(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 827 103**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **01 08820**

(51) Int Cl[7] : **H 04 L 12/56,** H 04 L 1/20

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 03.07.01.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 10.01.03 Bulletin 03/02.

(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) :** *ELYSEAN NETWORKS Société à responsabilité limitée* — FR.

(72) **Inventeur(s) :** CAI HUAIYU, L HOUR YVES MARIE et TABARDEL NICOLAS.

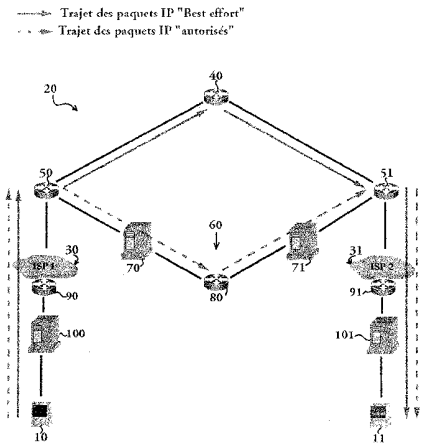
(73) **Titulaire(s) :**

(74) **Mandataire(s) :**

(54) PROCEDE DE ROUTAGE DE DONNEES PAR PAQUETS.

(57) La présente invention se rapporte à un procédé de routage de données par paquets entre une pluralité d'utilisateurs (10, 11) par l'intermédiaire d'un réseau de réseau de télécommunication du type Internet ou d'une interconnexion de réseaux de télécommunications (20), lesdits utilisateurs (10, 11) étant reliés chacun à un opérateur de réseau (30, 31) source et/ ou destination utilisant le protocole Internet IP, lesdits opérateurs de réseau (30, 31) étant reliés chacun à au moins un noeud d'échange (40), par l'intermédiaire d'un routeur (50, 51), caractérisée en ce que lesdites données sont marquées afin de les autoriser à emprunter au moins un noeud d'échange particulier (60) et en ce que l'on prévoit au moins un dispositif de filtrage (70, 71), autorisant lesdites données ainsi marquées à transiter par ledit noeud d'échange particulier (60).

La présente invention se rapporte également à un dispositif pour la mise en oeuvre du procédé.



FR 2 827 103 - A1

PROCÉDÉ DE ROUTAGE DE DONNÉES PAR PAQUETS

La présente invention se rapporte au domaine du routage de données par paquets sur les réseaux de télécommunication.

La présente invention se rapporte plus particulièrement à un procédé de routage de données par paquets entre une pluralité d'utilisateurs par l'intermédiaire d'un réseau de réseau de télécommunication du type Internet ou d'une interconnexion de réseaux de télécommunications, lesdits utilisateurs étant reliés chacun à un opérateur de réseau source et/ou destination utilisant le protocole Internet IP, lesdits opérateurs de réseau étant reliés chacun à au moins un nœud d'échange, par l'intermédiaire d'un routeur de bord.

On utilise, ci-après, le terme réseau dans le sens de système autonome (ou AS pour Autonomous System), c'est à dire un ensemble d'infrastructures informatiques et télécoms suivant une politique de routage identique. En général, le réseau d'un opérateur est constitué d'un seul AS, mais ce n'est pas nécessairement toujours le cas, et les procédés et dispositifs décrits dans ce document peuvent alors être utilisés pour améliorer les communications inter-AS au sein du réseau d'un même opérateur. Ceci dit, dans le but de simplifier les descriptions, dans la suite du document nous supposerons que le réseau d'un opérateur est constitué d'un AS unique.

Pour échanger du trafic avec le reste de l'Internet, un opérateur de réseau utilisant le protocole Internet IP peut envisager deux possibilités suivant la taille relative de son réseau par rapport à celle des autres réseaux. Soit il souscrit à un contrat de transit

(moyennant versement d'une compensation financière) auprès d'un autre opérateur, soit il négocie un accord d'interconnexion avec un autre opérateur sans compensation financière, dit accord de peering, public ou privé selon le site où s'effectue l'interconnexion.

Les trois caractéristiques du peering sont :

- Il n'y pas de compensations financières entre les opérateurs.

- Le trafic est échangé sur une base 'best effort', c'est à dire que chacun des opérateurs ne garantie aucune qualité de service au trafic qu'il reçoit d'un autre opérateur via un nœud de peering. En conséquence, les paquets de données IP sont échangés selon une politique 'patate chaude' (ou encore 'hot potato routing'), qui consiste, pour chaque opérateur à se débarrasser le plus rapidement possible du trafic qui est destiné à des adresses situées hors de son réseau.

- Dans un accord de peering, chacun des deux opérateurs ne donne accès qu'à son seul réseau ; c'est à dire que chaque opérateur accepte uniquement le trafic qui est destiné à une adresse IP appartenant à son propre réseau, et refuse de laisser des paquets générés à l'extérieur traverser son réseau pour atteindre une destination située sur un troisième réseau.

Pour nombre des nouvelles applications qui font chaque jour leur apparition sur l'Internet, notamment les applications temps réel, bidirectionnelles et interactives (comme par exemple la voix sur IP ou la vidéoconférence), le service de transport 'Best Effort' de l'Internet n'est plus adapté. La livraison en elle-même de l'information n'est plus suffisante. Ces applications exigent une certaine Qualité de Service (QoS pour Quality of Service)

de bout en bout que l'Internet est encore incapable de garantir.

La QoS correspond à un certain niveau de service qui peut être assuré à un élément du réseau (une application, une machine ou un routeur, par exemple) afin que ces exigences en terme de service et de trafic soient satisfaites. Les services avec QoS exigent la coopération de toutes les couches réseau de haut en bas, et celle de tous les éléments du réseau de bout en bout. La QoS de bout en bout correspond au minimum de celle de tous les segments du chemin emprunté par ce flux, entre l'expéditeur et le destinataire.

La QoS de bout en bout est absente de l'Internet public essentiellement pour deux raisons :

1- Du point de vue technologique, deux mécanismes fondamentaux nécessaires pour offrir les garanties de QoS de bout en bout sont absents de la plupart des réseaux de télécommunications IP : ce sont la signalisation et la gestion intelligente des files d'attente dans les équipements réseaux. Le réseau IP n'a ainsi aucun moyen d'informer une application à l'aide d'une signalisation adéquate de ce qu'elle peut exiger du réseau, ni d'anticiper les congestions en remontant les informations liées au trafic.

Les récentes avancées technologiques permettent d'ajouter de nombreux compléments au protocole IP pour combler l'absence des mécanismes cités ci-dessus. Le premier est le Resource ReSerVation Protocol (RSVP) qui offre les mécanismes de signalisation. Le second est le Differentiated Services (DiffServ) qui permet la gestion de priorité du trafic. Ces protocoles et algorithmes de gestion de QoS ne sont ni concurrents, ni mutuellement exclusifs. Ils sont au contraire complémentaires. Ils sont

conçus pour être utilisés ensemble afin de répondre à des exigences opérationnelles très variables dans différents contextes de réseau. Bien entendu, ils ne permettent pas, à eux seuls, de résoudre totalement la problématique technologique. En effet, tous ces protocoles permettent d'améliorer la qualité du trafic Internet sur un seul système autonome, mais ne permettent pas de résoudre ces problèmes lorsque les paquets IP doivent traverser plusieurs réseaux gérés par des opérateurs différents. C'est notamment à ce niveau qu'intervient la présente invention.

2- Du point de vue politique, aujourd'hui, sauf dans le cas d'un accord de transit, où l'opérateur client paye pour le trafic qu'il déverse chez l'opérateur fournisseur du transit, c'est toujours l'opérateur vendeur de services qui garde tout l'argent récolté et ne paye rien pour déverser du trafic chez l'autre opérateur. Ceci est vrai aussi bien pour les opérateurs participant à un accord de peering que pour l'opérateur fournisseur du transit vis-à-vis d'un de ses clients opérateurs. C'est le modèle Sender Keep All (SKA). Ce modèle d'interconnexion est le plus stable de l'industrie des opérateurs. Mais il n'est pas adapté aux exigences de QoS de bout en bout dans un environnement multi-opérateurs. La commercialisation des services garantissant la QoS de bout en bout nécessite la mise en place des mécanismes d'interconnexion de QoS portant, entre autres, sur des paramètres comme la latence (le temps de traversée du réseau), la gigue (la variation de la latence) et le taux de pertes ou d'erreurs, outre le seul paramètre de bande passante précisé habituellement. Elle oblige l'opérateur qui a initié le signal de QoS à partager le revenu généré par ce service de QoS avec tous les opérateurs qui interviennent sur le chemin emprunté par le flux de QoS de bout en bout.

La mise en place d'accords d'interconnexion avec garanties de qualité de service exige donc la mise en place préalable d'incitations ou de compensations financières entre les opérateurs, de façon similaire à l'industrie de la téléphonie. Or l'industrie des télécommunications téléphoniques diffère sur deux points de l'industrie des réseaux IP :

- Internet est basé sur la commutation par paquets, ou routage, qui est par nature non déterministe : on ne peut a priori pas connaître à l'avance le trajet qu'emploiera un paquet IP pour aller d'un point A à un point B. Il est donc difficile voire impossible de définir contractuellement les points d'interconnexion où un paquet IP donné passera d'un réseau à un nœud d'échange. Les opérateurs ont adopté en matière de peering la politique du routage « patate chaude » (ou « hot potato routing ») qui consiste pour un opérateur à se débarrasser le plus rapidement possible des paquets destinés à une adresse IP située hors de son réseau. L'opérateur de terminaison, quand à lui, va faire en sorte de recevoir ces paquets le plus tard possible (affectation du trafic reçu d'un autre opérateur à une file d'attente à priorité réduite, déconnexion du lien pendant de courte période, dégradation volontaire et/ou artificielle de la métrique…). Il en résulte que chaque nœud d'échange constitue actuellement un centre de conflit entre les politiques de routage des deux opérateurs. En téléphonie, la situation est bien entendu complètement différente dans la mesure où le circuit établi lors d'une communication est complètement prédéterminé.
- Contrairement à la téléphonie, la mesure de la qualité de service doit être effectuée sur les réseaux de bout en bout. En effet, en téléphonie, l'appelant envoie une

demande d'établissement de circuit point à point entre les deux réseaux pour une classe de service donnée. Cette demande est soit acceptée (auquel cas le circuit est effectivement établi avec cette classe de service, et les minutes de communication entre les deux points décomptées), soit rejetée (auquel cas, aucun circuit n'est établi, et il n'y a donc pas de trafic entre les deux points). Le réseau appelant sait donc que, lorsque le circuit est établi, la qualité de service est effectivement livrée de bout en bout, y compris sur le réseau de l'opérateur de terminaison. On constate que le cas d'Internet est effectivement différent puisque la problématique n'est pas binaire (circuit établi donc QoS effectivement livrée, ou circuit non établi, et donc aucune QoS effectivement livrée), dans la mesure où il peut y avoir livraison de paquets sans que l'opérateur de terminaison n'assure pour autant la qualité de service, et sans que l'opérateur envoyeur puisse avoir connaissance de la QoS effectivement livrée. Cette information ne peut aujourd'hui être mesurée et donnée au premier opérateur que par et avec le consentement de l'opérateur de terminaison ; On peut naturellement s'interroger sur la valeur donnée à cette information sans l'existence d'un tiers de confiance pour valider la mesure.

Les nœuds d'échange habituels (GIXs pour Global Internet eXchanges) proposent des infrastructures et des services d'interconnexion aux opérateurs. Ils sont hébergés dans des centres d'hébergement techniques spécialisés et sécurisés (datacenters, carrier hotels, telecom hotels…).

La plupart d'entre eux ne sont pas neutres: ils sont gérés par des opérateurs ou quelque fois par un consortium d'opérateurs. Ils ne sont pas en mesure de

garantir et de mesurer la Qualité de Service effectivement livrée de bout en bout parce qu'ils sont uniquement présents au point d'échange et utilisent des commutateurs ATM (invisibles au niveau IP).

Le peering public joue encore un rôle important dans l'interconnexion des grands réseaux Internet : les principaux opérateurs sont liés par des centaines d'accords bilatéraux de peering. Ces accords sont conclus sur une base 'best effort', et ils ne permettent donc pas de garantir des niveaux de performance quand les données sont envoyées d'un réseau à l'autre : les points de peering publics sont congestionnés.

Actuellement beaucoup d'opérateurs prétendent que 80% de leurs accords de peering sont privés, et la qualité du peering privé est supposée être meilleure. Cependant les utilisateurs constatent que, malgré tout, le trafic Internet reste lent et congestionné, alors que tous les 'tuyaux' des opérateurs sont complètement surdimensionnés. En effet, les paquets IP transitent et accèdent aux nœuds d'échange de façon non déterministe, ce qui ne permet pas aux opérateurs ni de prévoir a priori le coût effectif du transport de paquets IP d'un point A vers un point B avec des garanties de qualité de service, ni de garantir une quelconque qualité de service à leurs clients. Par ailleurs faire uniquement du peering privé de très haute qualité reviendrait extrêmement cher aux opérateurs dans la mesure ou seule une minorité de leurs clients serait prête à payer une prime à la QoS.

La présente invention entend remédier aux inconvénients de l'art antérieur.

Pour ce faire, la présente invention est du type décrit ci-dessus et elle est remarquable, dans son acception la plus large, en ce que lesdites données sont marquées afin de les autoriser à emprunter au moins un nœud d'échange particulier et en ce que l'on prévoit au moins un dispositif de filtrage, autorisant lesdites données ainsi marquées à transiter par ledit nœud d'échange particulier.

Lesdites données sont de préférence marquées au niveau d'éléments actifs au niveau IP (routeurs, serveurs…) situés entre le poste dudit utilisateur et un routeur de bord dudit opérateur de réseau source.

Ledit nœud d'échange particulier comporte de préférence au moins un routeur écran destiné à venir se connecter aux routeurs des opérateurs de réseau au niveau de la couche IP.

Ledit routeur écran annonce de préférence la présence du nœud d'échange particulier pour les données marquées et n'annonce pas la présence du nœud d'échange particulier pour les données non marquées.

Ledit marquage des données permet respectivement aux routeurs de bord de l'opérateur de router de préférence les paquets marqués du réseau de l'opérateur vers le routeur écran du nœud d'échange particulier.

Le nœud d'échange particulier filtre et n'accepte de préférence de router que les paquets correctement marqués.

Ledit nœud d'échange particulier n'accepte de préférence de transférer lesdites données que si les

opérateurs de réseau source et destination sont directement et/ou exclusivement reliés à un ou plusieurs nœuds d'échange particuliers.

Dans une variante, le nœud d'échange particulier est réalisé de façon virtuelle sur des infrastructures d'interconnexion déjà affectées à des interconnexions, en utilisant la possibilité de certains routeurs de porter plusieurs adresses IP différentes et de traiter différemment les paquets IP dirigés vers ces adresses différentes.

L'étape de marquage peut être réalisée de manière récursive, afin de permettre auxdits opérateurs de réseaux d'introduire une dose définie de déterminisme au trajet des paquets marqués au sein de leurs réseaux respectifs.

La présente invention se rapporte également à un dispositif pour la mise en œuvre du procédé selon l'invention.

Le dispositif est de préférence constitué au moins par une interconnexion de réseaux comportant une pluralité de nœuds d'échange particuliers.

Avantageusement, le procédé selon l'invention permet de prédéfinir de façon complètement déterministe le point où s'effectuera le transfert de paquets d'un réseau à l'autre, permettant ainsi à chaque opérateur de donner un prix à son service, et l'engageant par là même à assurer une qualité de service préalablement déterminée dans les termes d'un contrat de SLA (Service Level Agreement) aux paquets provenant d'un réseau extérieur (par exemple

compatibilité des politiques de routage avec celles de ses partenaires, non dégradation de la métrique, etc.).

Avantageusement également, le procédé selon l'invention permet aux opérateurs connectés au nœud d'échange particulier d'une part d'effectuer de la différenciation de service pour leurs clients finaux sans avoir à implémenter des protocoles spécifiques tels que DiffServ et MPLS sur leurs réseaux et d'autre part de proposer des services et des tarifs discriminés à leurs clients et maximiser ainsi leurs revenus.

L'administrateur du nœud d'échange particulier peut également jouer le rôle d'un tiers de confiance puisqu'il est capable, grâce aux dispositifs placés chez les utilisateurs finaux, de mesurer la qualité de service de bout en bout sur tous les systèmes autonomes, de façon à garantir aux opérateurs interconnectés via le nœud d'échange particulier une mesure neutre de la Qualité de Service sur tous les réseaux connectés au nœud d'échange particulier.

On comprendra mieux l'invention à l'aide de la description, faite ci-après à titre purement explicatif, d'un mode de réalisation de l'invention, en référence aux figures annexées :

- la figure 1 illustre le schéma des annonces de routes par les routeurs écrans dans le procédé selon l'invention ;
- la figure 2 illustre les trajets des paquets de données IP standards (ou paquets "Best effort"), et des paquets de données IP marqués (autorisés à accéder au nœud d'échange particulier), grâce au procédé selon l'invention ;

- la figure 3 illustre une utilisation récursive du procédé permettant à un opérateur de gérer le degré de déterminisme qu'il veut imposer au routage de certains paquets autorisés ;
- la figure 4 illustre un exemple de généralisation de l'utilisation du nœud d'échange particulier entre une pluralité d'opérateurs ; et
- la figure 5 illustre la réalisation d'un nœud d'échange particulier virtuel entre deux opérateurs de réseaux.

La présente invention concerne un procédé destiné à router et filtrer certains paquets de données réalisés sous protocole Internet IP (Internet Protocol), dits autorisés, envoyés par un premier système autonome d'un opérateur N°1 de réseau (30) source vers un nœud d'échange particulier (60) interconnecté à un ou plusieurs autres systèmes autonomes d'un opérateur N°2 de réseau destination (31), comme illustré figures 1 et 2. Les paquets autorisés sont déterminés selon divers paramètres (type d'application, adresse de source ou de destination...). Ce procédé peut notamment être utilisé pour permettre aux paquets de données IP autorisés de court-circuiter certains points de congestion de l'Internet (points de Peering, nœuds d'interconnexion de systèmes autonomes, etc.) et ainsi d'assurer des garanties de Qualité de Service (ou QoS) de bout en bout sur des réseaux gérés par des opérateurs différents.

Ce procédé utilise deux moyens : un premier dispositif de routage (100, 101), placé entre les postes des utilisateurs finaux (10, 11) et les routeurs de bord côté clients (90, 91), permettant de "marquer" les paquets autorisés à emprunter le nœud d'échange particulier (60),

et un second moyen de filtrage (70, 71), placé entre les routeurs des opérateurs (50, 51) et celui (80) du nœud d'échange particulier, qui "nettoie" les paquets "marqués" et assure qu'aucun paquets non autorisé n'accède au nœud d'échange particulier.

Selon la présente invention, l'administrateur du nœud d'échange particulier (60) peut mesurer la QoS entre les deux dispositifs de routage (100, 101) placés chez les clients finaux. Par ailleurs, l'administrateur du nœud d'échange particulier (60) peut agir comme une chambre de compensation entre tous les opérateurs de façon à leur garantir que le trafic qu'ils envoient sur le nœud d'échange particulier (60) sera traité avec une classe de service déterminée de la source jusqu'à sa destination moyennant une éventuelle compensation financière.

Les points de peering publics ou privés classiques ne disposent ni des infrastructures, ni du modèle économique qui leur permettrait d'offrir des garanties de QoS de bout en bout similaires à celles rendues possibles par le procédé selon l'invention. En effet, ces nœuds d'échange utilisent exclusivement des commutateurs ATM alors que la gestion des paramètres de QoS nécessite une gestion au niveau IP (au niveau 3 du modèle OSI (Open System Interconnection)) et donc un routeur (80), appelé écran, uniquement accessible aux paquets autorisés.

La solution proposée permet ainsi aux opérateurs connectés au nœud d'échange particulier de proposer à leurs clients (10, 11) des services qu'ils ne sont pas en mesure de réaliser seuls (par exemple Réseaux Privés Virtuels IP multi-opérateurs pour Intranet ou Extranet entre plusieurs organismes, Voix sur IP et vidéoconférence entre différents systèmes autonomes…).

La solution selon l'invention consiste à :

- Disposer des nœuds d'échange particuliers (60), déployés dans les principaux datacenters (centres d'hébergement de matériel télécoms, …) où s'effectuent notamment les échanges de trafic IP entre opérateurs (accords de Peering, achat de transit …). Ces différents nœuds d'échange particuliers peuvent éventuellement être eux-mêmes reliés entre eux par un réseau (par exemple de fibres optiques), que ce soit à une échelle locale, métropolitaine, nationale ou internationale, de façon à rendre équivalents tous ces points. Dans chacun de ces nœuds d'échange, on placera un ou plusieurs routeurs dits écrans (80) qui viendront s'interconnecter aux routeurs de peering ou routeurs de bord (50, 51) des opérateurs au niveau de la couche IP.
- Prévoir des dispositifs (logiciel ou matériel) de routage (100, 101) et de filtrage (70, 71) qui permettent aux flux de paquets IP autorisés initiés par les utilisateurs finaux connectés aux réseaux des opérateurs interconnectés via le nœud d'échange particulier d'être déversés sur le nœud d'échange sans les autres flux 'best effort' (non autorisés).
- Réaliser l'interconnexion des réseaux des opérateurs connectés au nœud d'échange particulier entre lesquels l'administrateur du nœud d'échange peut, éventuellement, jouer un rôle de chambre de compensation et/ou de tiers de confiance (en assurant la mesure de la qualité de service effectivement livrée de bout en bout et en redistribuant les pénalités et compensations financières entre opérateurs).

La Figure 2 représente la mise en place des deux parties du dispositif de routage/filtrage au sein des

trois réseaux, ainsi que les trajets des paquets IP non autorisés (ou paquets "Best effort"), représenté en traits pleins, et des paquets IP "autorisés" (autorisés à accéder au nœud d'échange particulier), représenté en traits pointillés, lorsque les paquets doivent aller du réseau de l'opérateur N°1, opérateur de réseau (30) source, vers le réseau de l'opérateur N°2, opérateur de réseau (31) destination.

Le concept de ce filtrage permet de réaliser un passage et/ou un réseau invisibles pour tous les routeurs des réseaux adjacents et utilisables uniquement par les paquets autorisés.

Le ou les routeur(s) écran(s) (80) de ce nœud d'échange particulier (60) n'annonce(nt) aucune route aux routeurs de bord (50, 51) des autres réseaux similaires au réseau de l'opérateur source (30). Ainsi, aucun paquet non autorisé ne sera dirigé vers ces routeurs. Par contre les routeurs écrans (80) du nœud d'échange signalent leur existence comme tout routeur, en envoyant des signaux KEEPALIVE (commande utilisée pour vérifier qu'un interlocuteur est effectivement actif) à leurs voisins (50, 51), de façon à ce que la route correspondante reste ouverte (ne soit pas fermée par les voisins …).

Dans son principe, le dispositif est réalisable d'au moins deux manières différentes, suivant les références, les technologies et les politiques des utilisateurs, des administrateurs du nœud d'échange particulier et/ou des utilisateurs finaux : par des technologies de routage à la source (source-routing), ou par un procédé d'encapsulation.

Les nœuds d'échange particuliers (60) acceptent les paquets IP autorisés confiés par les systèmes autonomes des opérateurs connectés aux nœuds d'échange particuliers et déversent sur leurs réseaux les trafics autorisés en provenance d'autres réseaux d'opérateurs interconnectés aux nœuds d'échange particuliers. Les nœuds d'échange particuliers (60) n'acceptent de transporter des flux que si les deux extrémités de ces flux se trouvent dans le réseau de deux opérateurs interconnectés directement aux nœuds d'échange particuliers.

Chaque nœud d'échange particulier ne communique donc avec d'autres réseaux que via des routeurs écrans de façon à demeurer totalement invisible vis à vis des routeurs de bords des réseaux adjacents. Le nœud d'échange particulier ne reçoit donc que des paquets marqués, il les désencapsule et les transmet aux réseaux destinataires si ceux-ci sont connectés directement au nœud d'échange particulier, le réseau de destination s'engageant contractuellement à traiter les paquets IP qui lui sont transmis par le nœud d'échange particulier avec certaines garanties de qualité de service, ; notamment au niveau de l'interconnexion avec le nœud d'échange (60). Des compensations financières peuvent éventuellement être mises en place afin d'inciter les opérateurs à livrer cette qualité de service de bout en bout.

Les paquets IP autorisés seront donc traités avec une qualité de service particulière de bout en bout au travers des trois systèmes autonomes au moins traversés (AS du premier opérateur, au moins un nœud d'échange particulier, AS du deuxième opérateur).

La solution de routage/filtrage selon l'invention utilise les technologies de routage à la source

(source-routing) et/ou d'encapsulation qui permettent aux opérateurs connectés au nœud d'échange particulier d'envoyer à ce dernier uniquement des flux QoS qu'ils souhaitent lui confier. Le système de filtrage (70, 71) placé au niveau du nœud d'échange particulier permet donc ainsi de recevoir sur le nœud particulier uniquement des paquets marqués et de détruire les paquets non autorisés qui auraient pu y parvenir.

Les deux dispositifs constituant le système de routage/filtrage sont plus précisément décrits dans les lignes qui suivent (cf. figure 2) :

Le premier dispositif de routage (100, 101) se décline en plusieurs versions suivant le réseau des opérateurs. Il est placé entre les « Customer Terminal Devices », utilisateurs (10, 11) et les « Customer Edge Routers », routeurs de bord (90, 91) :

- Il marque le champ TOS (Type of Service) de l'en-tête des paquets IP autorisés pour distinguer les paquets autorisés des paquets non autorisés, et éventuellement les traiter de façon différenciées au niveau des nœuds d'échange particuliers.
- Il dirige les paquets autorisés vers le nœud d'échange particulier (60) :
  - si l'opérateur dispose d'un réseau MPLS, ce dispositif utilise un tunnel MPLS pour diriger le trafic autorisé directement vers le routeur écran (80) du nœud d'échange particulier.
  - si l'opérateur ne dispose pas d'un réseau MPLS mais qu'il supporte le routage à la source (source-routing), le dispositif utilise le routage à la source (par exemple le routage mou ou Loose Routing) qui permet d'imposer le passage, entre l'adresse IP source et l'adresse IP destination, par le routeur écran (80) du nœud

d'échange caractérisé lui-même par une adresse IP intermédiaire.

- Si l'opérateur ne supporte pas le routage à la source (source-routing), le dispositif utilise un procédé d'encapsulation IP (par exemple IP tunneling) de façon à faire passer les paquets marqués par l'adresse IP tampon du routeur écran (80), avant de les diriger au final vers l'adresse IP de destination de l'utilisateur destination (11).

Ces techniques permettent de faire en sorte que le trafic originaire d'un premier opérateur de réseau (30) (hébergeant la machine d'adresse IP source), destiné à un deuxième opérateur de réseau (31) (hébergeant la machine d'adresse IP destination) passe par un routeur d'adresse particulière (l'adresse du routeur écran (80) en question appartenant au nœud d'échange particulier (60)). Ainsi, les routeurs (50, 51) routent ces paquets vers le routeur écran (80) sans se préoccuper plus avant du fait que selon leurs tables de routage ce routeur constitue une voie sans issue.

Ce premier dispositif peut prendre la forme d'une carte physique ou d'un logiciel implanté au niveau des postes utilisateurs qui désirent envoyer des paquets autorisés. Les cartes doivent être enchâssées sur des serveurs hébergés sur le réseau. Plusieurs types de cartes sont proposées de façon à s'adapter aux différents systèmes d'exploitation utilisés sur les serveurs (Linux, Windows NT, Windows 98, Windows 2000 …, marques déposées)

Le second dispositif, le dispositif de filtrage (70, 71) est un filtre qui est placé entre les routeurs de bord (50, 51) des opérateurs et le routeur écran (80) qui

communique avec les routeurs de bord (50, 51). Il effectue plusieurs tâches :

- Il filtre tous les paquets à destination du routeur écran (80) du nœud d'échange et élimine tous les paquets non autorisés.
- Il filtre tous les messages BGP d'annonce de routes du routeur écran (80) à l'attention des routeurs de bord (50, 51) des opérateurs sans toucher aux autres messages de routage. Par conséquent, pour les routeurs de bord (50, 51) des opérateurs, le routeur écran (80) du nœud d'échange ne connaît aucune route mais reste 'vivant'.
- Si le premier dispositif, le dispositif de routage (100, 101) utilise l'encapsulation, le second doit aussi désencapsuler les paquets.

Ce deuxième dispositif est, de préférence, placé au niveau du nœud d'échange particulier (60), par exemple sur les routeurs écrans (80). Certaines des fonctionnalités de ce dispositif peuvent être directement configurables sur certains routeurs, et ne nécessitent donc pas obligatoirement l'adjonction d'une carte ou d'un logiciel. Une carte physique ou un logiciel peuvent néanmoins être implanté à ce niveau afin de compléter les fonctionnalités des routeurs écrans (filtrage, sécurisation …). Le protocole MPLS (MultiProtocol Label Switching) est, de préférence, implémenté sur l'ensemble du nœud d'échange particulier (60).

Les paquets IP autorisés, parvenus au niveau du nœud d'échange particulier (60), sont ensuite transmis au réseau de l'opérateur hébergeant l'adresse IP de destination et connecté au nœud d'échange particulier.

Le nœud d'échange particulier utilise le RSVP pour allouer de la bande passante aux 'tunnels' MPLS. En

combinant les trois protocoles RSVP, DiffServ et MPLS, le nœud d'échange est capable de garantir la QoS sur le réseau local ou métropolitain. Pour pouvoir garantir la QoS de bout en bout, il faut que les deux opérateurs source et destination assurent également la QoS sur leurs réseaux respectifs, et surtout, l'échange de la QoS à la transmission des paquets au niveau de la frontière.

Avec des opérateurs disposant d'un réseau MPLS, le nœud d'échange particulier peut échanger le label qui contient les paramètres de QoS. Avec les autres opérateurs, on utilise le champ DS (inclus dans le champ TOS) pour marquer les paquets (DiffServ) avant qu'ils quittent le routeur de bord (90, 91) des opérateurs.

Quelques remarques sur ce procédé et son utilisation :

La solution proposée concerne uniquement les paquets sortants qui ne peuvent pas véhiculer une attaque extérieure contre l'émetteur si son système de défense fonctionne correctement.

Tous les paquets transitant par le nœud d'échange particulier sont désencapsulés et transmis au réseau de l'opérateur destinataire. Il n'existe donc pas de problème spécifique vis-à-vis des dispositifs de protection du type 'firewalls' des réseaux qui reçoivent les paquets.

Dans le cas où un dispositif à translation d'adresse est implémenté sur le réseau, on peut placer le dispositif en aval des routeurs NAT.

Si l'opérateur est déjà en mesure de garantir la QoS à l'intérieur de son réseau, l'impact de la solution sur son réseau est minime, puisque le dispositif proposé s'adapte au réseau de l'opérateur, et pas l'inverse. L'opérateur peut s'interconnecter au nœud d'échange

particulier à son point de peering habituel. Il suffit que l'opérateur garantisse la bande passante entre les utilisateurs finaux (10, 11) situés sur son réseau et sa tête de pont constituée par le routeur (50, 51) au point de peering.

L'opérateur ne risque pas plus de perturbations avec le nœud d'échange particulier qu'avec son propre réseau car le nœud d'échange particulier est construit pour assurer uniquement la QoS tandis que le sien doit mélanger 'Best Effort' et QoS

Les techniques de cryptographie au-dessus de la couche transport (couche 4 du modèle Open System Interconnection - OSI) TCP ou UDP, sont par essence compatibles avec toutes ces technologies de QoS/Ingénierie des réseaux.

L'utilisation récurrente du système décrit dans la présente demande de brevet peut également permettre aux opérateurs des systèmes autonomes connectés au nœud d'échange particulier d'imposer une dose bien définie de déterminisme au routage de certains paquets lorsqu'ils circulent sur leur système autonome (cf. figure 3).

En effet, il est possible d'utiliser de façon récurrente le processus d'encapsulation de façon à imposer le passage par plusieurs routeurs écrans intermédiaires (82) du réseau d'un premier opérateur de réseau (30) N° 1. C'est-à-dire qu'il devient possible d'imposer aux paquets IP autorisés, non seulement le point de passage d'un système autonome à l'autre (passage obligé par le routeur écran du nœud d'échange particulier 60), mais également un certain nombre d'autres points intermédiaires permettant à l'opérateur d'un premier système autonome de contrôler à son gré le nombre et le numéro IP des routeurs écrans intermédiaires (82) par lesquels il souhaite imposer le passage de certains paquets IP. Pour chaque point de

passage imposé, il est alors nécessaire de réaliser une encapsulation du type IP-IP, comme décrit plus haut. Ces encapsulations peuvent être effectuées soit juste après leur génération sur le poste de l'utilisateur source (10), soit sur la route de leur acheminement avant le premier routeur imposé (90). Chaque routeur intermédiaire joue alors le rôle d'un routeur écran intermédiaire dont le principe de fonctionnement est similaire à celui du nœud d'échange particulier. Les paquets IP autorisés subissent ainsi une désencapsulation au niveau de chaque routeur écran intermédiaire. La figure 3 illustre le cas où l'opérateur 1 a choisi d'imposer deux routeurs écran intermédiaires sur son réseau. Entre ces routeurs, le routage des paquets suit la politique de routage en vigueur sur le réseau de l'opérateur 1 et reste donc a priori non déterministe.

Il est également possible, comme illustré figure 4, d'imaginer la traversée de plus de deux système autonomes, chaque interconnexion de systèmes autonomes étant réalisée grâce à un nœud d'échange particulier (60, 61). Dans ce cas les réseaux des opérateurs pouvant transporter des paquets marqués ne sont plus nécessairement exclusivement les réseaux des opérateurs d'initiation et de terminaison du trafic. Il est alors possible de faire transiter les paquets IP autorisés via un ou plusieurs autres opérateurs (32) N°3 pourvu qu'à chaque fois que les paquets autorisés passent d'un réseau à l'autre, ce soit via un nœud d'échange particulier. Ce procédé peut se révéler particulièrement intéressant lorsque les opérateurs d'initiation et de terminaison du trafic n'ont pas passé directement un accord d'interconnexion bilatéral via un nœud d'échange particulier.

La figure 4 illustre utilisation de plusieurs nœuds d'échange particuliers (60, 61) afin d'assurer la QoS à travers plus de deux réseaux d'opérateurs :

Un utilisateur (10) situé sur le réseau de l'opérateur 1 souhaite envoyer des paquets IP vers un utilisateur (11) situé sur le réseau de l'opérateur 2. Les opérateurs de réseau (30, 31) source et destination utilisant le protocole Internet (opérateurs 1 et 2) ne sont pas directement interconnectés via un nœud particulier (60, 61). Ce peut être le cas de deux opérateurs locaux situés dans des zones géographiques éloignées (un opérateur local en Asie, et un opérateur local en Europe par exemple). Ces deux opérateurs ne peuvent communiquer entre eux qu'en utilisant un ou plusieurs opérateurs de réseau (32) intermédiaires, dits opérateurs de transit, disposant d'un réseau reliant ces deux zones géographiques éloignées (« opérateurs tiers N°3 », par exemple, disposant d'un réseau mondial). Sur la figure 4, l'opérateur N°3 joue le rôle d'opérateur de transit entre les deux opérateurs opérateur N°1 et opérateur N°2.

Le dispositif peut être mis en place de deux façons.

On peut, d'une part procéder en encapsulant les paquets autorisés en une fois sur le réseau émetteur. En ce cas, les paquets IP autorisés émis par l'utilisateur (10) situé sur le réseau de l'opérateur 1 sont encapsulés deux fois (IP-IP décrit dans la première partie du document) et dirigés vers le routeur écran (80) du nœud d'échange particulier 1. Le dispositif placé au niveau du premier nœud d'échange particulier (60) va alors désencapsuler une première fois les paquets, puis les router en direction du routeur écran (81) du prochain nœud d'échange particulier (61) sur le trajet jusqu'à l'opérateur 2 de terminaison.

On peut, d'autre part, procéder en encapsulant une seule fois les paquets par exemple au niveau du routeur d'entrée (90, 92) de chaque réseau, et en les désencapsulant au niveau du nœud d'échange particulier (80, 81) auquel ils sont ensuite transmis.

Enfin, comme illustré figure 5, il faut noter que tous ces dispositifs peuvent être implantés de façon virtuelle directement sur les routeurs de bords (50, 51) des opérateurs, sans que la mise en place physique d'un nœud d'échange particulier soit nécessaire : certains routeurs (50, 51) peuvent en effet porter plusieurs adresse IP et traiter avec des priorités différentes les paquets adressés à l'une ou l'autre de ces adresses ; il suffit donc de réserver l'une de ces adresses qui sera utilisée exclusivement pour le routage des paquets autorisés. On réalise ainsi un nœud d'échange particulier complètement virtuel qui ne nécessite pas la mise en place physique de nouveaux routeurs et de nouveaux liens. Les paquets autorisés et non autorisés utilisent alors les mêmes liens entre les opérateurs, mais sont traités de façon différenciée au niveau des routeurs de bord (50, 51). Chacun des routeurs (50, 51) joue alors le rôle d'un routeur écran lorsqu'il reçoit les paquets IP générés sur le réseau de l'autre opérateur.

L'invention est décrite dans ce qui précède à titre d'exemple. Il est entendu que l'homme du métier est à même de réaliser différentes variantes de l'invention sans pour autant sortir du cadre du brevet.

REVENDICATIONS

1. Procédé de routage de données par paquets entre une pluralité d'utilisateurs (10, 11) par l'intermédiaire d'un réseau de réseau de télécommunication du type Internet ou d'une interconnexion de réseaux de télécommunications (20), lesdits utilisateurs (10, 11) étant reliés chacun à un opérateur de réseau (30, 31) source et/ou destination utilisant le protocole Internet IP, lesdits opérateurs de réseau (30, 31) étant reliés chacun à au moins un nœud d'échange (40), par l'intermédiaire d'un routeur de bord (50, 51), caractérisée en ce que lesdites données sont marquées afin de les autoriser à emprunter au moins un nœud d'échange particulier (60) et en ce que l'on prévoit au moins un dispositif de filtrage (70,71), autorisant lesdites données ainsi marquées à transiter par ledit nœud d'échange particulier (60).

2. Procédé de routage de données par paquets selon la revendication 1, caractérisée en ce que lesdites données sont marquées au niveau d'éléments actifs au niveau IP (routeurs, serveurs…) situés entre le poste dudit utilisateur (10, 11) et un routeur de bord (90, 91) dudit opérateur de réseau (30, 31) source.

3. Procédé de routage de données par paquets selon la revendication 1 ou la revendication 2, caractérisée en ce que ledit nœud d'échange particulier (60) comporte au moins un routeur écran (80) destiné à venir se connecter aux routeurs (50, 51) des opérateurs de réseau (30, 31) au niveau de la couche IP.

4. Procédé de routage de données par paquets selon la revendication 3, caractérisée en ce que ledit routeur écran annonce la présence du nœud d'échange particulier (60) pour les données marquées et n'annonce pas

la présence du nœud d'échange particulier (60) pour les données non marquées.

5. Procédé de routage de données par paquets selon l'une quelconque des revendications 1 à 4, caractérisée en ce que le marquage desdites données permet respectivement aux routeurs (50, 51) de router lesdits paquets marqués dudit opérateur de réseau (30, 31) vers ledit routeur écran (80) du nœud d'échange particulier (60).

6. Procédé de routage de données par paquets selon l'une quelconque des revendications 1 à 5, caractérisée en ce que ledit nœud d'échange particulier (60) filtre et n'accepte de router que les paquets correctement marqués.

7. Procédé de routage de données par paquets selon l'une quelconque des revendications 1 à 6, caractérisée en ce que ledit nœud d'échange particulier (60) n'accepte de transférer lesdites données que si les opérateurs de réseau (30, 31) source et destination sont directement et/ou exclusivement reliés à un ou plusieurs nœuds d'échange particuliers (60).

8. Procédé de routage de données par paquets selon l'une quelconque des revendications 1 à 7, caractérisée en ce que ledit nœud d'échange particulier (60) est réalisé de façon virtuelle sur des infrastructures d'interconnexion déjà affectées à des interconnexions, en utilisant la possibilité de certains routeurs de porter plusieurs adresses IP différentes et de traiter différemment les paquets IP dirigés vers ces adresses différentes.

9. Procédé de routage de données par paquets selon l'une quelconque des revendications 1 à 6, caractérisée en ce que l'étape de marquage est réalisée de manière récursive, afin de permettre auxdits opérateurs de réseaux d'introduire une dose définie de déterminisme au

trajet des paquets marqués au sein de leurs réseaux respectifs.

10. Dispositif pour la mise en œuvre du procédé selon l'une quelconque des revendications 1 à 9.

11. Dispositif selon la revendication 10, caractérisée en ce qu'il est constitué au moins par une interconnexion de réseaux comportant une pluralité de nœuds d'échange particuliers (60).

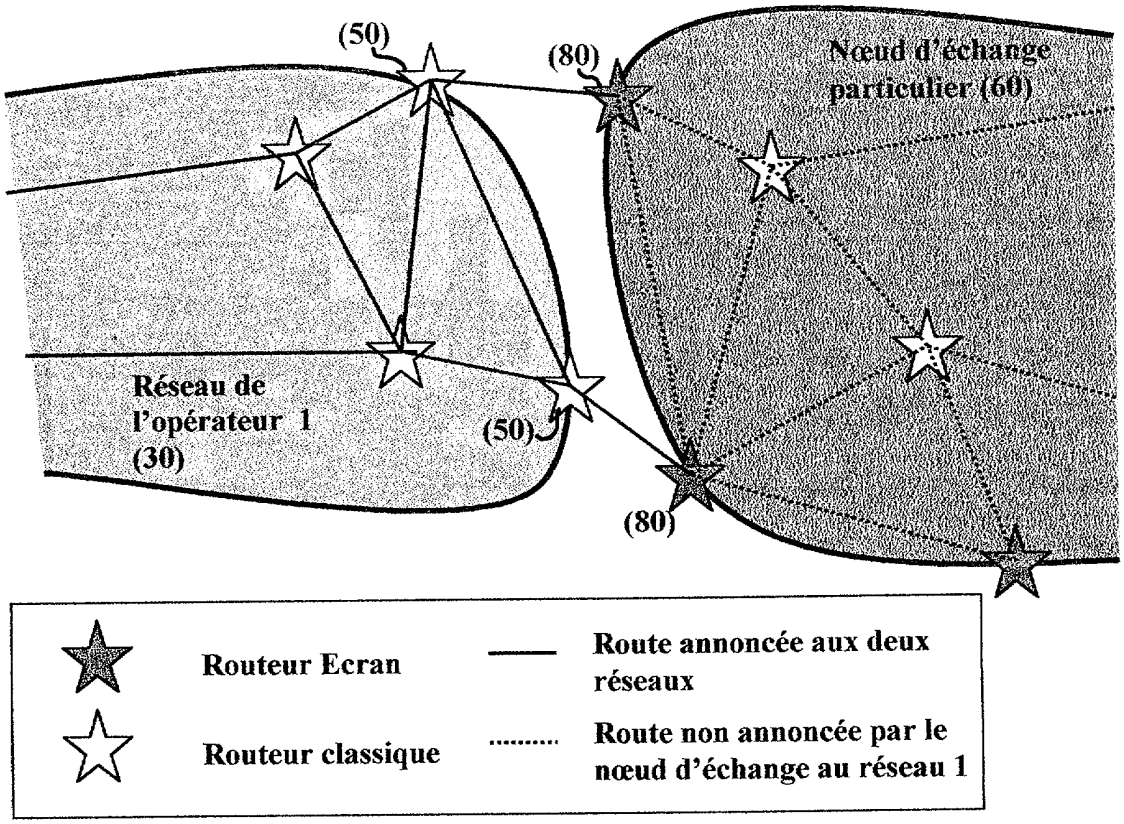

(50)
(80)
Nœud d'échange particulier (60)
Réseau de l'opérateur 1 (30)
(50)
(80)
Routeur Ecran
Routeur classique
Route annoncée aux deux réseaux
Route non annoncée par le nœud d'échange au réseau 1

FIG. 1

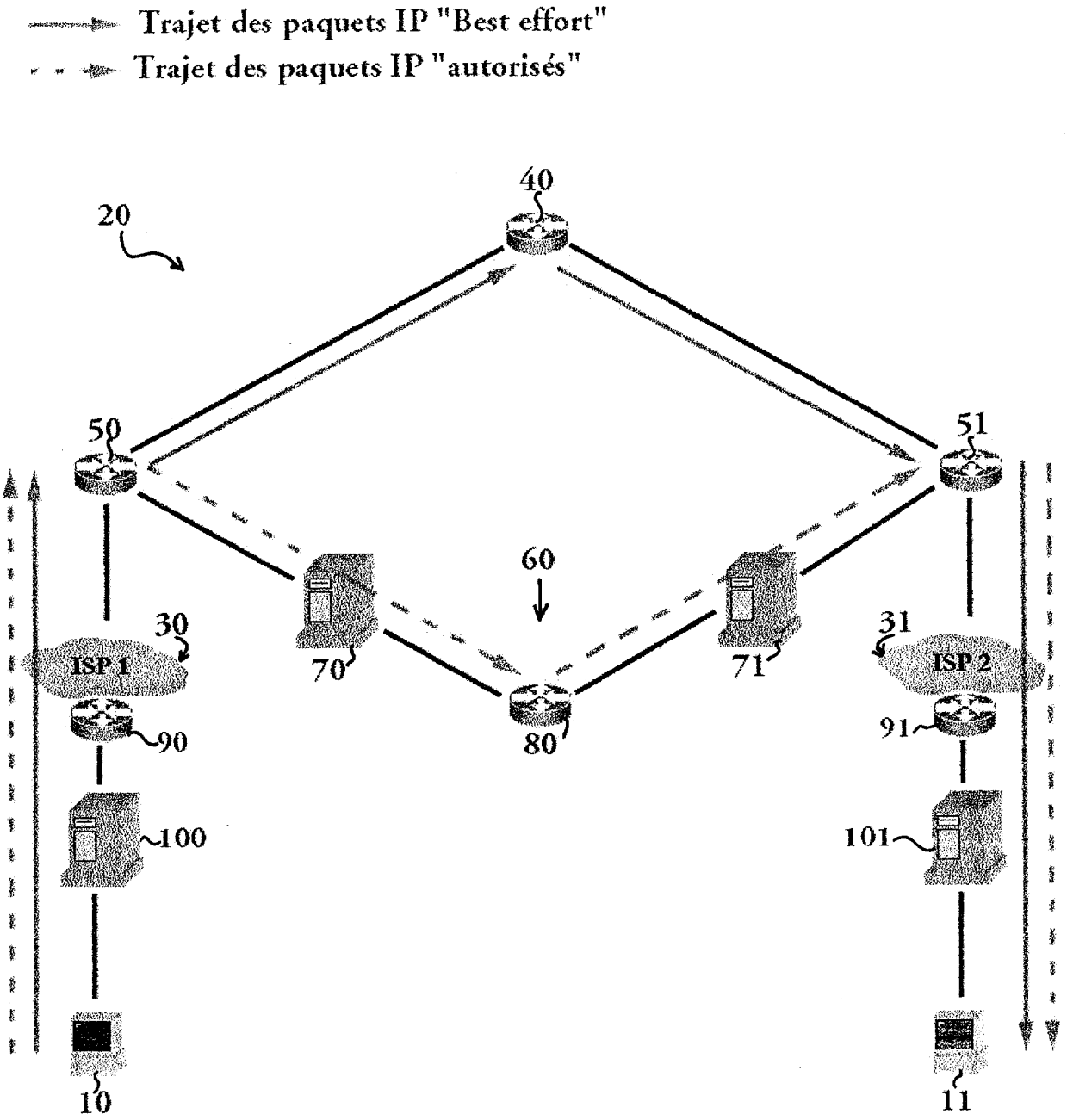

Trajet des paquets IP "Best effort"
Trajet des paquets IP "autorisés"
20
40
50
51
60
30
31
ISP 1
ISP 2
70
71
80
90
91
100
101
10
11

FIG. 2

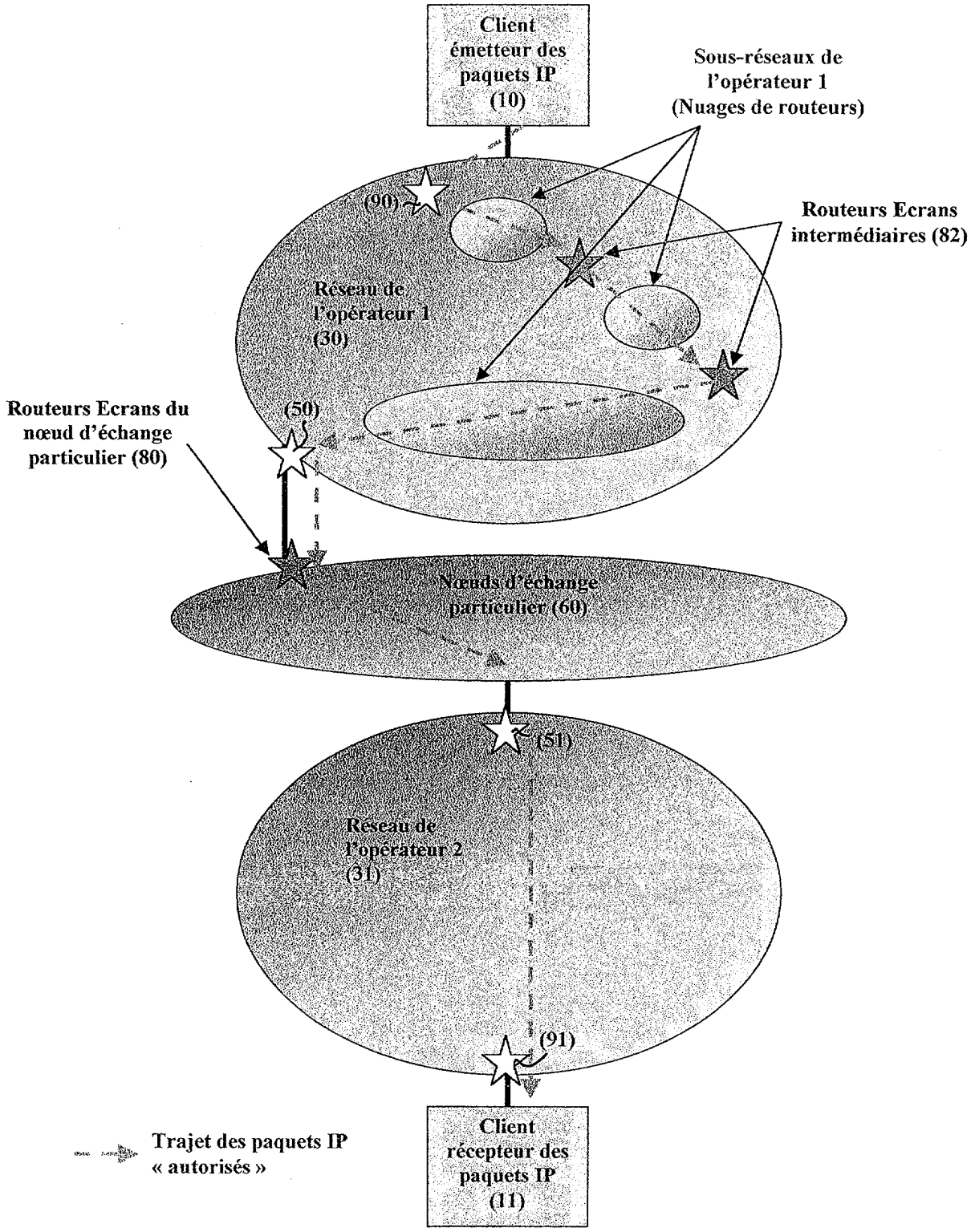

Client émetteur des paquets IP (10)
Sous-réseaux de l'opérateur 1 (Nuages de routeurs)
(90)
Routeurs Ecrans intermédiaires (82)
Réseau de l'opérateur 1 (30)
Routeurs Ecrans du nœud d'échange particulier (80)
(50)
Nœuds d'échange particulier (60)
(51)
Réseau de l'opérateur 2 (31)
(91)
Client récepteur des paquets IP (11)
Trajet des paquets IP « autorisés »

FIG. 3

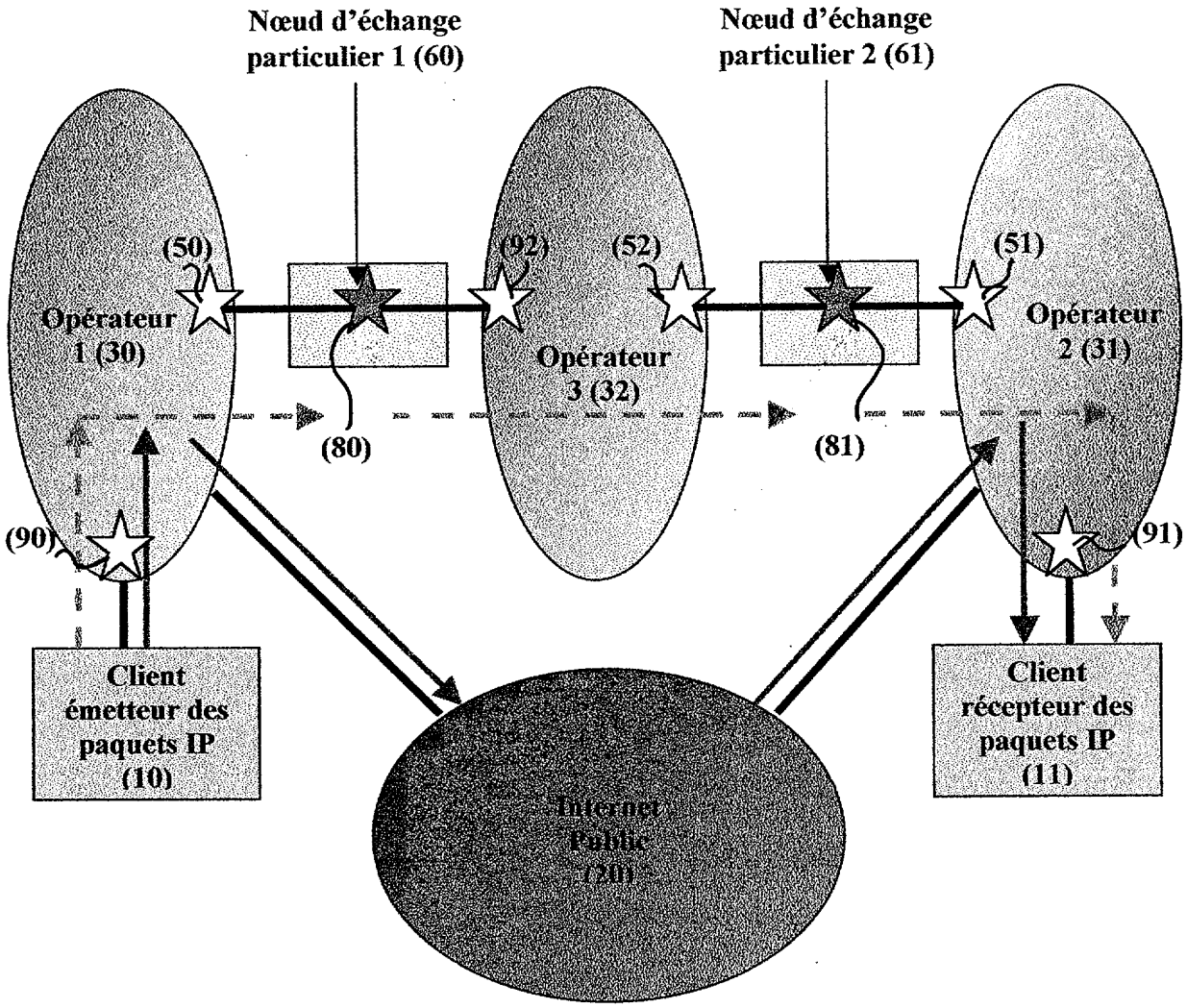

Nœud d'échange particulier 1 (60)
Nœud d'échange particulier 2 (61)
(50)
(92)
(52)
(51)
Opérateur 1 (30)
Opérateur 3 (32)
Opérateur 2 (31)
(80)
(81)
(90)
(91)
Client émetteur des paquets IP (10)
Client récepteur des paquets IP (11)
Internet Public (20)
Trajet des paquets IP "autorisés"
Trajet des paquets IP "Best effort"

FIG. 4

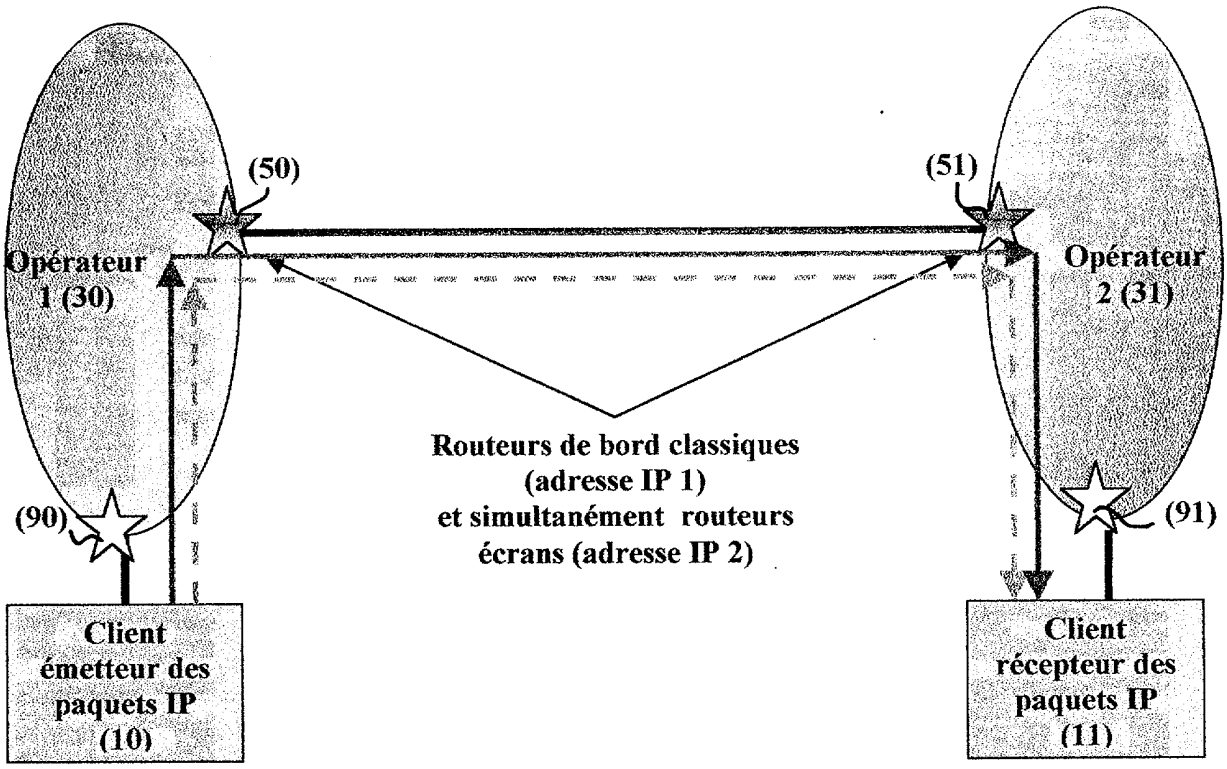

(50)
(51)
Opérateur 1 (30)
Opérateur 2 (31)
Routeurs de bord classiques (adresse IP 1) et simultanément routeurs écrans (adresse IP 2)
(90)
(91)
Client émetteur des paquets IP (10)
Client récepteur des paquets IP (11)
Trajet des paquets IP "autorisés"
Trajet des paquets IP "Best effort"

FIG. 5

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2827103

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 608155
FR 0108820

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 [1]		
X	EP 0 404 443 A (AMERICAN TELEPHONE & TELEGRAPH) 27 décembre 1990 (1990-12-27) * colonne 4, ligne 28 - ligne 33 * * colonne 8, ligne 26 - ligne 30 * * colonne 8, ligne 47 - ligne 52 * * colonne 9, ligne 31 - ligne 34 * * colonne 10, ligne 1 - ligne 7 *	1-11	H04L12/56 H04L1/20
A	WO 01 15386 A (ERICSSON TELEFON AB L M) 1 mars 2001 (2001-03-01) * page 3, ligne 7 - page 4, ligne 22 *	1-11	
A	WO 01 22686 A (INFINEON TECHNOLOGIES CORP) 29 mars 2001 (2001-03-29) * page 3, alinéa 4 - page 4, alinéa 1 *	1-11	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			H04L

Date d'achèvement de la recherche: 21 février 2002

Examinateur: Veen, G

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

1

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0108820 FA 608155

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 21-02-2002
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
EP 0404443 A	27-12-1990	US 5042032 A	20-08-1991
		CA 2015402 A1	23-12-1990
		EP 0404443 A2	27-12-1990
		JP 3131145 A	04-06-1991
WO 0115386 A	01-03-2001	AU 6331700 A	19-03-2001
		WO 0115386 A2	01-03-2001
WO 0122686 A	29-03-2001	WO 0122686 A1	29-03-2001

EPO FORM P0465