au moins un paramètre de configuration, dit protocole de configuration dynamique, pour l'établissement d'une session d'accès audit service,

caractérisé en ce qu'elle comprend également:

- des moyens d'émission d'une première requête d'établissement d'une session d'accès conforme audit protocole de type point à point, dite session point à point;
- des moyens, activés après rupture d'établissement de ladite session point à point, d'émission d'une deuxième requête d'établissement d'une session d'accès conforme audit protocole de configuration dynamique;
- des moyens de réception d'au moins un paramètre de configuration fourni par un serveur d'authentification lors de l'établissement de ladite session point à point, pour établissement d'une session d'accès conforme audit protocole de configuration dynamique.

10. Programme d'ordinateur (74) comprenant des instructions de code de programme pour l'exécution des étapes du procédé selon l'une quelconque des revendications 1 à 6 lorsque ledit programme est exécuté sur un ordinateur.

11. Support d'enregistrement lisible par un ordinateur sur lequel est enregistré un programme d'ordinateur comprenant des instructions pour l'exécution des étapes du procédé d'accès selon l'une quelconque des revendications 1 à 6.

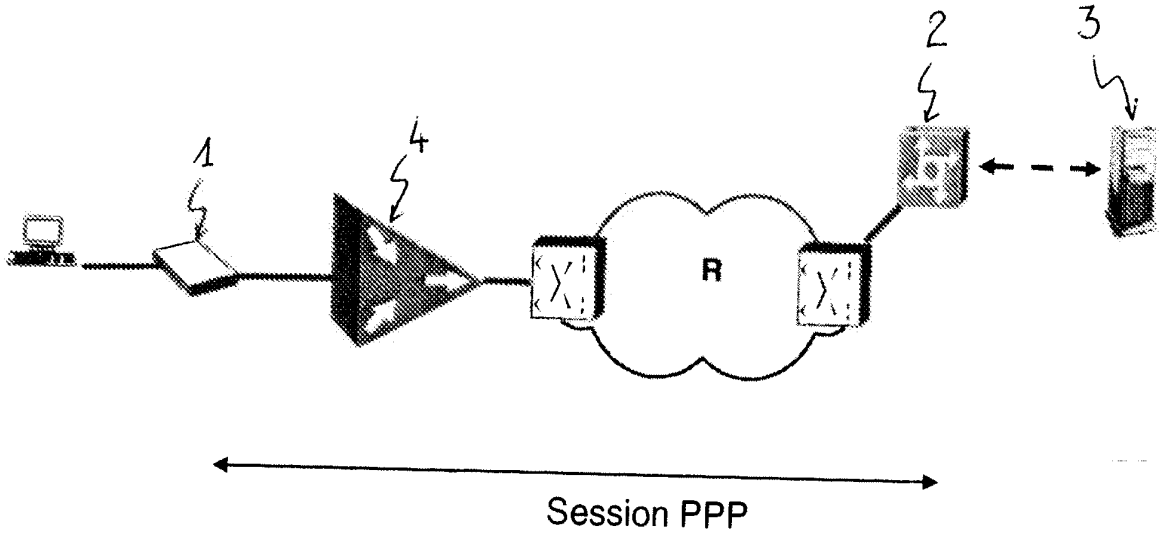


Figure 1

1/4

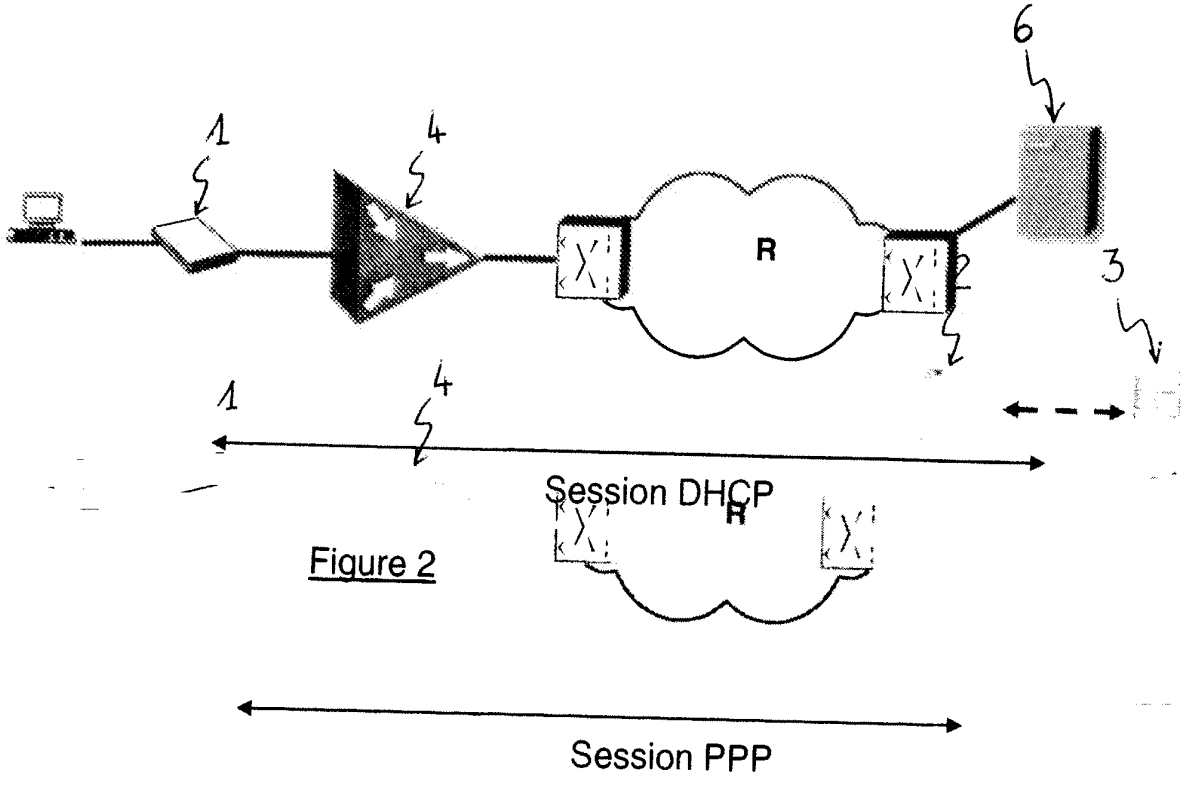


Figure 2

Figure 1

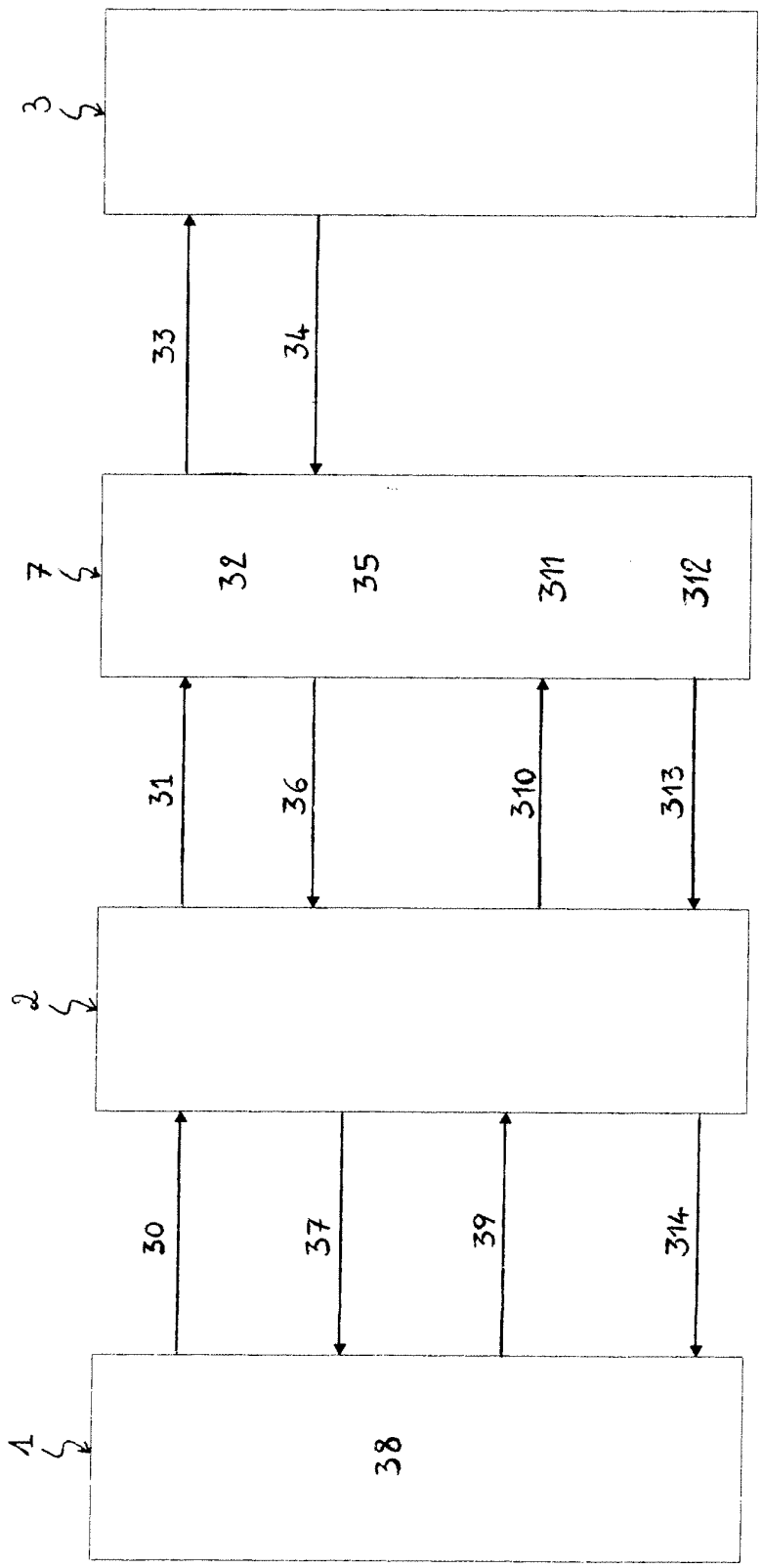


FIGURE 3

3/4

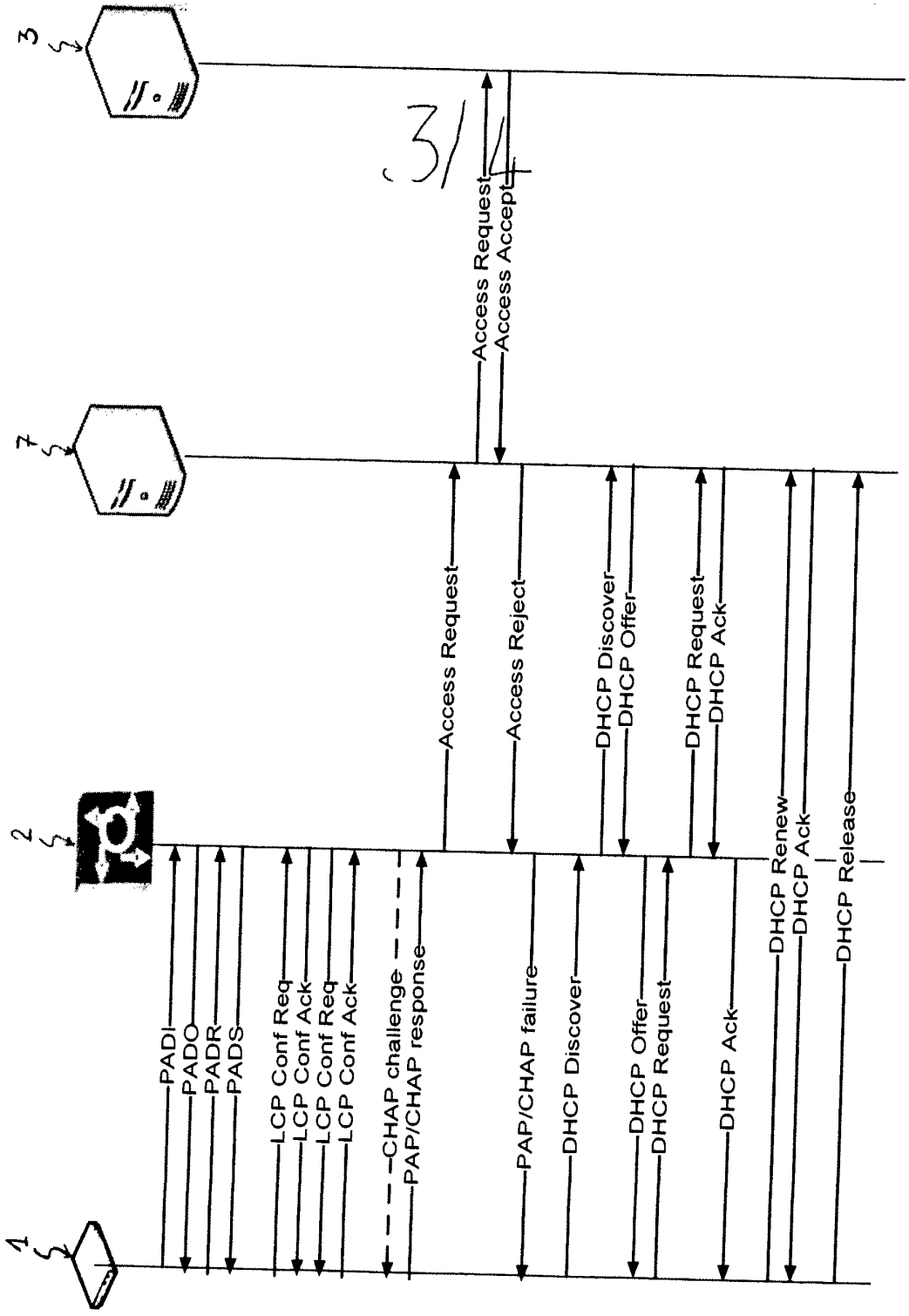

1
2
3
7
PADI
PADO
PADR
PADS
LCP Conf Req
LCP Conf Ack
LCP Conf Req
LCP Conf Ack
CHAP challenge
PAP/CHAP response
Access Request
Access Accept
Access Request
Access Reject
PAP/CHAP failure
DHCP Discover
DHCP Offer
DHCP Request
DHCP Ack
DHCP Discover
DHCP Offer
DHCP Request
DHCP Ack
DHCP Renew
DHCP Ack
DHCP Release

FIGURE 4

4/4

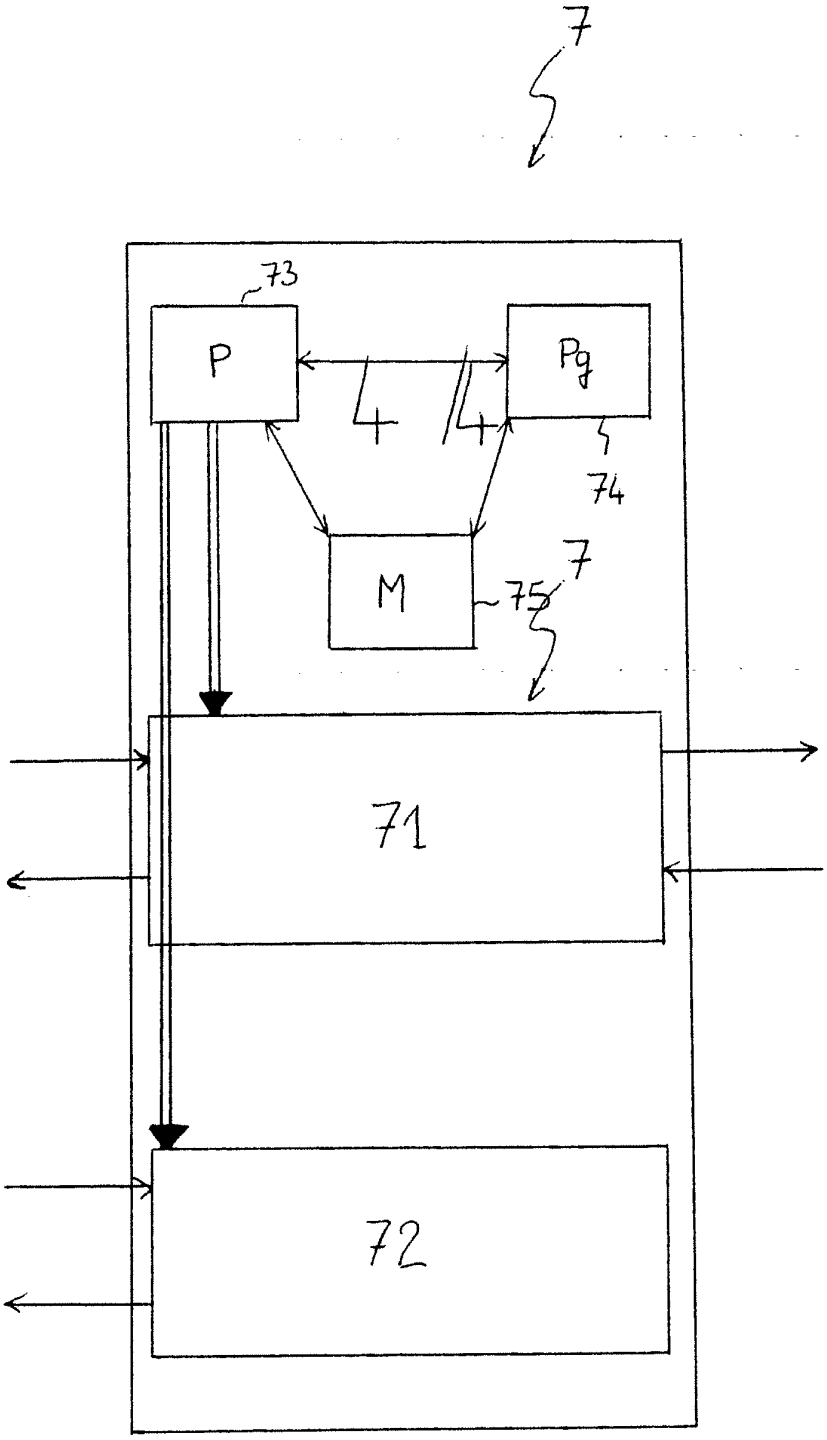


FIGURE 5

RÉPUBLIQUE FRANÇAISE

2904503

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 682621
FR 0653161

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	WO 2005/060208 A (ERICSSON TELEFON AB L M [SE]; MELSEN TORBEN [DK]) 30 juin 2005 (2005-06-30) * page 14, ligne 1 - page 15, ligne 4 *	1-3,7-11	
A	EP 1 571 781 A (FRANCE TELECOM [FR]) 7 septembre 2005 (2005-09-07) * alinéas [0034] - [0036] * * alinéas [0039], [0040] * * alinéas [0059] - [0063] *	1,7,9-11	
A	US 2002/023160 A1 (GARRETT JOHN W [US] ET AL) 21 février 2002 (2002-02-21) * alinéas [0004], [0006] * * alinéas [0036], [0038]; figure 9 *	1,7,9-11	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04L

Date d'achèvement de la recherche	Examinateur
16 février 2007	RUIZ SANCHEZ, J

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

.....

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0653161 FA 682621

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 16-02-2007
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2005060208 A	30-06-2005	AU 2003290477 A1	05-07-2005
		CN 1879379 A	13-12-2006
EP 1571781 A	07-09-2005	WO 2005096551 A1	13-10-2005
US 2002023160 A1	21-02-2002	AUCUN	

EPO FORM P0465