(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 836 314**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **02 02437**

(51) Int Cl[7] : **H 04 L 12/24,** H 04 L 12/56, G 06 F 11/30

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 21.02.02.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 22.08.03 Bulletin 03/34.

(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.

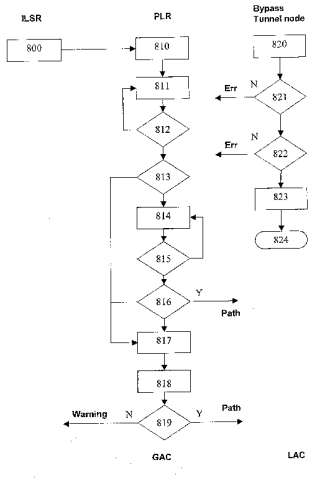
(72) **Inventeur(s) :** LE ROUX JEAN LOUIS, CALVIGNAC GERALDINE et MOIGNARD RENAUD.

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

(74) **Mandataire(s) :** CABINET LE GUEN ET MAILLET.

(54) METHODE DYNAMIQUE ET DISTRIBUEE DE PROTECTION LOCALE D'UN CHEMIN A COMMUTATION D'ETIQUETTES.

(57) L'invention concerne une méthode de protection d'un chemin à commutation d'étiquettes dans un réseau MPLS comprenant une pluralité de noeuds reliés par des liens IP, ledit chemin commençant à un noeud d'entrée et se terminant à un noeud de sortie dudit réseau en passant par une série déterminée de nœuds et de liens dudit réseau, dits éléments dudit chemin. Lorsque ledit noeud d'entrée requiert la protection d'un élément du chemin, dans une première phase, un noeud dudit chemin, dit point PLR, en amont dudit élément à protéger détermine un chemin de secours, dit tunnel de bypass, rejoignant le chemin en aval dudit élément à protéger en un noeud, dit point PM, et, dans une seconde phase, des ressources du réseau sont réservées sur chacun des liens du tunnel de bypass pour secourir ledit chemin en cas de défaillance dudit élément.



FR 2 836 314 - A1

La présente invention concerne une méthode de protection de chemins à commutation d'étiquettes dans un réseau MPLS (MultiProtocol Label Switching). Plus particulièrement la présente invention a trait à une méthode de protection locale de tels chemins avec partage de ressources.

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.

On a représenté de manière schématique en Fig. 1 un réseau MPLS, 100, comprenant une pluralité de routeurs dénommés LSR (Label Switching Routers) tels que 110, 111, 120, 121, 130, 131, 140, reliés entre eux par des liens IP. Lorsqu'un paquet IP arrive sur un nœud périphérique d'entrée 110, dénommé Ingress LSR, ce dernier lui attribue une étiquette (ici 24) en fonction de son en-tête 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 (dans l'exemple en question, 24 est remplacé par 13) et le processus se répète de nœud en nœud jusqu'au routeur de sortie 140 (encore dénommé Egress LSR) qui supprime l'étiquette avant de transmettre le paquet. Alternativement, la suppression d'étiquette peut être déjà effectuée par le penultième routeur puisque le routeur de sortie n'utilise pas l'étiquette entrante.

Comme indiqué en Fig. 2, 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). Ainsi, par exemple, le routeur A remplace les étiquettes des paquets IP arrivant sur le port 3 et de valeur 16 par des étiquettes de valeur 28 puis envoie les paquets ainsi réétiquetés sur le port 2.

Le chemin parcouru par un paquet à travers le réseau du routeur d'entrée (Ingress LSR) jusqu'au routeur de sortie (Egress LSR) est appelé chemin à étiquettes commutées ou LSP (Label Switched Path). Les routeurs LSR traversés par le chemin et distincts des routeurs d'entrée et de sortie 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.

Un des intérêts du protocole MPLS est de pouvoir 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 ingéniérie 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), notammment 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 nœuds du chemin du routeur d'entrée jusqu'au routeur de sortie. Lorsque tous les nœuds du chemin sont fixés, on parle de routage explicite au sens strict. Un chemin LSP déterminé selon un mode explicite est encore appelé tunnel MPLS.

La détermination d'un ou des chemins peut se faire de manière centralisée ou distribuée.

Selon la méthode distribuée encore 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 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 nœud en nœud par des messages IGP étendu, 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 d'entrée (Ingress LSR) en prenant également en compte d'autres contraintes fixées par l'opérateur du réseau (par exemple éviter tel ou tel nœud ou éviter les liens de tel ou tel type). Le routeur 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 nœuds du chemin LSP au moyen des protocoles de signalisation connus sous les abbréviations 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-TE, le routeur d'entrée A transmet, comme indiqué en Fig. 3A, un message « Path » dans un paquet IP au routeur de sortie F. Ce message spécifie la liste des nœuds par lesquels le chemin LSP doit passer. A chaque nœud le message « Path » établit le chemin et fait une réservation d'état. Lorsque le message « Path » atteint le routeur de sortie, un message d'acquittement « Resv » est renvoyé par le même chemin au routeur d'entrée, comme indiqué en Fig. 3B. A chaque nœud, 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 10 unités (MHz) pour le chemin, les bandes passantes respectivement affectées à chaque lien sont décrémentées de la valeur réservée (10) lors de la rétropropagation du message d'acquittement / 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 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 d'entrée sont ensuite avertis par le serveur du ou des tunnels pour lesquels ils sont le nœud d'entrée. Les tunnels sont alors établis comme indiqué en Fig. 3A et 3B. La méthode de détermination centralisée présente l'avantage d'une grande stabilité et prédictibilité puisqu'un seul organe effectue le calcul préalable de tous les tunnels. Elle présente en contrepartie l'inconvénient de de pas s'adapter facilement aux variations rapides de la topologie du réseau, par exemple en cas de rupture d'une liaison physique, supprimant les liens IP qu'elle supporte.

Qu'ils aient été calculés de manière centralisée ou distribuée, les tunnels sont susceptibles d'être détruits en cas de coupure d'une liaison physique sous-jacente. Il faut alors prévoir des mécanismes de secours permettant d'établir un nouveau tunnel entre le même routeur d'entrée et le même routeur de sortie. On peut distinguer les mécanismes de restauration établissant un tunnel de secours après la coupure et les mécanismes de protection préétablissant un tunnel de secours en prévision d'une coupure possible.

L'avantage des mécanismes de protection est de permettre une reprise très rapide du trafic, un tunnel de secours étant déjà disponible. En contrepartie, ils présentent l'inconvénient de mobiliser des ressources importantes du réseau. Plus précisément, les mécanismes de protection connus de l'état de la technique se divisent en méthodes de protection locale et méthodes de protection de bout en bout. Dans les premières, des tunnels de secours locaux sont préétablis en prévision d'une défaillance d'un élément (nœud, lien) du tunnel initial. Lorsque la défaillance se produit, le trafic est détourné dans le tunnel local pour contourner l'élément défaillant. Dans les méthodes de protection de bout en bout, un tunnel de secours est établi du routeur d'entrée au routeur de sortie. A l'inverse des méthodes de restauration (où les tunnels de secours sont créés à la demande), les méthodes de protection (où les tunnels de secours sont créés au préalable) sont gourmandes en ressources de réseau.

On connaît de l'état de la technique, en particulier du document intitulé « Fast-Reroute Techniques in RSVP-TE » de P. Pan et al. disponible sur le site de l'IETF sus-mentionné sous la référence « draft-pan-rsvp-fastreroute-00.txt », différentes méthodes de protection locale (ou FRR pour Fast ReRoute) d'un tunnel. Le principe général de cette protection locale est rappelé en Fig. 4. Pour un élément (lien, nœud) du tunnel à protéger, on prévoit un tunnel de secours local pour le contourner. Par exemple pour contourner le lien CD, on prévoit un tunnel de secours T(CD) ayant pour chemin C,C',E. Le routeur en amont qui détecte et répare la défaillance du chemin en orientant les paquets sur le tunnel de secours est dénommé point PLR (pour « Point of Local Repair »). Le routeur en aval de la défaillance où le tunnel de secours rejoint le tunnel initial est dénommé point PM (pour « Point of Merging »). Dans le cas présent, le routeur C détecte la défaillance du lien CD (symbolisée par un éclair) par l'absence de messages RSVP « Hello » transmis à intervalles réguliers sur le lien CD par le routeur D ou par une alerte de la couche physique sous-jacente. Le routeur C réachemine alors le trafic du chemin initial sur le tunnel de bypass CC'E. La jonction entre le chemin initial et le tunnel de bypass est réalisée en E.

Une première méthode de protection locale de chemin LSP, dénommée « one-to-one », consiste à créer pour chaque élément du chemin à protéger un tunnel de secours local, encore appelé « détour ». On a illustré en Fig. 5 une méthode de protection locale de type « one-to-one ». Chaque élément K du chemin est protégé par un détour noté T(K). On notera qu'un détour T(N) pour un nœud N protége également le lien en amont et le lien en aval du nœud. Si le tunnel comporte n nœuds, il peut

donc y avoir jusqu'à (n-1) détours. Si plusieurs tunnels sont à protéger dans le réseau MPLS, une série de détours devra être prévue pour chacun d'entre eux. Cette méthode de protection n'est donc pas extensible (scalable).

Il est important de noter que les détours sont créés dynamiquement lors de l'établissement du chemin. En outre, les détours sont créés de manière distribuée par les routeurs de transit du chemin, à l'initiative du routeur d'entrée. Ainsi en cas de changement de topologie du réseau ou de modification des contraintes de ressources, les détours ne seront pas nécessairement les mêmes pour un même chemin. La procédure de création des détours nécessite une modification de la signalisation RSVP, comme décrit dans le document sus-mentionné.

Selon une seconde méthode de protection locale de chemin LSP, dénommée « many-to-one », un tunnel de secours, dénommé tunnel de bypass, est prévu par l'opérateur pour protéger un ou plusieurs éléments (nœud, lien) du réseau MPLS. Un tunnel de bypass peut servir à secourir une pluralité de chemins empruntant ledit ou lesdits éléments. A titre d'exemple, on a illustré en Fig. 6 deux chemins à protéger T_1=ABCDE et T_2=A'BCDE partageant le chemin BCDE. Dans le cas présent, l'opérateur a prévu de protéger le nœud C en configurant un tunnel de bypass ayant pour chemin BB'D'D. Ce tunnel de bypass permet de secourir les deux chemins T_1 et T_2 en cas de défaillance du nœud C (ou d'un des liens BC, CD). De manière générale, un tunnel de bypass permet de secourir une pluralité de chemins qui l'intersectent en amont de la défaillance en un point commun PLR et en aval de la défaillance en un point commun PM. Le tunnel de bypass tire parti de la possibilité d'empiler les étiquettes (label stacking) en leur attribuant différents niveaux de hiérarchie pour réacheminer les paquets de manière transparente. Plus précisément, comme indiqué sur la Fig. 6, les routeurs le long du chemin T_1 commutent les étiquettes 12,18,45 et 37. Lorsqu'une défaillance du nœud C intervient, le routeur B empile une étiquette (ici 67) représentant localement le tunnel de bypass. Au penultième nœud du tunnel de bypass (ici D'), l'étiquette représentant localement le tunnel de bypass (ici 38) est dépilée de sorte que le point PM reçoit une étiquette identique à celle (45) d'un paquet qui n'aurait pas été réacheminé.

On distinguera dans la suite deux types de tunnels de bypass : ceux qui protègent un lien, encore appelés NHOP bypass (pour next-hop bypass) et ceux qui protègent un nœud ou NNHOP bypass (pour next-next-hop bypass).

Il est important de noter que les tunnels de bypass sont déterminés au préalable, de manière statique et/ou centralisée par un serveur spécialisé, sans tenir compte *a priori* des besoins en ressources des futurs chemins LSP à établir et les variations en ressources du réseau. En particulier, la bande passante du tunnel de bypass peut ne pas être suffisante pour transporter la bande requise du chemin à protéger. Ainsi, bien qu'un tunnel de bypass soit présent, il ne permettra pas de secourir efficacement le chemin à protéger.

Le problème à la base de l'invention est de proposer une méthode de protection de chemins LSP qui remédie aux inconvénients précités, en particulier qui soit extensible et qui soit adaptée à prendre en compte les variations rapides de ressources du réseau tout en garantissant une efficacité de protection.

Un problème subsidiaire à la base d'un mode de réalisation de l'invention est de proposer une méthode de protection de tunnels LSP qui consomme moins de ressources que les méthodes de protection connues de l'état de la technique.

Le problème est résolu par l'objet de l'invention, défini comme une méthode de protection d'un chemin à commutation d'étiquettes dans un réseau MPLS comprenant une pluralité de nœuds reliés par des liens IP, ledit chemin commençant à un nœud d'entrée et se terminant à un nœud de sortie dudit réseau en passant par une série déterminée de nœuds et de liens dudit réseau, dits éléments dudit chemin. Lorsque ledit nœud d'entrée requiert la protection d'un élément du chemin, dans une première phase, un nœud dudit chemin, dit point PLR, en amont dudit élément à protéger détermine un chemin de secours, dit tunnel de bypass, rejoignant le chemin en aval dudit élément à protéger en un nœud, dit point PM, et, dans une seconde phase, des ressources du réseau sont réservées sur chacun des liens du tunnel de bypass pour secourir ledit chemin en cas de défaillance dudit élément.

Lesdites ressources sur un lien du tunnel de bypass comprennent par exemple une bande passante réservée relative à ce lien.

Avantageusement, pour chaque élément physique dudit réseau, on détermine un groupe de liens dudit réseau atteints par la défaillance dudit élément physique et, réciproquement, pour chaque lien dudit réseau, on détermine la liste, dite liste SRLG, desdits groupes auxquels il appartient.

Avantageusement, le point PLR recherche, dans une première étape de la première phase, les tunnels de bypass existants dans le réseau susceptibles de protéger ledit élément.

Si l'élément à protéger est un lien, le point PLR détermine si un tunnel de bypass existant est susceptible de protéger ledit lien en vérifiant que ledit tunnel ne comprend pas ledit lien et que, la liste SRLG associée à chaque lien dudit tunnel existant et la liste SRLG associée au lien à protéger ont une intesection vide.

Si l'élément à protéger est un nœud, le point PLR détermine si un tunnel de bypass existant est susceptible de protéger le nœud en vérifiant que ledit tunnel ne comprend pas ledit nœud et que la liste SRLG associée à chaque lien dudit tunnel existant et la liste SRLG associée au lien joignant le point PLR et ledit nœud ont une intersection vide.

Ensuite, pour chaque tunnel de bypass existant susceptible de protéger ledit élément, dit tunnel candidat, le point PLR simule, pour chaque lien du tunnel candidat, une augmentation de la bande passante réservée sur ce lien de la valeur de la bande passante du chemin à étiquettes commutées et vérifie si la valeur de la bande passante ainsi obtenue est inférieure à une bande passante maximale réservable sur ce lien .

Alternativement, pour chaque tunnel de bypass existant susceptible de protéger ledit élément, dit tunnel candidat, le point PLR simule une protection dudit élément par ledit tunnel candidat et détermine, pour chaque lien dudit tunnel candidat, la plus grande bande passante à réserver sur ce lien pour supporter les tunnels de bypass passant par ce lien, y compris le tunnel candidat, en cas de défaillance d'un élément physique quelconque du réseau et l'on vérifie si ladite plus grande bande passante est inférieure à une bande passante maximale réservable sur ce lien .

S'il n'existe aucun tunnel candidat ou si la vérification est négative pour au moins un lien de chaque tunnel candidat, le point PLR détermine un nouveau tunnel de bypass.

Avantageusement, dans ladite seconde phase, le point PLR transmet un premier message se propageant de nœud en nœud sur le tunnel de bypass vers le point PM et qu'un second message est retourné le long tunnel de bypass vers le point PLR, et lors du passage du premier ou du second message, on vérifie pour chaque lien du tunnel de bypass, qu'il est susceptible de protéger ledit élément et que lesdites ressources sont effectivement disponibles sur ce lien, et dans l'affirmative l'on procède à la réservation desdites ressources.

L'objet de l'invention est également défini par de nouveaux messages de protocoles existants.

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

La Fig. 1 illustre un réseau MPLS connu de l'état de la technique ;

La Fig. 2 illustre schématiquement la création d'un chemin à étiquettes commutées ;

La Fig. 3A illustre schématiquement une première phase de la procédure d'établissement d'un chemin LSP ;

La Fig. 3B illustre schématiquement une seconde phase de la procédure d'établissement d'un chemin LSP ;

La Fig. 4 illustre schématiquement le principe de réparation locale d'un chemin LSP ;

La Fig. 5 illustre schématiquement une méthode distribuée de protection locale d'un chemin LSP, connue de l'état de la technique ;

La Fig. 6 illustre schématiquement une méthode centralisée de protection locale d'un chemin LSP, connue de l'état de la technique ;

La Fig. 7 illustre le concept d'entité de risque partagé ;

La Fig. 8 illustre schématiquement une méthode distribuée de protection locale de chemins LSP selon la présente invention .

L'idée à la base de l'invention est de prévoir une méthode de génération dynamique et distribuée de tunnels de bypass. De manière générale, lorsqu'un chemin LSP doit faire l'objet d'une protection locale, le routeur d'entrée avertit le point PLR (Point of Local Repair) en amont de l'élément à protéger. Ce point détermine tout d'abord s'il existe un tunnel de bypass qui passe par lui et qui est susceptible de protéger ledit élément. Le cas échéant, il vérifie si le tunnel de bypass présente les ressources suffisantes, notamment en bande passante, pour supporter le trafic du chemin à protéger et, dans la négative, il s'assure qu'il peut les augmenter. Si aucun tunnel de bypass ne peut être retenu ou s'il n'est pas possible d'augmenter les ressources du tunnel retenu, le point PLR tente alors de déterminer un nouveau tunnel de bypass permettant de protéger l'élément en question. Avantageusement, il utilise pour ce faire des éléments de tunnels existants et en partage les ressources. Enfin, si

aucun tunnel de bypass ne peut être établi, le point PLR en avertit le routeur d'entrée. Lorsque le chemin LSP est supprimé, le routeur d'entrée peut transmettre un message de suppression au point PLR qui libère alors les ressources qui avaient été réservées pour la protection de l'élément considéré.

Les ressources qui peuvent être réservées ou libérées respectivement lors de la création et de la suppression d'un tunnel de bypass sont notamment la bande passante. On entend ici par bande passante, une bande passante logique dédiée à la protection, sans rapport direct avec la bande passante physique. Plus précisément, une bande passante physique associée à un élément du réseau (par exemple un lien) comprend une bande passante logique dédiée au trafic normal et une bande de passante logique dédiée au trafic secouru. Cette dernière, encore appelée bande passante de protection pourra être utilisée, partiellement ou entièrement, par les tunnels de bypass. On notera RBP(L) la valeur de la bande passsante de protection sur un lien L du réseau et rBP(L) la valeur de la bande passante effectivement utilisée ou réservée par les tunnels de bypass empruntant ce lien.

Nous supposerons tout d'abord que chaque nœud (routeur LSR) du réseau a non seulement connaissance de la topologie du réseau mais également des tunnels de bypass existants, de leurs caractéristiques (liste de nœuds et liens, bande passante à protéger) et, pour chaque tunnel de bypass, de l'élément du réseau qu'il protège. Cette information peut être diffusée dans le réseau comme celle relative à la topologie du réseau par le biais de messages dont nous expliciterons plus loin le contenu. Chaque PLR ayant créé un tunnel de bypass envoie à ses voisins un message (annonce) identifiant ledit tunnel, ses caractéristiques et l'élément qu'il protège. Ce message est répercuté de nœud en nœud dans tout le réseau Lorsque le tunnel de bypass est supprimé, un message de suppression est également transmis et diffusé dans tout le réseau.

On appellera par la suite entité de risque partagé ou SRLG (pour Shared Risk Link Group) associé à un lien, l'ensemble des liens du réseau partageant une même ressource physique avec le lien précité et tous atteints par la défaillance de cette ressource physique. Ce concept d'entité de risque partagé a été introduit par K. Kompella et al. dans un document intitulé « Routing extensions in support of generalized MPLS » disponible sur le site de l'IETF sous la référence « draft-ietf-

ccamp-gmpls-routing-01.txt ». Un lien peut appartenir à plusieurs SRLG ou n'en appartenir à aucun. On définit la liste SRLG d'un lien comme la liste des SRLG dans lesquels ce lien apparaît. Deux liens présentent une diversité de SRLG si leurs listes SRLG ont une intersection vide. En particulier deux liens n'appartenant à aucun SRLG ont une diversité de SRLG.

Le concept de liste de SRLG sera mieux compris à l'aide de l'exemple de la Fig. 7. On suppose que trois routeurs R_1, R_2, R_3 sont interconnectés au moyen de brasseurs optiques (OXC) O_1, O_2, O_3. Ces brasseurs optiques sont inteconnectés au moyen de fibres optiques f_1, f_2 avec muliplexage WDM. Soient S_1, S_2, les SRLG associés respectivement aux fibres f_1 et f_2. Le lien R_1R_2 utilise le seulement trajet lumineux O_1-O_2 sa liste SRLG est $\{S_1\}$. Le lien R_1R_3 utilise le trajet lumineux O_1-O_2-O_3, sa liste SRLG est par conséquent $\{S_1,S_2\}$. Le lien R_2R_3 utilise le trajet lumineux O_2-O_3, sa liste SRLG se résume donc à $\{S_2\}$. On constate donc que les liens R_1R_2 et R_2R_3 ont une diversité de SRLG mais que ceux-ci n'en ont pas avec le lien avec le lien R_1R_3 .

On définit une défaillance de SRLG comme la défaillance de la ressource physique partagée par les différents éléments du SRLG. Ainsi, dans l'exemple précédent, une défaillance du SRLG S_2 correspond à une défaillance de la fibre f_2.

Une défaillance de SRLG peut causer la défaillance de plusieurs liens. Ainsi, dans l'exemple précédent, la défaillance du SRLG S_2 entraînera la défaillance des liens R_1R_3 et R_2R_3. De manière générale, la défaillance d'un SRLG donné entraînera la défaillance des liens dont les listes de SRLG le contiennent.

Réciproquement, la défaillance d'un lien peut ne pas être liée à la défaillance d'un SRLG. Ainsi, dans l'exemple précédent, la défaillance du lien R_2O_2 connectant R_2 à R_3 entraîne une défaillance du lien R_2R_3 mais non du SRLG S_2. De manière générale si un lien n'appartient pas à aucun SRLG, la défaillance de ce lien ne sera pas liée à la défaillance d'un SRLG.

La méthode de protection locale selon l'invention comprend deux phases, une première phase dite de contrôle d'admission générale ou GAC (General Admission Control) et une seconde phase dite de contrôle d'admission locale ou LAC (Local Admission Control) de tunnel de bypass. Lors de la première phase, un point PLR d'un chemin LSP détermine, à partir d'une requête du routeur d'entrée, si une protection locale est à réaliser et, le cas échéant, le type de la protection demandée (lien, nœud) ainsi que la valeur de la bande passante requise pour protéger le chemin LSP. Le point PLR détermine ensuite le chemin du tunnel de bypass tout en simulant

son admission par le réseau. Dans la seconde phase, le PLR procède à la création effective du tunnel de bypass de manière similaire à celle d'un chemin LSP classique en transmettant un message analogue à un message « Path » le long du chemin du tunnel de bypass et en recevant le message d'acquittement « Resv » correspondant.

Nous exposerons tout d'abord un premier mode de réalisation de l'invention.

Le contrôle d'admission générale comprend deux étapes. Dans la première étape, le PLR détermine s'il existe un ou des tunnels de bypass existants permettant d'assurer la protection demandée. On obtient ainsi des tunnels de bypass candidats. Les tunnels de bypass candidats ne peuvent utiliser l'élément à protéger.

- dans le cas d'un lien à protéger, le PLR détermine à partir de sa base de données locale, pour chaque lien du tunnel de bypass (NHOP) candidat, s'il présente une diversité de SRLG avec ce lien : dans la négative le tunnel de bypass candidat n'est pas compatible en terme de risque et ne peut être retenu;

- dans le cas d'un nœud à protéger, le PLR détermine à partir de sa base de données locale, pour chaque lien du tunnel de bypass (NNHOP) candidat, s'il présente une diversité de SRLG avec le lien joignant le PLR et le nœud à protéger : dans la négative le tunnel de bypass n'est pas compatible en terme de risque et ne peut être retenu .

S'il existe au moins un tunnel de bypass candidat T satisfaisant au critère de compatibilité, le nœud PLR simule une augmentation de la bande passante b(T) du tunnel de la valeur b(LSP) de la bande passante requise pour protéger le chemin LSP. Le noeud PLR vérifie ensuite si, pour chaque lien L du tunnel de bypass, la nouvelle valeur b(T) est telle que $b(T) \leq RBP(L)$. Si c'est le cas le tunnel de bypass est définitivement retenu. A défaut, les autres tunnels candidats satisfaisant au critère de compatibilité sont testés l'un après l'autre.

Si aucun des tunnels de bypass candidats ne peut être retenu pour des raisons d'incompatibilité de risque ou de bande passante insuffisante, le point PLR simule, dans une seconde étape, la création d'un nouveau tunnel de bypass.

La construction d'un nouveau tunnel de bypass est simulée de la manière suivante : à partir du point PLR jusqu'à un point PM (Point of Merging) du chemin LSP en aval de l'élément à protéger, le PLR sélectionne parmi les liens du réseau,

ceux qui peuvent supporter le tunnel de bypass. Les critères d'admission utilisés pour un lien L sont les mêmes que ceux indiqués plus haut, à savoir :

- le lien L doit être distinct du lien à protéger ;
- si l'élément à protéger est un lien, le lien L doit présenter une diversité de SRLG avec le lien à protéger ;
- si l'élément à protéger est un nœud, le lien L doit présenter une diversité de SRLG avec le lien joignant le PLR et le nœud à protéger .

En outre, si une protection de la bande passante est requise, le point PLR simule pour chaque lien L une augmentation de la bande passante réservée à la protection sur ce lien, soit : $rBP(L)=rBP(L)+b(LSP)$ et teste si la condition $rBP(L)\leq RBP(L)$ est vérifiée. Dans la négative, le lien ne peut accueillir le tunnel de bypass et est rejeté. Dans l'affirmative, en revanche, le tunnel de bypass peut *a priori* emprunter le lien et est sélectionné.

Le résultat de la sélection précédente est un sous-réseau du réseau initial où les liens non sélectionnés ont été élagués. Le point PLR détermine alors le chemin le plus court dans le sous-réseau (CSPF), par exemple au moyen de l'algorithme de Dijkstra. Ce chemin sera celui qu'empruntera le tunnel de bypass.

Si aucun tunnel de bypass ne peut être construit, le point PLR en avertit le routeur d'entrée via le chemin LSP.

Il convient de noter que certains nœuds du réseau pourront être exclus par l'opérateur comme ne pouvant assurer une protection locale. Autrement dit, un tel nœud ne pourra être PLR pour un chemin LSP quelconque le traversant. Dans ce cas, lorsqu'un tel nœud reçoit une requête de protection locale, il avertit le routeur d'entrée, via le chemin LSP, que la protection ne pourra être réalisée.

On a supposé dans ce qui précède qu'il fallait protéger la bande passante du chemin LSP (b(LSP)). Cependant, il peut s'avérer qu'une protection de la bande passante ne soit pas nécessaire (la protection du chemin LSP est alors de type « Best Effort »). Dans ce cas, un tunnel de bypass spécifique, consacré à la protection «Best Effort », sera utilisé par le PLR.

Lorsqu'un tunnel de bypass à été déterminé par le point PLR, on passe à une phase de signalisation avec un contrôle d'admission locale qui crée réellement le tunnel de bypass. Le point PLR transmet alors un message de type « Path » indiquant notamment le chemin du tunnel de bypass et la bande passante requise pour la protection, b(LSP). Chaque lien procède à nouveau à la vérification de sa diversité

SRLG avec l'élément à protéger. Si cette diversité SRLG est vérifiée, on teste à nouveau si la condition $rBP(L) \leq RBP(L)$ est vérifiée et dans l'affirmative, on procède à la modification effective de la bande passante réservée à la protection sur ce lien soit $rBP(L)=rBP(L)+b(LSP)$. Ces nouvelles étapes de vérification s'expliquent par le fait que la situation de diversité ou les ressources du lien ont pu évoluer entre les phases de contrôle d'admission générale et locale, notamment si d'autres tunnels de bypass ont été créés dans l'intervalle. Si toutes les vérifications sont positives, on est certain d'avoir une protection efficace de la bande passante du chemin LSP. En revanche, si l'une des étapes de vérification échoue, un message d'erreur est transmis le long du tunnel de bypass au point PLR qui pourra ensuite avertir le routeur d'entrée.

Comme pour un chemin LSP classique, les tables MPLS du tunnel de bypass sont établies lors de la rétropropagation du message d'acquittement « Resv ».

On notera que la réservation effective de la bande passante pourra être réalisée lors de l'acheminement du message « Path » ou bien lors de la rétropropagation du message d'acquittement.

Nous exposerons maintenant un second mode de réalisation de l'invention.

Selon ce second mode de réalisation, la construction du tunnel de bypass est réalisée en partageant des ressources de tunnels déjà existants. Ce mode de réalisation trouve sa justification dans le fait que deux éléments physiques du réseau n'ont qu'une très faible probabilité d'être défaillants en même temps. La défaillance d'un élément physique entraîne la défaillance d'un certain nombre de liens IP et/ou de nœuds du réseau qui l'utilisent. Ainsi, en cas de défaillance d'un élément physique, seuls certains chemins seront affectés. Les ressources de protection permettant de protéger des chemins qui ne sont pas affectés en même temps par la défaillance d'un même élément physique sont susceptibles d'être partagées et par conséquent économisées.

Dans ce but, on définit un risque de défaillance ou FR (pour Failure Risk) comme un lien, un nœud ou un SRLG. Bien entendu, pour un SRLG, le risque réel de défaillance concerne la ressource physique sous-jacente mais, par souci de simplification, on associera le SRLG à la ressource physique en question.

En outre, on définit le groupe de risques de défaillance ou TFRG (pour Tunnel Failure Risk Group) d'un tunnel de bypass comme l'ensemble des risques de défaillance que protège ce tunnel. Ainsi, le TFRG d'un tunnel de bypass NHOP est l'ensemble formé par le lien en aval et la liste SRLG de ce lien. De même, le TFRG

d'un tunnel de bypass NNHOP est l'ensemble formé par le nœud qu'il protège, le lien reliant le point PLR à ce nœud et la liste SRLG de ce lien.

De même, on définit le groupe de risques de défaillance ou LFRG (pour Link Failure Risk Group) d'un lien comme l'ensemble des risques de défaillance que protègent les tunnels de bypass passant par ce lien.

Enfin, on définit la bande passante de protection d'un risque de défaillance Φ par un lien L d'un tunnel de bypass protégeant Φ (autrement dit dont le TFRG contient Φ), et on la note $BP(\Phi,L)$, la bande passante réservée ou à réserver sur ce lien pour protéger Φ. Bien entendu, cette bande passante devra être inférieure à la bande de protection sur le lien L, c'est-à-dire $BP(\Phi,L) \leq RBP(L)$.

La méthode de protection selon le second mode de réalisation comprend également une phase d'admission générale et une phase d'admission locale.

La phase d'admission générale du second mode diffère de celle du premier mode lorsqu'une protection de la bande passante est requise.

Lors de la première étape où le PLR cherche à utiliser un tunnel de bypass existant, au lieu de simuler l'augmentation de la bande passante rBP(L), on calcule pour chaque lien L du tunnel candidat la nouvelle bande passante qu'il faudrait réserver pour protéger l'élément en question du chemin LSP, soit $rBP(L)=\max(BP(\Phi,L))$ où $\Phi \in LFRG(L)$, étant entendu que pour ce calcul, on a supposé que le tunnel de bypass candidat passait par le lien L.

On teste ensuite si la condition $rBP(L) \leq RBP(L)$ est vérifiée pour déterminer si le lien L peut encore supporter le tunnel de bypass candidat. Si cette condition est vérifiée pour tous les liens du tunnel bypass candidat, celui-ci est retenu. Les tunnels candidats satisfaisant au critère de compatibilité sont testés l'un après l'autre. Un tunnel est ensuite choisi parmi ceux retenus par exemple selon un critère de taux d'occupation de la bande passante de protection.

De même, pour la seconde étape, c'est-à-dire lorsque l'on doit simuler la construction d'un tunnel de bypass, le critère de sélection d'un lien L doit être modifié de la manière suivante : au lieu de simuler l'augmentation de la bande passante sur le lien candidat, on simule une protection de l'élément considéré et l'on calcule pour le lien L la nouvelle bande passante qu'il faudrait réserver pour accueillir le tunnel de bypass, soit $rBP(L)=\max(BP(\Phi,L))$ où $\Phi \in LFRG(L)$, étant entendu que pour ce

calcul, le tunnel de bypass est supposé passer par le lien L. Comme précédemment, on teste ensuite si la condition rBP(L)≤RBP(L) est vérifiée. Dans l'affirmative, le lien candidat est sélectionné pour la détermination du CSPF.

La phase d'admission locale du second mode diffère de celle du premier mode lorsqu'une protection de la bande passante est requise. Pour un lien L donné du tunnel de bypass, on procède, après avoir vérifié la diversité du lien avec l'élément à protéger, à la modification effective de la bande passante réservée à la protection sur ce lien, soit rBP(L)=max(BP(Φ,L)) et l'on teste à nouveau si la condition rBP(L)≤RBP(L) est vérifiée. Comme dans le premier mode de réalisation, si toutes les vérifications sont positives, on est certain d'avoir une protection efficace de la bande passante du chemin LSP. En revanche, si l'une des étapes de vérification échoue, un message d'erreur est transmis le long du tunnel de bypass au point PLR.

La Fig. 8 illustre schématiquement la méthode de protection locale selon un exemple de réalisation de la présente invention. La demande de protection locale est demandée en 800 par le routeur d'entrée (Ingress LSR) du chemin LSP au moyen de paramètres de protection inclus dans l'objet Session_Attribute Object (SAO) du protocole RSVP-TE. La requête de protection est indiquée par un drapeau dans l'objet SAO.

En outre, un bit de protection locale LPD (Local Protection Bit) dans l'objet SAO indique à chaque PLR si un tunnel de bypass doit être recherché/ construit.

Un bit de protection de nœud NPD (Node Protection Bit) dans l'objet SAO indique à chaque PLR le type de la protection demandée (NNHOP ou NHOP).

Enfin, un bit de protection de bande passante BPD (Bandwith Protection Bit) dans l'objet SAO indique à chaque PLR si le tunnel de bypass doit offrir une protection de la bande passante ou non.

Le point PLR détermine à partir du bit LPD si un tunnel de bypass est demandé et, dans l'affirmative, initie en 810 la phase de GAC. En 811, le point PLR détermine les tunnels de bypass candidats, c'est-à-dire les tunnels existants susceptibles d'assurer la protection demandée. Il vérifie en 812 la condition de diversité pour chaque lien de chaque tunnel de bypass candidat. Si pour un lien quelconque elle n'est pas vérifiée, le candidat n'est pas retenu. En 813, on teste si au moins un candidat est retenu. Dans la négative on passe directement à l'étape de construction 817. Pour

chaque candidat retenu, on simule en 814 la protection du chemin LSP par le tunnel de bypass candidat et l'on calcule la nouvelle valeur de bande passante à réserver (selon le premier mode ou le second mode de réalisation) pour chaque lien du bypass. On teste en 815 si la bande passante de protection sur le lien est suffisante pour autoriser cette valeur. Le test est effectué pour chaque lien du bypass. On vérifie en 816 si le test est positif pour tous les liens du bypass candidat. Si c'est le cas, le PLR transmet un message « Path » et l'on passe à la phase d'admission locale. Dans le cas contraire on passe au candidat suivant jusqu'à ce qu'ils aient été tous testés. Selon une variante, si plusieurs candidats retenus satisfont à la condition de bande passante, on en choisira un selon un critère prédéterminé, par exemple un critère d'occupation de la bande passante de protection.

Si tous les candidats ont été testés et aucun finalement retenu, on simule en 817 la création d'un nouveau tunnel de bypass, en ne considérant que les liens du réseau qui satisfont aux conditions de diversité et de bande passante, comme expliqué plus haut. Le chemin CSPF est ensuite calculé en 818. Le PLR teste en 819 si un tunnel de bypass a pu être construit. Dans la négative, il en avertit le routeur d'entrée. Dans l'affirmative, le PLR transmet un message « Path » et l'on passe à la phase d'admission locale.

Chaque lien du tunnel de bypass initie en 820 un contrôle d'admission locale et vérifie en 821 si la condition de diversité est encore vérifiée. Dans la négative, un message d'erreur est transmis au PLR. Si elle est bien vérifiée, on teste en 822 si la condition de suffisance de bande passante de protection est vérifiée et dans l'affirmative on met à jour en 823 la valeur de bande passante réservée rBP(L). Dans la négative, on transmet un message d'erreur au PLR. Le contrôle d'admission locale se termine en 824.

La mise en oeuvre de la méthode de protection selon l'invention suppose que chaque nœud du réseau susceptible d'être PLR ait accès à un certain nombre d'informations comme la bande passante de protection RBP(L) sur chaque lien L, la bande passante réservée rBP(L), les tunnels de bypass existants et leurs caractéristiques. Ces informations font l'objet d'annonces dans le réseau et servent à mettre à jour les bases de données locales TED. Réciproquement, lorsqu'un point PLR retient un tunnel de bypass existant pour protéger un nouvel élément du réseau ou

lorsqu'il crée un nouveau tunnel de bypass (utilisant ou non des ressources de tunnels existants) ce tunnel de bypass doit être signalé au réseau.

Avantageusement, les annonces sont réalisées au moyen d'une extension du protocole OSPF-TE ou bien d'une extension du protocole ISIS-TE. On trouvera notamment une description du protocole OSPF-TE dans le document de D. Katz et al. intitulé « Traffic Engineering Extensions to OSPF » et du protocole ISIS-TE dans le document de H. Smit et al. intitulé « IS-IS extensions for Traffic Engineering ». Ces deux documents sont disponibles sur le site de l'IETF précité. On rappelle que les protocoles OSPF-TE et ISIS-TE permettent de diffuser sur le réseau des informations nécessaires à l'ingéniérie de trafic comme les liens immédiats de chaque nœud et les contraintes (par exemple la bande passante maximale réservable, la métrique etc.) associées à chaque lien. Ces informations sont transmises sous forme de messages comprenant un en-tête et un certain nombre de données, chacune se présentant sous un format dit TLV (pour Type, Length, Value) indiquant le type, la longueur et la valeur de la donnée. Une donnée sous ce format, appelée encore par assimilation TLV, peut comprendre d'autre données selon un format TLV, appelées pour cette raison sub-TLV.

Les protocoles OSPF-TE et ISIS-TE peuvent être étendus en ajoutant de nouveaux TLV ou de nouveaux sub-TLV dans les TLV existants.

Ainsi, le TLV donnant les caractéristiques d'un lien (Link TLV dans le protocole OSPF-TE et IS reachability dans le protocole ISIS-TE) est étendu au moyen des sub-TLV suivants :

- sub-TLV indiquant la bande passante de protection réservable (RBP(L)) sur ce lien
- sub-TLV indiquant la bande passante sur ce lien effectivement réservée à la protection rBP(L)
- sub-TLV indiquant la liste SRLG de ce lien.

On introduit également un nouveau TLV, dénommé bypass TLV, donnant les caractéristiques d'un tunnel de bypass et comprenant trois sub-TLV :

- sub-TLV « Tail Router Id » donnant l'adresse IP servant à identifier le nœud PM (Point of Merging) où le tunnel de bypass rejoint le chemin LSP protégé
- sub-TLV « Path » donnant le chemin emprunté par le tunnel de bypass
- sub-TLV « Information » donnant le type de tunnel de bypass (NHOP, NNHOP), l'adresse IP du nœud protégé (si type=NNHOP), les adresses IP locale (adresse IP du point PLR) et distante (adresse IP du nœud en aval du point PLR) du lien protégé (si type=NHOP) et la bande passante du tunnel de bypass.

En outre, la phase d'admission locale du tunnel de bypass suppose que l'on étende le protocole RSVP-TE en modifiant notamment le message « Path ». Un nouvel objet est introduit dans ce message pour définir le tunnel de bypass. Il contient les champs suivants :

- type de bypass (NHOP ou NNHOP)
- adresse IP du nœud protégé, si type=NNHOP
- adresse IP du point PLR en amont du lien protégé (adresse IP locale), si type=NHOP
- adresse IP du nœud en aval (PLR next hop) du lien protégé, (adresse IP distante), si type=NHOP
- liste SRLG du lien protégé s'il s'agit d'un lien ou du lien joignant ledit point PLR et le nœud en aval dudit point PLR, s'il s'agit d'un nœud.

Bien entendu, l'homme du métier peut étendre le protocole CR-LDP de manière équivalente.

REVENDICATIONS

1) Méthode de protection d'un chemin à commutation d'étiquettes dans un réseau MPLS comprenant une pluralité de nœuds reliés par des liens IP, ledit chemin commençant à un nœud d'entrée et se terminant à un nœud de sortie dudit réseau en passant par une série déterminée de nœuds et de liens dudit réseau, dits éléments dudit chemin, caractérisée en ce que, lorsque ledit nœud d'entrée requiert la protection d'un élément du chemin, dans une première phase, un nœud dudit chemin, dit point PLR, en amont dudit élément à protéger détermine un chemin de secours, dit tunnel de bypass, rejoignant le chemin en aval dudit élément à protéger en un nœud, dit point PM, et, dans une seconde phase, des ressources du réseau sont réservées sur chacun des liens du tunnel de bypass pour secourir ledit chemin en cas de défaillance dudit élément.

2) Méthode de protection selon la revendication 1, caractérisée en ce que lesdites ressources sur un lien du tunnel de bypass comprennent une bande passante réservée (rBP(L)) relative à ce lien.

3) Méthode de protection selon la revendication 1 ou 2, caractérisée en ce que, pour chaque élément physique dudit réseau, on détermine un groupe (SRLG) de liens dudit réseau atteints par la défaillance dudit élément physique.

4) Méthode de protection selon la revendication 3, caractérisée en ce que pour chaque lien dudit réseau, on détermine la liste, dite liste SRLG, desdits groupes auxquels il appartient.

5) Méthode de protection selon l'une des revendications précédentes, caractérisée en ce que le point PLR recherche, dans une première étape de la première phase, les tunnels de bypass existants dans le réseau susceptibles de protéger ledit élément.

6) Méthode de protection selon les revendications 4 et 5, caractérisée en ce que, si l'élément à protéger est un lien, le point PLR détermine si un tunnel de bypass existant est susceptible de protéger ledit lien en vérifiant que ledit tunnel ne comprend pas ledit lien et que, la liste SRLG associée à chaque lien dudit tunnel existant et la liste SRLG associée au lien à protéger ont une intesection vide.

7) Méthode de protection selon les revendications 4 et 5, caractérisée en ce que, si l'élément à protéger est un nœud, le point PLR détermine si un tunnel de bypass existant est susceptible de protéger le nœud en vérifiant que ledit tunnel ne comprend pas ledit nœud et que la liste SRLG associée à chaque lien dudit tunnel existant et la liste SRLG associée au lien joignant le point PLR et ledit nœud ont une intesection vide.

8) Méthode de protection selon la revendication 6 ou 7, caractérisée en ce que, pour chaque tunnel de bypass existant susceptible de protéger ledit élément, dit tunnel candidat, le point PLR simule, pour chaque lien du tunnel candidat, une augmentation de la bande passante réservée sur ce lien de la valeur de la bande passante du chemin à étiquettes commutées et vérifie si la valeur de la bande passante ainsi obtenue est inférieure à une bande passante maximale (RBP(L)) réservable sur ce lien .

9) Méthode de protection selon la revendication 6 ou 7, caractérisée en ce que pour chaque tunnel de bypass existant susceptible de protéger ledit élément, dit tunnel candidat, le point PLR simule une protection dudit élément par ledit tunnel candidat et détermine, pour chaque lien dudit tunnel candidat, la plus grande bande passante à réserver sur ce lien pour supporter les tunnels de bypass passant par ce lien, y compris le tunnel candidat, en cas de défaillance d'un élément physique quelconque du réseau et que l'on vérifie si ladite plus grande bande passante est inférieure à une bande passante maximale (RBP(L)) réservable sur ce lien .

10) Méthode de protection selon la revendication 8 ou 9, caractérisée en ce que s'il n'existe aucun tunnel candidat ou si la vérification est négative pour au moins un lien de chaque tunnel candidat, le point PLR détermine un nouveau tunnel de bypass.

11) Méthode de protection selon l'une des revendications précédentes, caractérisée en ce que, dans ladite seconde phase, le point PLR transmet un premier message (Path) se propageant de nœud en nœud sur le tunnel de bypass vers le point PM et qu'un second message (Resv) est retourné le long tunnel de bypass vers le point PLR, et que lors du passage du premier ou du second message, on vérifie pour chaque lien du tunnel de bypass, qu'il est susceptible de protéger ledit élément et que lesdites ressources sont effectivement disponibles sur ce lien, et dans l'affirmative on procède à la réservation desdites ressources.

12) Message de protocole RSVP-TE ou CR-LDP destiné à être transmis lors de la seconde phase de la méthode selon l'une des revendications précédentes, caractérisé en ce qu'il comprend les champs suivants :

- type du tunnel de bypass, indiquant s'il protège un nœud ou un lien du chemin à commutation d'étiquettes ;
- adresse IP du nœud protégé, s'il s'agit d'un nœud
- adresse IP du point PLR, s'il s'agit d'un lien ;
- adresse IP du nœud en aval dudit point PLR, s'il s'agit d'un lien ;
- liste SRLG du lien protégé s'il s'agit d'un lien ou du lien joignant ledit point PLR et le nœud en aval dudit point PLR, s'il s'agit d'un nœud.

13) Message de protocole OSPF-TE ou ISIS-TE destiné à être transmis par un nœud du réseau MPLS pour la mise en œuvre de la méthode selon l'une des revendications 1 à 11, ledit message étant relatif à un lien donné du réseau MPLS, caractérisé en ce qu'il comprend les champs suivants :

- bande passante réservable à la protection sur ledit lien ;
- bande passante sur ledit lien effectivement réservée à la protection ;
- liste SRLG dudit lien.

14) Message de protocole OSPF-TE ou ISIS-TE destiné à être transmis par un nœud du réseau MPLS pour la mise en œuvre de la méthode selon l'une des revendications 1 à 11, ledit message étant relatif à un tunnel de bypass du réseau MPLS, caractérisé en ce qu'il comprend les champs suivants :

- adresse IP du point PM dudit tunnel de bypass ;

- identification du chemin emprunté par ledit tunnel de bypass ;
- type dudit tunnel de bypass indiquant s'il protège un nœud ou un lien du chemin à commutation d'étiquettes ; adresse IP du nœud protégé, s'il s'agit d'un nœud ; adresse IP du point PLR et adresse IP du nœud en aval dudit point PLR, s'il s'agit d'un lien ; bande passante dudit tunnel de bypass.

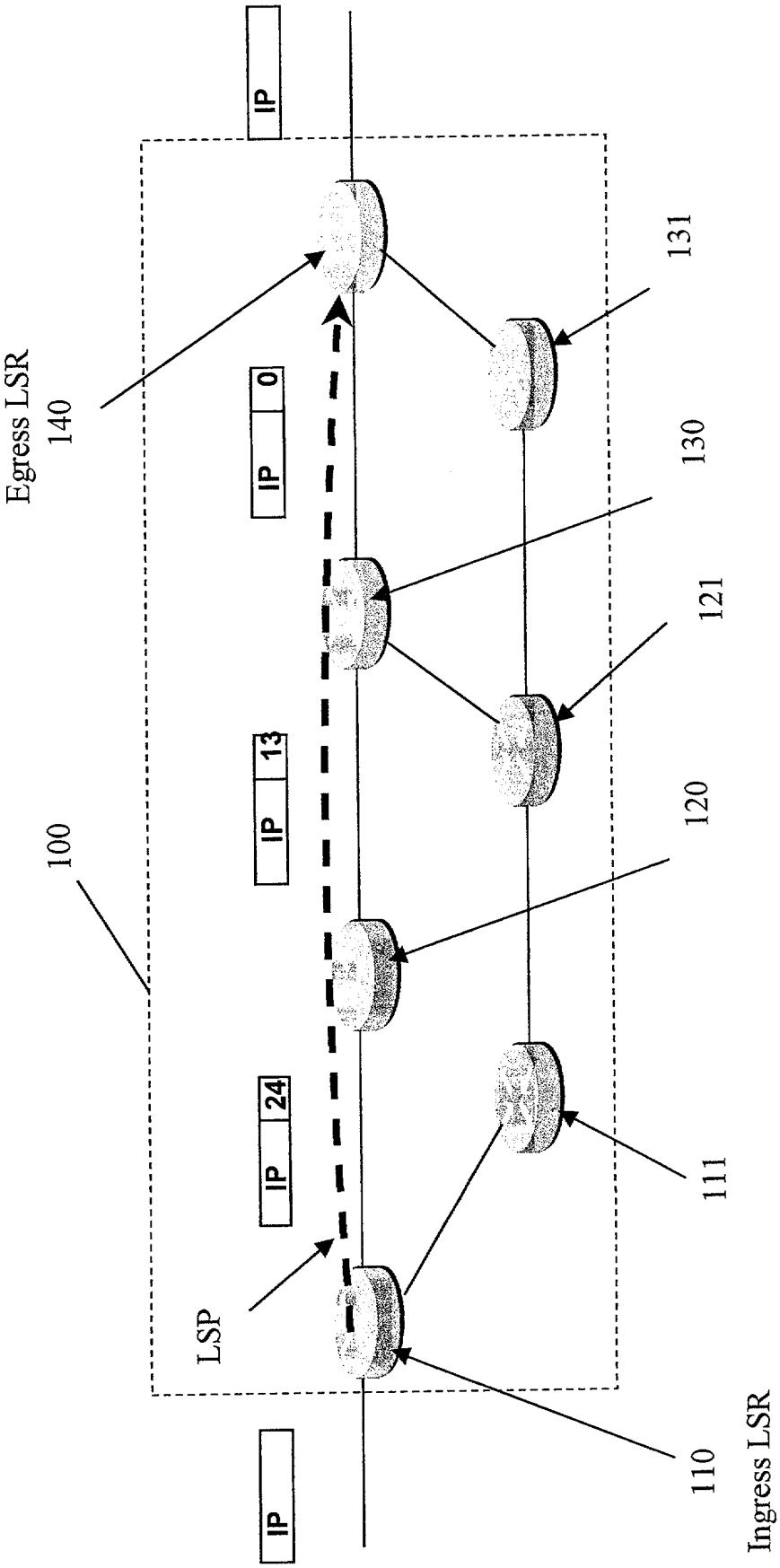
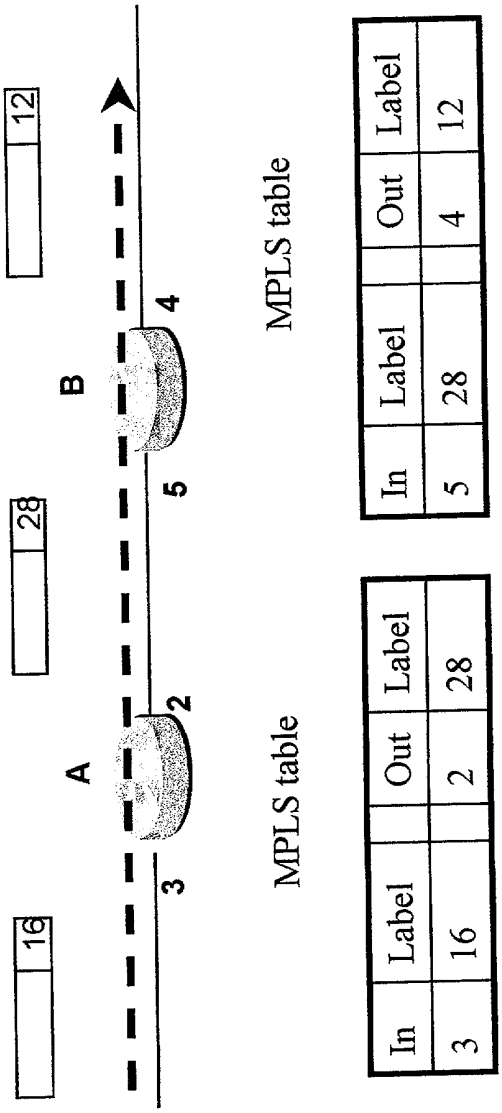

IP
Egress LSR
140
IP 0
131
130
IP 13
121
100
120
IP 24
LSP
111
IP
110
Ingress LSR

Fig. 1



MPLS table

In	Label	Out	Label
3	16	2	28

MPLS table

In	Label	Out	Label
5	28	4	12

Fig. 2

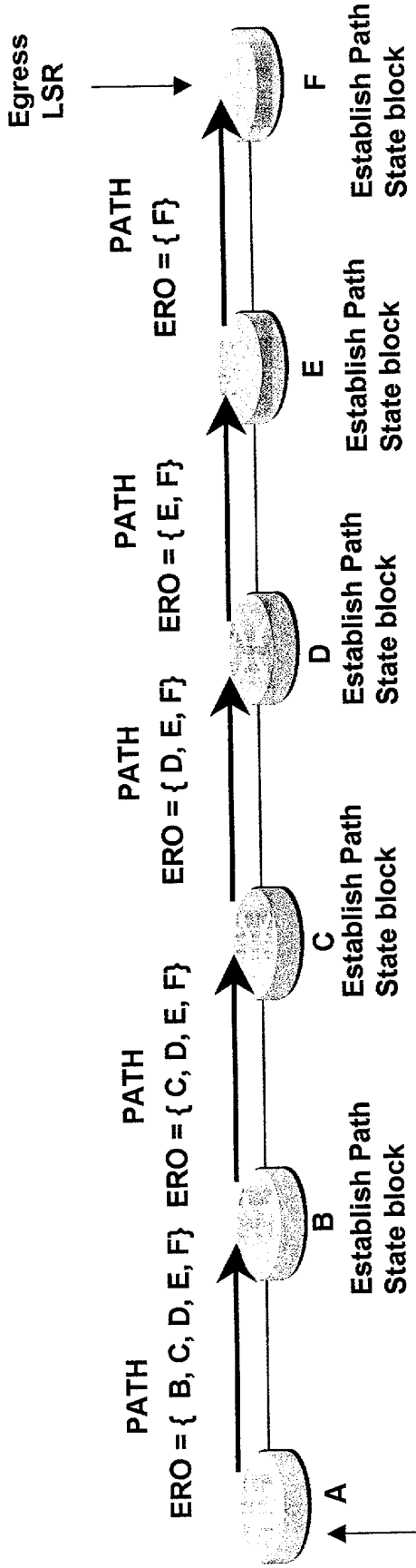

Egress LSR
PATH
ERO = { B, C, D, E, F}
PATH
ERO = { C, D, E, F}
PATH
ERO = { D, E, F}
PATH
ERO = { E, F}
PATH
ERO = { F}
A
B
C
D
E
F
Establish Path State block
Establish Path State block
Establish Path State block
Establish Path State block
Establish Path State block
Ingress LSR

Fig. 3A

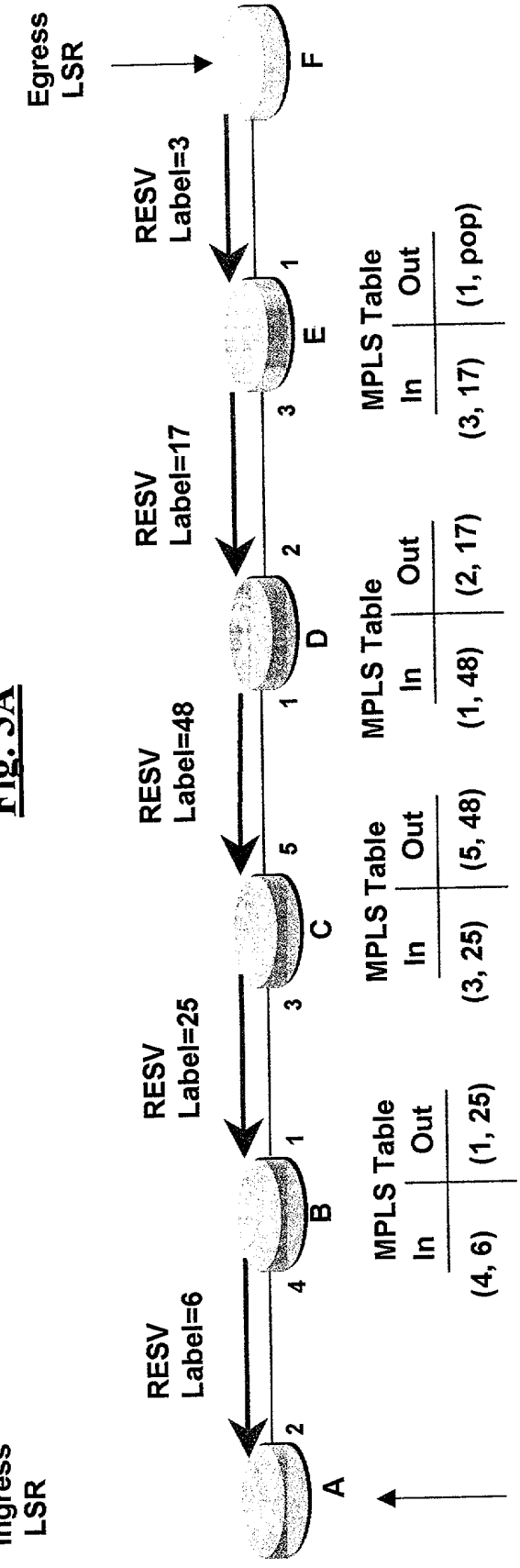

Egress LSR
RESV Label=3
RESV Label=17
RESV Label=48
RESV Label=25
RESV Label=6
A
B
C
D
E
F
1
2
3
4
5
MPLS Table
In | Out
(4, 6) | (1, 25)
MPLS Table
In | Out
(3, 25) | (5, 48)
MPLS Table
In | Out
(1, 48) | (2, 17)
MPLS Table
In | Out
(3, 17) | (1, pop)
Ingress LSR

Fig. 3B

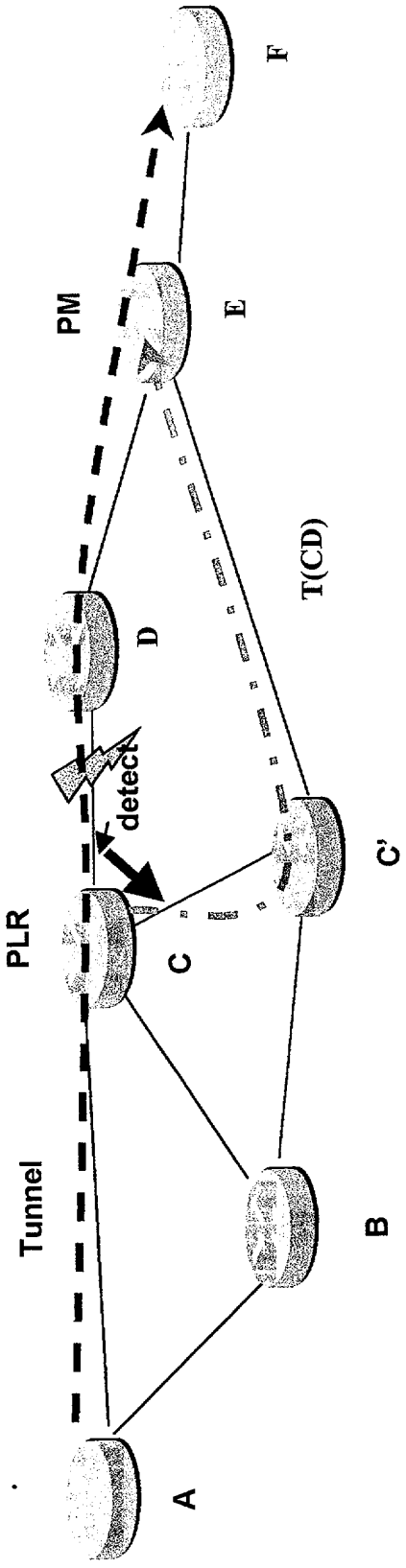


Fig. 4

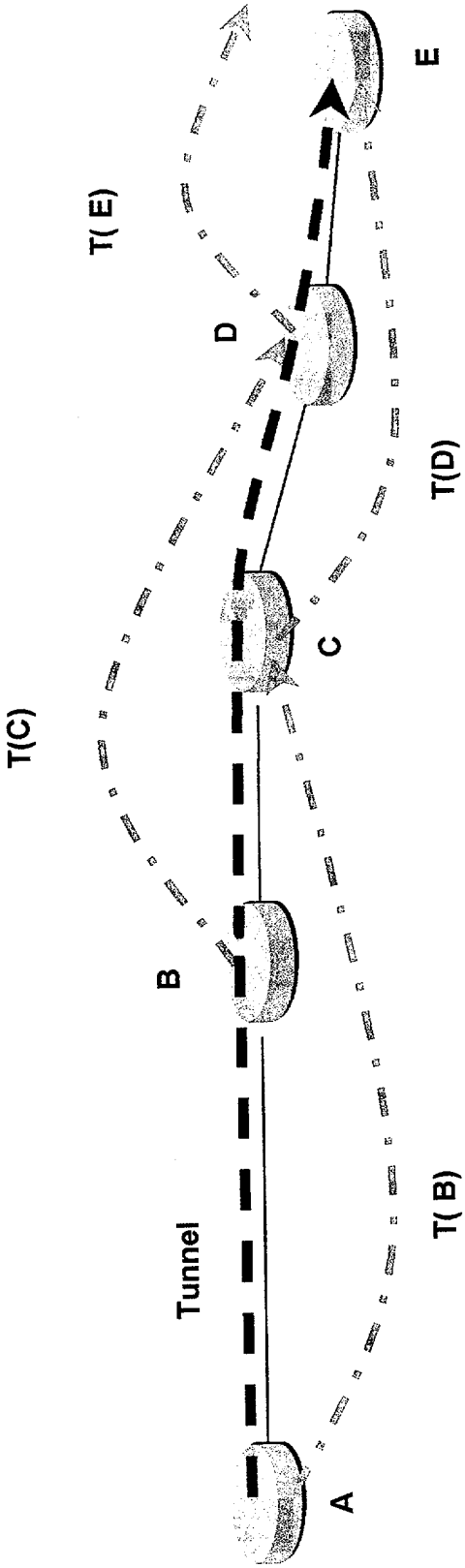


Fig. 5

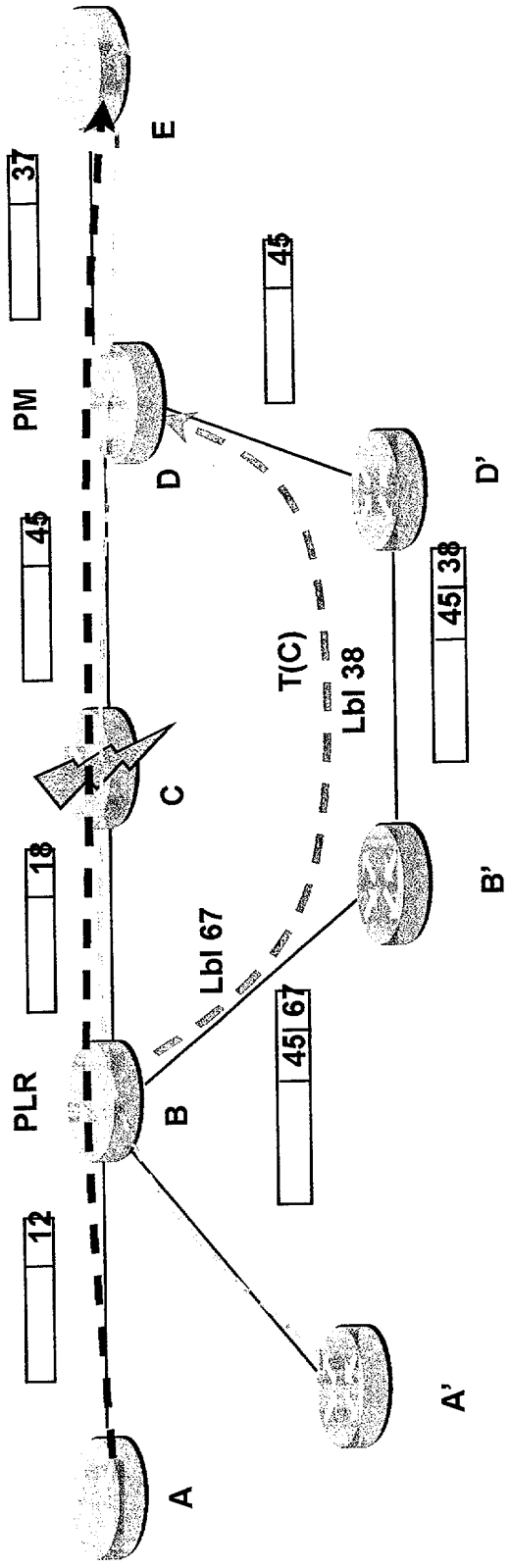


Fig. 6

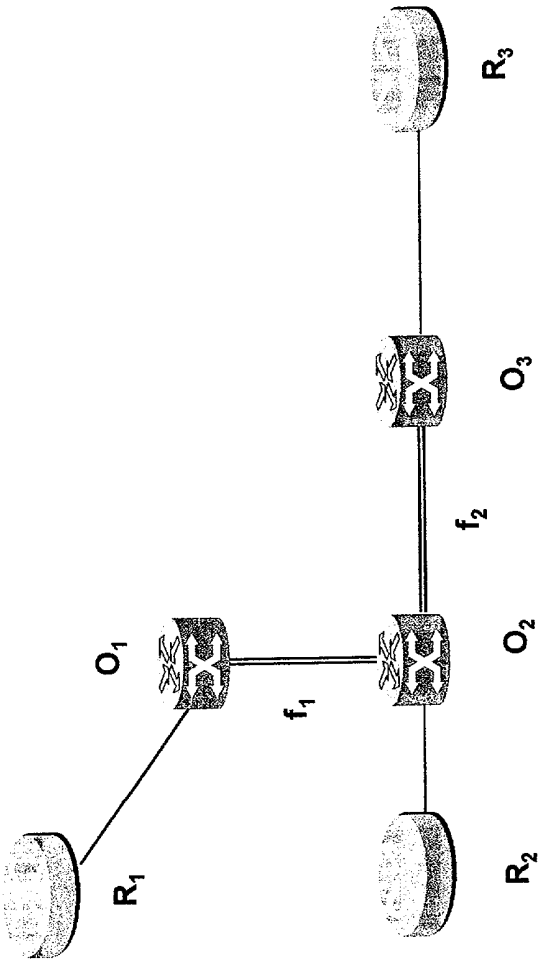


Fig. 7

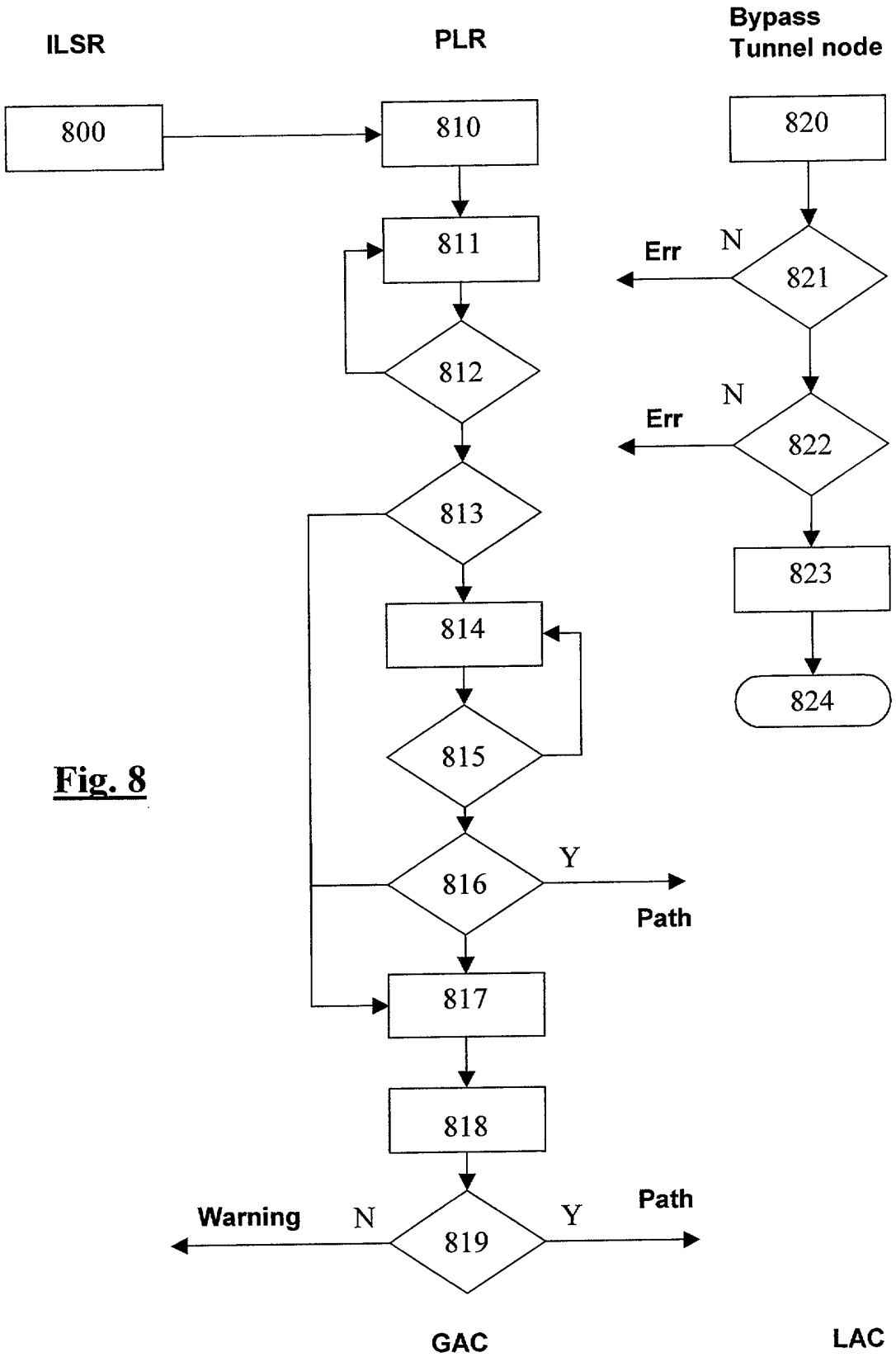

ILSR
PLR
Bypass Tunnel node
800
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
Err
N
Err
N
Y
Path
Warning
N
Y
Path
GAC
LAC

Fig. 8

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

2836314
N° d'enregistrement national

FA 617363
FR 0202437

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	P. PAN, D. GAN, G. SWALLOW, JP. VASSEUR, D. COOPER, A. ATLAS, M. JORK: "Fast Reroute Extensions to RSVP-TE for LSP Tunnels" IETF INTERNET DRAFT, 'en ligne! janvier 2002 (2002-01), pages 1-33, XP002222575 Extrait de l'Internet: <URL:http://www.watersprings.org/pub/id/draft-ietf-mpls-rsvp-lsp-fastreroute-00.txt> 'extrait le 2002-11-26! * alinéa '001.! * * alinéa '01.2! * * alinéa '03.1! * * alinéa '03.4! * * alinéa '06.2! * * alinéa '07.1! * * page 20, ligne 30 - page 21, ligne 1 * * page 26, ligne 4 - ligne 8 *	1-7,11	H04L12/24 H04L12/56 G06F11/30
Y A	---	8,9,13 10,12,14	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
Y	MANER A ET AL: "On-demand optimization of label switched paths in MPLS networks" COMPUTER COMMUNICATIONS AND NETWORKS, 2000. PROCEEDINGS. NINTH INTERNATIONAL CONFERENCE ON LAS VEGAS, NV, USA 16-18 OCT. 2000, PISCATAWAY, NJ, USA,IEEE, US, 16 octobre 2000 (2000-10-16), pages 107-113, XP010524495 ISBN: 0-7803-6494-5 * page 107, colonne de droite, ligne 8 - ligne 24 *	8	H04L
	--- -/--		

Date d'achèvement de la recherche	Examinateur
28 novembre 2002	Perrier, S

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

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2836314

N° d'enregistrement national

FA 617363
FR 0202437

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

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		
Y	KODIALAM M ET AL: "Dynamic routing of locally restorable bandwidth guaranteed tunnels using aggregated link usage information" PROCEEDINGS IEEE INFOCOM 2001. THE CONFERENCE ON COMPUTER COMMUNICATIONS. 20TH. ANNUAL JOINT CONFERENCE OF THE IEEE COMPUTER ANDCOMMUNICATIONS SOCIETIES. ANCHORAGE, AK, APRIL 22 - 26, 2001, PROCEEDINGS IEEE INFOCOM. THE CONFERENCE ON COMPUTER COMMUNI, vol. 1 OF 3. CONF. 20, 22 avril 2001 (2001-04-22), pages 376-385, XP010538718 ISBN: 0-7803-7016-3 * page 379, colonne de droite, ligne 31 - page 378, colonne de droite, ligne 37 * ---	9	
A	AWDUCHE D., BERGER L., GAN D., LI T., SRINIVANSAN V., SWALLOW G.: "RSVP-TE: Extensions to RSVP for LSP Tunnels" IETF RFC 3209, 'en ligne! décembre 2001 (2001-12), pages 1-61, XP002222576 Extrait de l'Internet: <URL:http://www.cs.utk.edu/{moore/RFC-PDF/rfc3209.pdf> 'extrait le 2002-11-27! * page 3, ligne 33 - ligne 39 * * alinéa '02.2! * --- -/--	11	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

Date d'achèvement de la recherche	Examinateur
28 novembre 2002	Perrier, S

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

2

EPO FORM 1503 12.99 (P04C14)

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

2836314 N° d'enregistrement national

FA 617363
FR 0202437

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		
Y	P. SRISURESH, P. JOSEPH: "TE LSAs to extend OSPF for Traffic Engineering" IETF DRAFT, 'en ligne! 4 janvier 2002 (2002-01-04), pages 1-41, XP002222577 Extrait de l'Internet: <URL:http://www.watersprings.org/pub/id/draft-srisuresh-ospf-te-02.txt> 'extrait le 2002-11-27! * alinéa '09.1! * * alinéa '9.1.4! * -----	13	

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

Date d'achèvement de la recherche	Examinateur
28 novembre 2002	Perrier, S

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

2

EPO FORM 1503 12.99 (P04C14)