

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

(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international



PCT



(43) Date de la publication internationale  
20 avril 2006 (20.04.2006)

(10) Numéro de publication internationale  
**WO 2006/040431 A1**

(51) Classification internationale des brevets :  
**H04L 12/56** (2006.01) **H04L 29/06** (2006.01)

(21) Numéro de la demande internationale :  
PCT/FR2005/002406

(22) Date de dépôt international :  
28 septembre 2005 (28.09.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :  
0410675 8 octobre 2004 (08.10.2004) FR

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

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : **VU DUONG, Thang** [VN/FR]; 54, résidence Duroux, F-22300 Lannion (FR). **FROMYTOUX, Gaël** [FR/FR]; 1, rue des Dunes, F-22560 Pleumeur Bodou (FR). **LE ROUX, Jean-Louis** [FR/FR]; 1, rue Paul Le Flem, F-22300 Lannion (FR).

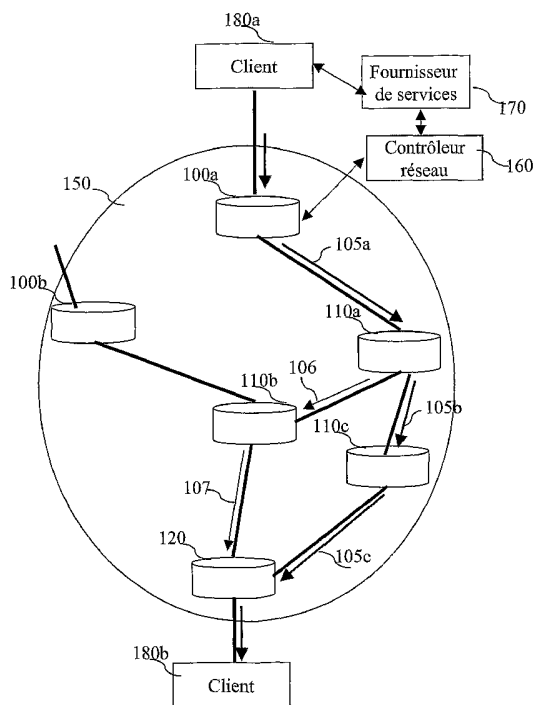
(74) Mandataire : **MAILLET, Alain**; Cabinet Le Guen Maillet, 5, place Newquay, B.P. 70250, F-35802 Dinard Cedex (FR).

(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,

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR CONTROLLING ADMISSION TO A GUARANTEED QUALITY OF SERVICE IN A MPLS NETWORK

(54) Titre : PROCÉDE ET DISPOSITIF DE CONTROLE D'ADMISSION A UN SERVICE A QUALITE DE SERVICE GARANTIE DANS UN RESEAU MPLS



180A CLIENT  
180B CLIENT  
170 SERVICE PROVIDER  
160 NETWORK CONTROLLER

(57) Abstract: The invention concerns a method and a device for controlling admission to a guaranteed quality of service in a MPLS network (150), the MPLS network consisting of at least one input peripheral router (100) and one output peripheral router (120), the data flows being transported in the MPLS network through tunnels. The invention is characterized in that the input peripheral router receives request from a client (180a) for setting up a guaranteed quality of service in the MPLS network, obtains traffic engineering parameters corresponding to the service requested by the client, determines whether the creation of a tunnel for transporting the data flow(s) related to the guaranteed quality of service between the input peripheral router and the output peripheral router is possible in the MPLS network and transfers to the client a message of denial of the request of the client for setting up a guaranteed quality of service in the MPLS network if it is not possible to create a tunnel for carrying the data flow(s) related to the guaranteed quality of service between the input peripheral router and the output peripheral router in the network.

(57) Abrégé : L'invention concerne un procédé et un dispositif de contrôle d'admission à un service à qualité de service garantie dans un réseau MPLS (150), le réseau MPLS étant constitué d'au moins un routeur périphérique d'entrée (100) et un routeur périphérique de sortie (120), les flux de données étant véhiculés dans le réseau MPLS par des tunnels. Selon l'invention, le routeur périphérique d'entrée reçoit une requête d'un client (180a) pour l'établissement d'un service à qualité de service garantie dans le réseau MPLS, obtient des paramètres d'ingénierie de trafic correspondant au service demandé

[Suite sur la page suivante]

WO 2006/040431 A1



GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, 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, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, 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 :**

- avec rapport de recherche internationale
- avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues

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

---

par le client, détermine si la création d'un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie est possible dans le réseau MPLS et transfère au client un message de rejet de la requête du client pour un établissement d'un service à qualité de service garantie dans le réseau MPLS s'il n'est pas possible de créer un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie dans le réseau.

Procédé et dispositif de contrôle d'admission à un service à qualité de service  
garantie dans un réseau MPLS

La présente invention concerne un procédé et un dispositif de contrôle d'admission à un service à qualité de service garantie dans un réseau de télécommunication.

5 Plus précisément, la présente invention concerne une méthode de contrôle d'admission distribuée à un service à qualité de service garantie dans un réseau de télécommunication à permutation d'étiquettes MPLS, acronyme de Multi Protocol Label Switching.

10 La norme MPLS, publiée sous les auspices de l'IETF (Internet Engineering Task Force) est une technique basée sur la permutation d'étiquettes (label switching) permettant de créer un réseau orienté connexion à partir d'un réseau de type datagramme comme le réseau IP. On trouvera une documentation détaillée du protocole MPLS sous le site [www.ietf.org](http://www.ietf.org).

15 On a représenté de manière schématique en Fig. 1 un réseau MPLS 150, comprenant une pluralité de routeurs dénommés LSR (Label Switching Routers) tels

que 100a, 100b, 110a, 110b, 110c et 120 reliés entre eux par des liens IP. Lorsqu'un paquet IP arrive sur un routeur périphérique d'entrée 100a ou 100b, dénommé Ingress LSR, ce dernier lui attribue une étiquette en fonction de son entête IP et la concatène audit paquet. Le routeur qui reçoit le paquet étiqueté remplace l'étiquette (entrante) par une étiquette sortante en fonction de sa table d'acheminement et le processus se répète de routeur en routeur jusqu'au routeur périphérique de sortie 120 (encore dénommé Egress LSR) qui supprime l'étiquette avant de transmettre le paquet. Alternativement, la suppression d'étiquette peut être déjà effectuée par le pénultième routeur puisque le routeur de sortie 120 n'utilise pas l'étiquette entrante. Un routeur LSR utilise l'étiquette du paquet entrant (étiquette entrante) pour déterminer le port de sortie et l'étiquette du paquet sortant (étiquette sortante). Le chemin parcouru par un paquet à travers le réseau du routeur d'entrée 100a jusqu'au routeur de sortie 120 est appelé chemin à étiquettes commutées ou LSP (Label Switched Path). Selon l'exemple de la Fig. 1 dans lequel un chemin est représenté par les flèches 105a, 105b et 105c, les routeurs LSR 110a, 110c traversés par le chemin et distincts des routeurs périphériques d'entrée 100a et de sortie 120 sont appelés routeurs de transit. D'autre part, on appelle classe d'équivalence ou FEC (Forward Equivalence Class) l'ensemble des paquets IP qui sont transmis le long d'un même chemin.

Le protocole MPLS permet de forcer les paquets IP à suivre un chemin LSP préétabli qui n'est en général pas le chemin IP optimal en terme de nombre de bonds ou de métrique de chemin. La technique de détermination du chemin ou des chemins à emprunter est appelée ingénierie de trafic ou MPLS-TE (pour MPLS Traffic Engineering). La détermination du chemin prend en compte des contraintes sur les ressources disponibles (constraint based routing), notamment en bande passante sur les différents liens du réseau. Au contraire du routage IGP classique opérant selon un mode bond par bond (hop-by-hop routing), la détermination d'un chemin LSP est effectué selon un mode dit explicite (explicitly routed LSP ou ER-LSP) dans lequel on détermine certains ou tous les noeuds du chemin du routeur d'entrée jusqu'au routeur de sortie. Lorsque tous les noeuds du chemin sont fixés, on parle de routage explicite au sens strict. Un chemin déterminé selon un mode explicite est encore appelé tunnel MPLS.

Le choix d'un ou des tunnels MPLS peut se faire de manière centralisée ou distribuée. Selon la méthode distribuée basée sur la technique appelée Constraint based Routing, chaque routeur est renseigné sur la topologie du réseau et les

contraintes affectant les différents liens du réseau. Pour ce faire, chaque routeur détermine et transmet à ses voisins un message indiquant ses liens immédiats et les contraintes (ou attributs) qui y sont associées. Ces messages sont ensuite propagés de noeud en noeud par des messages IGP étendus, selon un mécanisme d'inondation (flooding) jusqu'à ce que tous les routeurs soient renseignés. Ainsi, chaque routeur dispose en propre d'une base de données (dite TED pour Traffic Engineering Database) lui donnant la topologie du réseau et ses contraintes.

La détermination du chemin à commutation d'étiquettes est ensuite effectuée par le routeur périphérique d'entrée en prenant également en compte d'autres contraintes fixées par l'opérateur du réseau (par exemple éviter tel ou tel noeud ou éviter les liens de tel ou tel type). Le routeur périphérique d'entrée détermine alors, par exemple au moyen de l'algorithme de Dijkstra, le chemin le plus court satisfaisant à l'ensemble des contraintes (Constraint Shortest Path First ou CSPF), celles affectant les liens comme celles fixées par l'opérateur. Ce chemin le plus court est ensuite signalé aux routeurs du chemin LSP au moyen des protocoles de signalisation connus sous les abréviations RSVP-TE (Resource reSerVation Protocol for Traffic Engineering) ou bien CR-LDP (Constrained Route Label Distribution Protocol). On trouvera une description du protocole RSVP-TE dans le document de D. Adwuche et al. intitulé « RSVP-TE : extensions to RSVP for LSP tunnels » disponible sous le site de l'IETF précité.

Ces protocoles de signalisation MPLS permettent la distribution des étiquettes le long du chemin et la réservation des ressources.

Par exemple, si l'on utilise le protocole de signalisation RSVP, le routeur d'entrée 100a transmet un message Path dans un paquet IP au routeur de sortie 120. Ce message spécifie la liste des noeuds 110a, 110c par lesquels le chemin LSP doit passer. A chaque noeud le message Path établit le chemin et fait une réservation d'état. Lorsque le message Path atteint le routeur de sortie 120, un message d'acquiescement Resv est renvoyé par le même chemin au routeur d'entrée 100a.

A chaque noeud, la table de routage MPLS est actualisée et la réservation de ressource est effectuée. Par exemple, si la ressource est une bande passante et que l'on souhaite réserver est de 10 Mbits pour le chemin, les bandes passantes respectivement affectées à chaque lien sont décrémentées de la valeur réservée de 10 Mbits lors de la rétro propagation du message d'acquiescement/réservation. Il convient de noter que la ressource en question (par exemple la bande passante) est une

ressource logique sur le lien IP et non une ressource physique. Lorsque le message d'acquittement est reçu par le routeur d'entrée, le tunnel est établi.

Comme on l'a indiqué plus haut, la détermination des chemins LSP peut être réalisée de manière centralisée. Dans ce cas, un serveur a connaissance de la topologie  
5 du réseau et prend en compte les contraintes sur les liens et les contraintes fixées par l'opérateur du réseau pour déterminer des tunnels entre les routeurs d'entrée et les routeurs de sortie. Les routeurs périphériques d'entrée sont ensuite avertis par le serveur du ou des tunnels pour lesquels ils sont le noeud d'entrée. Les tunnels sont alors établis comme indiqué précédemment.

10 La recommandation de l'IETF RFC 2475 intitulée « An architecture for Differentiated Services » propose une méthode dans laquelle des priorités sont allouées selon des classes aux flux de données IP dans le réseau MPLS 150. Ces classes sont définies à partir des champs DSCP des paquets IP transférés dans le réseau MPLS. DSCP est l'acronyme de « DiffServ Code Point ». Cette méthode  
15 garantit que les flux de données prioritaires seront traités préférentiellement aux flux de données moins prioritaires mais elle ne garantit aucune qualité de service, par exemple en terme de réservation de bande passante, pour les flux de données qui transitent dans le réseau de télécommunication MPLS.

La recommandation de l'IETF RFC 3270 intitulée « MPLS support for  
20 differentiated services » propose une méthode dans laquelle des priorités sont allouées à la fois aux trames de données MPLS et aux paquets IP sans prendre en compte les contraintes de chaque classe pour leur routage. Cette méthode est ainsi basée sur un routage agrégé des différentes classes de services dans chaque routeur LSP du réseau MPLS et ne permet pas de garantir une qualité de service pour chaque classe de  
25 service et chaque flux d'informations.

La recommandation de l'IETF RFC 3564 intitulée « Requirements for support of Differentiated Services-aware MPLS Traffic Engineering » propose quant à elle une méthode dans laquelle le routage des flux d'informations est effectué en considérant les contraintes liées à chaque classe de service et permet ainsi de garantir  
30 une certaine qualité de service dans le réseau MPLS.

Ces techniques ne proposent pas une méthode de contrôle d'admission à un service à qualité de service garantie dans un réseau de télécommunication à permutation d'étiquettes. Lorsqu'un nombre important de clients accède à des services à qualité de service garantie dans un réseau de télécommunication à permutation

d'étiquettes, les flux transférés lorsque ces services sont établis sont parfois si importants qu'il n'est plus possible pour le réseau de télécommunication à permutation d'étiquettes d'assurer un transport de ceux-ci en respectant une qualité de service, pénalisant ainsi au moins une partie des clients utilisant ces services.

5 Certains réseaux de télécommunication de taille relativement réduite utilisent des systèmes de contrôle d'admission à un service à qualité de service garantie centralisés. De tels systèmes ne sont pas adaptés au réseau de télécommunication à permutation d'étiquettes de grande taille.

L'invention a pour but de résoudre les inconvénients de l'art antérieur en  
10 proposant un procédé et un dispositif de contrôle d'admission distribué à un service à qualité de service garantie dans un réseau de télécommunication à permutation d'étiquettes MPLS de grande taille.

A cette fin, selon un premier aspect, l'invention propose un procédé de contrôle  
15 d'admission à un service à qualité de service garantie dans un réseau de télécommunication à permutation d'étiquettes, le réseau de télécommunication à permutation d'étiquettes étant constitué d'au moins un routeur périphérique d'entrée et un routeur périphérique de sortie, les flux de données étant véhiculés dans le réseau de télécommunication à permutation d'étiquettes dans des tunnels.

Conformément à l'invention, ce procédé comporte les étapes  
20 suivantes effectuées par le routeur périphérique d'entrée de :

- réception d'une requête d'un client pour l'établissement d'un service à qualité de service garantie dans le réseau de télécommunication,
- obtention de paramètres d'ingénierie de trafic correspondant au service demandé par le client,
- 25 - détermination si la création d'un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie est possible dans le réseau de télécommunication à permutation d'étiquettes,
- transfert au client d'un message de rejet de la requête du client pour un  
30 établissement d'un service à qualité de service garantie dans le réseau de télécommunication s'il n'est pas possible de créer un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie dans le réseau de télécommunication à permutation d'étiquettes.

Corrélativement, l'invention concerne un dispositif de contrôle d'admission à un service à qualité de service garantie dans un réseau de télécommunication à permutation d'étiquettes, le réseau de télécommunication à permutation d'étiquettes étant constitué d'au moins un routeur périphérique d'entrée et un routeur périphérique de sortie, les flux de données étant véhiculés dans le réseau de télécommunication à permutation d'étiquettes dans des tunnels.

Conformément à l'invention, ce dispositif de contrôle d'admission est compris dans le routeur périphérique d'entrée et comporte :

- des moyens de réception d'une requête d'un client pour l'établissement d'un service à qualité de service garantie dans le réseau de télécommunication,
- des moyens d'obtention de paramètres d'ingénierie de trafic correspondant au service demandé par le client et de règles applicables pour la mise à la disposition des ressources du réseau de télécommunication à permutation d'étiquettes,
- des moyens de détermination si la création d'un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie est possible dans le réseau de télécommunication à permutation d'étiquettes,
- des moyens de rejet de la requête du client pour un établissement d'un service à qualité de service garantie dans le réseau de télécommunication s'il n'est pas possible de créer un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie dans le réseau de télécommunication à permutation d'étiquettes.

Ainsi, en contrôlant l'admission à un service à qualité de service garantie dans un réseau de télécommunication à commutation d'étiquettes, il est possible d'éviter que le réseau de télécommunication à commutation d'étiquettes soit congestionné. De plus, en confiant à chaque routeur périphérique d'entrée du réseau de télécommunication à commutation d'étiquettes la tâche de contrôle d'admission, les problèmes liés aux systèmes centralisés sont résolus de manière simple.

Selon un autre aspect de l'invention, si la création d'un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie est possible dans le réseau de télécommunication à permutation d'étiquettes, on transfère au client un message d'acceptation de la requête du client pour un établissement d'un service à qualité de service garantie dans le réseau de télécommunication.

Ainsi, il est possible de garantir à chaque client souhaitant accéder à un service à qualité de service garantie dans le réseau de télécommunication que la qualité de service sera maintenue tout au long de la session de communication. En effet, aucune congestion du réseau de télécommunication n'est susceptible d'apparaître, les requêtes d'établissement étant rejetées lorsque les ressources du réseau de télécommunication deviennent limitées.

Selon un autre aspect de l'invention, préalablement à la détermination si la création d'un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie est possible dans le réseau de télécommunication à permutation d'étiquettes, on détermine si un tunnel du réseau de télécommunication à permutation d'étiquettes est apte à véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie.

Ainsi, on évite qu'un nombre trop important de tunnels soit créé dans le réseau de télécommunication à permutation d'étiquettes. L'utilisation des tunnels existants dans le réseau de télécommunication est ainsi optimisée, de même que les ressources du réseau de télécommunication.

Selon un autre aspect de l'invention, lors de l'obtention de paramètres d'ingénierie de trafic correspondant au service demandé par le client, on obtient en outre des règles applicables au client pour la mise à la disposition des ressources du réseau de télécommunication à permutation d'étiquettes.

Ainsi, il est possible de contrôler les ressources du réseau mises à la disposition d'un client.

Selon un autre aspect de l'invention, préalablement à l'obtention de paramètres d'ingénierie de trafic correspondant au service demandé par le client et de règles applicables au client pour la mise à la disposition des ressources du réseau de télécommunication à permutation d'étiquettes, on vérifie, par l'intermédiaire d'un contrôleur de réseau, si le client ayant émis la requête est habilité à accéder au service à qualité de service garantie.

Ainsi, il est possible de restreindre l'accès aux services proposés par le réseau de télécommunication.

Selon un autre aspect de l'invention, les paramètres d'ingénierie correspondant au service demandé par le client comprennent au moins un des éléments du groupe

contenant le débit alloué pour un service, le délai de traitement, la classe de service d'ingénierie de trafic et le fait que le service soit uni ou bidirectionnel.

Selon un autre aspect de l'invention, les règles applicables au client comprennent au moins un des éléments du groupe contenant le débit maximal autorisé pour l'ensemble des services demandés par le client et le nombre maximal de sessions autorisées pour le client.

Selon un autre aspect de l'invention, on met à jour une base de données référençant l'ensemble des accès par les clients reliés au routeur périphérique d'entrée aux services à qualité de service garantie dans le réseau de télécommunication.

L'invention concerne aussi le programme d'ordinateur stocké sur un support d'informations, ledit programme comportant des instructions permettant de mettre en œuvre le procédé précédemment décrit, lorsqu'il est chargé et exécuté par un système informatique.

Les caractéristiques de l'invention mentionnées ci-dessus, ainsi que d'autres, apparaîtront plus clairement à la lecture de la description suivante d'un exemple de réalisation, ladite description étant faite en relation avec les dessins joints, parmi lesquels :

la Fig. 1 représente un réseau de télécommunication utilisant le protocole MPLS dans lequel la présente invention est implémentée ;

la Fig. 2 représente une représentation fonctionnelle du routeur périphérique d'entrée selon la présente invention ;

la Fig. 3 représente l'algorithme exécuté par le routeur périphérique d'entrée selon la présente invention.

La Fig. 1 représente un réseau de télécommunication utilisant le protocole MPLS dans lequel la présente invention est implémentée.

Le réseau MPLS 150 est accessible à des dispositifs clients 180, appelés par la suite clients 180 pour transmettre et/ou recevoir des informations. Selon l'exemple de la Fig. 1, seulement deux clients 180a et 180b sont reliés au réseau MPLS 150. Bien entendu un nombre plus important de clients 180 accède au réseau MPLS 150.

Les clients 180a et 180b sont reliés au réseau MPLS 150 par l'intermédiaire d'un réseau de type Internet classique non représenté en Fig. 1 ou par un lien direct apte à assurer le transport de paquets IP avec le réseau MPLS 150.

Pour accéder au service de fourniture de service à qualité de service garantie, un client, par exemple le client 180a, doit souscrire auprès d'un fournisseur de services 170 un tel service. Le fournisseur de services 170 est par exemple et de manière non limitative, un fournisseur de services 170 offrant la possibilité au client 180a  
5 d'accéder au réseau Internet avec une garantie de bande passante et/ou d'établir entre au moins deux clients des sessions de conférences dans lesquelles une certaine qualité de service est garantie.

Lorsque le client 180a abonné à de tels services désire qu'une session de communication soit établie, celui-ci génère une requête d'établissement de session au  
10 routeur périphérique d'entrée 100a auquel il est associé. La requête d'établissement de session comprend entre autres un identifiant du client 180a ainsi que l'identifiant du service demandé, voire un mot de passe ou un identifiant du correspondant avec lequel le client 180a souhaite que le service soit établi.

Le routeur périphérique d'entrée 100a transfère selon l'invention la requête  
15 d'accès à un contrôleur de réseau 160 inclus ou non dans le réseau MPLS 150. Le contrôleur de réseau 160 est apte à traiter les différentes requêtes transférées par les routeurs périphériques d'entrée 100a et 100b du réseau MPLS 150. Le contrôleur de réseau 160 mémorise les différents paramètres d'ingénierie de trafic correspondant à chacun des services accessibles par les clients 180 ainsi que les règles applicables  
20 pour la mise à la disposition des ressources du réseau MPLS 150. Les paramètres d'ingénierie sont par exemple et de manière non limitative, le débit alloué pour un service, le délai de traitement et la classe de service d'ingénierie de trafic, le fait que le service soit uni ou bidirectionnel. Le contrôleur de réseau 160 est apte à interroger le fournisseur de services 170 du client 180a de manière à vérifier si le client 180a est  
25 habilité à utiliser un tel service. Le contrôleur de réseau 160 communique au fournisseur de services 170 dont l'identifiant est compris dans la requête du client 180a, l'identifiant du client 180a ainsi que l'identifiant du service demandé. Le fournisseur de services 170, selon l'abonnement du client 180a, autorise ou non l'accès à un tel service. Le contrôleur de réseau 160 transfère au routeur périphérique  
30 d'entrée 100a les différents paramètres d'ingénierie de trafic correspondant au service accessible par le client 180a ainsi que les règles applicables pour la mise à la disposition des ressources du réseau MPLS 150 lorsque le client 180a est autorisé à accéder au service ou à transférer au routeur périphérique d'entrée 100a un message représentatif du rejet, par le fournisseur d'accès 170, de la demande d'accès au

service. Le routeur périphérique d'entrée 100a est apte à allouer un tunnel dans le réseau MPLS 150 pour l'établissement de la session demandée. Le tunnel alloué est un tunnel existant ou un tunnel créé pour la session demandée.

Le routeur périphérique d'entrée 100a est apte à autoriser l'accès ou non au  
5 réseau MPLS 150 en fonction des ressources disponibles du réseau MPLS 150 ainsi que des paramètres d'ingénierie du service fournis par le contrôleur de réseau 160.

Le routeur périphérique d'entrée 100a est apte à autoriser l'accès ou non au réseau MPLS 150 en fonction des ressources du réseau MPLS déjà allouées au client 180a.

10 La **Fig. 2** représente une représentation fonctionnelle du routeur périphérique d'entrée selon la présente invention.

Un routeur périphérique d'entrée 100 comprend selon l'invention un module d'interface client 101. Le module d'interface client 101 assure l'émission de messages vers le client 180a et/ou la réception des messages émis par le client 180a  
15 lorsque celui-ci souhaite accéder à un service à qualité de service garantie. Le module d'interface client 101 reçoit du client 180a une requête pour accéder à un service à qualité de service garantie. Cette requête comprend entre autres, un identifiant du service demandé, un identifiant du client 180a, l'adresse IP de destination avec laquelle le client 180a souhaite que le service à qualité de service  
20 garantie soit établi, voire un mot de passe permettant d'authentifier le client 180a au service demandé. Le module d'interface client 101 est apte à transférer le contenu de cette requête vers le module de contrôle d'admission 102 du routeur périphérique d'entrée 100. Le module d'interface client 101 est apte à transférer vers le client 180a des messages représentatifs de l'acceptation ou du rejet de l'accès au service à qualité  
25 de service garantie.

Le module de contrôle d'admission 102 est apte à traiter une requête effectuée par un client 180a pour l'accès à un service à qualité de service garantie. Pour cela, le module de contrôle d'admission 102 commande la génération d'une requête à destination du contrôleur réseau 160 pour accéder au service demandé. Cette requête  
30 est transmise par l'intermédiaire de l'interface contrôleur 103 et comprend l'identifiant du service demandé, l'identifiant du client 180, l'adresse IP de destination avec laquelle le client 180 souhaite que le service à qualité de service garantie soit établi, l'adresse IP du routeur périphérique d'entrée 100a, voire un mot de passe permettant d'authentifier le client 180 au service demandé.

Le module de contrôle d'admission 102 obtient les règles de traitement à observer pour le service demandé. Ces règles de traitement sont obtenues de la base de traitement de flux 105 du routeur périphérique d'entrée 100 ou du contrôleur réseau 160. Préférentiellement, le module de contrôle d'admission 102 obtient les règles de traitement de la base de traitement de flux 105. Sous certaines conditions, par exemple lorsque la base de traitement de flux 105 ne comprend pas les règles de traitement relatives à un service demandé par un client ou lorsque les règles de traitement relatives à un service demandé par un client sont comprises depuis un temps prédéterminé dans la base de traitement de flux 105, le module de contrôle d'admission 102 obtient les règles de traitement du contrôleur réseau 160. Le module de contrôle d'admission 102 est apte à mettre à jour la base de traitement de flux 105 avec les données transmises par le contrôleur réseau 160.

Le module de contrôle d'admission 102 est apte à commander la génération d'un message de rejet d'accès au service demandé par le client 180 si le contrôleur 160 du réseau MPLS a répondu à la requête de manière négative.

Lorsque les règles de traitement à observer pour le service demandé ont été obtenues, le module de contrôle d'admission 102 est apte à commander à l'agent tunnel 107 du routeur périphérique d'entrée 100, l'établissement d'une connexion qui soit apte à supporter le service demandé par le client 180. L'agent tunnel 107 sélectionne un tunnel existant entre les routeurs périphériques d'entrée et de sortie ou crée, à partir des règles de traitement comprenant les paramètres d'ingénierie de trafic liés au service demandé, une nouvelle connexion entre les routeurs périphériques d'entrée et de sortie.

L'agent tunnel 107 dialogue avec le routeur périphérique de sortie 120 auquel est rattachée l'adresse IP de destination avec laquelle le client 180 souhaite que le service de transfert de flux de données selon une qualité service garantie soit établi.

Le routeur périphérique de sortie 120 est déterminé par exemple à partir de l'adresse IP de destination avec laquelle le client 180 souhaite que le service à qualité de service garantie soit établi. L'agent tunnel 107 transfère au routeur périphérique de sortie 120 l'identifiant du tunnel utilisé pour le service dans le sens routeur périphérique d'entrée vers routeur périphérique de sortie et devant être utilisé par le routeur périphérique de sortie dans le sens routeur périphérique de sortie vers routeur périphérique d'entrée. Ce transfert est assuré par l'intermédiaire du module de contrôle d'admission 102 et du module de signalisation 104.

L'agent tunnel 107 détermine le chemin le plus court satisfaisant à l'ensemble des contraintes. Ce chemin le plus court est ensuite signalé aux routeurs du chemin LSP au moyen des protocoles de signalisation connus sous les abréviations RSVP-TE ou CR-LDP.

5 Le routeur périphérique d'entrée comporte aussi une base de données de sessions de clients 106. La base de données de sessions de clients 106, accessible par le module de contrôle d'admission 102, mémorise les informations liées à chacune des sessions de services qui transitent par le routeur périphérique d'entrée 100. Pour  
10 chacune des sessions en cours, les paramètres d'ingénierie de trafic alloué à la session sont mémorisés dans la base de données de sessions de clients 106. La base de données de sessions de clients 106 est mise à jour par le module de contrôle d'admission 102 lorsque des sessions sont établies ou arrêtées.

La **Fig. 3** représente l'algorithme exécuté par le routeur périphérique d'entrée selon la présente invention.

15 L'algorithme de la Fig. 3 est exécuté par chaque routeur périphérique d'entrée 100 du réseau MPLS 150.

A l'étape E300, une requête pour accéder à un service à qualité de service garantie est détectée par l'intermédiaire de l'interface client 101 de la Fig. 2. Cette requête comprend entre autres l'identifiant du client 180a ainsi que l'identifiant du  
20 service demandé, voire un mot de passe.

A l'étape suivante E301, il est vérifié si le client ayant émis la requête est habilité à accéder au service à qualité de service garantie. Pour cela, le routeur périphérique d'entrée 100a, auquel est relié le client 180a ayant émis la requête, transfère la requête d'accès au contrôleur de réseau 160. Le contrôleur de réseau 160  
25 interroge le fournisseur du service 170 qui, en retour autorise ou non le client 180a à accéder au service à qualité de service garantie.

A l'étape suivante E302, le routeur périphérique d'entrée 100 vérifie si le client est autorisé ou non à accéder. Dans la négative, à l'étape E303, un message de rejet est transmis par l'intermédiaire de l'interface client 101 au client 180 ayant émis la  
30 requête. Dans l'affirmative, l'algorithme passe à l'étape suivante E304.

A l'étape E304 les différents paramètres d'ingénierie de trafic correspondant au service demandé par le client 180a ainsi que les règles applicables pour la mise à la disposition des ressources du réseau MPLS 150 sont obtenus. Les paramètres et règles sont obtenus de la base des règles de traitement 105 et/ou du contrôleur réseau

160. Nous rappelons ici que les paramètres d'ingénierie sont par exemple et de manière non limitative le débit alloué pour un service, le délai de traitement et la classe de service d'ingénierie de trafic, le fait que le service soit uni ou bi directionnel. Les règles applicables sont par exemple et de manière non limitative le  
5 débit maximal autorisé pour l'ensemble des services demandé par le client 180a et/ou le nombre maximal de sessions autorisées pour le client 180a. Les règles et paramètres obtenus, l'algorithme passe à l'étape suivante E305 qui consiste à transférer ceux-ci au module agent tunnel 107. En outre, la classe du service demandé par le client 180 prise au sens de la recommandation DiffServ, les adresses  
10 IP du client 180 et de son correspondant sont aussi transférées au module agent tunnel 107.

L'étape suivante E306 consiste à rechercher si un tunnel du réseau MPLS 150 est apte à supporter le service demandé. Pour cela, le module agent tunnel 107 consulte une table de tunnels comprenant entre autres la source et la destination de  
15 chaque tunnel ainsi que la bande passante disponible de chaque tunnel, le délai de traitement, la classe de service d'ingénierie de trafic, le fait que le service soit uni ou bidirectionnel. Il est à remarquer ici que les tunnels du réseau MPLS 150 peuvent être créés de manière centralisée ou par chaque routeur périphérique d'entrée 100 du réseau MPLS 150. Ces tunnels peuvent être créés à partir des prévisions moyennes  
20 de trafic et de statistiques de trafic. Ces tunnels ou au moins une partie de ces tunnels peuvent aussi être créés de manière dynamique en fonction des besoins ponctuels des clients 180 du réseau MPLS 150.

A l'étape suivante E307, il est vérifié s'il existe un tunnel adapté aux besoins du service demandé. Dans l'affirmative, le processeur passe à l'étape E311 qui sera  
25 décrite ultérieurement. Dans la négative, l'algorithme passe à l'étape E308.

L'étape suivante E308 consiste à rechercher un nouveau tunnel dans le réseau MPLS 150. Pour cela, il est déterminé la plus grande bande passante disponible dans le réseau MPLS 150 entre le routeur périphérique d'entrée 100 et le routeur  
30 périphérique de sortie 120 auquel est relié le correspondant du client 180 ayant émis la requête. Par exemple, il peut être déterminé que le chemin entre le routeur périphérique d'entrée 100 et le routeur périphérique de sortie 120 marqué par les flèches 105a, 106 et 107 de la Fig. 1 soit le chemin qui a la plus grande bande passante. Il est ensuite vérifié si cette bande passante est supérieure **ou égale** à la bande passante requise pour le service demandé.

Cette opération effectuée, l'algorithme passe à l'étape suivante E309. L'étape E309 consiste à déterminer si un nouveau tunnel peut être créé dans le réseau MPLS 150. Il est vérifié que la plus grande bande passante disponible dans le réseau MPLS 150 entre le routeur périphérique d'entrée 100 et le routeur périphérique de sortie 120 est supérieure à la bande passante requise pour le service demandé. Dans l'affirmative, un nouveau tunnel est créé par le routeur périphérique d'entrée 100 et l'algorithme passe à l'étape E311. Dans la négative, l'algorithme passe à l'étape E310 qui consiste à générer un message à destination du client 180 ayant émis la requête indiquant que le réseau MPLS 150 est saturé et qu'il n'est pas possible de satisfaire à la requête d'établissement de service. Le message transféré, le présent algorithme prend fin et attend une nouvelle requête d'un client 100 à l'étape E300.

Si le test de l'étape E307 ou de l'étape E309 est positif, l'algorithme passe à l'étape E311. A cette étape, la base de données de session clients 106 est mise à jour en insérant dans celle-ci le nouveau flux de données.

A l'étape suivante E312, un message d'acceptation de la requête du client pour un établissement d'un service à qualité de service garantie dans le réseau de télécommunication est transféré au client 180.

L'étape suivante E313 est une boucle d'attente de la fin de la session nouvellement établie. Lorsque la session est interrompue, l'algorithme passe à l'étape suivante E314 et met à jour la base de données de session clients 106 en supprimant dans celle-ci le flux de données. La base de données de session clients 106 mise à jour, le présent algorithme prend fin et attend une nouvelle requête d'un client 100 à l'étape E300.

Bien entendu, la présente invention n'est nullement limitée aux modes de réalisation décrits ici, mais englobe, bien au contraire, toute variante à la portée de l'homme du métier.

## REVENDICATIONS

1) Procédé de contrôle d'admission à un service à qualité de service garantie dans un réseau de télécommunication à permutation d'étiquettes, le réseau de télécommunication à permutation d'étiquettes étant constitué d'au moins un routeur périphérique d'entrée et un routeur périphérique de sortie, les flux de données étant véhiculés dans le réseau de télécommunication à permutation d'étiquettes par des tunnels, caractérisé en ce que le procédé comporte les étapes effectuées par le routeur périphérique d'entrée de :

- réception d'une requête d'un client pour l'établissement d'un service à qualité de service garantie dans le réseau de télécommunication,
- 10 - obtention de paramètres d'ingénierie de trafic correspondant au service demandé par le client,
- détermination si la création d'un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie est possible dans le réseau de télécommunication à permutation d'étiquettes,
- 15 - transfert au client d'un message de rejet de la requête du client pour un établissement d'un service à qualité de service garantie dans le réseau de télécommunication s'il n'est pas possible de créer un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie dans le réseau de télécommunication à permutation d'étiquettes.
- 20

2) Procédé selon la revendication 1, caractérisé en ce que si la création d'un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie est possible dans le réseau de télécommunication à permutation d'étiquettes, le procédé comporte une étape de transfert au client d'un message d'acceptation de la requête du client pour un établissement d'un service à qualité de service garantie dans le réseau de télécommunication.

30

3) Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que préalablement à l'étape de détermination si la création d'un tunnel pour

véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie est possible dans le réseau de télécommunication à permutation d'étiquettes, le procédé comporte une étape de détermination si un tunnel du réseau de télécommunication à permutation d'étiquettes est apte à véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie.

4) Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que lors de l'étape d'obtention de paramètres d'ingénierie de trafic correspondant au service demandé par le client, le procédé obtient en outre des règles applicables au client pour la mise à la disposition des ressources du réseau de télécommunication à permutation d'étiquettes.

5) Procédé selon la revendication 4, caractérisé en ce que préalablement à l'étape d'obtention de paramètres d'ingénierie de trafic correspondant au service demandé par le client et de règles applicables au client pour la mise à la disposition des ressources du réseau de télécommunication à permutation d'étiquettes, le procédé comporte l'étape de vérification, par l'intermédiaire d'un contrôleur de réseau, si le client ayant émis la requête est habilité à accéder au service à qualité de service garantie.

6) Procédé selon la revendication 5, caractérisé en ce que les paramètres d'ingénierie de trafic correspondant au service demandé par le client comprennent au moins un des éléments du groupe contenant le débit alloué pour un service, le délai de traitement, la classe de service d'ingénierie de trafic et le fait que le service soit uni ou bi directionnel.

7) Procédé selon la revendication 6, caractérisé en ce que les règles applicables au client comprennent au moins un des éléments du groupe contenant le débit maximal autorisé pour l'ensemble des services demandé par le client et le nombre maximal de sessions autorisées pour le client.

8) Procédé selon l'une quelconque des revendications 2 à 7, caractérisé en ce que le procédé comporte une étape de mise à jour d'une base de données référençant l'ensemble des accès par les clients reliés au routeur périphérique d'entrée aux services à qualité de service garantie dans le réseau de télécommunication.

5

9) Dispositif de contrôle d'admission à un service à qualité de service garantie dans un réseau de télécommunication à permutation d'étiquettes, le réseau de télécommunication à permutation d'étiquettes étant constitué d'au moins un routeur périphérique d'entrée et un routeur périphérique de sortie, les flux de données étant véhiculés dans le réseau de télécommunication à permutation d'étiquettes par des tunnels, caractérisé en ce que le dispositif de contrôle d'admission est compris dans le routeur périphérique d'entrée et comporte :

10 - des moyens de réception d'une requête d'un client pour l'établissement d'un service à qualité de service garantie dans le réseau de télécommunication,

15 - des moyens d'obtention de paramètres d'ingénierie de trafic correspondant au service demandé par le client et de règles applicables pour la mise à la disposition des ressources du réseau de télécommunication à permutation d'étiquettes,

20 - des moyens de détermination si la création d'un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie est possible dans le réseau de télécommunication à permutation d'étiquettes,

25 - des moyens de rejet de la requête du client pour un établissement d'un service à qualité de service garantie dans le réseau de télécommunication s'il n'est pas possible de créer un tunnel pour véhiculer le ou les flux de données liés au service à qualité de service garantie entre le routeur périphérique d'entrée et le routeur périphérique de sortie dans le réseau de télécommunication à permutation d'étiquettes.

10) Programme d'ordinateur stocké sur un support d'informations, ledit programme comportant des instructions permettant de mettre en œuvre le procédé selon l'une quelconque des revendications 1 à 8, lorsqu'il est chargé et exécuté par un système informatique.

30

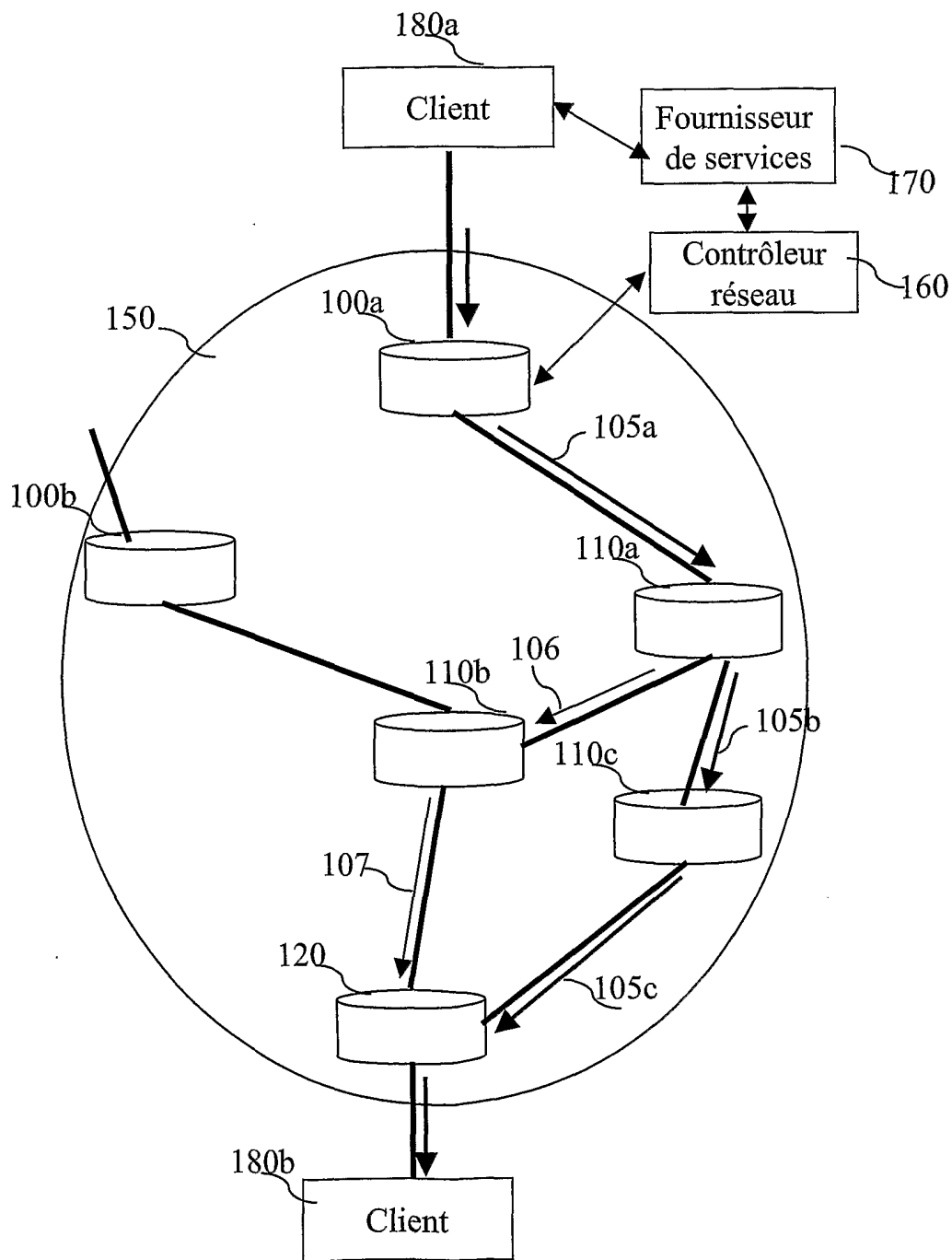


Fig. 1

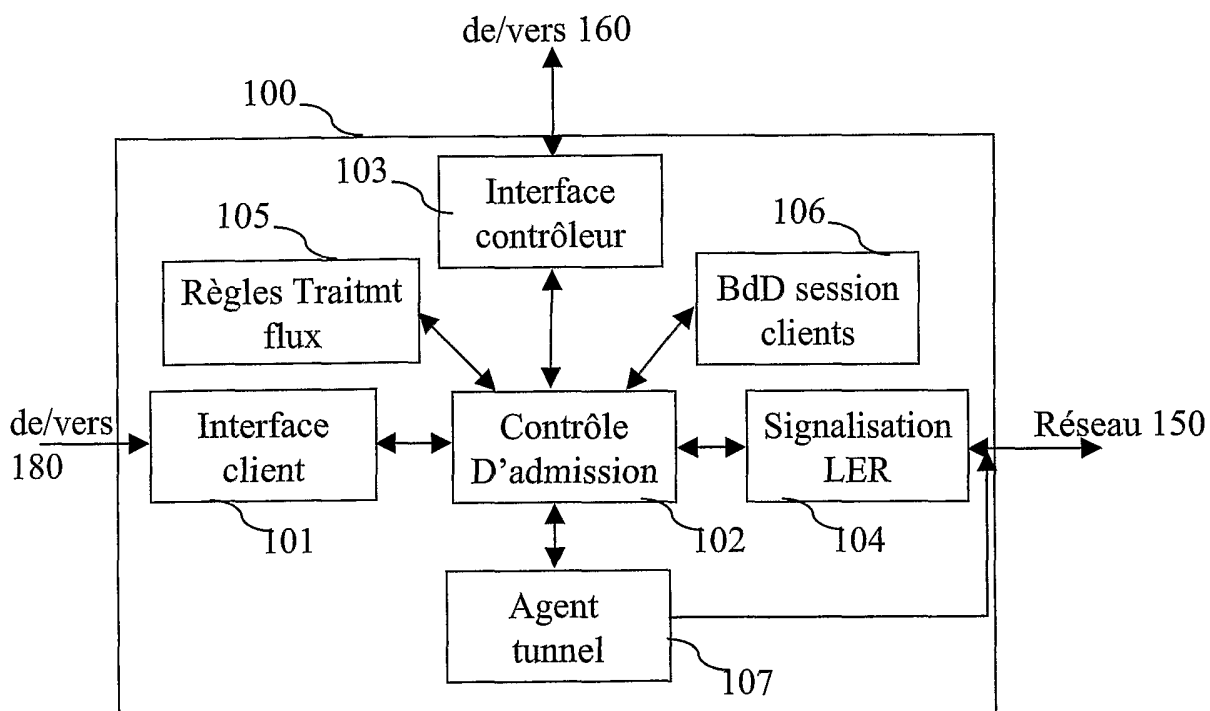


Fig. 2

3/3

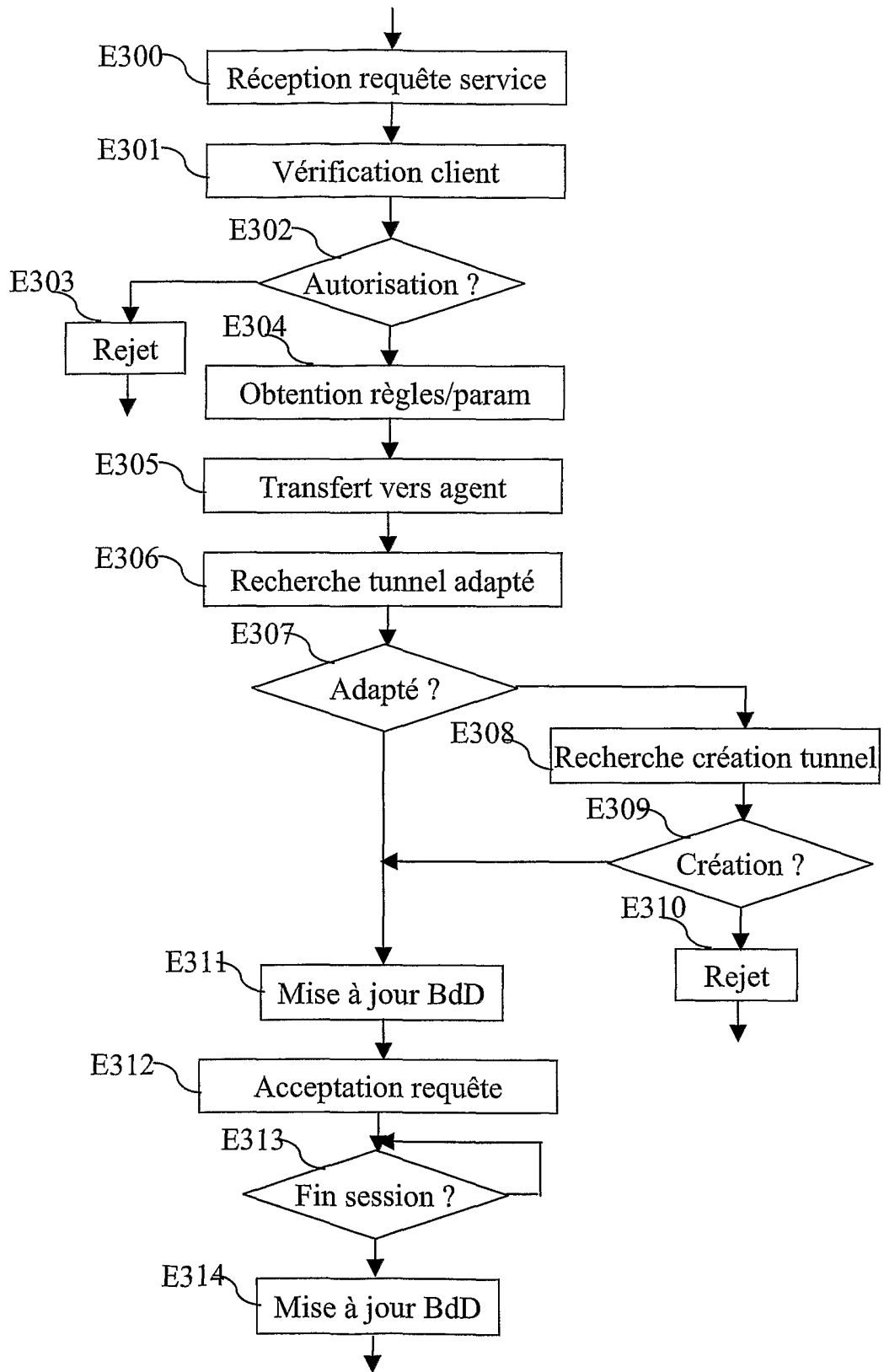


Fig. 3

**INTERNATIONAL SEARCH REPORT**

International Application No  
PCT/FR2005/002406

|   |   |                                     |
|---|---|-------------------------------------|
| <b>A. CLASSIFICATION OF SUBJECT MATTER</b><br>H04L12/56      H04L29/06  |   |                                     |
| According to International Patent Classification (IPC) or to both national classification and IPC   |   |                                     |
| <b>B. FIELDS SEARCHED</b>   |   |                                     |
| Minimum documentation searched (classification system followed by classification symbols)<br>H04L   |   |                                     |
| Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched   |   |                                     |
| Electronic data base consulted during the international search (name of data base and, where practical, search terms used)<br>EPO-Internal, WPI Data, PAJ   |   |                                     |
| <b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>   |   |                                     |
| Category *  | Citation of document, with indication, where appropriate, of the relevant passages  | Relevant to claim No.               |
| X   | US 2004/044789 A1 (ANGEL ELI ET AL)<br>4 March 2004 (2004-03-04)<br>paragraphs '0035!, '0036!, '0040!,<br>'0041!, '0061!, '0062!, '0066! -<br>'0069!, '0085!, '0088!, '0155! - '0157!<br>-----  | 1-10                                |
| X   | EP 1 202 501 A (NORTEL NETWORKS LIMITED) ·<br>2 May 2002 (2002-05-02)<br>abstract<br>paragraphs '0009!, '0010!, '0018!,<br>'0041!, '0051! - '0053!, '0063!<br>-----   | 1-10                                |
| X   | EP 1 065 858 A (NORTEL NETWORKS LIMITED)<br>3 January 2001 (2001-01-03)<br>abstract<br>paragraphs '0008!, '0011! - '0013!,<br>'0029!<br>-----<br>-/--   | 1-10                                |
| <input checked="" type="checkbox"/>   | Further documents are listed in the continuation of box C.  | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/>   | Patent family members are listed in annex.  |                                     |
| * Special categories of cited documents :   |   |                                     |
| *A* document defining the general state of the art which is not considered to be of particular relevance<br>*E* earlier document but published on or after the international filing date<br>*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)<br>*O* document referring to an oral disclosure, use, exhibition or other means<br>*P* document published prior to the international filing date but later than the priority date claimed | *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention<br>*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone<br>*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.<br>*Z* document member of the same patent family |                                     |
| Date of the actual completion of the international search<br><br>20 January 2006  | Date of mailing of the international search report<br><br>27/01/2006  |                                     |
| Name and mailing address of the ISA<br>European Patent Office, P.B. 5816 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016  | Authorized officer<br><br>Ramenzoni, S  |                                     |

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR2005/002406

| C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT |  |                       |
|--|--|-----------------------|
| Category *   | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
| X  | GB 2 399 257 A (* HUAWEI TECHNOLOGIES CO LTD) 8 September 2004 (2004-09-08)<br>abstract<br>page 2, line 1 - line 9<br>page 6, line 9 - page 7, line 14<br>page 10, line 20 - line 26 | 1-10                  |
| A  | AWDUCHE D O ET AL: "RSVP-TE: Extensions to RSVP for LSP Tunnels"<br>RFC 3209, 1 February 2001 (2001-02-01), XP002199928<br>cited in the application<br>alinéas 2.1, 2.5              | 1-10                  |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

|   |
|---|
| International Application No<br>PCT/FR2005/002406 |
|---|

| Patent document cited in search report | A1 | Publication date | Patent family member(s)  | Publication date   |
|--|----|------------------|--|--|
| US 2004044789                          | A1 | 04-03-2004       | NONE   |  |
| EP 1202501                             | A  | 02-05-2002       | US 6795445 B1  | 21-09-2004   |
| EP 1065858                             | A  | 03-01-2001       | CA 2300343 A1<br>US 6778494 B1   | 10-09-2000<br>17-08-2004   |
| GB 2399257                             | A  | 08-09-2004       | AU 2004200280 A1<br>BR 0400906 A<br>CN 1523834 A<br>DE 102004008376 A1<br>ES 2238928 A1<br>JP 2004254328 A<br>US 2004215817 A1 | 09-09-2004<br>16-11-2004<br>25-08-2004<br>09-09-2004<br>01-09-2005<br>09-09-2004<br>28-10-2004 |

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No  
PCT/FR2005/002406

|  |   |  |
|--|---|--|
| <b>A. CLASSEMENT DE L'OBJET DE LA DEMANDE</b><br>H04L12/56      H04L29/06  |   |  |
| <i>*Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB</i>  |   |  |
| <b>B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE</b><br>Documentation minimale consultée (système de classification suivi des symboles de classement)<br>H04L  |   |  |
| Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche  |   |  |
| Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)<br>EPO-Internal, WPI Data, PAJ  |   |  |
| <b>C. DOCUMENTS CONSIDERES COMME PERTINENTS</b>  |   |  |
| Catégorie *  | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents  | no. des revendications visées  |
| X  | US 2004/044789 A1 (ANGEL ELI ET AL)<br>4 mars 2004 (2004-03-04)<br>alinéas '0035!, '0036!, '0040!, '0041!,<br>'0061!, '0062!, '0066! - '0069!,<br>'0085!, '0088!, '0155! - '0157!<br>-----  | 1-10   |
| X  | EP 1 202 501 A (NORTEL NETWORKS LIMITED)<br>2 mai 2002 (2002-05-02)<br>abrégé<br>alinéas '0009!, '0010!, '0018!, '0041!,<br>'0051! - '0053!, '0063!<br>-----  | 1-10   |
| X  | EP 1 065 858 A (NORTEL NETWORKS LIMITED)<br>3 janvier 2001 (2001-01-03)<br>abrégé<br>alinéas '0008!, '0011! - '0013!, '0029!<br>-----   | 1-10   |
| -/-  |   |  |
| <input checked="" type="checkbox"/> Voir la suite du cadre C pour la fin de la liste des documents   |   | <input checked="" type="checkbox"/> Les documents de familles de brevets sont indiqués en annexe |
| * Catégories spéciales de documents cités:   |   |  |
| *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent<br>*E* document antérieur, mais publié à la date de dépôt international ou après cette date<br>*L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)<br>*O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens<br>*P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée | *T* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention<br>*X* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément<br>*Y* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier<br>*&* document qui fait partie de la même famille de brevets |  |
| Date à laquelle la recherche internationale a été effectivement achevée  | Date d'expédition du présent rapport de recherche internationale  |  |
| 20 janvier 2006  | 27/01/2006  |  |
| Nom et adresse postale de l'administration chargée de la recherche internationale  | Fonctionnaire autorisé  |  |
| Office Européen des Brevets, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016   | Ramenzoni, S  |  |

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No  
PCT/FR2005/002406

| C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS |   |                               |
|---|---|-------------------------------|
| Catégorie                                       | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents  | no. des revendications visées |
| X   | <p>GB 2 399 257 A (* HUAWEI TECHNOLOGIES CO LTD) 8 septembre 2004 (2004-09-08)<br/>abrégé<br/>page 2, ligne 1 - ligne 9<br/>page 6, ligne 9 - page 7, ligne 14<br/>page 10, ligne 20 - ligne 26</p> | 1-10                          |
| A   | <p>AWDUCHE D O ET AL: "RSVP-TE: Extensions to RSVP for LSP Tunnels"<br/>RFC 3209, 1 février 2001 (2001-02-01), XP002199928<br/>cité dans la demande<br/>alinéas 2.1, 2.5</p>                        | 1-10                          |

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No

PCT/FR2005/002406

| Document brevet cité<br>au rapport de recherche | Date de<br>publication | Membre(s) de la<br>famille de brevet(s)  | Date de<br>publication   |
|---|------------------------|--|--|
| US 2004044789 A1                                | 04-03-2004             | AUCUN  |  |
| EP 1202501 A                                    | 02-05-2002             | US 6795445 B1  | 21-09-2004   |
| EP 1065858 A                                    | 03-01-2001             | CA 2300343 A1<br>US 6778494 B1   | 10-09-2000<br>17-08-2004   |
| GB 2399257 A                                    | 08-09-2004             | AU 2004200280 A1<br>BR 0400906 A<br>CN 1523834 A<br>DE 102004008376 A1<br>ES 2238928 A1<br>JP 2004254328 A<br>US 2004215817 A1 | 09-09-2004<br>16-11-2004<br>25-08-2004<br>09-09-2004<br>01-09-2005<br>09-09-2004<br>28-10-2004 |