(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 836 313**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **02 02436**

(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.

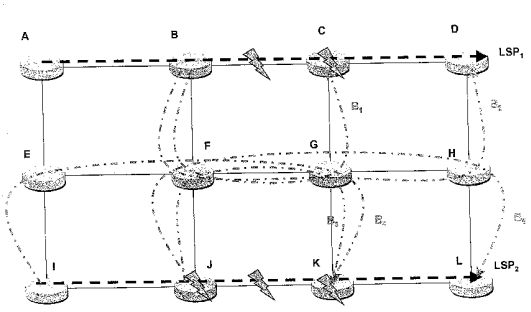
(72) **Inventeur(s) :** LE ROUX JEAN LOUIS, CALVIGNAC GERALDINE et MOIGNARD RENAUD.

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

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

(54) METHODE DE PROTECTION LOCALE DE CHEMINS A COMMUTATION D'ETIQUETTES AVEC PARTAGE DE RESSOURCES.

(57) L'invention concerne une méthode de protection de chemins à commutation d'étiquettes dans un réseau MPLS comprenant une pluralité de nœuds reliés par des liens IP, chaque chemin passant par une série déterminée de nœuds et de liens dudit réseau, dits éléments dudit chemin. Un élément d'un premier chemin ayant été protégé à l'aide d'un chemin, dit de bypass du premier chemin, partant d'un noeud du premier chemin en amont dudit élément à protéger et se terminant en un noeud du premier chemin en aval dudit élément à protéger, un certain nombre de ressources du réseau ayant été réservées pour ledit chemin de bypass du premier chemin, ce dernier étant actif en cas de défaillance dudit élément du premier chemin, on protège un élément d'un second chemin à l'aide d'un chemin, dit de bypass du second chemin, partant d'un noeud du second chemin en amont de cet élément et se terminant en un noeud du second chemin en aval de cet élément, le chemin de bypass du second chemin utilisant au moins une partie des ressources réservées pour le chemin de bypass du premier chemin.



FR 2 836 313 - 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.

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 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 déterminé selon un mode explicite est encore appelé tunnel MPLS.

La détermination d'un ou des tunnels MPLS 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 commutaion 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, 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 tunnel 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 tunnel initial sur le tunnel de bypass CC'E. La jonction entre le tunnel 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 chemin comporte n nœuds, il peut

donc y avoir jusqu'à (n-1) détours. Si plusieurs chemins 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 tel tunnel de bypass peut alors 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.

Il est important de noter que les tunnels de bypass sont déterminés au préalable, de manière statique et/ou centralisée par un serveur sans tenir compte *a priori* des besoins en ressources des futurs chemins LSP à établir. 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 consomme moins de ressources que les méthodes de protection connues de l'état de la technique, tout en garantissant un degré élevé d'extensibilité (scalability) et une bonne garantie d'efficacité.

Le problème est résolu par l'objet de l'invention, défini comme une méthode de protection de chemins à commutation d'étiquettes dans un réseau MPLS comprenant une pluralité de nœuds reliés par des liens IP, un chemin passant par une série déterminée de nœuds et de liens dudit réseau, dits éléments dudit chemin. Un élément d'un premier chemin ayant été protégé à l'aide d'un chemin, dit de bypass du premier chemin, partant d'un nœud du premier chemin en amont dudit élément à protéger et se terminant en un nœud du premier chemin en aval dudit élément à protéger et un certain nombre de ressources du réseau ayant été réservées pour ledit chemin de bypass du premier chemin, ce dernier étant actif en cas de défaillance dudit élément du premier chemin, on protège un élément d'un second chemin à l'aide d'un chemin, dit de bypass du second chemin, partant d'un nœud du second chemin en amont de cet élément et se terminant en un nœud du second chemin en aval de cet élément, le chemin de bypass du second chemin utilisant au moins une partie des ressources réservées pour le chemin de bypass du premier chemin .

On peut ainsi économiser les ressources du réseau en les partageant entre les premier et second chemins.

Avantageusement, si l'élément à protéger du second chemin est un lien, on sélectionne ledit chemin de bypass dudit second chemin parmi une pluralité de chemins candidats ne comprenant pas ledit lien, la sélection étant effectuée en testant si chaque lien du chemin candidat présente un risque de défaillance indépendant du risque de défaillance dudit lien à protéger.

Pour ce faire, on détermine pour chaque élément physique dudit réseau, un groupe de liens dudit réseau atteints par la défaillance dudit élément physique.

Réciproquement, pour chaque lien dudit réseau, on détermine la liste desdits groupes auxquels il appartient.

Pour tester si un lien du chemin candidat présente un risque de défaillance indépendant du risque de défaillance dudit lien à protéger, on détermine si les listes

desdits groupes, respectivement associées au lien à protéger et au lien du chemin candidat sont disjointes.

Si l'élément à protéger du second chemin est un nœud, on sélectionne ledit chemin de bypass dudit second chemin parmi une pluralité de chemins candidats ne comprenant pas ledit nœud, la sélection étant effectuée en testant si chaque lien du chemin candidat présente un risque de défaillance indépendant du risque de défaillance du lien, dit lien amont, joignant le nœud (PLR) en amont dudit nœud à protéger et ce dernier nœud.

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 de protection locale de chemins LSP selon la présente invention .

L'idée à la base de l'invention part de la constatation qu'une défaillance dans un réseau n'affecte généralement qu'un seul élément physique du réseau 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. Ainsi, en cas de défaillance d'un élément physique, seuls certains chemins seront affectés. L'idée de base de l'invention est de partager 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. Ainsi, des tunnels de bypass protégeant différents chemins pourront se partager des ressources de protection et économiser les ressources du réseau comme la bande passante. En outre en dimensionnant convenablement, les ressources partagées, on obtiendra une bonne garantie que les chemins à protéger soient effectivement secourus en cas de défaillance.

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, une défaillance de SRLG peut intervenir indépendamment de la défaillance d'un lien. Ainsi, dans l'exemple précédent, la défaillance du lien R_2O_2 connectant R_2 à O_2 entraîne une défaillance du lien R_2R_3 mais non du SRLG S_3. De manière générale si un lien n'appartient pas à un SRLG, la défaillance de ce lien n'entraînera pas celle du SRLG.

On supposera dans ce qui suit que la probabilité pour que le réseau soit affecté de plus d'une défaillance de nœud ou de lien ou de SRLG est faible.

On distingue 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).

Un tunnel NNHOP bypass commence à un point PLR et se termine deux bonds en aval, voire plus loin. Bien entendu, il ne doit pas utiliser le nœud qu'il protège ni le lien en aval du point PLR. Il doit également présenter une diversité de SRLG avec ce dernier. On notera qu'un tunnel NNHOP bypass protège non seulement le nœud en aval du point PLR mais également le lien en aval de ce dernier.

On définit également 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 B 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.

On supposera par la suite qu'un tunnel de bypass protège un lien ou un nœud (c'est-à-dire est du type NHOP ou NNHOP). On dira que deux tunnels de bypass présentent une diversité de FRG (Failure Risk Group) si :

- ils ne protègent pas le même lien
- ils ne protègent pas le même nœud
- les liens qu'ils protègent présentent une diversité de SRLG

Comme précédemment, 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(Φ,L), la bande passante réservée ou à réserver sur ce lien pour protéger Φ. Il convient de préciser que l'on entend ici par bande passante une bande passante logique et non une bande passante physique. Plus précisément la bande passante physique d'une ressource physique pourra comportera une bande passante primaire dédiée au trafic normal et une bande passante secondaire dédiée à la protection. La totalité de la bande passante de protection secondaire n'est pas nécessairement réservée et pour un lien donné L on distinguera la valeur courante effectivement réservée à la protection rBP(L) de la valeur maximale réservable RBP(L).

On suppose maintenant que plusieurs chemins ont été créés dans le réseau MPLS entre routeurs d'entrée et routeurs de sortie, de manière centralisée ou distribuée comme on l'a vu dans la partie introductive. On cherche à créer des tunnels de bypass qui protégeront les élements (nœud, lien) de chacun de ces chemins. L'opérateur peut avoir spécifié, pour certains de ces éléments ou pour le chemin tout entier, qu'il ne sera pas nécessaire de prévoir une protection. De même, il peut avoir spécifié, que certains éléments du réseau ne seront pas éligibles à une fonction de protection d'un chemin. En tenant compte de ces spécifications, la méthode de détermination des tunnels de bypass opère de la manière suivante, successivement pour chacun des chemins à protéger et dans un chemin, pour chaque élément à protéger:

(1) on détermine s'il existe déjà un tunnel de bypass à partir du PLR et, de manière plus générale, s'il existe déjà dans le réseau des tunnels de bypass dont on peut réutiliser partiellement ou totalement les éléments. On obtient ainsi des tunnels de bypass candidats. Les tunnels de bypass candidats ne peuvent utiliser l'élément à protéger.

(2) dans le cas d'un lien à protéger, on détermine pour chaque lien du tunnel de bypass 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;

(3) dans le cas d'un nœud à protéger, on détermine pour chaque lien du tunnel de bypass 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 ;

(4) dans l'affirmative, en revanche, on simule une protection de d'élément considéré par le tunnel de bypass candidat et on calcule pour chaque lien du tunnel la nouvelle bande passante à réserver, soit rBP(L)=max (BP(Φ,L)) où Φ ∈ LFRG(L);

(5) on teste si la condition rBP(L) ≤ RBP(L) est vérifiée pour tous les liens du tunnel de bypass candidat, dans la négative le tunnel n'est pas retenu ;

(6) la procédure est répétée pour tous les tunnels de bypass candidats.

Un exemple permettra de mieux comprendre la mise en œuvre de la méthode de détermination des tunnels de bypass. Considérons le réseau MPLS de la Fig. 8 et supposons qu'un premier chemin LSP_1=ABCD de bande passante 10 unités ait été établi dans le réseau. On suppose en outre que tous les liens IP ont une bande bassante de trafic de 10 unités, une bande passante de protection de 10 unités sauf le lien FG qui a une bande passante de protection de 20 unités. Les spécifications de l'opérateur indiquent que seuls le lien BC et le nœud C ont besoin d'être secourus. Ces deux éléments sont respectivement protégés par un premier tunnel de bypass NHOP B_1 et un second tunnel de bypass NNHOP B_2 ayant chacune une bande passante de 10 unités. On fait l'hypothèse que la liste SRLG du lien BC est $\{S_1, S_2\}$ et que celle du lien FG est $\{S_3\}$ avec S_1, S_2, S_3 distincts.

Supposons maintenant qu'il faille protéger un second chemin LSP_2=IJKL de bande passante 10 unités. Les spécifications indiquent que seuls le lien JK et les nœuds J et K ont besoin d'être secourus. Aucun tunnel de bypass n'est disponible à partir de I et J. On considère le tunnel de bypass candidat B_3=JFGK réutilisant le lien FG de B_1.

<u>lien JK</u> :

Supposons que le lien JK ait pour liste SRLG=$\{S_3, S_4\}$ avec S_4 distinct de S_1, S_2, S_3 . Dans ce cas, le tunnel de bypass candidat JFGK ne peut être retenu car le lien FG ne présente pas de diversité de SRLG avec le lien JK. Un autre tunnel de bypass doit alors être recherché.

Supposons maintenant que le lien JK ait pour liste SRLG={S_2}. On teste successivement si les liens JF, FG et GK ont une diversité de SRLG avec {S_2}. Dans l'affirmative, le tunnel JFGK peut être retenu. Pour l'être définitivement, le tunnel de bypass JFGK doit offrir une bande passante suffisante pour secourir le trafic sur le lien JK.

On simule la protection de JK par le tunnel de bypass candidat B_3. On obtient :

LFRG(JF)={JK} et rBP(JF)=10
BP(JK,JF)=10

LFRG(GK)={JK} et rBP(GK)=10
BP(JK,GK)=10

LFRG(FG)={BC, C, JK, S_1, S_2}
BP(BC, FG)= bande passante (B_1)+ bande passante (B_2)=20
BP(JK,FG)= bande passante (B_3) =10
BP(C,FG)= bande passante (B_2)=10
BP(S_1,FG)= bande passante (B_1) + bande passante (B_2)=20
BP(S_2,FG)= bande passante (B_1)+ bande passante (B_2) + bande passante (B_3)= 30

On remarque que ce dernier cas correspond à une défaillance de la ressource physique sous-jacente de S_2. Dans ce cas, les liens BC et JK sont simultanément défaillants et les tunnels de bypass B_1, B_2, B_3 sont tous trois activés. Autrement dit, les tunnels B_1, B_2, B_3 ne présentent pas de diversité de FRG.

rBP(FG)=max (BP(Φ, FG)) où $\Phi \in$ LFRG(FG)
c'est-à-dire, rBP(FG)=30≥RBP(FG). Le tunnel B_3 ne peut être retenu.

Supposons maintenant que le lien JK ait pour liste SRLG={S_4}. On teste comme précédemment si les liens JF, FG et GK ont une diversité de SRLG avec {S_4}. Dans l'affirmative, pour que le tunnel JFGK soit définitivement retenu, le tunnel de bypass JFGK doit offrir une bande passante suffisante pour secourir le trafic sur le lien JK.

Le calcul de BP(JK,JF) et BP(JK,GK) est identique à celui ci-dessus. Cependant pour le lien FG :

LFRG(FG)={BC, C, JK, S_1, S_2, S_4}
BP(BC, FG)= bande passante (B_1)+ bande passante (B_2)=20
BP(JK,FG)= bande passante (B_3) =10
BP(C,FG)= bande passante (B_2)=10
BP(S_1,FG)= bande passante (B_1) + bande passante (B_2)=20
BP(S_2,FG)= bande passante (B_1)+ bande passante (B_2)=20
BP(S_4,FG)= bande passante (B_3)=10
c'est-à-dire, rBP(FG)=20. Puisque rBP(FG)≤RBP(FG) le tunnel B_3 est retenu.

Ici la bande de protection à réserver est plus faible car les liens JK et BC présentent une diversité de SRLG. On gardera cette hypothèse dans la suite.

nœud J :

Le chemin B_4=IEFGK est un tunnel de bypass candidat qui présente une diversité de SRLG avec le lien IJ. On obtient :

LFRG(IE)={J} et BP(J,IE)=10

LFRG(EF)={J} et BP(J,EF)=10

LFRG(GK)={J} et BP(J,GK)=10

LFRG(FG)={BC, C, JK, J, S_1, S_2, S_4}
BP(BC,FG)= bande passante (B_1)+ bande passante (B_2)=20
BP(C,FG)= bande passante (B_2)=10
BP(JK,FG)= bande passante (B_3) =10
BP(J,FG)= bande passante (B_4)=10
BP(S_1,FG)= bande passante (B_1) + bande passante (B_2)=20
BP(S_2,FG)= bande passante (B_1)+ bande passante (B_2)=20
BP(S_4,FG)= bande passante (B_3)=10

d'où rBP(FG)=20. Le tunnel B_4 est retenu puisque rBP(FG)≤RBP(FG). On notera que B_4 permet également de protéger le lien IJ sans réservation supplémentaire de bande passante sur le lien FG.

nœud K :

Le chemin B_5=JFGHL est un tunnel de bypass candidat qui présente une diversité de SRLG avec le lien JK. On obtient :

LFRG(JF)={K} et BP(K,JF)=10
LFRG(GH)={K} et BP(K,GH)=10

LFRG(HL)={K} et BP(K,HL)=10

LFRG(FG)= {BC, C, JK, J, K, S_1, S_2, S_4}
BP(BC,FG)= bande passante (B_1)+ bande passante (B_2)=20
BP(C,FG)= bande passante (B_2)=10
BP(JK,FG)= bande passante (B_3) =10
BP(J,FG)= bande passante (B_4)=10
BP(K,FG)=bande passante(B_5)=10
BP(S_1,FG)= bande passante (B_1) + bande passante (B_2)=20
BP(S_2,FG)= bande passante (B_1)+ bande passante (B_2)=20
BP(S_4,FG)= bande passante (B_3)=10

d'où, là aussi, rBP(FG)=20. Le tunnel B_5 est retenu puisque rBP(FG)≤RBP(FG). On notera que B_5 permet également de protéger le lien KL sans réservation supplémentaire de bande passante sur le lien FG.

Selon un premier mode de réalisation, les tunnels de bypass sont créés de manière centralisé par un serveur spécialisé. Celui-ci dispose de la topologie du réseau et connaît les bandes passantes réservées pour le trafic et pour la protection sur chacun des liens du réseau. Il prend en compte également les spécifications de l'opérateur

quant aux éléments non susceptibles de protection et/ou ceux ne pouvant servir à la protection.

Selon un second mode de réalisation, de type distribué, lorsqu'un chemin est établi à travers le réseau, le routeur d'entrée peut spécifier que le chemin en question doit faire l'objet de protection. Pour ce faire, il est prévu une extension du protocole IGP (ou des protocoles ISIS ou OSPF qui sont des protocoles IGP déjà étendus pour l'ingéniérie de trafic) permettant, selon un mécanisme d'inondation, de renseigner chaque nœud non seulement sur la topologie du réseau et sur les tunnels créés, comme dans l'état de la technique, mais également sur les tunnels de bypass déjà créés et les éléments respectifs protégés par ces tunnels. La base de données locale (TED) de chaque nœud contient ainsi une information indiquant les tunnels de bypass créés avec leurs caractéristiques (NHOP, NNHOP, chemin, bande passante, par exemple) ainsi que les éléments qu'ils protègent. Lorsqu'un tunnel de bypass est créé ou détruit, les nœuds du réseau en sont avertis au moyen de messages de création/ destruction permettant de mettre à jour leurs bases de données respectives.

La protection est demandée par le routeur d'entrée au moyen du message « Path » du protocole RSVP-TE, mentionné dans la partie introductive. Plus précisément, ce routeur incorpore dans l'objet « attribut de session » ou SAO (pour Session_Attribute Object) les informations suivantes :

- un bit LPD (Local Protection Desired) indiquant à chaque routeur de transit qu'une protection locale du chemin est requise ;
- un bit NPD (Node Protection Desired) indiquant à chaque routeur de transit qu'un tunnel de bypass de type NNHOP est requis. *A contrario*, un tunnel de bypass de type NHOP est utilisé ;
- un bit BPD (Bandwidth Protection Desired) indiquant à chaque routeur qu'une protection de la bande passante est requise c'est-à-dire que le tunnel de bypass doit offrir une bande passante au moins égale à celle du chemin à protéger.

Lorsqu'un routeur de transit R sur le chemin en question reçoit un message « Path » du protocole RSVP-TE, il recherche tout d'abord si une protection est requise et quel est son type (NHOP, NNHOP). Selon le cas, la protection concerne soit le lien, soit le nœud, en aval du routeur sur le chemin. Le routeur R recherche ensuite dans sa base de données locale s'il existe déjà au moins un tunnel de bypass passant

par R. Si ce n'est pas le cas, il recherche s'il peut construire un tunnel de bypass utilisant partiellement ou entièrement des éléments de tunnels de bypass existants. Le routeur obtient ainsi un certain nombre de tunnels de bypass candidats qui sont soumis aux étapes de sélection (2) à (5) indiquées plus haut. Si l'un des candidats est retenu, le routeur, après qu'il a reçu réception du message « RESV » du protocole RSVP, crée effectivement le tunnel de bypass et lui attribue la bande passante nécessaire. Pour chaque lien L constituant le tunnel de bypass on procède à une réservation de bande passante $rBP(L)=\max(BP(\Phi, L))$ où $\Phi \in LFRG(L)$. Si le routeur de transit ne peut établir de tunnel de bypass, par exemple pour raison de bande passante insuffisante, il en avertit le routeur d'entrée.

Il est clair pour l'homme du métier que la requête de protection et l'acquittement de réservation peuvent également être transmis au moyen du protocole CR-LDP en lieu et place du protocole RSVP-TE.

REVENDICATIONS

1) Méthode de protection de chemins à commutation d'étiquettes dans un réseau MPLS comprenant une pluralité de nœuds reliés par des liens IP, un chemin passant par une série déterminée de nœuds et de liens dudit réseau, dits éléments dudit chemin, caractérisée en ce qu'un élément d'un premier chemin ayant été protégé à l'aide d'un chemin, dit de bypass du premier chemin, partant d'un nœud du premier chemin en amont dudit élément à protéger et se terminant en un nœud du premier chemin en aval dudit élément à protéger, un certain nombre de ressources du réseau ayant été réservées pour ledit chemin de bypass du premier chemin, ce dernier étant actif en cas de défaillance dudit élément du premier chemin, on protège un élément d'un second chemin à l'aide d'un chemin, dit de bypass du second chemin, partant d'un nœud du second chemin en amont de cet élément et se terminant en un nœud du second chemin en aval de cet élément, le chemin de bypass du second chemin utilisant au moins une partie des ressources réservées pour le chemin de bypass du premier chemin .

2) Méthode de protection selon la revendication 1, caractérisée en ce que l'élément à protéger du second chemin étant un lien, on sélectionne ledit chemin de bypass dudit second chemin parmi une pluralité de chemins candidats ne comprenant pas ledit lien, la sélection étant effectuée en testant si chaque lien du chemin candidat présente un risque de défaillance indépendant du risque de défaillance dudit lien à protéger.

3) Méthode de protection selon la revendication 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 desdits groupes auxquels il appartient.

5) Méthode de protection selon la revendication 4, caractérisée en ce que pour tester si un lien du chemin candidat présente un risque de défaillance indépendant du risque de défaillance dudit lien à protéger, on détermine si les listes desdits groupes, respectivement associées au lien à protéger et au lien du chemin candidat sont disjointes.

6) Méthode de protection selon la revendication 1, caractérisée en ce que l'élément à protéger du second chemin étant un nœud, on sélectionne ledit chemin de bypass dudit second chemin parmi une pluralité de chemins candidats ne comprenant pas ledit nœud, la sélection étant effectuée en testant si chaque lien du chemin candidat présente un risque de défaillance indépendant du risque de défaillance du lien, dit lien amont, joignant le nœud (PLR) en amont dudit nœud à protéger et ce dernier nœud.

7) Méthode de protection selon la revendication 6, 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.

8) Méthode de protection selon la revendication 7, caractérisée en ce que, pour chaque lien dudit réseau, on détermine la liste desdits groupes auxquels il appartient.

9) Méthode de protection selon la revendication 8, caractérisée en ce que pour tester si un lien du chemin candidat présente un risque de défaillance indépendant du risque de défaillance dudit lien à protéger, on détermine si les listes desdits groupes, respectivement associées audit lien amont et au lien du chemin candidat sont disjointes.

10) Méthode de protection selon l'une des revendications 2 à 9, caractérisée en ce que lesdits ressources réservées comprennent une bande passante sur un lien dudit réseau.

11) Méthode de protection selon la revendication 10, caractérisée en ce que, pour un lien donné dudit réseau, une bande passante maximale est réservable à la protection et que l'on détermine pour chaque lien du chemin candidat, la plus grande

bande passante à réserver sur ce lien pour supporter le chemin ou les chemins de bypass passant par ce lien en cas de défaillance d'un élément physique quelconque du réseau et l'on teste si ladite plus grande bande passante est inférieure à ladite bande passante maximale.

12) Méthode de protection selon la revendication 11, caractérisée en ce que, pour chaque lien du chemin candidat, on détermine ladite plus grande passante à réserver sur ce lien comme la somme maximale de bandes passantes des chemins de bypass passant par ce lien et pouvant être simultanément actifs.

13) Méthode de protection selon l'une des revendications précédentes, caractérisée en ce que lesdits chemins de bypass sont déterminés de manière centralisé par un serveur.

14) Méthode de protection selon l'une des revendications 1 à 12, caractérisée en ce qu'un chemin de bypass d'un élément d'un chemin à protéger est déterminé par un nœud en amont dudit élément sur ce dernier chemin.

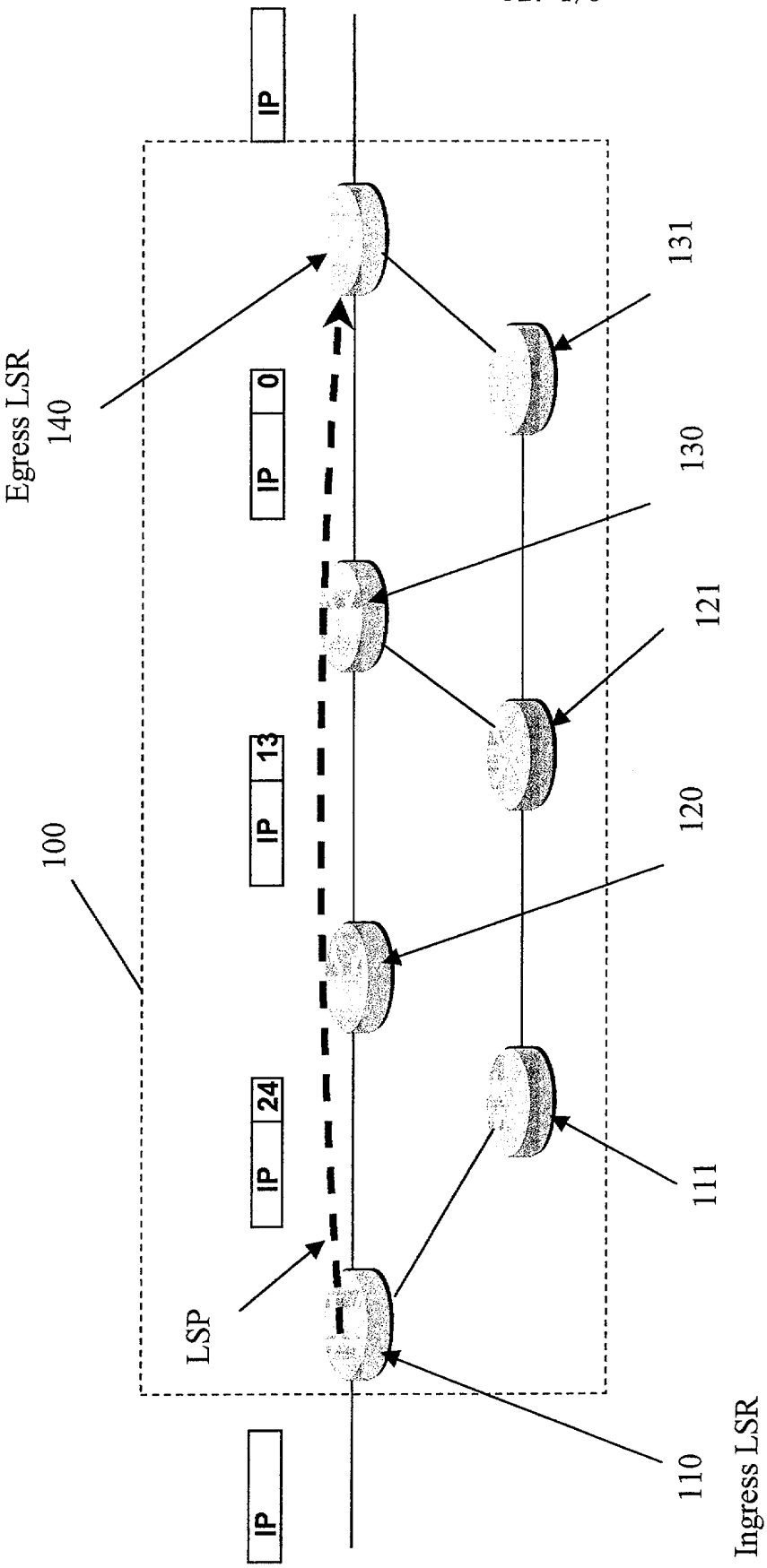
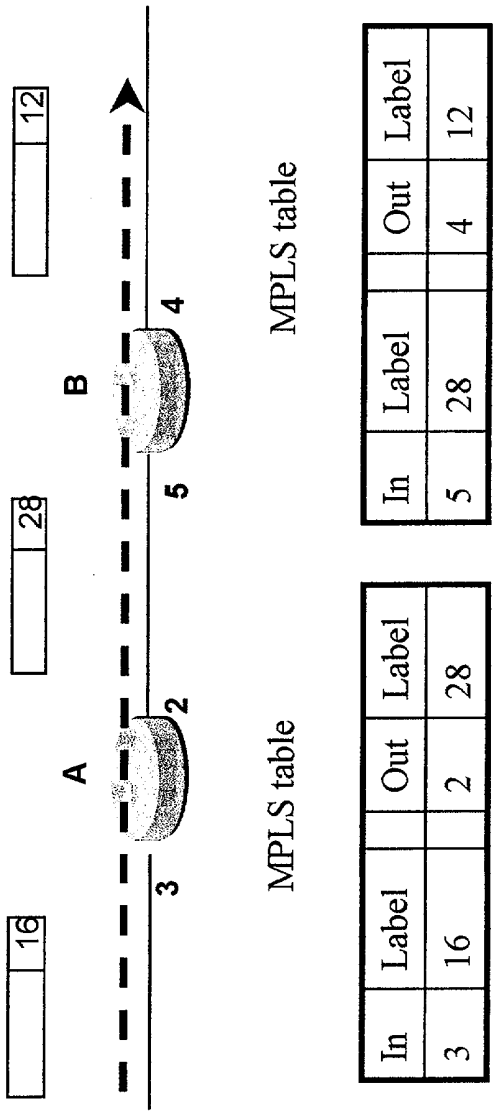

IP
IP 0
IP 13
IP 24
IP
Egress LSR
140
100
LSP
Ingress LSR
110
111
120
121
130
131

Fig. 1



MPLS table

In	Label	Out	Label
3	16	2	28

MPLS table

In	Label	Out	Label
5	28	4	12

Fig. 2

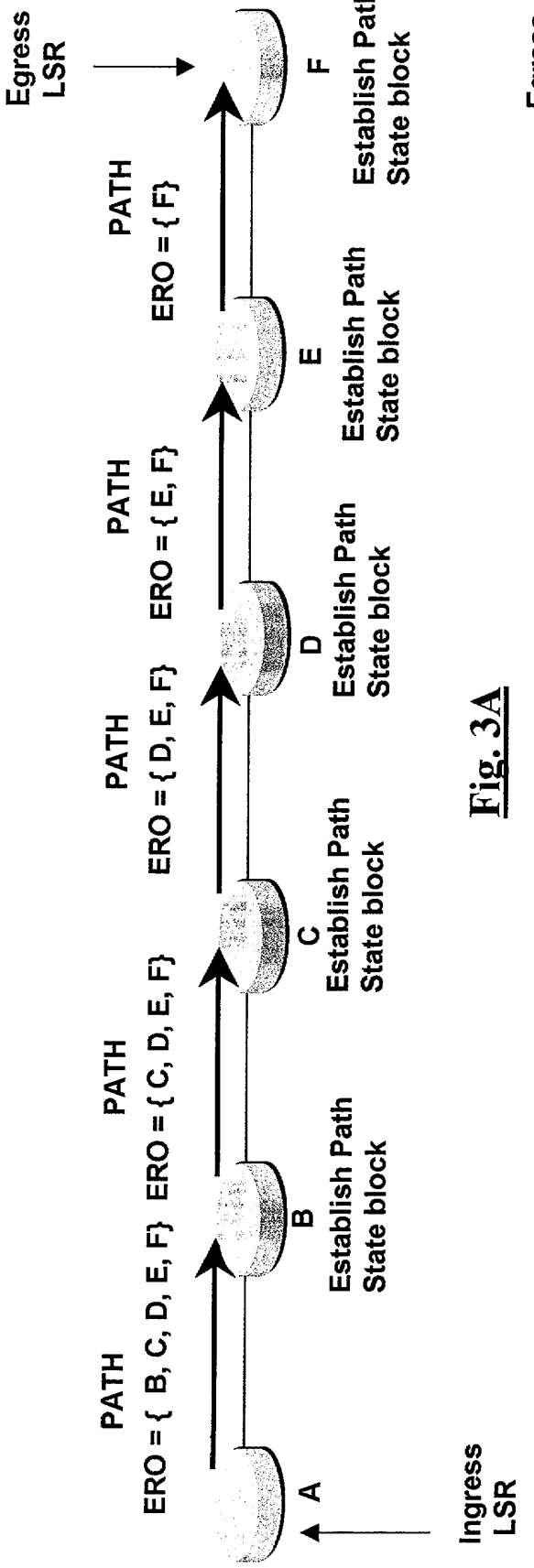

Egress LSR
PATH
ERO = { B, C, D, E, F}
PATH
ERO = { C, D, E, F}
PATH
ERO = { D, E, F}
PATH
ERO = { E, F}
PATH
ERO = { F}
A
B
C
D
E
F
Establish Path State block
Establish Path State block
Establish Path State block
Establish Path State block
Establish Path State block
Ingress LSR

Fig. 3A

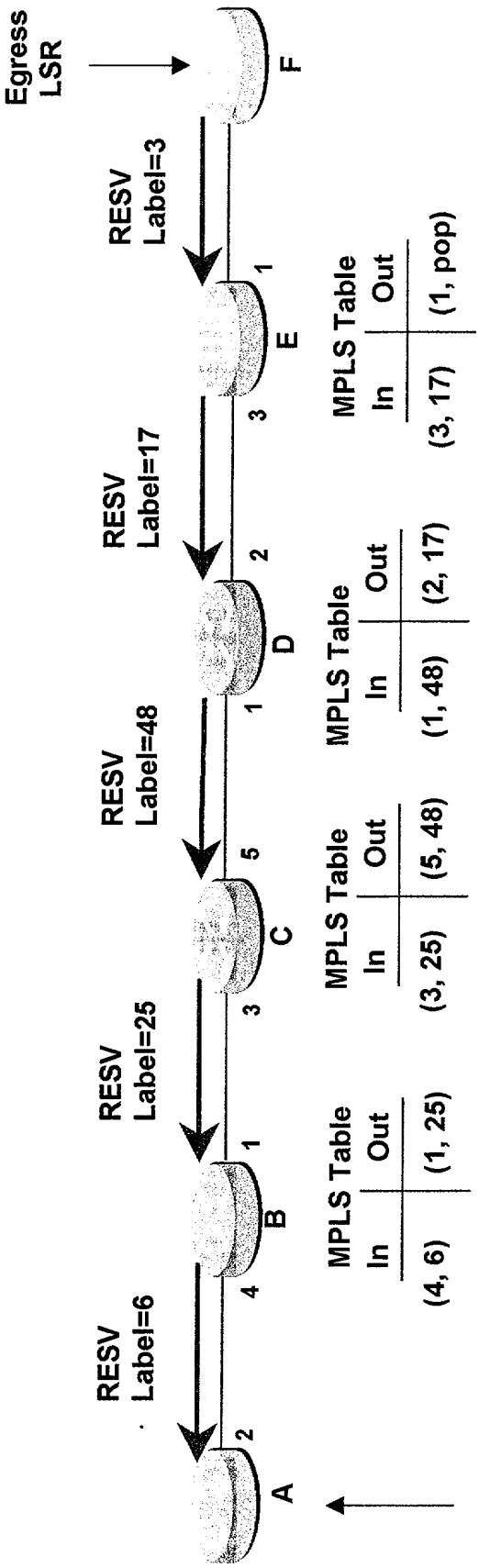

Egress LSR
RESV Label=3
RESV Label=17
RESV Label=48
RESV Label=25
RESV Label=6
A
B
C
D
E
F
MPLS Table
In | Out
(4, 6) | (1, 25)
MPLS Table
In | Out
(3, 25) | (5, 48)
MPLS Table
In | Out
(1, 48) | (2, 17)
MPLS Table
In | Out
(3, 17) | (1, pop)
Ingress LSR

Fig. 3B

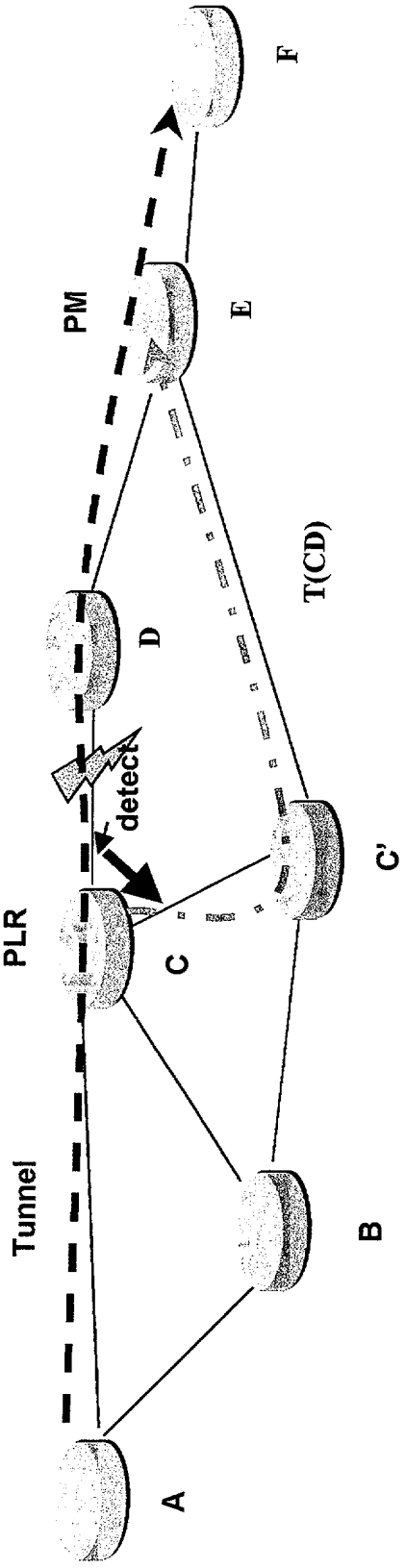


Fig. 4

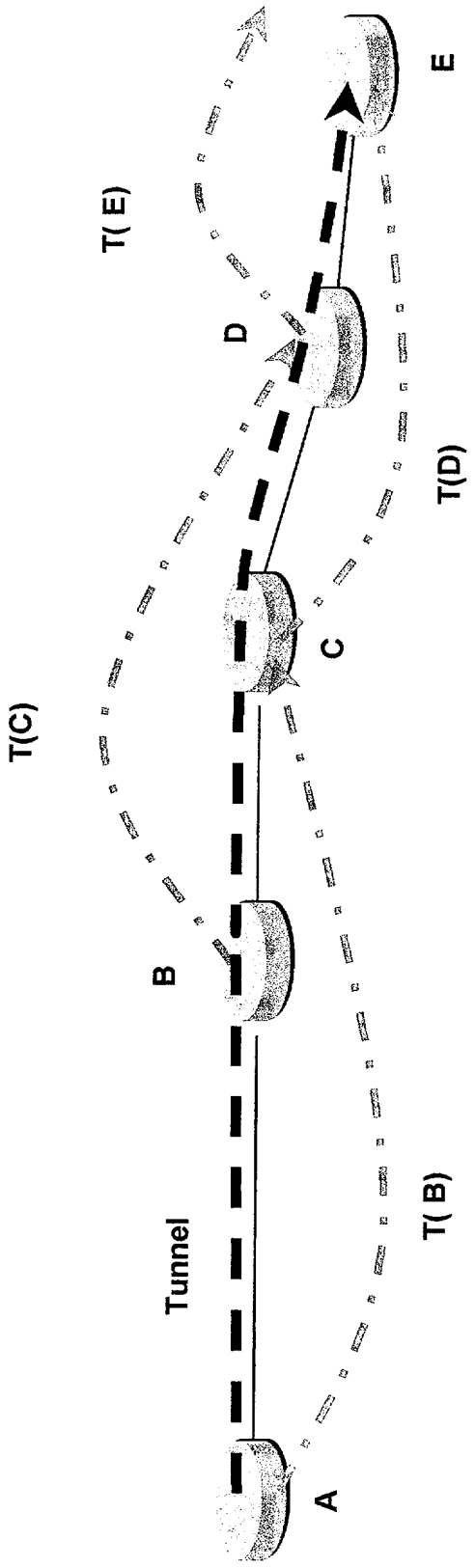


Fig. 5

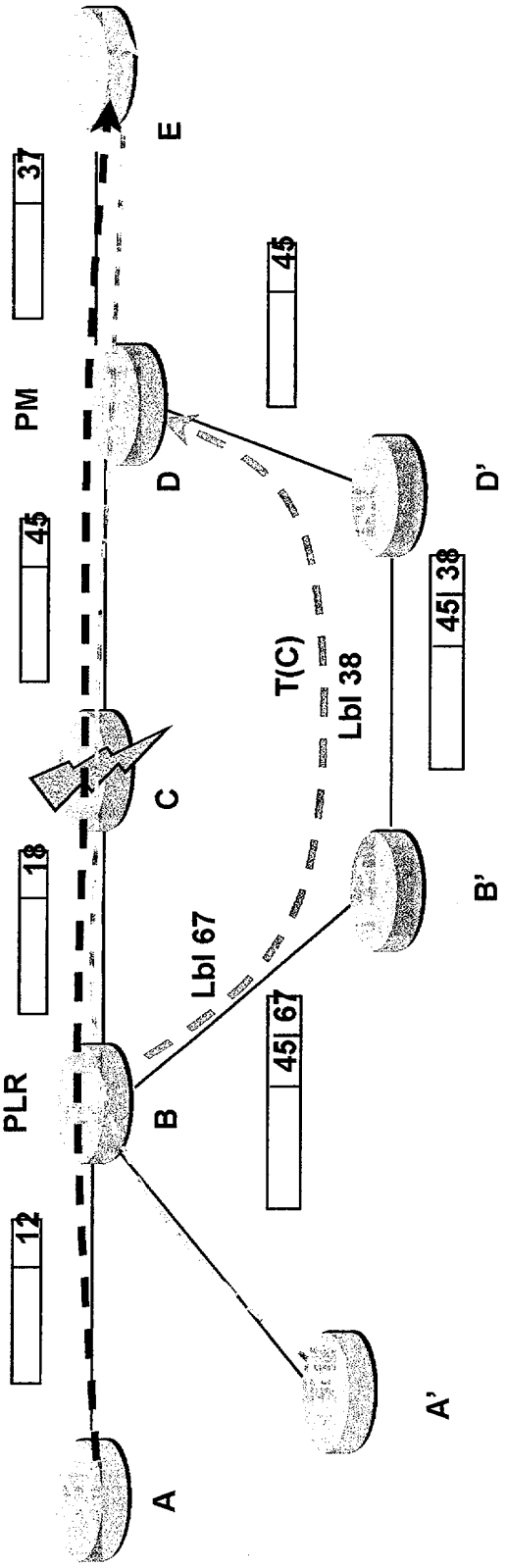


Fig. 6

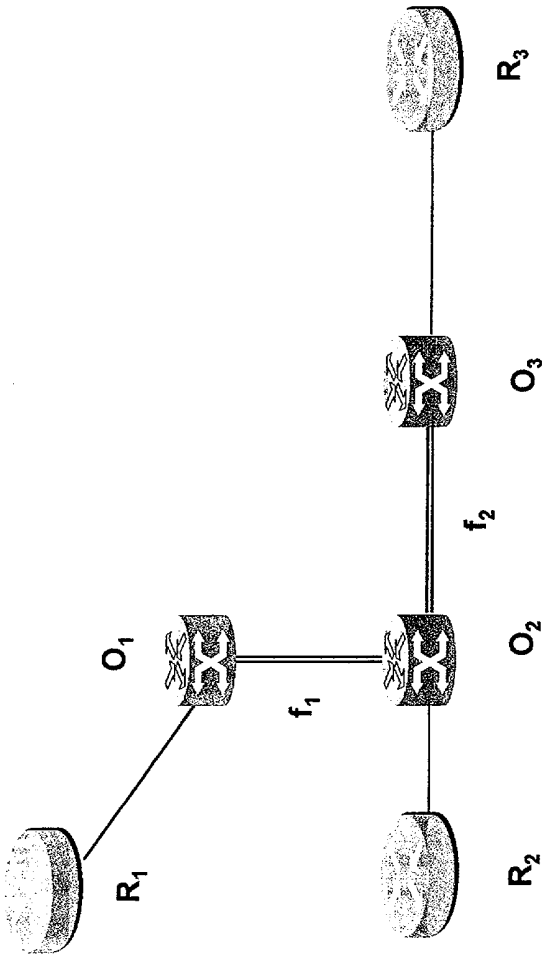


Fig. 7

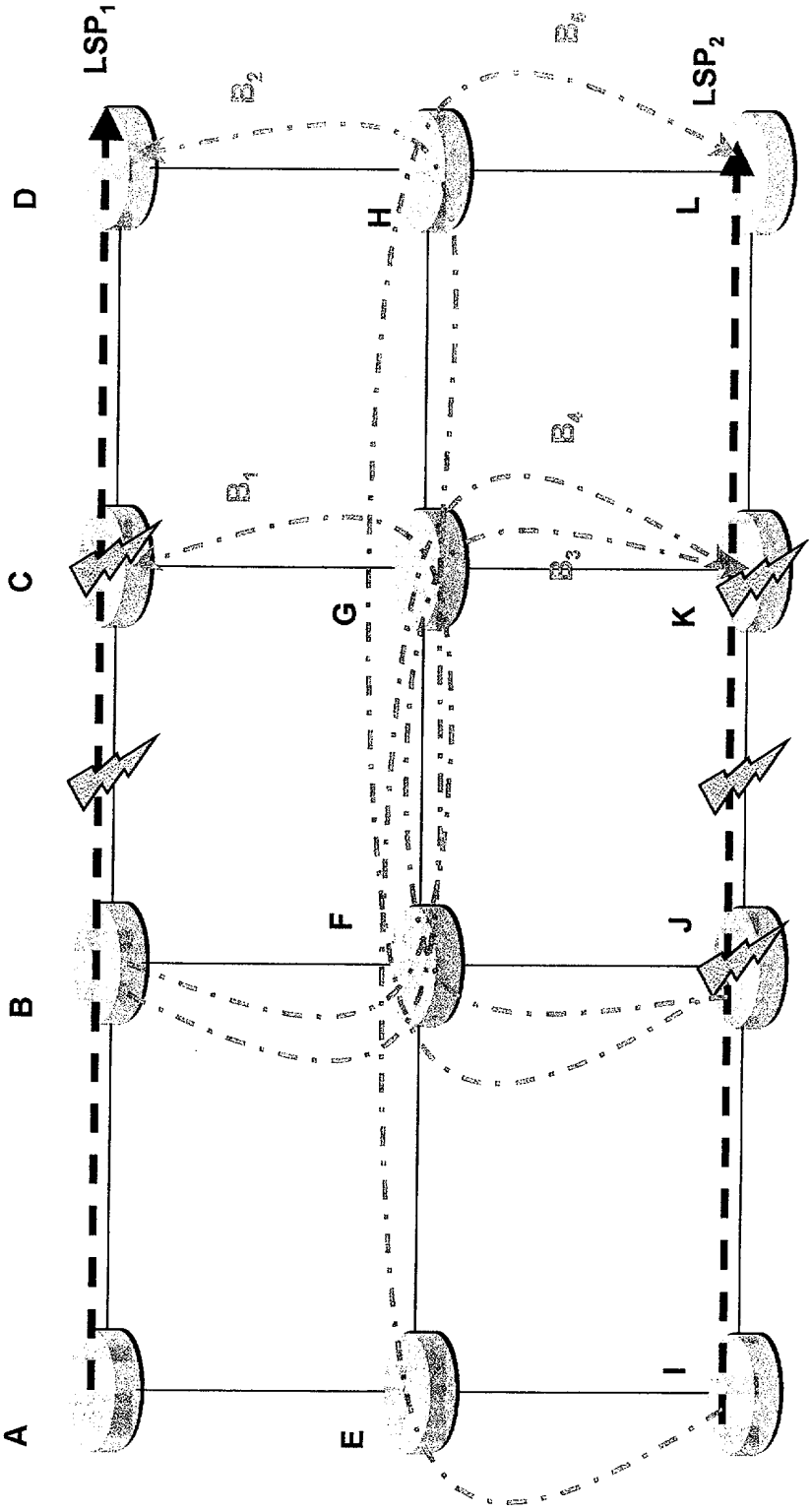


Fig. 8

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2836313

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 615301
FR 0202436

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	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 378, colonne de droite, ligne 2 - ligne 38 * * page 379, colonne de gauche, ligne 32 - page 380, colonne de droite, ligne 37 *	1,2,6, 10-14	H04M1/723 H04M9/00
Y	---	3-5,7-9	
Y	K. KOMPELLA, Y. REKHTER, A. BANERJEE, J. DRAKE, G. BERNSTEIN, D. FEDYK, E. MANNIE, D. SAHA, V. SHARMA, D. BASAK: "Routing extensions in Support of Generalized MPLS" IETF DRAFT, juin 2001 (2001-06), pages 1-19, XP002222762 * alinéa '006.! * * alinéa '6.3.! *	3-5,7-9	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) H04L

Date d'achèvement de la recherche: 28 novembre 2002

Examinateur: 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

EPO FORM 1503 12.99 (P04C14)