

19) RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

11) N° de publication : **2 918 232**
(à n'utiliser que pour les
commandes de reproduction)

21) N° d'enregistrement national : **07 56129**

51) Int Cl⁸ : **H 04 L 12/56 (2006.01), G 06 F 11/30**

12)

DEMANDE DE BREVET D'INVENTION

A1

22) Date de dépôt : 28.06.07.

30) Priorité :

43) Date de mise à la disposition du public de la demande : 02.01.09 Bulletin 09/01.

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) : AIRBUS FRANCE Société par actions simplifiée — FR.

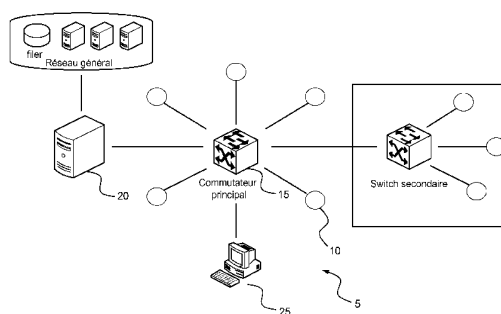
72) Inventeur(s) : DESSERTENNE FRANCK.

73) Titulaire(s) :

74) Mandataire(s) : SANTARELLI.

54) PROCÉDES ET DISPOSITIFS POUR LA COMMUNICATION DE DONNÉES DE DIAGNOSTIC DANS UN RESEAU DE COMMUNICATION TEMPS REEL.

57) L'invention a pour objet des procédés et des dispositifs d'identification et de communication non intrusifs entre un noeud serveur (25) et au moins un noeud client (10) dans un réseau de communication (5). Un message d'identification est tout d'abord émis à destination d'au moins un noeud client, le message d'identification comprenant au niveau applicatif une duplication des données d'adressage (l'adresse physique et l'adresse Internet dudit noeud serveur) par ailleurs contenue dans les couches MAC et IP. La réception d'au moins un couple d'adresses d'au moins un noeud client en réponse à l'émission d'un message d'identification, un couple d'adresses d'un noeud client comprenant une adresse physique et une adresse Internet (selon la même stratégie de duplication), permet d'identifier auprès du serveur le noeud client. De façon similaire, l'invention permet d'identifier, dans un noeud client, au moins un noeud serveur dans un réseau.



FR 2 918 232 - A1



5 La présente invention concerne des procédés et des dispositifs d'identification et de communication non intrusif entre un nœud serveur et plusieurs nœuds clients au sein d'un réseau commuté temps réel.

Un réseau de type « *switch fabric* » est basé sur une architecture commutée, c'est-à-dire que les équipements terminaux chargés de l'émission et
10 de la réception des données s'organisent autour des commutateurs chargés du transport de ces données, à N entrées et N sorties. La communication est réalisée par l'envoi et la réception de paquets, ces derniers étant émis en parallèle.

De manière plus générale, l'invention concerne, dans un réseau de
15 traitement de données en temps réel comprenant au moins un serveur et au moins un client, les principes régissant la communication de données de diagnostic entre ces éléments du réseau de sorte à être non intrusif sur la communication temps réel circulant par ailleurs sur ce même réseau.

L'invention s'applique notamment dans un réseau de simulation de
20 composants d'un aéronef en temps réel, où un diagnostic de ces composants doit être effectué sans perturber le réseau de simulation.

La simulation de composants d'un aéronef est utilisée pour assurer le développement et l'intégration des systèmes électroniques et informatiques embarqués dans les aéronefs, en particulier avant le premier vol.

25 L'architecture de simulation comprend une pluralité de terminaux aussi appelés nœuds du réseau, chacun de ces terminaux étant apte à réaliser les calculs de simulation ou constituant l'interface électronique avec l'environnement réel, permettant de vérifier le fonctionnement des équipements réels de l'aéronef. Ainsi, cette architecture comprend notamment un terminal de
30 simulation apte à émettre des données selon une séquence synchrone selon le principe requête / réponse.

Des nœuds du réseau sont constitués des calculateurs de simulation et des cartes d'entrée / sortie d'interfaces électroniques.

L'échange des données entre les différents nœuds du réseau est réalisé sur un port UDP (acronyme de « *User Datagram Protocol* » en terminologie anglo-saxonne) spécifique et en temps réel, c'est-à-dire que la simulation des comportements des équipements est réalisée à la vitesse de leur déroulement réel.

Afin de réaliser des diagnostics sur une telle architecture réseau, il peut être connecté à tout moment au réseau un équipement de diagnostic apte à identifier les dysfonctionnements des différents nœuds du réseau.

Toutefois, sans une phase d'apprentissage spécifique de la topologie du réseau, les échanges de messages génèrent un trafic supplémentaire sur le réseau entre l'équipement de diagnostic et les différents nœuds du réseau. Les messages échangés sont par typiquement des messages ARP (acronyme de « *Address Resolution Protocol* » en terminologie anglo-saxonne).

Une telle mise en œuvre présente l'inconvénient qu'un grand nombre de messages ARP entre l'équipement de diagnostic et les nœuds du réseau sont transmis ce qui perturbe l'exécution en temps réel de la simulation.

La présente invention a pour objet de remédier à au moins un des inconvénients des techniques et processus de l'art antérieur précité. Pour ce faire, l'invention propose notamment un procédé et un dispositif d'identification dynamique, dans un nœud serveur, d'au moins un nœud client dans un réseau de communication et un procédé et un dispositif d'identification, dans un nœud client, d'un nœud serveur dans un réseau de communication aptes à respecter des contraintes fortes telles que la non perturbation du déroulement en temps réel de la simulation.

L'invention a ainsi pour objet un procédé d'identification, dans un nœud serveur connecté à un réseau, d'au moins un nœud client connecté au réseau, le procédé comprenant les étapes suivantes,

- une étape d'émission d'un message d'identification à au moins un nœud client, le message d'identification comprenant l'adresse physique et l'adresse Internet dudit nœud serveur, et

- une étape de réception d'au moins un message contenant le couple d'adresses d'au moins un nœud client en réponse à l'étape d'émission d'un message d'identification, un couple d'adresses d'un nœud client comprenant une adresse physique (MAC) et une adresse Internet (IP).

5 Le procédé selon l'invention permet ainsi de déterminer dynamiquement la topologie du réseau sans nécessiter de connexion point à point ni la connaissance préalable de sa définition topologique. Ce procédé permet de respecter des contraintes de non intrusion permettant le déroulement de simulations en temps réel.

10 De façon avantageuse, ledit au moins un couple d'adresses de nœud client est mémorisé statiquement dans une table de correspondance entre une adresse physique et une adresse Internet, telle que la table ARP du système d'exploitation, dans ledit nœud serveur pour contrôler les messages générés par le système d'exploitation, c'est-à-dire par exemple pour contraindre les
15 mécanismes ARP.

Selon un mode de réalisation particulier, l'émission dudit message d'identification est réalisée en mode *multicast*.

L'invention a aussi pour objet un procédé d'échange de données de diagnostic dans un réseau entre un nœud du réseau et un terminal de
20 diagnostic connecté au réseau, le procédé comprenant les étapes suivantes,

- identification d'au moins un nœud du réseau selon le procédé d'identification décrit précédemment ; et,

- transmission d'une commande de diagnostic audit au moins un nœud identifié du réseau.

25 Le procédé selon l'invention permet ainsi d'échanger des données de diagnostic sans perturber le fonctionnement temps réel du réseau tout en gardant des caractéristiques standard de réseau.

L'invention a également pour objet un procédé d'identification, dans un nœud client connecté à un réseau, d'un nœud serveur connecté au réseau,
30 le procédé comprenant les étapes suivantes,

- une étape de réception d'un message d'identification provenant dudit nœud serveur, le message d'identification comprenant l'adresse physique (MAC) et l'adresse Internet (IP) dudit nœud serveur, et

5 - une étape d'émission audit nœud serveur d'un message contenant le couple d'adresses dudit nœud client en réponse à l'étape de réception du message d'identification, le couple d'adresses comprenant une adresse physique (MAC) et une adresse Internet (IP) du nœud client.

De façon avantageuse, ledit au moins un couple d'adresses du nœud serveur est mémorisé statiquement dans une table de correspondance entre
10 une adresse physique et une adresse Internet, telle que la table ARP du système d'exploitation, dans ledit nœud client.

L'invention a aussi pour objet un procédé d'échange de données de diagnostic, dans un nœud client connecté à un réseau, caractérisé en ce qu'il comprend les étapes suivantes,

15 - identification d'au moins un nœud serveur selon le procédé d'identification décrit précédemment ; et,

- activation d'une tâche de gestion de données de diagnostic à la réception d'une commande de diagnostic selon l'état d'activation d'une tâche de gestion de données de simulation.

20 Le procédé selon l'invention met ainsi en œuvre une gestion par priorité des services pour limiter l'intrusion des opérations de diagnostic sur des opérations de simulations.

Avantageusement, les tâches de gestion de données de diagnostic et de simulation utilisent des ports différents.

25 L'invention a aussi pour objet un programme d'ordinateur comprenant des instructions adaptées à la mise en œuvre de chacune des étapes des procédés décrits précédemment.

L'invention a également pour objet un dispositif comprenant des moyens adaptés à la mise en œuvre de chacune des étapes des procédés
30 décrits précédemment.

D'autres avantages, buts et caractéristiques de la présente invention ressortent de la description détaillée qui suit, faite à titre d'exemple non limitatif, au regard des dessins annexés dans lesquels:

- 5 - la figure 1 illustre une architecture réseau de simulation intégrant un terminal de diagnostic conformément à l'invention ; et
- la figure 2 présente les couches de programmation du système et les interactions avec les modules de diagnostic client et serveur conformément à l'invention.

10 Conformément à l'invention, le diagnostic d'un réseau de simulation de composants, notamment de composants avioniques, est centralisé et intégré. Cette simulation est basée sur des contraintes temps réel fortes de sorte que celle-ci ne doit nullement être perturbée afin de simuler au mieux le comportement réel des composants.

Les fonctionnalités du diagnostic sont notamment les suivantes :

- 15 - détermination des nœuds réseau qui sont présents, notamment de façon centralisée, c'est-à-dire sans avoir une connexion point à point directe avec chacun des équipements d'interface électronique utilisés ;
- surveillance en temps réel avec la possibilité de déporter l'interface graphique de surveillance et de diagnostic ;
- 20 - établir la cartographie des nœuds du réseau, notamment la liste des équipements du réseau et leur configuration (logiciels, matériels constitutifs et paramétrage) ;
- consulter ou modifier le paramétrage des nœuds du réseau ;
- surveiller les paramètres internes et élaborer des statistiques ;
- 25 - forcer des voies d'entrée/sortie et d'autres paramètres ;
- enregistrer en temps réel des paramètres, notamment en mémoire volatile ;
- enregistrer des contextes de panne, notamment en mémoire non volatile ;
- 30 - obtenir des tables de paramétrage, de configuration, de contextes de panne et d'enregistrement ; et,

- gérer des statistiques avancées, telles que la durée de traitement des messages de simulation, de la pile IP (acronyme de « *Internet Protocol* » en terminologie anglo-saxonne) et de la pile de messages.

Selon un mode de réalisation particulier, le système de diagnostic est intégré au réseau de simulation et une seule connectique réseau est nécessaire. En outre, la fonction diagnostic est centralisée.

Il n'y a pas de charge des terminaux supplémentaires et l'investigation est réalisée en mode opérationnel sans déconnecter les nœuds.

Pour ce faire, selon un mode de réalisation de l'invention, le réseau de simulation, illustré en Figure 1, comprend un ensemble de nœuds réseau aptes à fonctionner ensemble afin de réaliser la simulation de composants, notamment de composants avioniques connectés entre eux dans un réseau commuté de type *switch fabric*.

Ainsi, chacun des nœuds 10 du réseau 5 est connecté à un commutateur principal 15. Ces nœuds 10 sont notamment des nœuds de calcul, des cartes d'entrée / sortie, des nœuds intermédiaires et des concentrateurs.

A ce réseau 5 sont connectés un calculateur principal de simulation 20 (« *host* » en terminologie anglo-saxonne) sur le commutateur principal 15 et un équipement de diagnostic 25.

Afin de respecter au mieux le temps réel, le réseau est un réseau haut débit, par exemple un réseau de cent méga bits par seconde ou d'un giga bits par seconde.

Conformément à l'invention, un module, notamment un module logiciel (appelé « *plugin* » en terminologie anglo-saxonne) est installé dans différents nœuds du réseau à diagnostiquer, appelé module de diagnostic client, et dans l'équipement de diagnostic 25, appelé module de diagnostic serveur.

Ce module logiciel est un programme intégré à l'applicatif opérationnel de chaque nœud de l'interface électronique.

Conformément à l'invention, une mise en œuvre particulière de la couche message est réalisée en s'appuyant autant que possible sur les

couches de programmation POSIX (acronyme de « *Portable Operating System Interface* » en terminologie anglo-saxonne) du système d'exploitation des nœuds et de l'équipement de diagnostic 25.

En outre, l'équipement serveur de diagnostic doit réaliser, au
5 démarrage, l'apprentissage de la topologie du réseau. Cet apprentissage est dynamique, c'est-à-dire qu'il est obtenu par interrogation des différents nœuds du réseau, notamment par l'émission d'un message spécifique d'identification et par traitement des messages réponses associées.

L'échange de messages peut être réalisée selon un mode synchrone
10 ou un mode asynchrone (aussi appelé mode « TRAP » en terminologie anglo-saxonne).

Selon un mode de réalisation synchrone, une requête de diagnostic est émise par le terminal de diagnostic (nœud serveur) et une réponse est émise par le nœud diagnostiqué (nœud client) à l'issue du traitement.

15 Selon un mode de réalisation asynchrone, un traitement est activé au moyen d'un message *unicast*, c'est-à-dire selon un mode point à point, ou d'un message *multicast*, c'est-à-dire d'un message destiné à un groupe de nœuds réseau. L'obtention des données de diagnostic est dans ce cas réalisée périodiquement et automatiquement selon une période programmable
20 (émission de messages spontanée et périodique par les nœuds clients configurés dans ce mode).

Conformément à l'invention, l'intrusion du diagnostic sur le fonctionnement temps réel de la simulation est maîtrisé, notamment par le contrôle des émissions des protocoles de la couche réseau, par la maîtrise de
25 la latence d'accès concurrent à l'interface réseau des nœuds et par la maîtrise de la latence noyau et applicative induite sur les nœuds du réseau.

Conformément à l'invention, les modules logiciels utilisent l'interface de programmation d'application *socket* standard, notamment pour la mise en œuvre du protocole UDP.

30 En outre, sur chacun des nœuds du réseau, notamment sur les nœuds d'interfaces électroniques, une gestion par service est réalisée de la façon suivante :

- une tâche gérant un port UDP spécifique pour les données de simulation. Cette tâche possède la priorité maximale ; et,

- une tâche gérant un port UDP spécifique pour les données de diagnostic. Cette tâche possède la priorité minimale.

5 En outre, la fragmentation des paquets IP lors de l'émission de messages vers des nœuds du réseau est interdite. Toute fragmentation de message doit donc être réalisée au niveau de la couche message afin de ne pas charger la pile IP, évitant de la sorte le risque de latence du noyau, ce dernier mettant en œuvre un sémaphore (aussi appelé « *mutex* » pour « *Mutual*
10 *Exclusion* » en terminologie anglo-saxonne) d'accès à l'unique interface réseau de chaque nœud.

De plus, l'émission de messages fragmentés est étalée temporellement, par exemple un message par cycle, soit toutes les 10 ms si la durée d'un cycle est de 10 ms.

15 Lorsque l'équipement de diagnostic souhaite émettre un message, notamment une trame Ethernet à destination d'un nœud du réseau dont il connaît l'adresse Internet aussi appelée adresse IP, il interroge sa mémoire tampon ARP à la recherche d'une entrée correspondant à l'adresse IP de la machine cible.

20 Une mémoire tampon ARP, aussi appelée un cache ARP, est un ensemble de couples (adresse IP, adresse physique) contenu dans la mémoire d'un ordinateur utilisant le protocole ARP, c'est à dire un espace mémoire dans lequel est enregistrée une table listant des correspondances adresse physique -
25 L'adresse physique est ici l'adresse MAC (acronyme de « *Media Access Control* » en terminologie anglo-saxonne) du nœud réseau.

30 Si l'adresse IP du destinataire est présente dans le cache ARP de l'émetteur, le système d'exploitation renseigne l'adresse physique de destination correspondante pour envoyer la trame Ethernet. Le mécanisme ARP s'arrête ici dans ce cas.

Dans le cas contraire, si l'adresse IP est absente de la mémoire tampon de l'émetteur, l'équipement de diagnostic place son émission en attente

et effectue une requête ARP, notamment selon le mode *broadcast*. Cette requête est de type « quelle est l'adresse physique correspondant à l'adresse IP *adresseIP* ? Répondez à *adressePhysique* ». Puisqu'une telle requête est émise en mode *broadcast*, tous les noeuds connectés au réseau à travers le commutateur reçoivent la requête. Le noeud concerné répond alors à l'émetteur de la requête ARP.

Cette solution présente l'inconvénient de perturber le réseau de simulation temps réel.

Pour ne pas perturber la communication temps réel des données de simulation, les trames ARP générées automatiquement par le système d'exploitation sont bloquées en insérant des entrées permanentes (statiques) dans la mémoire tampon ARP.

Ainsi, conformément à l'invention, la mémoire tampon ARP est remplie au moyen d'entrées permanentes, notamment au moyen d'une interface de programmation POSIX.

Pour ce faire, une requête d'identification est tout d'abord émise en mode *multicast* par l'équipement de diagnostic (serveur), notamment par le module de diagnostic serveur, avant toute émission de messages *unicast* à destination de noeuds clients. Cette requête est émise à destination d'une adresse *multicast* convenue, sur laquelle les différents noeuds clients se sont préalablement abonnés.

A partir des réponses d'identification des noeuds du réseau présents, il est constitué des couples d'adresses (adresse physique, adresse IP). Ceci est réalisé par exemple par duplication explicite des couples (adresse physique, adresse IP) dans la couche message de la réponse d'identification. De la sorte, la topologie du réseau est constituée.

En outre, chaque couple (adresse physique, adresse IP) est placé en tant qu'entrée permanente, c'est-à-dire de façon statique dans le cache ARP avant toute émission de message de diagnostic, ces messages pouvant être des requêtes ou des réponses. Ensuite, par construction, aucun message de type ARP n'est émis par l'équipement de diagnostic ou par les noeuds.

Au cours du diagnostic, l'équipement de diagnostic, notamment le module de diagnostic serveur, émet des messages de préférence en mode *unicast*, le mode *multicast* étant néanmoins autorisé puisque ne générant pas de trafic ARP. Toutefois, afin d'éviter l'émission d'un grand nombre de messages pouvant « inonder » le réseau et donc perturber la simulation en temps réel, l'émission de messages de diagnostic en mode *broadcast* est proscrite.

Selon un mode de réalisation particulier sur le nœud serveur, l'adressage en mode *unicast* est réalisé par la tâche diagnostic de manière cyclique sur les clients, par exemple un message pour un client par cycle, avec une temporisation entre chaque émission.

En outre, en mode asynchrone, un message de fin du mode asynchrone doit être émis par le serveur de diagnostic avant la fin d'exécution du module de diagnostic pour éviter toute émission ultérieure de message ICMP (acronyme de « *Internet Control Message Protocol* » en terminologie anglo-saxonne) par les clients concernés (c'est à dire des clients dont le mode TRAP est activé), notamment l'émission de message « *ICMP port unreachable* ». Ce protocole est mis en œuvre pour véhiculer des messages de contrôle et d'erreur.

Du côté des nœuds clients du réseau, le module de diagnostic client rend actif la couche IGMP (acronyme de « *Internet Group Management Protocol* » en terminologie anglo-saxonne) à l'initialisation de sorte à gérer le *multicast*.

A l'initialisation, le module de diagnostic client émet une requête d'abonnement à une adresse *multicast* spécifique convenue, notamment l'adresse IP de diagnostic pour configurer la table de redirection du commutateur pour la gestion des groupes *multicast*, de sorte à éviter l'émission en mode *broadcast* par le commutateur d'un paquet *multicast* qu'il doit router et qui n'a aucune interface abonnée à cette adresse.

En outre, afin d'empêcher toute émission de message ARP, le couple d'adresses (adresse physique, adresse IP) de l'équipement de diagnostic (serveur) est obtenu par les nœuds clients lors de la requête

d'identification, notamment par duplication explicite du couple MAC / IP (adresse physique, adresse IP) dans la couche message de la requête d'identification, puis est placé en tant qu'entrée permanente, c'est-à-dire de façon statique, dans le cache ARP avant toute émission *unicast* de message de
5 diagnostic.

Au cours du diagnostic, les nœuds du réseau, notamment les modules de diagnostic client, émettent des messages en mode *unicast*. Ces messages sont émis, en mode synchrone, sur réception d'une requête, et sont émis de façon périodique quand le mode de communication asynchrone est
10 activé (mode TRAP).

Il est maintenant décrit, en référence à la Figure 2, les couches de programmation du système et les interactions avec les modules de diagnostic client et serveur.

La programmation des modules de diagnostic client et serveur utilise
15 une interface de programmation POSIX située dans l'espace utilisateur du système d'exploitation.

Cet espace est situé, selon la hiérarchie des couches de communication, au dessus de l'espace noyau.

L'espace noyau comprend, au plus bas de la hiérarchie des couches
20 protocolaires, un pilote réseau (appelé « *driver* » en terminologie anglo-saxonne) sur lequel une couche réseau s'appuie, comprenant notamment une couche IGMP, une couche ICMP, une couche IP et une couche ARP.

Au dessus de la couche réseau et s'appuyant sur la couche ICMP ou sur la couche IP se trouve la couche UDP formant en partie la couche transport.

25 La référence 21 illustre la communication entre le module de diagnostic client et la couche IGMP, via l'interface POSIX, afin de réaliser l'abonnement à une adresse IP *multicast*.

La référence 22 illustre la communication entre le module de diagnostic client ou le module de diagnostic serveur et la couche UDP, via
30 l'interface POSIX, pour l'émission et la réception de message asynchrone.

La référence 23 illustre la communication entre le module de diagnostic client ou le module de diagnostic serveur et la couche ARP, via

l'interface POSIX, afin de réaliser l'ajout d'entrées permanentes dans le cache ARP.

Naturellement, pour satisfaire des besoins spécifiques, une personne compétente dans le domaine de l'invention pourra appliquer des modifications
5 dans la description précédente.

REVENDEICATIONS

- 5 1. Procédé d'identification, dans un nœud serveur (25) connecté à un réseau (5), d'au moins un nœud client (10) connecté au réseau, caractérisé en ce qu'il comprend les étapes suivantes,
- une étape d'émission d'un message d'identification à au moins un nœud client, le message d'identification comprenant l'adresse physique et
 - 10 l'adresse Internet dudit nœud serveur, et
 - une étape de réception d'au moins un message contenant le couple d'adresses d'au moins un nœud client en réponse à l'étape d'émission d'un message d'identification, un couple d'adresses d'un nœud client comprenant une adresse physique et une adresse Internet.
- 15 2. Procédé d'identification selon la revendication 1 caractérisé en ce que ledit au moins un couple d'adresses de nœud client est mémorisé statiquement dans une table de correspondance entre une adresse physique et une adresse Internet dans ledit nœud serveur.
3. Procédé d'identification selon la revendication 1 ou la
- 20 revendication 2 caractérisé en ce que l'émission dudit message d'identification est réalisée en mode *multicast*.
4. Procédé d'échange de données de diagnostic dans un réseau entre un nœud du réseau et un terminal de diagnostic connecté au réseau, le procédé étant caractérisé en ce qu'il comprend les étapes suivantes,
- 25 - identification d'au moins un nœud du réseau selon l'une quelconque des revendications précédentes ; et,
- transmission d'une commande de diagnostic audit au moins un nœud identifié du réseau.
5. Procédé d'identification, dans un nœud client (10) connecté à un
- 30 réseau (5), d'un nœud serveur (25) connecté au réseau, caractérisé en ce qu'il comprend les étapes suivantes,

- une étape de réception d'un message d'identification provenant dudit nœud serveur, le message d'identification comprenant l'adresse physique et l'adresse Internet dudit nœud serveur, et

5 - une étape d'émission audit nœud serveur d'un message contenant le couple d'adresses dudit nœud client en réponse à l'étape de réception du message d'identification, le couple d'adresses comprenant une adresse physique et une adresse Internet du nœud client.

6. Procédé d'identification selon la revendication 5, caractérisé en ce que ledit au moins un couple d'adresses du nœud serveur est mémorisé
10 statiquement dans une table de correspondance entre une adresse physique et une adresse Internet dans ledit nœud client.

7. Procédé d'échange de données de diagnostic, dans un nœud client connecté à un réseau, caractérisé en ce qu'il comprend les étapes suivantes,

15 - identification d'au moins un nœud serveur selon l'une des revendications 5 et 6 ; et,

- activation d'une tâche de gestion de données de diagnostic à la réception d'une commande de diagnostic selon l'état d'activation d'une tâche de gestion de données de simulation.

20 8. Procédé selon la revendication 7 caractérisé en ce que les tâches de gestion de données de diagnostic et de simulation utilisent des ports spécifiques différents.

9. Programme d'ordinateur comprenant des instructions adaptées à la mise en œuvre de chacune des étapes du procédé selon l'une quelconque
25 des revendications précédentes.

10. Dispositif comprenant des moyens adaptés à la mise en œuvre de chacune des étapes du procédé selon l'une quelconque des revendications 1 à 8.

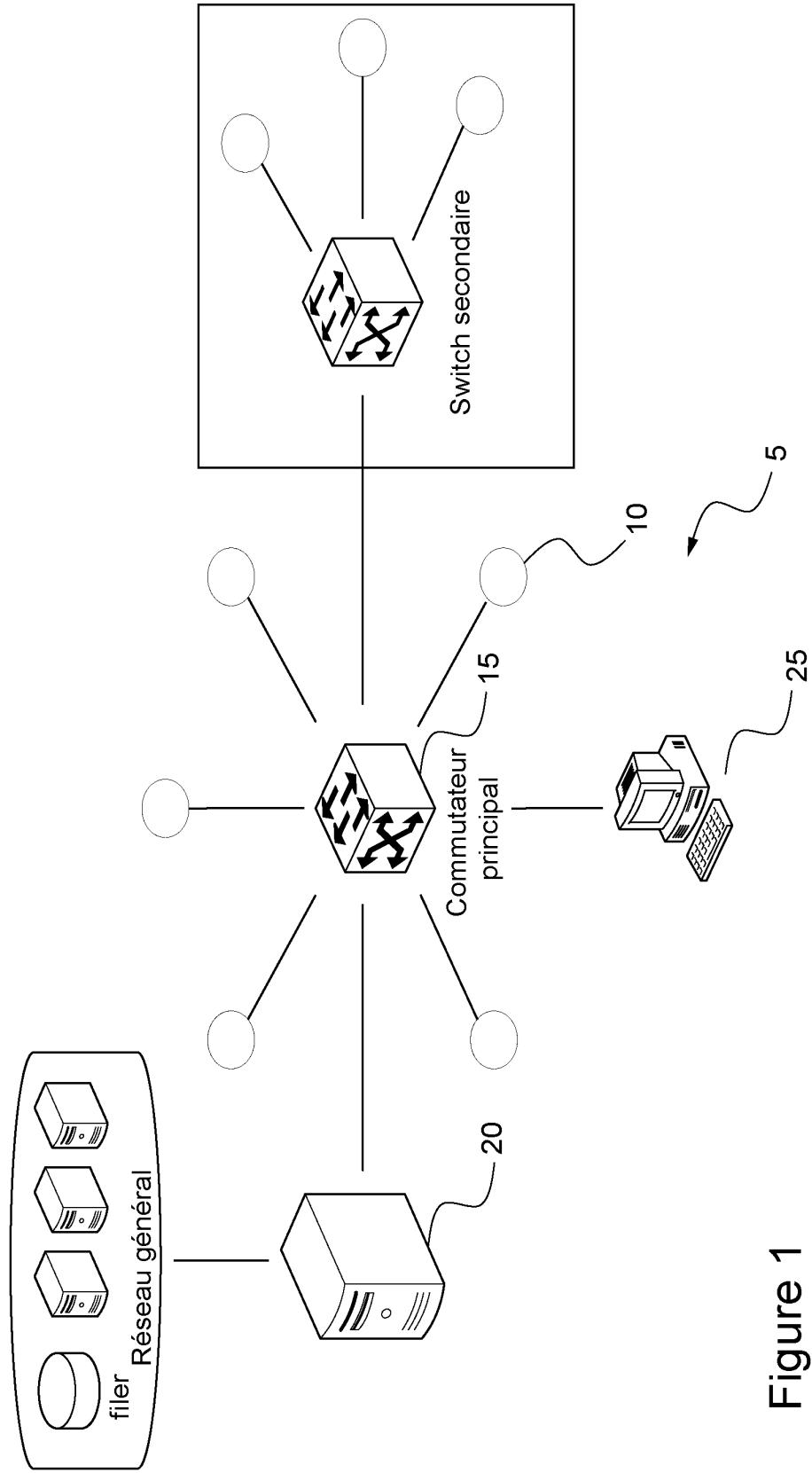


Figure 1

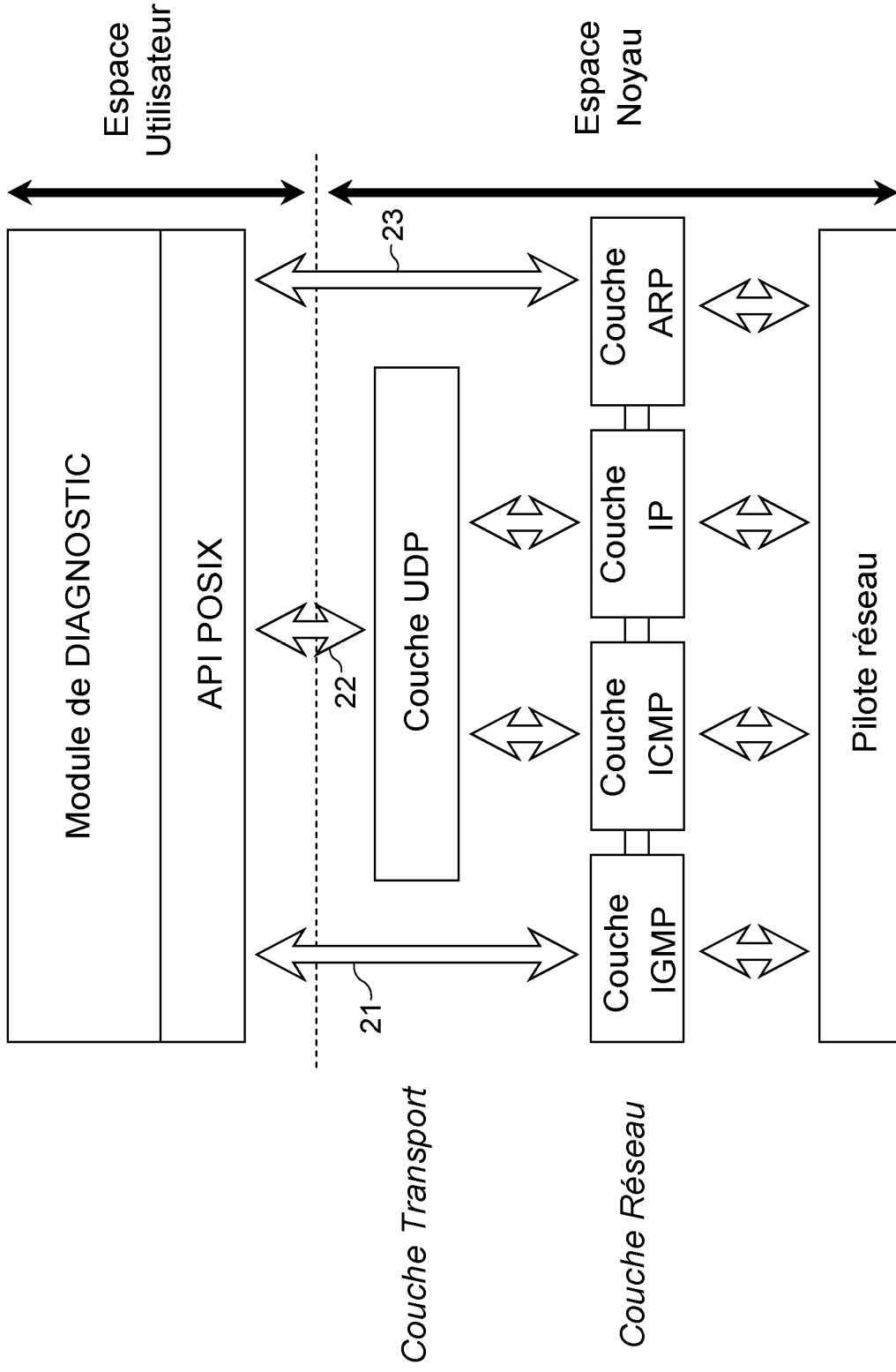


Figure 2



**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

N° d'enregistrement
national

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

FA 697143
FR 0756129

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		
X	NARTEN T ET AL: "Neighbor Discovery for IP version 6 (IPv6); draft-ietf-ipv6-2461bis-11.t" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, vol. ipv6, no. 11, mars 2007 (2007-03), XP015049437 ISSN: 0000-0004 * page 55, alinéa 7.2 - page 60, dernière ligne * * page 65, alinéa 7.3.3 * -----	1-10	H04L12/56 G06F11/30
X	MARCEL WIGET SIMON BRYDEN GEOFF MATTSON NORTEL NETWORKS: "Dynamic VPLS solution over multicast enabled IP backbone; draft-wiget-dynamic-vpls-00.txt;" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, décembre 1999 (1999-12), XP015036853 ISSN: 0000-0004 * page 9, alinéa 2.1. - alinéa 2.2. * * page 11, alinéa 3.1 * * page 13, alinéa 3.3. - page 15, alinéa 3.3.2. * -----	1-10	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04L
X	JP 08 237285 A (MITSUBISHI ELECTRIC CORP) 13 septembre 1996 (1996-09-13) * abrégé * ----- -/--	1-10	
Date d'achèvement de la recherche		Examineur	
18 mars 2008		Lebas, Yves	
<p>CATÉGORIE DES DOCUMENTS CITÉS</p> <p>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</p>		<p>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</p>	

EPO FORM 1503 12.99 (P04C14) 2



**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

N° d'enregistrement national

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

FA 697143
FR 0756129

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	<p>DAVID C PLUMMER (DCP@MIT-MC): "An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware; rfc826.txt"</p> <p>IETF STANDARD, INTERNET ENGINEERING TASK FORCE, IETF, CH, novembre 1982 (1982-11), XP015006811</p> <p>ISSN: 0000-0003</p> <p>* le document en entier *</p> <p style="text-align: center;">-----</p>	1-10	<p>DOMAINES TECHNIQUES RECHERCHÉS (IPC)</p>
Date d'achèvement de la recherche		Examineur	
18 mars 2008		Lebas, Yves	
<p>CATÉGORIE DES DOCUMENTS CITÉS</p> <p>X : particulièrement pertinent à lui seul</p> <p>Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie</p> <p>A : arrière-plan technologique</p> <p>O : divulgation non-écrite</p> <p>P : document intercalaire</p>		<p>T : théorie ou principe à la base de l'invention</p> <p>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.</p> <p>D : cité dans la demande</p> <p>L : cité pour d'autres raisons</p> <p>.....</p> <p>& : membre de la même famille, document correspondant</p>	

EPO FORM 1503 12.99 (P04C14) 2

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0756129 FA 697143**

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 **18-03-2008**

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
JP 8237285	A	13-09-1996	AUCUN
