

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 25.09.06.

30 Priorité :

43 Date de mise à la disposition du public de la demande : 28.03.08 Bulletin 08/13.

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, DE CRAENE BRUNO et TRANSY ESTELLE.

73 Titulaire(s) :

74 Mandataire(s) : CABINET BEAU DE LOMENIE.

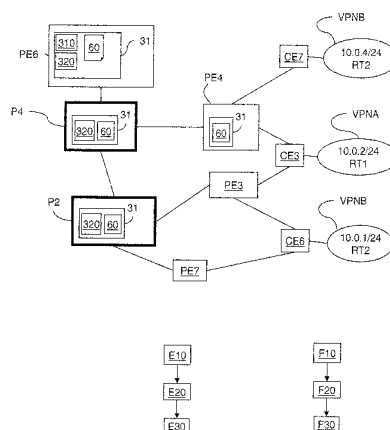
54 SYSTEME POUR SECURISER L'ACCES A UNE DESTINATION D'UN RESEAU PRIVE VIRTUEL.

57 Ce système pour sécuriser l'accès à une destination (D) d'un réseau privé virtuel (VPNA) raccordé à un routeur d'accès nominal (PE3) comporte un routeur coeur (P2) apte à:

- détecter une panne affectant une communication avec le routeur d'accès nominal (PE3); et
- basculer le trafic vers un routeur d'accès protecteur (PE6) dans un tunnel de secours (T1) évitant le routeur d'accès nominal (PE3).

Le routeur d'accès protecteur (PE6) est apte à:

- substituer, dans un paquet MPLS, un label VPN nominal (101) propre au routeur d'accès nominal (PE3) par un label VPN de secours (201) propre à un routeur d'accès de secours (PE4) raccordé à cette destination (D); et
- rediriger ledit paquet vers le routeur d'accès de secours (PE4) dans un tunnel (T2) évitant le routeur d'accès nominal (PE3).



Arrière-plan de l'invention

5 L'invention se situe dans le domaine des télécommunications, et plus particulièrement des réseaux privés virtuels (VPN).

L'invention se situe dans le contexte d'un réseau privé virtuel (VPN) de niveau 3, constitué de routeurs de cœurs, appelés routeurs P, de routeurs d'accès appelés PE, et de routeurs clients appelés CE, utilisant la
10 technologie MPLS VPN définie dans le document de l'Internet Engineering Task Force (IETF), Request for Comment RFC 4364.

La technologie MPLS VPN n'est pas décrite ici, pour plus d'informations on peut se référer au document RFC 4364 précité.

Certains services de communication VPN ont de fortes exigences
15 en termes de disponibilité de CE à CE (par exemple service de voix (VoIP), télé médecine). Ces services nécessitent un reroutage déterministe en moins de 100ms en cas de panne de lien ou de nœud. Aujourd'hui, la seule technologie permettant de telles performances de reroutage est le Fast Reroute consistant à établir à l'avance des chemins de secours locaux
20 contournant l'élément protégé. En cas de panne, le nœud directement en amont met à jour sa table de routage et bascule le trafic sur le chemin de secours. Cette méthode ne nécessite aucun calcul de route ni signalisation après la panne. De plus, les routes de secours sont préinstallées dans les tables de commutation des routeurs, ce qui garantit un temps de re-
25 routage déterministe inférieur à 100ms.

Il existe deux modes pour réaliser cette protection :

- le mode Fast Reroute MPLS reposant sur l'établissement de tunnels primaires MPLS-TE de bout en bout, protégés localement par des tunnels de secours MPLS-TE, ce mode étant décrit dans le document RFC
30 4090 de l'IETF ;

- le mode Fast Reroute IP reposant sur une protection de routes IP par des routes de secours évitant l'élément protégé et sans risque de boucle. Ces routes de secours peuvent être en mode connecté avec des tunnels MPLS-TE de secours locaux ou en mode non connecté lorsqu'il n'y

a pas de risque de boucle. Pour plus de détails sur ce deuxième mode de réalisation, on peut se reporter aux documents suivants :

- Shen, Pan, « Nexthop Fast ReRoute for IP and MPLS » (<http://www.potaroo.net/ietf/all-ids/draft-shen-nhop-fastreroute-01.txt>) et
- 5 - Shand, Bryant, « IP Fast Reroute Framework », <http://www.ietf.org/internet-drafts/draft-ietf-rtgwg-ipfrr-framework-05.txt>.

On rappelle qu'un « tunnel » est une liaison virtuelle dans laquelle un paquet d'un protocole (eg IPv4, IPv6, MPLS,...) est placé dans un autre paquet "externe" du même ou d'un autre protocole (eg: IP, MPLS, ...) pour son transport d'un point à un autre. Dans ce mécanisme de tunnel, les équipements réseaux situés entre le point d'entrée et le point de sortie du tunnel ne traitent et n'ont connaissance que du paquet externe et pas du paquet interne.

Le mode Fast Reroute MPLS permet, avec un maillage des PEs par des tunnels MPLS-TE primaires, une protection des liens PE-P, P-P et des nœuds P. Il passe difficilement à l'échelle car il nécessite un maillage de tous les routeurs PE et requiert donc un nombre de tunnels au carré du nombre de PEs. Il n'est donc applicable en pratique qu'à un faible nombre de PEs (~100).

Le mode Fast Reroute IP permet une protection des liens CE-PE, PE-P, P-P et des nœuds P. Il ne nécessite pas de tunnels MPLS-TE primaires et passe donc beaucoup mieux à l'échelle.

Les techniques de Fast Reroute actuelles, présentées ci dessus ne permettent pas de protéger les routeurs d'accès d'un réseau MPLS-VPN.

En effet, la technique Fast Reroute MPLS ne peut protéger les routeurs d'accès car cela nécessiterait de faire démarrer les tunnels MPLS-TE sur les routeurs clients CEs.

Il n'existe pas aujourd'hui de mécanisme permettant de faire du MPLS-TE entre deux routeurs clients.

De plus même si un tel mécanisme était défini, il présenterait des limitations en terme de passage à l'échelle du fait qu'il nécessite un nombre de tunnels au carré du nombre de routeurs clients, et ne serait donc en pratique applicable qu'à un très faible nombre de routeurs clients.

Par ailleurs, la technique Fast Reroute IP ne permet pas de protéger les routeurs d'accès car pour le routeur coeur qui déclenche le

Fast Reroute, la destination est le routeur d'accès donc si le routeur d'accès disparaît, il n'a plus de destination.

De plus, même si on indique au routeur coeur un routeur d'accès de secours pour secourir un routeur d'accès nominal, les paquets
5 VPN ne pourront pas être traités par le routeur d'accès de secours qui ne connaît pas le contexte correct pour les traiter.

En effet le routeur coeur va basculer le trafic d'un routeur d'accès nominal vers un routeur d'accès de secours, sans changer le label VPN (car il n'en a pas connaissance).

10 Or, les labels VPN sont alloués localement par les routeurs d'accès et n'ont qu'une signification locale, si bien que le trafic serait donc routé vers un mauvais VPN sur le routeur d'accès de secours.

Les routeurs d'accès sont des équipements particulièrement sensibles, et ont une forte charge de travail (maintient et mise à jour des
15 tables VPN); les statistiques montrent qu'ils tombent fréquemment en panne.

Les seuls mécanismes de sécurisation contre les pannes de routeur d'accès disponibles aujourd'hui reposent sur la convergence du protocole BGP (pour "Border Gateway Protocol") qui offrent des temps de
20 sécurisation supérieurs à la seconde, incompatibles avec les exigences de disponibilité des services temps réels.

Il est donc primordial pour assurer une bonne disponibilité de routeur client à routeur client de définir de nouveaux mécanismes permettant de protéger rapidement les routeurs d'accès, et capables de
25 supporter un grand nombre de routeurs clients (i.e. passage à l'échelle).

Objet et résumé de l'invention

Selon un premier aspect, l'invention concerne un système pour sécuriser l'accès à une destination d'un réseau privé virtuel raccordé à au
30 moins un routeur d'accès nominal.

Ce système comporte :

- au moins un routeur coeur apte à :
 - détecter une panne affectant une communication avec ce routeur d'accès nominal ; et
 - 35 - basculer le trafic vers un routeur d'accès protecteur dans un tunnel de secours évitant le routeur d'accès nominal ;

- ce routeur d'accès protecteur étant apte à :
 - substituer, dans un paquet MPLS, un label VPN nominal annoncé par le routeur d'accès nominal par un label VPN de secours propre à un routeur d'accès de secours raccordé à cette destination ; et
- 5 - rediriger ce paquet vers le routeur d'accès de secours dans un tunnel évitant le routeur d'accès nominal.

10 Selon un deuxième aspect, l'invention vise aussi un routeur d'accès, dit routeur d'accès protecteur, susceptible d'être utilisé pour sécuriser l'accès à une destination dans un réseau privé virtuel, lors d'une panne affectant une communication avec un routeur d'accès nominal raccordé à ce réseau. Ce routeur d'accès protecteur comporte :

- des moyens pour identifier un label VPN nominal réservé par ledit routeur d'accès nominal pour ladite destination ;
- des moyens pour recevoir un paquet MPLS ;
- 15 - des moyens pour substituer, dans ce paquet MPLS, le label VPN nominal par un label VPN de secours propre à un routeur d'accès de secours pour cette destination ; et
- des moyens pour rediriger le paquet MPLS vers le routeur d'accès de secours dans un tunnel évitant le routeur d'accès nominal.

20 Corrélativement, l'invention vise aussi un procédé de routage susceptible d'être mis en œuvre dans un routeur d'accès protecteur pour sécuriser l'accès à une destination dans un réseau privé virtuel lors d'une panne affectant une communication avec un routeur d'accès nominal raccordé audit réseau, caractérisé en ce qu'il comporte :

- 25 - une étape de réception d'un paquet MPLS comportant un label VPN nominal réservé par ce routeur d'accès nominal pour la destination précitée ;
- une étape de substitution, dans ledit paquet MPLS, du label VPN nominal par un label VPN de secours propre à un routeur d'accès de secours pour cette destination ; et
- 30 - une étape de redirection de ce paquet MPLS vers le routeur d'accès de secours dans un tunnel évitant le routeur d'accès nominal.

L'invention permet de protéger un site d'un réseau privé virtuel raccordé à un routeur d'accès nominal et à au moins un routeur d'accès
35 de secours.

Le mécanisme selon l'invention repose sur une protection locale d'un routeur d'accès nominal par les routeurs coeurs directement raccordés à ce routeur d'accès nominal.

5 En cas de panne affectant le routeur d'accès nominal, le « routeur coeur protecteur », reroute le trafic VPN vers un routeur d'accès dit « routeur d'accès protecteur » capable de ré-aiguiller le trafic, dans un tunnel n'empruntant pas le routeur d'accès nominal.

Conformément à l'invention, le routeur d'accès nominal à protéger doit être raccordé en amont à au moins un routeur coeur
10 protecteur apte à détecter la panne.

L'invention comporte deux modes de réalisation principaux.

Dans un premier mode de réalisation, le routeur cœur envoie au routeur d'accès protecteur, dans le tunnel de secours, une information selon laquelle ce tunnel de secours est utilisé lors de la panne affectant le
15 routeur d'accès nominal.

Cette information peut par exemple être constituée par un label MPLS spécifique placé devant le label VPN.

Dans ce premier mode de réalisation, le routeur d'accès protecteur selon l'invention comporte :

- 20 - des moyens pour recevoir, en provenance du routeur cœur, via le tunnel de secours, une information selon laquelle ce tunnel est utilisé lors de la panne ; et
- des moyens pour créer une table de commutation MPLS contextuelle, cette table comportant des instructions pour :
- 25 - substituer, dans chaque paquet MPLS reçu dans ledit tunnel de secours, ledit label nominal par le label de secours ; et pour
- aiguiller ce paquet MPLS vers le routeur d'accès de secours via un deuxième tunnel de secours qui évite le routeur d'accès nominal.

Dans un mode préféré de cette première variante de réalisation,
30 le routeur d'accès protecteur selon l'invention comporte des moyens pour identifier le routeur d'accès de secours et obtenir les labels à partir des annonces BGP effectuées par les routeurs d'accès. Cette caractéristique évite une configuration explicite du routeur d'accès selon l'invention pour associer un label de secours à un label nominal.

Le deuxième mode de réalisation de l'invention est particulièrement avantageux lorsque le routeur cœur n'est pas capable d'envoyer l'information représentative de la panne dans le tunnel de secours. Dans ce mode de réalisation, on utilise avantageusement une
5 partition de l'espace des labels VPN.

Comme rappelé précédemment, les labels VPN sont alloués localement par les routeurs d'accès et n'ont qu'une signification locale.

Afin d'éviter les collisions de labels VPN, chaque routeur d'accès alloue, conformément à l'invention, ses labels VPN avec des valeurs qui lui
10 sont propres, de sorte que, les labels d'un routeur d'accès protecteur et de tous les routeurs d'accès nominaux protégés par ce même routeur d'accès protecteur soient différents.

Dans un mode particulier de cette deuxième variante de réalisation, on effectue une partition de l'espace de labels entre le routeur
15 d'accès protecteur et le routeur d'accès nominal qu'il protège et le routeur d'accès de secours.

Dans cette deuxième variante de réalisation, le routeur d'accès protecteur maintient dans sa table de commutation (table MPLS) le label VPN nominal réservé par le routeur d'accès nominal pour une destination
20 donnée, et pointant indirectement vers le routeur d'accès de secours correspondant avec le label VPN de secours réservé par le routeur d'accès de secours pour cette destination.

Le routeur d'accès de secours achemine finalement le trafic vers le bon site destination.

25 Dans un mode particulier de cette deuxième variante de réalisation, le routeur d'accès protecteur selon l'invention comporte des moyens pour identifier le routeur d'accès de secours et obtenir les labels à partir des annonces BGP effectuées par les routeurs d'accès.

Cette caractéristique évite une configuration explicite du routeur
30 d'accès selon l'invention pour associer un label de secours à un label nominal.

Pendant la panne du routeur d'accès nominal, un routeur d'accès protecteur protégeant un routeur d'accès nominal reçoit le trafic initialement à destination d'un routeur d'accès nominal avec les labels VPN
35 annoncés par ce routeur d'accès nominal pour les sites destinations situés derrière ce routeur d'accès nominal.

Il est chargé de ré-aiguiller les flux vers le ou les routeurs d'accès de secours correspondant, avec le label VPN annoncé par les routeurs d'accès de secours pour ces sites destinations.

Un routeur d'accès protecteur a connaissance de l'ensemble des
5 routeurs d'accès nominaux qu'il protège, par configuration, ou par découverte automatique.

Un routeur d'accès nominal et ses routeurs d'accès de secours, annoncent en BGP un ensemble de destinations atteignables, avec les labels VPN correspondants.

10 L'annonce par un routeur d'accès d'une adresse IP "D" dans un VPN V identifié par un Route Target "RT_V", avec le label VPN L est notée (routeur d'accès, RT_V, D, L).

Pour un VPN donné (c'est-à-dire un RT donné), les routeurs d'accès nominal et le routeur d'accès de secours doivent utiliser des
15 "routes distinguisher" (RD) BGP différents sur chacun des routeurs d'accès afin qu'une éventuelle utilisation d'un Route Réflecteur BGP ne masque pas la route de secours au routeur d'accès protecteur.

Dans un mode particulier de réalisation, les différentes étapes du procédé de routage tel que mentionné ci-dessus sont déterminées par
20 des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'au
25 moins un procédé de routage tel que décrit ci-dessus.

Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme
30 souhaitable.

L'invention vise aussi un support d'informations lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

Le support d'informations peut être n'importe quelle entité ou
35 dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD

ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

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

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

Brève description des dessins

15 D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent un exemple de réalisation dépourvu de tout caractère limitatif. Sur les figures :

20 - la figure 1 représente un système pour sécuriser l'accès à un site d'un réseau privé virtuel conforme à l'invention, dans un mode préféré de réalisation ;

- les figures 2 et 3 représentent, sous forme d'organigramme, les procédés de routage selon l'invention, dans des modes particuliers de réalisation.

25

Description détaillée d'une première variante de réalisation

A la **figure 1**, on a représenté deux réseaux privés virtuels (VPN) référencés respectivement VPNA et VPNB.

30 Ces réseaux privés virtuels sont identifiés de façon absolue par un identifiant unique (Route Target) respectivement RT1, RT2.

Le VPN VPNA peut être accédé via un routeur client CE3.

Localement, vu de ce routeur client CE3, le VPN VPNA correspond à la plage d'adresses IP 10.0.2/24.

35 Le VPN VPNB peut être accédé via deux routeurs clients CE6 et CE7.

Localement, vu du routeur client CE6 (respectivement CE7), le VPN VPNB correspond à la plage d'adresses IP 10.0.1/24, (respectivement 10.0.4/24).

Sur cette figure on a représenté :

- 5 - quatre routeurs d'accès référencés PE3, PE4, PE6 et PE7 adaptés à mettre en œuvre le protocole BGP ; et
- deux routeurs cœur référencés P2 et P4 adaptés à mettre en œuvre le protocole IGP (pour "Interior Gateway Protocol").

10 Conformément à l'invention, on associe, pour chacun de ces routeurs d'accès, et pour chaque route d'accès à un VPN, un identifiant RD (Route Distinguisher) propre à ce routeur d'accès et à ce VPN.

Dans l'exemple décrit ici, ces identifiants sont les suivants :

<u>Routeur d'accès</u>	<u>VPN</u>	<u>RD</u>
PE4	VPNA	RD1
PE4	VPNB	RD2
PE3	VPNA	RD3
PE3	VPNB	RD4
PE7	VPNB	RD5

15 Dans l'exemple décrit ici, chaque routeur d'accès comporte, dans sa mémoire non volatile de configuration 31, un fichier 60 de configuration dans lequel cette association est enregistrée.

A titre d'exemple, le fichier 60 de configuration du routeur d'accès PE4 comporte l'instruction suivante :

VRFA : RD1, VRFB : RD2

20 où VRFA et VRFB représentent les tables de routages VRF (pour "Virtual Routing and Forwarding Table") au niveau IP, associées respectivement aux VPN VPNA et VPNB.

Conformément à l'invention, des espaces de labels disjoints sont configurés sur chacun des routeurs d'accès PE3, PE4, PE6 et PE7.

25 Dans l'exemple décrit ici, les espaces de labels sont les suivants :

<u>Routeur d'accès</u>	<u>Espace de labels</u>
PE3	[101-200]
PE4	[201-300]
PE6	[401-500]
PE7	[301-400]

Dans l'exemple décrit ici, l'espace de labels est enregistré dans le fichier 60 de configuration du routeur d'accès concerné.

A titre d'exemple, le fichier 60 de configuration du routeur d'accès PE3 comporte l'expression :

5 PE3 Config : VPN Label Space 101-200

Dans l'exemple décrit ici, les routeurs d'accès reliés à au moins un routeur client CE3, CE6, CE7 sont les routeurs d'accès PE3, PE4 et PE7.

De façon connue, chaque routeur d'accès annonce aux autres routeurs d'accès, en utilisant le protocole BGP, les labels à utiliser pour
10 atteindre un VPN particulier.

Par exemple, le routeur d'accès PE3 diffuse l'annonce :

Announce 10.0.2/24 RT1 label 101

pour imposer à tous les autres routeurs d'accès, d'utiliser le label 101, pour atteindre le VPN VPNA correspondant à la plage d'adresses
15 IP 10.2.24, d'identifiant unique (route target) RT1.

Dans cet exemple on s'intéresse à la protection du routeur d'accès PE3, relié respectivement aux routeurs clients CE3 et CE6.

Dans l'exemple de réalisation décrit ici, le routeur d'accès PE3 est protégé par :

- 20 - les routeurs d'accès de secours PE4 et PE7 ;
 - le routeur d'accès protecteur PE6 conforme à l'invention ; et
 - le routeur cœur protecteur P2.

Conformément à l'invention, aucune configuration particulière n'est à apporter au niveau des routeurs d'accès de secours PE4 et PE7, à
25 l'exception des plages de labels.

Nous allons maintenant décrire, la configuration du routeur d'accès protecteur PE6.

Tout d'abord, on déclare le routeur d'accès PE6 en tant que routeur d'accès protecteur du routeur d'accès PE3.

30 Dans le mode de réalisation décrit ici, cette étape consiste à ajouter l'instruction suivante dans le fichier de configuration 60 du routeur d'accès PE6 :

Config : Protecting PE3

Ensuite, le routeur d'accès protecteur PE6 reçoit les annonces
35 BGP émises par les autres routeurs d'accès PE3, PE4 et PE7.

Pour pouvoir réaliser la fonction de ré-aiguillage le routeur d'accès protecteur PE6 installe dans une table BGP 310 de sa mémoire volatile de configuration 31, les labels VPN annoncés par tous les routeurs d'accès PE3, PE4 et PE7.

- 5 On suppose que les routes VPN reçues par le routeur d'accès protecteur PE6 au cours de l'étape E20 sont :

	<u>Routeur d'accès</u>	<u>Destination</u>	<u>Label VPN</u>
Receive :	PE4	10.0.2/24 RT1 RD1	label 201
Receive :	PE4	10.0.4/24 RT2 RD2	label 202
Receive :	PE3	10.0.2/24 RT1 RD3	label 101
Receive :	PE3	10.0.1/24 RT2 RD4	label 102
Receive :	PE7	10.0.1/24 RT2 RD5	label 301

- 10 A chaque fois qu'il reçoit une annonce en provenance du routeur d'accès PE3, le routeur d'accès protecteur PE6 identifie la destination à protéger.

En l'occurrence, il détermine que les destinations suivantes sont à protéger :

<u>Destination</u>
10.0.2/24 RT1
10.0.1/24 RT2

- 15 Pour chacune de ces deux destinations, le routeur d'accès protecteur PE6 recherche dans le tableau 310 une même annonce annoncée par un autre routeur d'accès avec la même destination (plage IP et Route Target).

L'identifiant de route RD n'est pas pris en compte.

- 20 Dans l'exemple décrit ici :

1) seule la première route du tableau 310 est candidate pour la première destination : 10.0.2/24 RT1.

	<u>Routeur d'accès</u>	<u>Destination</u>	<u>Label VPN</u>
Receive :	PE4	10.0.2/24 RT1 RD1	label 201

2) seule la cinquième route du tableau 310 est candidate pour la deuxième destination : 10.0.1/24 RT2.

	<u>Routeur d'accès</u>	<u>Destination</u>	<u>Label VPN</u>
Receive :	PE7	10.0.1/24 RT2	RD5 label 301

5 Lorsque plusieurs lignes du tableau sont candidates, le procédé selon l'invention met en œuvre, au cours de cette étape E30 de recherche, une sous-étape de décision, pour ne retenir qu'une seule route.

La recherche d'annonce est suivie par une mise à jour de la table de commutation MPLS 320.

10 Le résultat de cette étape de mise à jour est donné ci-dessous :

<u>Substitution labels</u>	<u>Routeur d'accès de secours</u>	<u>Action</u>
101 -> 201	PE4	(24, P4)
102 -> 301	PE7	(26, P4)

15 A titre d'exemple, la première ligne de la table de commutation 320 indique, que lorsque le routeur d'accès protecteur PE6 reçoit une trame dont le label VPN est 101, il doit :

- substituer ce label, par le label VPN de secours 201 ; et
- pour atteindre le routeur de secours PE4, envoyer le trafic dans le tunnel T2, permettant d'atteindre PE4, i.e. faire un PUSH 24 et transmettre la trame au routeur cœur P4.

20 L'homme du métier comprendra que la table de commutation du routeur cœur P4 comporte un enregistrement complémentaire :

24 (PE4) -> pop, PE4

de sorte que le routeur cœur P4, sur réception de la trame reçue du routeur d'accès protecteur PE6, dépile la valeur 24 et transmet la trame au routeur de secours PE4.

25 De même, la deuxième ligne de la table de commutation 320 indique que, lorsque le routeur d'accès protecteur PE6 reçoit une trame dont le label VPN est 102, il doit :

- substituer ce label, par le label VPN de secours 301 ; et

- pour atteindre le routeur de secours PE7, envoyer le trafic dans le tunnel T3, permettant d'atteindre PE7, i.e. faire un PUSH 26 et transmettre la trame au routeur cœur P4.

Dans l'exemple de réalisation décrit ici, les tunnels T2 et T3 vers
5 les routeurs de secours PE4, PE7 sont établis via LDP.

A chaque changement d'information susceptible de modifier le routage BGP, les opérations ci-dessus sont à effectuer.

Au cours de cette mise à jour de la table de commutation, on s'assure que ces tunnels T2 et T3 ne passent pas par le routeur d'accès nominal à protéger, PE3.
10

Conformément à l'invention le routeur cœur P2 est configuré comme routeur cœur protecteur. A cet effet le fichier de configuration 60 du routeur coeur P2 comporte l'instruction suivante :

Config : Link P2-PE3 : PE Protector = PE6.

15 La table de commutation 320 du routeur cœur P2, de format connu, est donnée ci-dessous :

26	(PE4)	->	24,	P4
30	(PE7)	->	pop,	PE7
31	(PE6)	->	27,	P4
23	(PE3)	->	pop,	PE3
	(PE3 backup PE6)	->	27,	P4

Conformément à l'invention, le routeur cœur protecteur P2
20 maintient deux sorties (respectivement aux quatrième et cinquième lignes) pour la destination PE3 :

- une sortie nominale vers PE3 ; et

une sortie de secours vers le routeur d'accès protecteur PE6, via le tunnel de secours T1 ne passant pas par le routeur d'accès nominal PE3. Dans
25 l'exemple de réalisation décrit ici, le tunnel T1 vers le routeur d'accès protecteur PE6 est établi via LDP.

Nous allons maintenant décrire en référence aux figures 2 et 3 le procédé de routage mis en œuvre dans le routeur protecteur P2 et le procédé de routage conforme à l'invention mis en œuvre dans le routeur
30 d'accès protecteur PE6.

En régime nominal le routeur cœur protecteur P2 envoie le trafic de destination 10.0.2/24...RT1, sur le routeur d'accès nominal PE3, avec le label VPN nominal 101 annoncé par le routeur d'accès nominal PE3 pour cette destination.

5 Lorsqu'une panne intervient sur le lien P2-PE3 ou au sein de PE3, le routeur cœur P2 détecte cette panne au cours d'une étape E10.

Puis, au cours d'une étape E20, le routeur cœur protecteur P2 bascule le trafic vers le routeur d'accès protecteur PE6 protégeant le routeur PE3, en conservant le label VPN 101.

10 Le routeur d'accès protecteur PE6 détecte, au cours d'une étape F10, de son procédé de routage que le paquet MPLS comporte un label VPN nominal réservé par le routeur d'accès nominal PE3 pour la destination 10.0.2 du VPNA.

15 Au cours d'une étape F20 de son procédé de routage, le routeur d'accès PE6 substitue dans le paquet MPLS reçu à l'étape précédente, le label VPN nominal 101 par le label VPN de secours 201 réservé par le routeur d'accès de secours PE4 pour cette destination.

20 Puis, le routeur d'accès PE6 redirige, au cours d'une étape E30 de son procédé de routage, le paquet MPLS vers le routeur d'accès de secours PE4.

Arrivé sur PE4 le trafic est bien acheminé vers la destination.

Il en est de même pour la destination 10.0.1 du VPN B.

Dans la description faite précédemment, le routeur d'accès protecteur effectue un routage MPLS vers les routeurs d'accès de secours.

25 Une autre option est, pour le routeur d'accès protecteur, de créer des VRF de secours.

On note VRF (RT_V, routeur d'accès nominal), la VRF de secours protégeant le VPN V (utilisant le RT RT_V) de la panne du routeur d'accès nominal.

30 Cette VRF contient toutes les routes VPN ayant un RT "RT_V" en excluant les routes ayant comme next-hop BGP "routeur d'accès nominal".

35 Pour chaque routeur d'accès nominal, et pour chaque annonce VPN (routeur d'accès nominal, RT_V, D, LN), effectuée par ce routeur d'accès nominal, le routeur d'accès protecteur installe dans la table de commutation MPLS l'entrée suivante:

LN -> look up dans la VRF de secours VRF(RT_V, routeur d'accès nominal).

Description détaillée d'une deuxième variante de réalisation

5

Dans la première variante de réalisation décrite ci-dessus, des espaces de labels disjoints sont configurés sur chacun des routeurs d'accès PE3, PE4, PE6 et PE7.

10 Nous allons maintenant décrire une deuxième variante de réalisation dans laquelle cette configuration n'est pas nécessaire.

Dans cette variante de réalisation, le routeur nominal protégé PE3 définit un espace de label, identifié par un label contextuel LB inséré devant le label nominal 101 dans le plan de transfert.

15 Le routeur d'accès protecteur PE6 indique au routeur cœur protecteur P2, le label contextuel LB à utiliser en cas de panne affectant la communication avec le routeur nominal PE3.

20 La distribution de ce label contextuel du routeur d'accès protecteur PE6 vers le routeur cœur protecteur P2 peut être réalisée par une session LDP dite "targetted". Une extension du protocole LDP, telle que définie dans le document RFC3036 de l'IETF est nécessaire pour annoncer le contexte, à savoir le routeur nominal PE3 protégé. Cette annonce peut être réalisée par un nouveau FEC TLV inséré dans un message LDP LabelMapping.

25 Dans cette variante de réalisation, le routeur d'accès protecteur PE6 selon l'invention maintient une table MPLS contextuelle, LFIB par routeur nominal à protéger (PE3). Cette table contient pour chaque destination VPN annoncée par PE3, le label VPN réservé par le routeur d'accès nominal (PE3), pointant vers un routeur de secours (PE4) avec le label VPN réservé par le routeur de secours pour cette destination.

30 La construction de cette table repose sur l'analyse des informations BGP annoncées par les routeurs d'accès nominaux et de secours. La procédure de construction de cette table est identique à celle décrite dans le premier mode de réalisation, à la différence près qu'ici une table MPLS contextuelle est dédiée à la protection d'un routeur d'accès nominal (PE3) et ne contient que les labels réservés par ce routeur d'accès
35 (évitant ainsi les risques de collision de label et donc le partitionnement).

A titre d'exemple, la table MPLS contextuelle associée à ce routeur nominal (PE3) est la suivante :

<u>Substitution labels</u>	<u>Routeur d'accès de secours</u>	<u>Action</u>
101 -> 201	PE4	(24, P4)
102 -> 301	PE7	(26, P4)

5 Il maintient également une table MPLS principale pointant vers les tables contextuelles. Dans cette table principale, le label contextuel LB pointe vers la table MPLS contextuelle LFIB associée à ce routeur nominal (PE3).

10 Pendant la panne du routeur nominal PE3, le routeur cœur protecteur P2 ré-aiguille le trafic à destination du routeur nominal PE3, dans le tunnel T1, vers le routeur d'accès protecteur PE6 en ajoutant, avant le label VPN, le label contextuel LB.

15 Autrement dit, le routeur cœur P2 envoie au routeur d'accès protecteur PE6, dans le tunnel de secours T1, une information selon laquelle ce tunnel de secours est utilisé lors de la panne affectant le routeur d'accès nominal PE3.

Dans l'exemple décrit ici, cette information est constituée par un label MPLS spécifique LB placé devant le label VPN.

20 Le routeur d'accès protecteur PE6 effectue donc deux lookup MPLS: un premier lookup dans la table de commutation MPLS principale, avec le label LB, permettant d'identifier la table de commutation MPLS contextuelle associée à PE3; puis un deuxième lookup, dans cette table contextuelle avec le label VPN nominal réservé par PE3 (101), permettant de déterminer le label VPN de secours (201) et le routeur d'accès de secours (PE4).

25

REVENDEICATIONS

1. Système pour sécuriser l'accès à une destination (D) d'un réseau privé virtuel (VPNA) raccordé à au moins un routeur d'accès nominal (PE3), ce système comportant :
- au moins un routeur cœur (P2) apte à :
 - détecter une panne affectant une communication avec ledit routeur d'accès nominal (PE3) ; et
 - basculer le trafic de paquets MPLS vers un routeur d'accès protecteur (PE6) dans un tunnel de secours (T1) évitant le routeur d'accès nominal (PE3) ;
 - ledit routeur d'accès protecteur (PE6) étant apte à :
 - substituer, dans un paquet MPLS, un label VPN nominal (101) propre audit routeur d'accès nominal (PE3) par un label VPN de secours (201) propre à un routeur d'accès de secours (PE4) raccordé à cette destination (D) ; et
 - rediriger ledit paquet vers ledit routeur d'accès de secours (PE4) dans un tunnel (T2) évitant ledit routeur d'accès nominal (PE3).
2. Système selon la revendication 1, caractérisé en ce qu'il comporte une partition de l'espace de labels VPN entre ledit routeur d'accès protecteur (PE6), ledit au moins un routeur d'accès nominal (PE3) et ledit au moins un routeur d'accès de secours (PE4).
3. Système selon la revendication 1, caractérisé en ce que ledit routeur cœur (P2) envoie audit routeur d'accès protecteur (PE6), dans ledit tunnel de secours (T1), une information (I1) selon laquelle ce tunnel de secours (T1) est utilisé lors de ladite panne.
4. Routeur d'accès protecteur (PE6) susceptible d'être utilisé pour sécuriser l'accès à une destination (D) dans un réseau privé virtuel (VPNA), lors d'une panne affectant une communication avec un routeur d'accès nominal (PE3) raccordé audit réseau (VPNA), caractérisé en ce qu'il comporte :
- des moyens pour identifier un label VPN nominal (101) propre audit routeur d'accès nominal (PE3) pour ladite destination (D) ;

- des moyens pour substituer, dans un paquet MPLS, ledit label VPN nominal (101) par un label VPN de secours (201) propre à un routeur d'accès de secours (PE4) pour ladite destination (D) ; et
- des moyens pour rediriger ledit paquet MPLS vers ledit routeur d'accès de secours (PE4) dans un tunnel (T2) évitant ledit routeur d'accès nominal (PE3).

5. Routeur d'accès protecteur (PE6) selon la revendication 4 caractérisé en ce qu'il comporte des moyens pour installer dans une table de commutation MPLS, ledit label nominal (101) propre audit routeur d'accès nominal (PE3) pour ladite destination (D), et pointant vers le routeur d'accès de secours (PE4) avec ledit label VPN de secours (201) propre à ce routeur d'accès de secours (PE4) pour cette destination (D).

6. Routeur d'accès protecteur (PE6) selon la revendication 4, caractérisé en ce qu'il comporte :
- des moyens pour recevoir, en provenance d'un routeur cœur (P2), via un tunnel de secours (T1), une information selon laquelle ledit tunnel (T1) est utilisé lors de ladite panne ; et
 - des moyens pour créer une table de commutation MPLS (LFIB1) contextuelle, cette table comportant des instructions pour :
 - substituer, dans chaque paquet MPLS reçu dans ledit tunnel de secours (T1), ledit label nominal (101) par ledit label de secours (201) ; et pour
 - aiguiller ce paquet MPLS vers ledit routeur d'accès de secours (PE4) via ledit tunnel (T2) évitant ledit routeur d'accès nominal (PE3).

7. Routeur d'accès protecteur (PE6) selon la revendication 4, 5, ou 6 caractérisé en ce qu'il comporte des moyens pour identifier ledit routeur d'accès de secours (PE4) et obtenir lesdits labels (101, 201) à partir des annonces BGP effectuées par lesdits routeurs d'accès.

8. Procédé de routage susceptible d'être mis en œuvre dans un routeur d'accès protecteur (PE6) pour sécuriser l'accès à une destination (D) dans un réseau privé virtuel lors d'une panne affectant une communication avec un routeur d'accès nominal raccordé audit réseau, caractérisé en ce qu'il comporte :

- une étape (F10) de réception d'un paquet MPLS comportant un label VPN nominal (101) propre audit routeur d'accès nominal (PE3) pour ladite destination (D) ;
 - une étape (F20) de substitution, dans ledit paquet MPLS, dudit label VPN nominal (101) par un label VPN de secours (201) propre à un routeur d'accès de secours (PE4) pour ladite destination (D) ; et
 - une étape (F30) de redirection dudit paquet MPLS vers ledit routeur d'accès de secours (PE4) dans un tunnel (T2) évitant ledit routeur d'accès nominal (PE3).
- 5
- 10
9. Programme d'ordinateur comportant des instructions pour l'exécution des étapes d'un procédé de routage selon la revendication 8 lorsque ledit programme est exécuté par un ordinateur.
- 15
10. Support d'enregistrement lisible par un ordinateur sur lequel est enregistré un programme d'ordinateur comprenant des instructions pour l'exécution des étapes d'un procédé de routage selon la revendication 8.

1/1

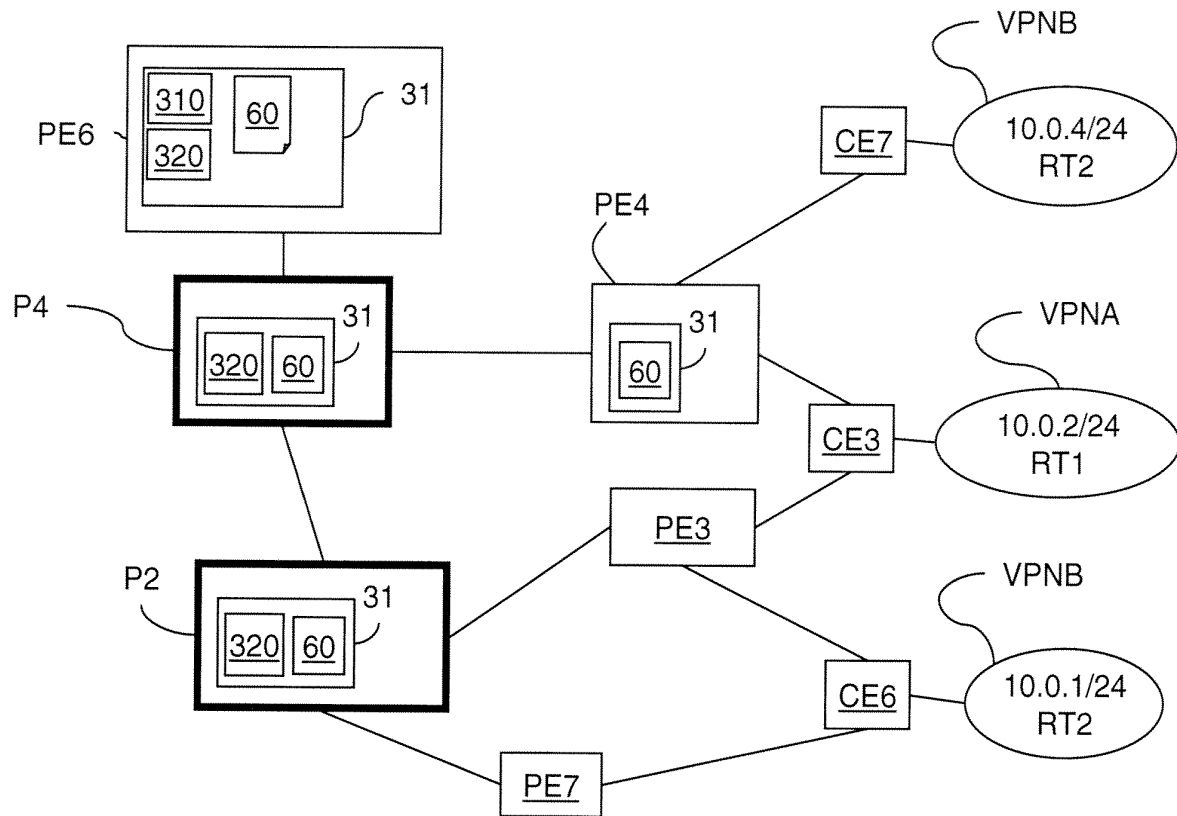


FIG. 1

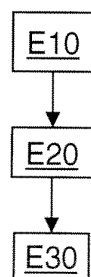


FIG. 2

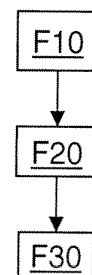


FIG. 3



RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 686334
FR 0653923

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	US 2006/153067 A1 (VASSEUR JEAN-PHILLIPE [US] ET AL) 13 juillet 2006 (2006-07-13) * abrégé * * alinéa [0014] - alinéa [0017] * * alinéa [0019] - alinéa [0021] * * alinéa [0042] - alinéa [0043] * * alinéa [0047] * * alinéa [0054] - alinéa [0059] * * alinéa [0061] - alinéa [0062] * * alinéa [0064] * * alinéa [0066] - alinéa [0072]; revendications 1,5,13,21,22; figures 1-7 * -----	1-10	H04L12/26
X	BLESS R ET AL: "Fast scoped rerouting for BGP" NETWORKS, 2003. ICON2003. THE 11TH IEEE INTERNATIONAL CONFERENCE ON SEPT. 28-OCT. 1, 2003, PISCATAWAY, NJ, USA,IEEE, 28 septembre 2003 (2003-09-28), pages 25-30, XP010683497 ISBN: 0-7803-7788-5 * page 26, alinéa III.THE.FAST.SCOPE.D.REROUTING.APROACH * ----- -/--	1-10	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04L
Date d'achèvement de la recherche		Examineur	
31 juillet 2007		Todorut, Cosmin	
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			

**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

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

N° d'enregistrement
national

FA 686334
FR 0653923

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	US 2006/209682 A1 (FILSFILS CLARENCE [BE] ET AL) 21 septembre 2006 (2006-09-21) * abrégé * * alinéa [0004] * * alinéa [0015] - alinéa [0017] * * alinéa [0019] - alinéa [0032]; figure 1 * * alinéa [0035] - alinéa [0036] * * alinéa [0057] * * alinéa [0065] - alinéa [0066]; figure 3 * * alinéa [0070] - alinéa [0072]; figure 4 * * alinéa [0076] - alinéa [0078]; figure 5 * * alinéa [0081] * * alinéa [0088] - alinéa [0093]; figures 8,9 * * alinéa [0112] - alinéa [0119]; revendications 1-3,18-20,24,30,33; figures 14,15 * -----	1-10	DOMAINES TECHNIQUES RECHERCHÉS (IPC)
X	US 2005/111351 A1 (SHEN NAIMING [US]) 26 mai 2005 (2005-05-26) * abrégé * * alinéa [0002] * * alinéa [0018] * * alinéa [0035] * * alinéa [0038] - alinéa [0045]; figures 1,7 * * alinéa [0048] - alinéa [0050] * * alinéa [0055] * * alinéa [0069] - alinéa [0078]; revendications 1-3,7,13-16 * ----- -/--	1-10	
Date d'achèvement de la recherche		Examineur	
31 juillet 2007		Todorut, Cosmin	
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			



RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 686334
FR 0653923

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	EP 1 318 648 A2 (NORTEL NETWORKS LTD [CA]) 11 juin 2003 (2003-06-11) * abrégé * * alinéa [0006] - alinéa [0009] * * alinéa [0012] * * alinéa [0025] - alinéa [0032]; revendications 1-4,14,15,20; figures 1,2 * -----	1-10	
A	EP 1 111 860 A2 (NORTEL NETWORKS LTD [CA]) 27 juin 2001 (2001-06-27) * le document en entier * -----	1-10	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
Date d'achèvement de la recherche		Examineur	
31 juillet 2007		Todorut, Cosmin	
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			

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0653923 FA 686334**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **31-07-2007**

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2006153067 A1	13-07-2006	AUCUN	
US 2006209682 A1	21-09-2006	WO 2006101825 A2	28-09-2006
US 2005111351 A1	26-05-2005	AUCUN	
EP 1318648 A2	11-06-2003	AUCUN	
EP 1111860 A2	27-06-2001	CA 2310872 A1	22-06-2001
		DE 60023828 D1	15-12-2005
		DE 60023828 T2	01-06-2006
		US 2004156310 A1	12-08-2004