

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

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
7 septembre 2007 (07.09.2007)

PCT

(10) Numéro de publication internationale
WO 2007/099245 A2

(51) Classification internationale des brevets :
H04L 12/26 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2007/050800

(22) Date de dépôt international :
14 février 2007 (14.02.2007)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0650695 28 février 2006 (28.02.2006) FR

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

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : **TRUONG, Patrick** [FR/FR]; Résidence du Léguer, Appartement B04, 7, allée Clémenceau, F-22300 Lannion (FR). **STEPHAN, Emile** [FR/FR]; Route de Pors Gelen, Ile Grande, F-22560 Pleumeur Bodou (FR). **BOUCAUD, Frédéric** [FR/FR]; 6, rue des Hortensias, F-22700 Louannec (FR).

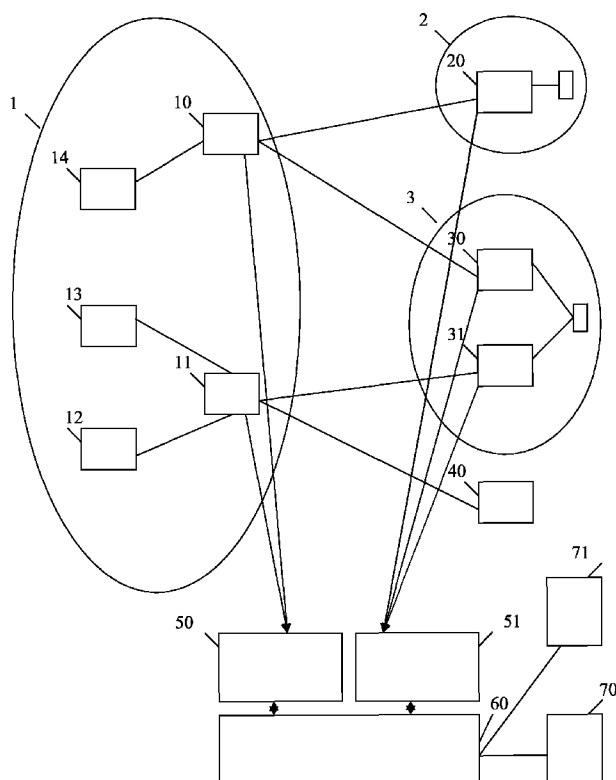
(74) Mandataire : **FRANCE TELECOM R & D/PIV/BREVETS**; Isabelle LECOMTE, 38-40, rue du Général Leclerc, F-92794 Issy les Moulineaux Cedex 9 (FR).

(81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP,

[Suite sur la page suivante]

(54) Title: METHOD OF COLLECTING DESCRIPTIONS OF STREAMS PERTAINING TO STREAMS RELATING TO AT LEAST ONE CLIENT NETWORK ATTACHED TO AN INTERCONNECTION NETWORK

(54) Titre : PROCEDE DE COLLECTE DE DESCRIPTIONS DE FLUX PORTANT SUR DES FLUX RELATIFS A AU MOINS UN RESEAU CLIENT RATTACHE A UN RESEAU D'INTERCONNEXION



(57) Abstract: Method of collecting descriptions of streams pertaining to streams relating to at least one client network, the client network being attached to an interconnection network comprising: a first step of receiving descriptions of streams, the descriptions of streams pertaining to streams originating from the client network; a first step of aggregating the descriptions of streams pertaining to the streams originating from the client network as a function of an aggregation criterion; a first step of transmitting descriptions of aggregated streams to a collection equipment; characterized in that it furthermore comprises: a step of analysing the descriptions of the streams pertaining to the streams originating from the client network so as to determine at least one stream characteristic specific to the client network; a second step of receiving descriptions of streams, said descriptions of streams pertaining to streams originating from the interconnection network; a step of filtering the descriptions of streams pertaining to the streams originating from the interconnection network, in which the descriptions of streams pertaining to streams that are devoid of the determined stream characteristic specific to the client network are eliminated; a second step of transmitting the filtered descriptions of streams to the collection equipment.

[Suite sur la page suivante]

WO 2007/099245 A2



KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) **États désignés** (*sauf indication contraire, pour tout titre de protection régionale disponible*) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT,

RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

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

(57) Abrégé : Procédé de collecte de descriptions de flux portant sur des flux relatifs à au moins un réseau client, le réseau client étant rattaché à un réseau d'interconnexion comprenant : une première étape de réception de descriptions de flux, les descriptions de flux portant sur des flux en provenance du réseau client ; une première étape d'agrégation des descriptions de flux portant sur les flux en provenance du réseau client en fonction d'un critère d'agrégation ; une première étape de transmission des descriptions de flux agrégées vers un équipement de collecte ; caractérisé en ce qu'il comprend en outre : une étape d'analyse des descriptions de flux portant sur les flux en provenance du réseau client afin de déterminer au moins une caractéristique de flux propre au réseau client ; une deuxième étape de réception de descriptions de flux, lesdites descriptions de flux portant sur des flux en provenance du réseau d'interconnexion ; une étape de filtrage des descriptions de flux portant sur les flux en provenance du réseau d'interconnexion, dans laquelle sont éliminées les descriptions de flux portant sur des flux dépourvus de la caractéristique de flux propre au réseau client déterminée ; une deuxième étape de transmission des descriptions de flux filtrées vers l'équipement de collecte.

Procédé de collecte de descriptions de flux portant sur des flux relatifs à au moins un réseau client rattaché à un réseau d'interconnexion

L'invention concerne un procédé de collecte de descriptions de flux portant sur des flux relatifs à au moins un réseau client rattaché à un réseau d'interconnexion.

5 La supervision des réseaux de communication est un besoin constant des opérateurs de réseau. Elle se décline en différentes applications telles que la détection d'attaques de type déni de service DoS pour "Denial of Service" en anglais, la supervision du réseau quant au trafic acheminé par les différents nœuds du réseau ou encore la supervision d'un réseau client rattaché à un réseau cœur.

10 On notera d'emblée qu'un flux correspond à un échange de paquets de données entre deux machines d'un réseau IP dont les paquets ont des caractéristiques communes notamment des caractéristiques communes d'origine, de destination et de service. Par la suite, ces caractéristiques sont appelées caractéristiques de flux.

15 Pour assurer la supervision d'un réseau, il est connu de mettre en œuvre un service global d'analyse de flux transitant à travers un réseau sur les nœuds chargés de l'acheminement dans ce réseau. A partir de mesures dites passives et basées sur l'observation des flux entrants dans ces nœuds, des descriptions des flux entrants sont générées. Ces descriptions de flux sont transmises à un équipement de collecte à l'aide d'un protocole spécifique. Il peut, par exemple, s'agir du protocole IPFIX en cours de
20 normalisation au sein de l'IETF (Internet Engineering Task Force) ou de tout autre protocole.

Chaque flux possède une identification de flux, laquelle est réalisée par exemple à l'aide des éléments suivants:

- l'adresse IP du nœud source,
- 25 - l'adresse IP du nœud destination,
- les ports source et destination, pour les segments TCP et les datagrammes UDP,
- le protocole utilisé, obtenu par analyse des informations de la couche IP, par exemple TCP, UDP ou ICMP,
- le champ TOS pour "Type Of Service" en anglais, identifiant pour le flux le type
30 de qualité de service requis (priorité du flux, délai d'acheminement,...),

- le champ Input qui correspond à un index de l'interface par laquelle le flux est entré dans le nœud, cet index étant défini pour l'administration du réseau.

Lorsqu'un nœud reçoit un paquet de données à acheminer contenant, pour certains éléments d'identification cités ci-dessus, des valeurs non connues, il initie une description de flux en ajoutant à l'identification du flux différents éléments permettant de décrire le flux tels que:

- le numéro de l'interface de sortie Output, cet index étant défini pour l'administration du réseau,
- DPkts, contenant le nombre de paquets comptabilisés pour ce flux ;
- DOctets, contenant le volume d'octets de niveau 3 (Couche IP) dans les paquets du flux ;
- First et Last, correspondant respectivement aux instants de début et de fin du flux.

A la réception de chaque nouveau paquet de données, le nœud met à jour les paramètres DPkts, DOctets et Last.

Après une durée prédéterminée d'inactivité du flux, ou bien de façon périodique, le nœud transmet à l'équipement de collecte les descriptions relatives à ce flux, qu'il a lui-même réalisées. La quantité de données ainsi transmises peut s'avérer importante et induire une charge importante dans le réseau de collecte, ce qui est d'autant plus difficile à gérer que le réseau est de grande taille.

Afin de réduire la quantité de données envoyées à l'équipement de collecte, il est connu d'implémenter dans les nœuds une fonction d'agrégation des descriptions de flux, ayant pour rôle d'agréger les descriptions de flux en fonction d'un critère d'agrégation. Ce critère peut consister par exemple à agréger les descriptions de flux relatives à un ensemble d'adresses IP source. Ces descriptions de flux agrégées sont transmises ensuite à l'équipement de collecte.

Suivant l'application de supervision à laquelle les descriptions de flux agrégées sont destinées, l'agrégation doit satisfaire à des contraintes différentes. A titre d'exemple:

- pour l'analyse du trafic IP, il est essentiel que l'agrégation permette de conserver les informations relatives aux ports source et de destination ;

- pour la détection d'attaques par déni de service, l'agrégation doit permettre de conserver des informations relatives au nombre de paquets envoyés à destination d'un serveur afin de pouvoir analyser la variation de ce volume ; et
 - pour des applications visant à élaborer des matrices de trafic, l'agrégation se fait
- 5 sur un système autonome ou bien sur des sous-ensembles de réseau.

Le nœud ne peut réaliser qu'un nombre très limité d'agrégations à la fois. Pour pallier ce problème, le nœud transmet parallèlement les mêmes descriptions de flux aux collecteurs des différents dispositifs plus spécifiquement en charge des différentes applications de supervision. Ceci induit une charge de travail supplémentaire pour le

10 nœud dont la fonction principale demeure d'assurer l'acheminement des paquets de données. Afin de limiter cette charge, les nœuds sont en général limités à deux exports en parallèle de descriptions de flux.

Le but de l'invention est donc de limiter le volume des descriptions agrégées transmis à l'équipement de collecte, notamment dans le cadre de la supervision d'un

15 réseau client rattaché à un réseau d'interconnexion.

A cet effet, l'invention concerne un procédé de collecte de descriptions de flux portant sur des flux relatifs à au moins un réseau client, le réseau client étant rattaché à un réseau d'interconnexion, le procédé comprenant:

- une première étape de réception de descriptions de flux, lesdites descriptions de flux portant sur des flux en provenance du réseau client ;
- une première étape d'agrégation des descriptions de flux portant sur les flux en provenance du réseau client en fonction d'un critère d'agrégation ;
- une première étape de transmission des descriptions de flux agrégées vers un équipement de collecte ;

25 caractérisé en ce qu'il comprend en outre:

- une étape d'analyse des descriptions des flux portant sur les flux en provenance du réseau client afin de déterminer au moins une caractéristique de flux propre au réseau client ;
 - une deuxième étape de réception de descriptions de flux, lesdites descriptions de flux portant sur des flux en provenance du réseau d'interconnexion ;
- 30

- une étape de filtrage des descriptions de flux portant sur les flux en provenance du réseau d'interconnexion, dans laquelle sont éliminées les descriptions de flux portant sur des flux dépourvus de la caractéristique de flux relatif au réseau client déterminée ;
- 5 - une deuxième étape de transmission des descriptions de flux filtrées vers l'équipement de collecte.

A partir des descriptions de flux portant sur des flux en provenance du réseau client et en fonction des interfaces du réseau client définies comme étant à observer, le procédé détermine au moins une caractéristique de flux et configure automatiquement
10 les traitements à réaliser sur les descriptions de flux portant sur des flux en provenance du réseau d'interconnexion. Les descriptions de flux sortants du réseau d'interconnexion sont, quant à elles, soumises à un filtrage afin de ne conserver que celles correspondant à la caractéristique de flux déterminée. Ainsi, le volume des informations transmis à l'équipement de collecte est réduit. Afin d'obtenir l'ensemble
15 des flux recherchés, il est nécessaire d'obtenir les descriptions de flux en provenance de différents nœuds du réseau d'interconnexion car les chemins utilisés pour les flux entrants et les flux sortants du réseau client ne sont pas obligatoirement les mêmes.

Les charges du réseau de collecte et de l'équipement de collecte sont également réduites puisque seules les informations utiles sont transmises.

20 La méthode présente également plus de souplesse car on peut définir un critère d'agrégation différent par client observé.

Ainsi, on obtient l'ensemble des informations nécessaires aux applications de supervision et uniquement celles-là, sans augmenter la charge de traitement des nœuds qui produisent ces descriptions de flux de bas niveau.

25 Avantageusement, le procédé comprend en outre une deuxième étape d'agrégation des descriptions de flux filtrées en fonction du critère d'agrégation.

Avant transmission des descriptions de flux portant sur des flux en provenance du réseau d'interconnexion et à destination du réseau client, on agrège les descriptions de flux filtrées, c'est-à-dire celles correspondant à la ou les

caractéristiques de flux déterminées. La charge des nœuds est ainsi encore réduite puisqu'ils ne sont pas en charge de l'agrégation de toutes les descriptions de flux.

Dans un mode de réalisation, la première étape d'agrégation comprend en outre une sous-étape d'affectation aux descriptions de flux agrégées d'un paramètre d'identification d'une demande d'agrégation et l'étape de filtrage des descriptions de flux comprend une sous-étape d'affectation aux descriptions de flux filtrées du même paramètre d'identification de la demande d'agrégation..

L'utilisation d'un même paramètre d'identification dans les descriptions de flux agrégées portant sur des flux en provenance du réseau client et dans les descriptions de flux filtrées ou agrégées portant sur des flux en provenance du réseau d'interconnexion permet ensuite à l'équipement de collecte de repérer les descriptions de flux correspondant à une même demande d'agrégation.

Dans un mode de réalisation, le procédé comprend en outre une troisième étape d'agrégation, ladite étape consistant à agréger les descriptions de flux agrégées portant sur des flux en provenance du réseau client et les descriptions de flux agrégées en provenance du réseau d'interconnexion afin d'obtenir des descriptions de flux agrégées bi-directionnelles avant transmission vers l'équipement de collecte.

Ainsi les descriptions de flux agrégées portant sur des flux en provenance de différents nœuds du réseau d'interconnexion et les descriptions de flux agrégées portant sur des flux en provenance des nœuds de raccordement du réseau client sont agrégées en des descriptions de flux bi-directionnelles. Grâce à cela, le procédé de l'invention fournit une vision globale du trafic sur le réseau client.

De préférence, il est en outre prévu une étape d'affectation aux descriptions de flux portant sur les flux en provenance du réseau client et aux descriptions de flux portant sur les flux en provenance du réseau d'interconnexion d'un paramètre représentatif d'un sens de transmission entre un client et un serveur, sens montant du client vers le serveur et sens descendant du serveur vers le client, en fonction des valeurs respectives des ports source et de destination contenues dans lesdites descriptions de flux, et lors des première et deuxième étapes d'agrégation, les

descriptions de flux sont agrégées en fonction dudit paramètre représentatif du sens de transmission et du critère d'agrégation.

On identifie dans une description de flux, le port dont la valeur est la plus faible entre les ports source et destination. Ce port correspond à celui du serveur (que le serveur soit dans le réseau client ou dans un autre réseau), l'autre au port du client (de l'architecture client-serveur). On obtient donc des informations agrégées qui conservent les éléments essentiels permettant de réaliser une supervision efficace. L'information sur le sens applicatif des flux permet de réagir rapidement s'il est constaté, par exemple, que les flux entrant et sortant sont asymétriques. Cela peut être révélateur d'une attaque en cours sur le réseau client ou d'un mauvais fonctionnement d'un serveur.

L'invention concerne également un système de collecte de descriptions de flux portant sur des flux relatifs à au moins un réseau client, le réseau client étant rattaché à un réseau d'interconnexion, le système comprenant:

- au moins un module de réception de descriptions de flux agencé pour recevoir des descriptions de flux portant sur des flux en provenance de l'un des deux réseaux d'interconnexion et client ;
- au moins un module d'agrégation de descriptions de flux, agencé pour agréger des descriptions de flux reçues en fonction d'un critère d'agrégation ;
- un module d'analyse de descriptions de flux, agencé pour analyser des descriptions de flux portant sur des flux en provenance du réseau client afin de déterminer au moins une caractéristique de flux propre au réseau client ;
- un module de filtrage de descriptions de flux, agencé pour éliminer, dans les descriptions de flux reçues, celles portant sur des flux dépourvus de la caractéristique de flux déterminée ;
- un module de transmission de descriptions de flux, agencé pour transmettre des descriptions de flux filtrées à un module de collecte.

L'invention sera mieux comprise à l'aide de la description suivante d'un mode de réalisation particulier du procédé de l'invention, en référence aux dessins annexés sur lesquels :

- la figure 1 représente une pluralité de réseaux clients rattachés à un réseau d'interconnexion ainsi qu'un système de collecte des descriptions de flux;
- la figure 2 représente les étapes du procédé de collecte de descriptions de flux portant sur des flux relatifs à au moins un réseau client selon un mode particulier de réalisation de l'invention;
- la figure 3 représente un système de collecte de descriptions de flux.

On notera d'emblée qu'un flux correspond à un échange de paquets de données entre deux machines d'un réseau IP dont les paquets ont des caractéristiques communes notamment des caractéristiques communes d'origine, de destination et de service. Par la suite, ces caractéristiques sont appelées caractéristiques de flux.

La figure 1 représente deux réseaux clients 2 et 3 rattachés à un réseau d'interconnexion 1. Le réseau d'interconnexion est en charge de l'acheminement des flux à destination des réseaux clients. Il s'agit par exemple de l'infrastructure d'un opérateur de télécommunication. Un réseau client peut par exemple être un réseau d'entreprise, un réseau domestique, un réseau mobile, un réseau privé virtuel (VPN pour "Virtual Private Network") à base de MPLS (pour "MultiProtocol Label Switching" en anglais), de VLAN (pour "Virtual Local-Area Network" en anglais), Dans l'exemple de la figure 1, le réseau d'interconnexion est un réseau cœur 1 comprenant une pluralité de nœuds 10, 11, 12, 13 et 14 en charge de l'acheminement des paquets entre une adresse de machine source et une adresse de machine destination. Les nœuds 10 et 11 sont des nœuds de sortie du réseau cœur 1 gérant des interfaces vers les réseaux clients 2 et 3 ou vers un nœud client 40. Le nœud client 40 n'appartient pas aux réseaux clients 2 et 3.

Les paquets à destination d'une adresse IP appartenant au réseau client 2 sont acheminés dans le réseau cœur 1 vers le nœud de sortie 10. Le nœud 10 transmet ensuite les paquets vers un nœud 20 du réseau client 2. Dans l'exemple, les adresses IP du réseau 2 correspondent à des adresses appartenant à l'ensemble 156.100.140.0 à 156.100.140.255, c'est-à-dire 156.100.140.0 avec un masque de 24, noté 156.100.140.0/24. Il s'agit de la notation CIDR (Classless Inter-Domain Routing) de routage interdomaine sans classe permettant d'identifier une plage d'adresses IP.

L'adresse IP avant la barre oblique "/" est la première adresse de la plage. La valeur située après la barre oblique "/" correspond au nombre de bits d'adresse octroyés au réseau client pour attribuer une adresse IP à ses machines.

5 Par la suite, on appellera "préfixe réseau" l'ensemble des adresses du réseau client.

Les paquets émis par une machine du réseau client 2 sont transmis par l'intermédiaire du nœud 20 au nœud 10 du réseau cœur 1.

10 Les paquets à destination d'une adresse IP appartenant au réseau client 3 sont acheminés dans le réseau cœur 1 vers les nœuds 10 et 11 de sortie. Le nœud 10 transmet ensuite les paquets vers un nœud 30 du réseau 3 du client. Le nœud 11 transmet ensuite les paquets vers un nœud 31 du réseau 3 du client. Dans l'exemple du premier mode de réalisation, les adresses IP du réseau 3 correspondent à l'ensemble des adresses de préfixe 140.100.140.0 avec un masque de 24, noté 140.100.140.0/24, et à l'ensemble des adresses de préfixe 139.100.140.0 avec un masque de 24, noté
15 139.100.140.0/24. Plus particulièrement, dans le réseau cœur 1, les paquets à destination du préfixe 139.100.140.0/24 sont routés vers le nœud 10 et ceux à destination du préfixe 140.100.140.0/24 vers le nœud 20. Les paquets émis par une machine du réseau 3 sont transmis soit par l'intermédiaire du nœud 30 au nœud 10 du réseau cœur 1, soit par l'intermédiaire du nœud 31 au nœud 11 du réseau cœur 1 en
20 partage de charge. Les adresses IP des nœuds 20, 30 et 31 sont respectivement 192.3.2.1, 192.3.2.2 et 192.3.2.3. Les adresses IP des nœuds 10 et 11 sont respectivement 192.3.2.4 et 192.3.2.5.

25 Dans les modes de réalisation décrits, les nœuds 10, 11, 20, 30 et 31 offrent la possibilité d'activer, sur requête, des mesures de descriptions de flux portant sur des flux entrants dans le nœud. Ces mesures peuvent être activées, par exemple, pour tous les flux entrants dans le nœud ou pour les flux entrants à travers certaines des interfaces du nœud seulement. Ces mesures sont ensuite transmises à un équipement de collecte. Selon l'invention, les mesures sont transmises à l'aide d'un protocole de type IPFIX, normalisé à l'IETF, vers des équipements de collecte intermédiaires 50, 51
30 et 60 avant d'être transmis à un équipement de collecte final 70. Par la suite, les

équipements de collecte intermédiaires 50 et 51 sont appelés pré-agrégateurs et l'équipement de collecte intermédiaire 60, un agrégateur. Ces différents équipements de collecte dialoguent entre eux à l'aide d'un protocole de type IPFIX.

Un serveur 71 permet de dialoguer avec l'agrégateur 60 afin notamment de
5 permettre la configuration du système de collecte qui sera décrit plus loin.

Le procédé de collecte de descriptions de flux portant sur des flux relatifs à un réseau client va maintenant être décrit en référence à la figure 2. Dans l'exemple du premier mode de réalisation décrit ici, les deux réseaux clients 2 et 3 sont supervisés conjointement. Le nœud client 40 n'est pas supervisé.

10 Dans une première étape E1 de configuration, le serveur 71 transmet une demande à l'agrégateur 60. Cette demande contient un critère d'agrégation AggrMode, les informations identifiant un ou plusieurs nœuds en charge de l'exportation des descriptions de flux et la liste des interfaces à observer pour chacun de ces nœuds ainsi qu'un type associé à ces interfaces suivant qu'il s'agisse d'une interface de flux sortants
15 du réseau client 2 ou 3 ou d'une interface de flux sortants du réseau d'interconnexion 1. De façon optionnelle, la demande comprend pour chaque réseau client un paramètre d'identification de la demande d'agrégation AggrID. Dans l'exemple considéré, il s'agit des interfaces de nœuds des réseaux clients 2 et 3, en l'espèce celles des nœuds 20 du réseau client 2 et celles des nœuds 30 et 31 du réseau client 3. Deux demandes de cette
20 table possèdent le même paramètre d'identification afin de faciliter par la suite le regroupement des données du réseau client 3, ce réseau client 3 possédant deux interfaces de sortie.

Le tableau I regroupe les demandes faites à l'agrégateur 60 dans l'exemple du premier mode de réalisation. L'ensemble des tableaux est regroupé dans l'Annexe.

25 Dans le tableau I, on notera que:

- "Client1" et "Client 2" correspondent respectivement aux réseaux clients 2 et 3.

- "Noeud1" correspond à l'identité du nœud 20, "Noeud2" à celle du nœud 30 et "Noeud3" à celle du nœud 31.

- "Adresse d'exportation" correspond à l'adresse du nœud en charge de l'exportation des descriptions de flux.

- "InterfaceId" correspond à l'identification de l'interface à observer.

- "Aggrmod" correspond à un critère d'agrégation utilisé pour définir le type d'agrégation à effectuer. Son fonctionnement est décrit lors de la description de l'étape E6 d'agrégation des descriptions de flux.

En variante à cette étape E1, l'agrégateur 60 pourrait identifier les interfaces à observer par lecture des bases de données d'administration associées aux nœuds.

A la suite de cette étape E1 de configuration, dans une deuxième étape de configuration E2, l'agrégateur 60 transmet à un pré-agrégateur une demande de pré-agrégation. La demande est transmise au(x) pré-agrégateur(s) en charge de la collecte des descriptions de flux en provenance du nœud gérant une des interfaces à observer appartenant à la liste des interfaces de nœud à observer, transmise par le serveur 71 (ou déterminée par l'agrégateur 60 dans la variante de réalisation), à l'étape E1. Dans l'exemple considéré, il s'agit du pré-agrégateur 51 qui est en charge de la collecte des descriptions de flux portant sur des flux en provenance des réseaux clients 2 et 3.

Dans une première variante, le mécanisme de description de flux est activé en continu sur l'ensemble des interfaces des nœuds.

Dans une deuxième variante, le mécanisme de description de flux est activé sur les nœuds 20, 30 et 31 par le pré-agrégateur 51 ou par l'agrégateur 60 par un protocole de type IPFIX.

Le pré-agrégateur 51 est alors configuré pour déterminer au moins une caractéristique de flux par analyse des descriptions de flux portant sur des flux en provenance des réseaux clients 2 et 3 et pour agréger ces descriptions de flux en fonction du critère d'agrégation.

Dans une troisième étape E3 de réception de descriptions de flux, le pré-agrégateur 51 reçoit des descriptions de flux portant sur des flux en provenance des réseaux clients 2 et 3, dans l'exemple particulier, envoyées par les nœuds 20, 30 et 31.

Dans le premier mode de réalisation, le pré-agrégateur 51 reçoit les informations contenues dans le tableau II.

Dans le tableau II, le champ "exporter" correspond à l'adresse IP du nœud qui a envoyé les descriptions de flux. Les autres champs correspondent à la description du flux.

Suite à la réception de descriptions de flux à l'étape E3, dans une quatrième
5 étape E4 d'analyse de descriptions de flux, le pré-agrégateur 51 analyse les descriptions de flux portant sur des flux en provenance du réseau client 2 ou 3 en fonction des informations reçues à l'étape de configuration E1 afin de déterminer, pour chaque réseau client à observer 2 ou 3, au moins une caractéristique de flux. Dans le premier mode de réalisation, il en déduit les caractéristiques de ce réseau client, en
10 particulier, le ou les préfixes IP du réseau client et le système autonome auquel appartient le réseau client. Ces caractéristiques sont propres au réseau client. Les informations relatives au masque réseau et au système autonome du réseau client sont contenues dans les descriptions de flux transmises. Les informations relatives au masque apparaissent dans le champ "Src Mask" du tableau II. Par souci de clarté, les
15 informations relatives au système autonome, contenues dans les descriptions de flux reçues par le pré-agrégateur 51, n'apparaissent pas dans le tableau II.

Dans l'exemple considéré, l'analyse du tableau II permet de déterminer les informations contenues dans le tableau III.

A l'issue de cette étape E4, le pré-agrégateur 51 connaît au moins l'une des
20 caractéristiques de flux à observer.

Dans une cinquième étape E5 de transmission de caractéristique de flux, le pré-agrégateur 51 transmet à l'agrégateur 60 la ou les caractéristiques de flux à observer déterminées à l'étape E4. Il s'agit dans l'exemple particulier des informations contenues dans le tableau III. A l'issue de cette étape E5, l'agrégateur 60 a
25 connaissance de la ou des caractéristiques de flux à observer.

En parallèle, dans une sixième étape E6 d'agrégation des descriptions de flux, le pré-agrégateur 51 agrège les descriptions de flux en fonction du critère d'agrégation AggrMod qu'il a reçu à l'étape E1.

Dans l'exemple particulier décrit ici, le critère d'agrégation est une
30 combinaison des deux paramètres "minPort" et "PrefixSrc", "minPort" représentant le

plus petit des ports source et destination et "PrefixSrc" représentant le préfixe réseau de la source du flux. L'agrégation sur la base d'un tel critère est décrite ci-après.

Dans une première sous-étape E61, pour chaque ligne du tableau II, le pré-agrégateur 51 détermine le plus petit des deux ports, entre le port source et le port de destination du flux, ces informations étant comprises dans la description du flux dans les champs SrcPort et DstPort. Si le port de destination correspond à la valeur déterminée comme étant la plus petite, le flux va être considéré comme montant entre un client et un serveur. Si le port source correspond à la valeur déterminée comme étant la plus petite, le flux est considéré comme descendant entre un serveur et un client. Le pré-agrégateur conserve la valeur la plus petite et affecte à la description de flux un paramètre représentatif d'un sens de transmission montant ou descendant entre un client et un serveur. Le tableau IV contient les informations issues du tableau II suite à cette sous-étape E61.

A l'issue de cette sous-étape E61 et dans une deuxième sous-étape E62, le pré-agrégateur 51 agrège les descriptions de flux en fonction du critère d'agrégation transmis à l'étape E1. Dans le premier mode de réalisation, le critère d'agrégation correspond à la combinaison de "MinPort" et "PrefixSrc". Il regroupe ainsi dans une seule description de flux agrégée l'ensemble des descriptions de flux relatives à des ports respectifs (MinPort) couverts par un même préfixe IP du réseau client et au même sens de transmission (montant ou descendant), envoyées par un même nœud identifié par le champ "exporter" de la description de flux. Les informations contenues dans le champ relatif à l'adresse de destination du flux DestAddr ne sont pas conservées dans les descriptions de flux agrégées. Les valeurs contenues dans les champs "octets" et "pkts" sont cumulées dans des champs agrégés respectifs.

De façon optionnelle, il affecte à la description de flux agrégée un paramètre d'identification de l'agrégation. Ces valeurs de paramètre ont été transmises à l'étape E1 de configuration dans le champ AggrID. Dans l'exemple décrit, les descriptions de flux agrégées sont contenues dans le tableau V.

De façon optionnelle et en fonction de la valeur du critère d'agrégation, le pré-agrégateur 51 affecte à la description de flux agrégée un paramètre temporel

représentatif de la répartition dans le temps des descriptions de flux qui ont été agrégées. Il peut s'agir, par exemple, de la valeur la plus faible parmi l'ensemble des valeurs contenues dans les champs "First" des descriptions de flux ayant été agrégées (ce champ "First" correspondant à l'instant de début de flux), et de la valeur la plus élevée parmi l'ensemble des valeurs contenues dans les champs "Last" des descriptions de flux ayant été agrégées (le champ "Last" correspondant à l'instant de fin de flux).

A l'issue de cette sous-étape E62, le pré-agrégateur 51 transmet dans une sous-étape E63 les descriptions de flux agrégées vers l'agrégateur 60.

L'étape E6 d'agrégation des descriptions de flux est effectuée uniquement pour les descriptions de flux correspondant aux flux sortants du réseau client. Ainsi, la transmission de descriptions de flux agrégées est limitée aux seuls flux sortants du réseau client (et donc entrants sur le réseau d'interconnexion). Il n'y a pas de description de flux transmise pour des réseaux clients non observés.

Suite à la réception des caractéristiques de flux propres au réseau client à observer lors de l'étape E5, dans une septième étape E7 de configuration, l'agrégateur 60 configure le pré-agrégateur 50 en lui transmettant les caractéristiques à observer, en particulier, les nœuds gérant une des interfaces à observer appartenant à la liste des interfaces de nœud à observer, la ou les caractéristiques de flux qu'il a obtenues à l'étape E5 et le critère d'agrégation. Optionnellement, il transmet le paramètre d'identification d'agrégation.

En variante, à l'étape E5, le pré-agrégateur 51 transmet directement ces caractéristiques au pré-agrégateur 50 et l'étape E7 n'est pas réalisée.

Suite à la réception de ces caractéristiques à l'étape E5 ou à l'étape E7, le pré-agrégateur 50 active l'agrégation des descriptions de flux portant sur des flux en provenance du réseau d'interconnexion 1 en fonction de la ou des caractéristiques de flux reçues et selon le critère d'agrégation, comme décrit ci-après.

Dans une huitième étape E8 de filtrage et d'agrégation des descriptions de flux, et plus particulièrement dans une sous-étape E81 de réception des descriptions de flux, le pré-agrégateur 50 reçoit des descriptions de flux portant sur des flux en provenance du réseau d'interconnexion 1, envoyées par les nœuds 10 et 11 dans

l'exemple particulier de réalisation, et filtre dans une sous-étape E82 les descriptions de flux reçues afin d'éliminer celles dont la caractéristique de flux correspondant à la caractéristique de flux propre au réseau client reçue n'est pas couverte par celle-ci. Il s'agit des descriptions de flux portant sur des flux dépourvus de la caractéristique de flux propre au réseau client déterminée. Dans le premier mode de réalisation, il élimine
5 celles dont l'adresse de destination n'est pas couverte par un des préfixes réseau déterminés du réseau client. Optionnellement, il affecte à chaque description de flux le paramètre d'identification d'agrégation. Dans l'exemple décrit, les descriptions de flux filtrées par le pré-agrégateur 50 sont contenues dans le tableau VI.

10 Ces descriptions de flux filtrées sont ensuite traitées de la même manière qu'à l'étape E6. Le pré-agrégateur 50 affecte, au cours d'une sous-étape E83, aux descriptions de flux filtrées un paramètre représentatif d'un sens de transmission montant ou descendant entre un client et un serveur. Il agrège ensuite, dans une sous-étape E84, dans une seule description de flux l'ensemble des descriptions de flux
15 filtrées selon le critère d'agrégation. Dans le premier mode de réalisation, il s'agit des descriptions de flux relatives à un des préfixes réseau déterminés du réseau client 2 ou 3 et au même sens de transmission montant ou descendant, envoyées par un nœud identifié par le champ "exporter" de la description de flux.

Dans l'exemple décrit, les descriptions de flux agrégées sont contenues dans
20 le tableau VII.

Le pré-agrégateur 50 transmet ensuite, au cours d'une sous-étape E85, les descriptions de flux agrégées à l'agrégateur 60.

A la suite des étapes E6 et E8, dans une neuvième étape E9 d'agrégation, l'agrégateur 60 agrège les descriptions de flux reçues du pré-agrégateur 51 à l'étape E6
25 et celles reçues du pré-agrégateur 50 à l'étape E8 en des descriptions de flux agrégées bi-directionnelles, comme décrit ci-après.

Dans le premier mode de réalisation, pour chaque description de flux agrégée en provenance du pré-agrégateur 51 contenant en tant qu'adresse source un des préfixes IP déterminés du réseau client 2 ou 3, l'agrégateur recherche dans les autres
30 descriptions de flux agrégées en provenance du même pré-agrégateur 51 s'il en existe

une contenant également comme adresse source le même préfixe IP. Si le paramètre de sens de transmission affecté à la description de flux a la même valeur que celui affecté à la description de flux provenant du pré-agrégateur 51, il agrège les deux descriptions de flux. Il recherche ensuite dans les descriptions de flux agrégées en provenance du pré-agrégateur 50 s'il en existe une contenant comme adresse de destination le même préfixe IP. Si le paramètre de sens de transmission affecté à la description de flux agrégée provenant du pré-agrégateur 50 est opposé à celui affecté à la description de flux provenant du pré-agrégateur 51, les autres paramètres de la description du flux étant semblables, l'agrégateur 60 agrège les deux descriptions de flux en une description de flux agrégée bi-directionnelle. Les agrégations sont réalisées en prenant en compte des informations temporelles afin de n'agréger que des descriptions de flux comprises dans un même intervalle de temps. Cette génération de descriptions de flux bi-directionnelles est facilitée par l'utilisation du paramètre d'identification de l'agrégation de la demande, AggrID, qui permet de détecter les descriptions de flux agrégées en provenance de différents pré-agrégateurs relatives à la même demande.

Dans l'exemple considéré, l'agrégateur 60 génère à partir des descriptions de flux agrégées contenues dans les tableaux V et VII des descriptions de flux bi-directionnelles contenues dans les tableaux VIII et IX. Le tableau VIII correspond aux descriptions de flux vers des serveurs externes au réseau client 2 ou 3. Il s'agit de l'agrégation bi-directionnelle des descriptions de flux correspondant à des flux descendants. Le tableau IX correspond aux descriptions de flux vers des serveurs présents dans le réseau client 2 ou 3, c'est-à-dire à des flux montants. Les descriptions de flux de Ag2 du flux TCP présentent une dissymétrie notable, ce qui conduit à supposer que les serveurs du réseau client 3 subissent une attaque en TCP.

Les informations relatives aux nœuds ayant transmis les descriptions de flux peuvent être conservées mais ne sont pas indiquées dans les tableaux VIII et IX pour des raisons de lisibilité.

D'autres formes de présentation des descriptions de flux bi-directionnelles sont également possibles. On notera également que les descriptions de flux agrégées présentent l'avantage de masquer les plans d'adressage internes au réseau client.

Suite à cette étape E9, les descriptions de flux bi-directionnelles sont ensuite transmises au cours d'une étape E10 vers un équipement de collecte 70. Cette transmission est paramétrable: elle peut se faire au fil de l'eau ou lorsque certaines valeurs dépassent un seuil. Avantageusement, l'agrégation inclut des détections sur
5 seuil par comparaison de valeurs comprises dans les descriptions de flux bi-directionnelles. Il peut s'agir d'une comparaison entre le nombre de paquets entrants et le nombre de paquets sortants. Il peut s'agir également de détection de seuil sur certains paramètres tels que le nombre de paquets, le volume d'octets.

Le procédé, hormis les étapes liées à la configuration de l'ensemble du
10 système de collecte, est continu, c'est-à-dire que les étapes E3 de réception de descriptions de flux, E6 d'agrégation des descriptions de flux, E8 de filtrage et d'agrégation des descriptions de flux et E9 d'agrégation se déroulent de façon continue dès que des descriptions de flux correspondant aux flux observés sont reçues des nœuds.

15 Le premier mode de réalisation est décrit en utilisant comme critère d'agrégation une valeur consistant à affecter un paramètre représentatif d'un sens de transmission entre un client et un serveur en fonction du port source et du port de destination contenus dans les descriptions de flux et à agréger ensuite les descriptions de flux par préfixe IP source au pré-agrégateur 51 traitant les descriptions de flux
20 portant sur des flux en provenance du réseau client 2 ou 3 et par préfixe IP destination au pré-agrégateur 50 traitant les descriptions de flux portant sur des flux en provenance du réseau cœur.

D'autres modes d'agrégation, fondés sur d'autres critères, sont également envisageables, notamment, sans que la liste suivante ne soit exhaustive:

- 25 - une agrégation en fonction du préfixe réseau source (AggrMode="PrefixSrc") ou du préfixe réseau destination (AggrMode="PrefixDst") ;
- une affectation d'un paramètre représentatif d'un sens de transmission suivie d'une agrégation en fonction du port source
30 (AggrMode="MinPort") ;

- une affectation d'un paramètre représentatif d'un sens de transmission suivie d'une agrégation en fonction du préfixe IP destination (AggrMode="MinPort+PrefixDst").

Suivant le type de réseau client à observer, l'affectation d'un paramètre représentatif du sens de transmission entre un client et un serveur n'est pas réalisée de la même façon. Des valeurs de ports source génériques sont réservées pour les serveurs dans une plage de 0 à 1023: par exemple, la valeur de 80 correspond à http, 12 à TCP, 21 à FTP, 161 à "SNMP Polling" et 162 à l'envoi des alarmes SNMP. Dans un réseau de recouvrement de type P2P, pour "Peer-to-Peer" en anglais, l'affectation des numéros de port aux serveurs est dynamique. Le port du serveur est partagé par l'ensemble des clients. On peut alors, par analyse des descriptions de flux reçues, identifier l'association adresse IP/port serveur et en déduire le port serveur utilisé de façon dynamique. Par contreposé, on peut également agréger des descriptions de flux relatives à des ports quasi-contigus en partant de l'hypothèse que l'affectation dynamique par un serveur à des clients se fait de cette manière.

Le premier mode de réalisation est décrit dans le cas où une répartition de la charge est réalisée entre les différents nœuds. On peut également envisager que seuls les nœuds en sortie du réseau client transmettent les descriptions de flux en provenance et à destination du réseau client.

Dans un deuxième mode de réalisation, le procédé permet d'observer des flux multicast.

Dans un mode "Broadcast", il peut s'agir par exemple de diffusion de télévision, de diffusion d'informations. La source d'émission est située dans le réseau client observé. Les flux en provenance du réseau client sont à destination d'une adresse dite multicast. Le réseau cœur est en charge de la rediffusion des flux à destination de l'adresse multicast vers les différentes adresses des terminaux IP unicast ayant demandé, à l'aide du protocole IGMP (Internet Group Management Protocol), à recevoir les flux. Il gère un arbre de diffusion multicast. Le pré-agrégateur 51 détecte l'adresse de destination multicast sur une interface de sortie du réseau client par analyse des descriptions de flux portant sur des flux en provenance du réseau client.

Suivant le type d'application envisagée, on peut identifier deux modes d'agrégation différents.

Dans une première variante, le but est de déterminer l'arbre Multicast, géré par le réseau cœur, associé à l'adresse multicast. On définit dans ce cas le critère d'agrégation à la valeur "broadcastTree". A l'étape E4 d'analyse des descriptions de flux portant sur des flux en provenance du réseau client, le pré-agrégateur 51 analyse les descriptions de flux afin de déterminer au moins l'adresse de la source unicast et/ou l'adresse de destination multicast. Ces caractéristiques sont propres au réseau client. A l'étape E5, il transmet ces caractéristiques de flux déterminées à l'agrégateur 60. A l'étape E62 d'agrégation des descriptions de flux portant sur des flux provenant du réseau client, le pré-agrégateur 51 agrège les descriptions de flux pour des flux dont les adresses source et destination correspondent au couple (adresse source unicast, adresse de destination multicast). A l'étape E7, l'agrégateur 60 configure des pré-agrégateurs en charge de descriptions de flux portant sur des flux en provenance du réseau cœur en leur fournissant les informations du flux déterminées et le critère d'agrégation. A l'étape E8, les pré-agrégateurs fournissent les descriptions de flux agrégées en fonction des caractéristiques de flux déterminées. Ils transmettent, associée aux descriptions de flux agrégées, une liste de nœuds (champ "Exporter") qui correspond aux nœuds par lesquels le flux multicast a été acheminé. A partir des informations contenues dans les descriptions de flux agrégées et en particulier les informations de routage qui y sont présentes (identification du prochain routeur pour l'acheminement, identification du système autonome, ...), l'application peut déterminer l'arbre du flux multicast. Par symétrie, cette variante est également applicable à la découverte de l'arbre du flux multicast, la source multicast étant diffusée dans le réseau client.

Dans une deuxième variante, le but est de d'estimer l'audience d'un service multicast d'une source de diffusion située dans le réseau client ou bien d'observer sa répartition par réseau. On définit dans ce cas le critère d'agrégation à la valeur "broadcastListener". Les étapes E4, E5, E62 et E8 sont identiques à la première variante. A l'étape E7, l'agrégateur configure des pré-agrégateurs en charge de

descriptions de flux portant sur des flux en provenance de réseaux d'accès en leur fournissant les caractéristiques de flux déterminées et le critère d'agrégation. A partir des descriptions de flux reçues à l'étape E8, l'application détermine ainsi une liste de nœuds d'accès multicast et/ou de nœuds de diffusion aux terminaux à interroger afin d'obtenir par la suite le nombre de sessions multicast associées à cette source. Ceci permet d'obtenir une bonne estimation instantanée de l'audience par simple cumul des sessions.

Dans un mode "Multicast", il peut s'agir également de trafic multidirectionnel, par exemple de conférence audio ou autre. L'application vise à déterminer la liste des membres d'un groupe Multicast. L'ensemble des membres du groupe Multicast, ayant chacun une adresse source unicast, émet à destination d'une adresse Multicast. On définit dans ce cas le critère d'agrégation à la valeur "multicastMember". A l'étape E4 d'analyse des descriptions de flux portant sur des flux en provenance du réseau client, le pré-agrégateur 51 détermine en tant que caractéristiques de flux l'adresse de la source unicast située dans le réseau client et l'adresse de destination multicast. Ces caractéristiques sont propres au réseau client. A l'étape E5, il transmet l'adresse de destination Multicast à l'agrégateur 60. A l'étape E62 d'agrégation des descriptions de flux portant sur des flux provenant du réseau client, le pré-agrégateur 51 agrège les descriptions de flux pour des flux dont les adresses source et destination correspondent au couple (adresse source unicast, adresse de destination multicast). A l'étape E7, l'agrégateur 60 configure des pré-agrégateurs en charge de descriptions de flux portant sur des flux en provenance du réseau cœur en leur fournissant la ou les caractéristiques de flux déterminées et le critère d'agrégation. A l'étape E8, les pré-agrégateurs fournissent les descriptions de flux filtrées en fonction de l'adresse de destination multicast et en conservant chaque adresse source. A partir de ces informations, l'application peut déterminer la liste des adresses sources émettant dans le même groupe multicast que l'adresse source unicast du réseau client et par conséquent, la liste des membres du groupe multicast.

On notera que le procédé fonctionne également dans le cas où les nœuds mettent en œuvre un échantillonnage des flux pour la constitution des descriptions de

flux. Le procédé prend alors en compte cette information qui peut être par exemple présente dans les descriptions de flux de bas niveau ou être connue par configuration des nœuds.

Le procédé est également applicable à la collecte de descriptions de flux sur d'autres types de réseaux client tels qu'un réseau privé virtuel, un réseau domestique, un réseau mobile. Il est particulièrement bien adapté à la collecte de descriptions de flux portant sur des flux en provenance de tout réseau rattaché à un réseau d'interconnexion de niveau supérieur.

On va maintenant décrire le système de collecte de descriptions de flux en référence à la figure 3.

Le système de collecte comprend les pré-agrégateurs 50, 51 et l'agrégateur 60.

Une partie du pré-agrégateur 51, ayant une fonction d'agrégation de descriptions de flux portant sur des flux en provenance d'un réseau client, appelée par la suite pré-agrégateur sortant, comprend les modules suivants:

- un module 510 de réception de descriptions de flux, agencé pour recevoir des descriptions de flux portant sur des flux en provenance du réseau client ;
- un module 512 d'agrégation de descriptions de flux, agencé pour agréger des descriptions de flux reçues en fonction d'un critère d'agrégation ;
- un module 511 d'analyse de descriptions de flux, agencé pour analyser des descriptions de flux portant sur des flux en provenance du réseau client afin de déterminer au moins une caractéristique de flux propre au réseau client ;
- un module 513 de transmission de descriptions de flux, agencé pour transmettre des descriptions de flux filtrées à un agrégateur 60 ou à un module de collecte 70 ;
- un module 514 de configuration, agencé pour recevoir des informations de configuration d'un agrégateur et pour transmettre à l'agrégateur la caractéristique de flux déterminée.

Une partie du pré-agrégateur 50, ayant une fonction d'agrégation de descriptions de flux portant sur des flux en provenance d'un réseau d'interconnexion, appelée par la suite pré-agrégateur entrant, comprend les modules suivants:

- un module 514 de configuration, agencé pour recevoir des informations de configuration d'un agrégateur 60 ;
- un module 510 de réception de descriptions de flux, agencé pour recevoir des descriptions de flux portant sur des flux en provenance du réseau d'interconnexion ;
- un module 515 de filtrage de descriptions de flux, agencé pour éliminer, dans les descriptions de flux reçues, celles portant sur des flux dépourvus de ladite au moins une caractéristique de flux reçue par le module 514 de configuration ;
- un module 513 de transmission de descriptions de flux, agencé pour transmettre des descriptions de flux filtrées à un agrégateur 60 ou à un module de collecte 70.

De façon optionnelle, le pré-agrégateur entrant 50 comprend en outre un module 512 d'agrégation de descriptions de flux, agencé pour agréger des descriptions de flux reçues en fonction d'un critère d'agrégation. Les descriptions de flux lui sont transmises par le module 515 de filtrage.

L'agrégateur 60 comprend les modules suivants:

- un module 600 de réception de descriptions de flux, agencé pour recevoir des descriptions de flux en provenance de pré-agrégateurs entrants et de pré-agrégateurs sortants ;
- un module 601 de configuration, agencé pour configurer les pré-agrégateurs et recevoir de pré-agrégateurs sortants la ou les caractéristiques de flux déterminées ;
- un module 602 d'agrégation, agencé pour agréger des descriptions de flux agrégées reçues de pré-agrégateurs sortants et des descriptions de flux agrégées reçues de pré-agrégateurs entrants.

Optionnellement, le système de collecte comprend un ou plusieurs modules 516 d'affectation à une description de flux d'un paramètre représentatif d'un sens de transmission entre un client et un serveur, sens montant du client vers le serveur et sens descendant du serveur vers le client, en fonction des valeurs respectives des ports source et de destination contenues dans ladite description de flux et le module

d'agrégation est agencé pour agréger les descriptions de flux en fonction dudit paramètre représentatif du sens de transmission et du critère d'agrégation. Ce module peut être intégré soit dans les pré-agrégateurs, soit dans l'agrégateur.

5 Les modules, tels que décrits, sont répartis sur différentes machines, distinctes des nœuds 20, 30, 31. Alternativement, il est possible de prévoir l'ensemble des modules nécessaires dans les nœuds ou éventuellement uniquement les modules prévus dans les pré-agrégateurs.

Dans une autre alternative, il n'y a pas d'agrégateur. Le pré-agrégateur sortant 51 transmet directement au pré-agrégateur entrant 50 les informations de configuration et la ou les caractéristique(s) de flux déterminée(s).

10

Les modules 510 à 515 et 600 à 602, qui mettent en œuvre le procédé précédemment décrit, sont de préférence des modules logiciels comprenant des instructions logicielles pour faire exécuter les étapes du procédé précédemment décrit par le serveur. Les modules logiciels peuvent être stockés dans ou transmis par un support de données. Celui-ci peut être un support matériel de stockage, par exemple un

15 CD-ROM, une disquette magnétique ou un disque dur, ou bien un support de transmission tel qu'un signal électrique, optique ou radio, ou un réseau de télécommunication.

ANNEXE

Tableau I

AggrID	ClientID	NodeID	InterfaceID	AggrMode	Adresse d'exportation
Ag1	Client1	Noeud1	Eth000001	minPort PrefixSrc	192.3.2.1
Ag2	Client2	Noeud2	Tunnel1	minPort PrefixSrc	192.3.2.2
Ag2	Client2	Noeud3	Vlan34	minPort PrefixSrc	192.3.2.3

Tableau II

exporter	If In de x	Dest Addr	Source Addr	Src Port	Dst Port	Proto col	Src Ma sk	octets	pkt s
192.3.2.1	1	1.2.3.4	156.100.140.5	12	3800	TCP	24	500	10
192.3.2.1	1	3.4.5.6	156.100.140.28	12	6600	TCP	24	500	10
192.3.2.1	1	8.2.3.1	156.100.140.24	12	7000	TCP	24	500	10
192.3.2.1	1	4.3.2.1	156.100.140.25	8000	12	TCP	24	2500	5
192.3.2.1	1	7.2.3.7	156.100.140.12	1730	161	UDP	24	5400	10
192.3.2.2	1	9.2.3.7	140.100.140.12	12	3400	TCP	24	500	10
192.3.2.2	1	23.2.3.7	140.100.140.9	12	6500	TCP	24	500	10
192.3.2.2	1	45.2.3.7	140.100.140.67	12	3200	TCP	24	500	10
192.3.2.2	1	86.2.3.7	140.100.140.48	5400	162	UDP	24	300	1
192.3.2.2	1	78.2.3.7	140.100.140.43	12	2000	TCP	24	500	10
192.3.2.3	1	9.2.3.7	140.100.140.12	12	2000	TCP	24	500	10
192.3.2.3	1	23.2.3.7	140.100.140.9	12	2000	TCP	24	500	10
192.3.2.3	1	45.2.3.7	140.100.140.67	12	2000	TCP	24	500	10
192.3.2.3	1	86.2.3.7	140.100.140.48	12	2000	TCP	24	500	10
192.3.2.3	1	78.2.3.7	140.100.140.43	12	2000	TCP	24	500	10
192.3.2.2	1	9.76.3.7	139.100.140.12	12	3400	TCP	24	500	10
192.3.2.2	1	48.2.3.7	139.100.140.9	12	6500	TCP	24	500	10
192.3.2.2	1	46.2.3.7	139.100.140.67	12	3200	TCP	24	500	10
192.3.2.2	1	35.2.3.7	139.100.140.48	12	5400	TCP	24	500	10
192.3.2.2	1	98.2.3.7	139.100.140.43	12	2000	TCP	24	500	10
192.3.2.3	1	9.76.3.7	139.100.140.12	12	2000	TCP	24	500	10
192.3.2.3	1	48.2.3.7	139.100.140.9	12	2000	TCP	24	500	10
192.3.2.3	1	46.2.3.7	139.100.140.67	12	2000	TCP	24	500	10
192.3.2.3	1	35.2.3.7	139.100.140.48	12	2000	TCP	24	500	10
192.3.2.3	1	98.2.3.7	139.100.140.43	12	2000	TCP	24	500	10

Tableau III

AggrID	ClientID	Exporter	AggrMode	Network	Netmask	AS
Ag1	Client1	192.3.2.1	minPort PrefixSrc	156.100.140. 0	24	-
Ag2	Client2	192.3.2.2	minPort PrefixSrc	139.100.140. 0	24	-
Ag2	Client2	192.3.2.3	minPort PrefixSrc	139.100.140. 0	24	-
Ag2	Client2	192.3.2.2	minPort PrefixSrc	140.100.140. 0	24	-
Ag2	Client2	192.3.2.3	minPort PrefixSrc	140.100.140. 0	24	-

Tableau IV

exporter	If In de x	Dest Addr	Source Addr	Port	Sens	Proto col	Src Ma sk	octets	pkt s
192.3.2.1	1	1.2.3.4	156.100.140.5	12	0	TCP	24	500	10
192.3.2.1	1	3.4.5.6	156.100.140.28	12	0	TCP	24	500	10
192.3.2.1	1	8.2.3.1	156.100.140.24	12	0	TCP	24	500	10
192.3.2.1	1	4.3.2.1	156.100.140.25	12	1	TCP	24	2500	5
192.3.2.1	1	7.2.3.7	156.100.140.12	161	1	UDP	24	5400	10
192.3.2.2	1	9.2.3.7	140.100.140.12	12	0	TCP	24	500	10
192.3.2.2	1	23.2.3.7	140.100.140.9	12	0	TCP	24	500	10
192.3.2.2	1	45.2.3.7	140.100.140.67	12	0	TCP	24	500	10
192.3.2.2	1	86.2.3.7	140.100.140.48	162	1	UDP	24	300	1
192.3.2.2	1	78.2.3.7	140.100.140.43	12	0	TCP	24	500	10
192.3.2.3	1	9.2.3.7	140.100.140.12	12	0	TCP	24	500	10
192.3.2.3	1	23.2.3.7	140.100.140.9	12	0	TCP	24	500	10
192.3.2.3	1	45.2.3.7	140.100.140.67	12	0	TCP	24	500	10
192.3.2.3	1	86.2.3.7	140.100.140.48	12	0	TCP	24	500	10
192.3.2.3	1	78.2.3.7	140.100.140.43	12	0	TCP	24	500	10
192.3.2.2	1	9.76.3.7	139.100.140.12	12	0	TCP	24	500	10
192.3.2.2	1	48.2.3.7	139.100.140.9	12	0	TCP	24	500	10
192.3.2.2	1	46.2.3.7	139.100.140.67	12	0	TCP	24	500	10
192.3.2.2	1	35.2.3.7	139.100.140.48	12	0	TCP	24	500	10
192.3.2.2	1	98.2.3.7	139.100.140.43	12	0	TCP	24	500	10
192.3.2.3	1	9.76.3.7	139.100.140.12	12	0	TCP	24	500	10
192.3.2.3	1	48.2.3.7	139.100.140.9	12	0	TCP	24	500	10
192.3.2.3	1	46.2.3.7	139.100.140.67	12	0	TCP	24	500	10
192.3.2.3	1	35.2.3.7	139.100.140.48	12	0	TCP	24	500	10
192.3.2.3	1	98.2.3.7	139.100.140.43	12	0	TCP	24	500	10

Tableau V

exporter	AggrID	If Index	Nbflux	Source Addr	Port Serveur	Sens	Protocol	Src Mask	octets	pkts
192.3.2.1	Ag1	1	3	156.100.140.0	12	0	TCP	24	1500	30
192.3.2.1	Ag1	1	1	156.100.140.0	12	1	TCP	24	2500	5
192.3.2.1	Ag1	1	1	156.100.140.0	161	1	UDP	24	5400	10
192.3.2.2	Ag2	1	4	140.100.140.0	12	0	TCP	24	2000	40
192.3.2.2	Ag2	1	1	140.100.140.0	162	1	UDP	24	300	1
192.3.2.3	Ag2	1	5	140.100.140.0	12	0	TCP	24	500	50
192.3.2.2	Ag2	1	5	139.100.140.0	12	0	TCP	24	2500	50
192.3.2.3	Ag2	1	5	139.100.140.0	12	0	TCP	24	2500	50

Tableau VI

Exporter	If Index	DstAddr	SrcAddr	Src Port	Dst Port	Protocol	Dst Mask	bytes	pkts
192.3.2.4	1	156.100.140.5	1.2.3.4	3800	12	TCP	24	4000	100
192.3.2.4	1	156.100.140.28	3.4.5.6	6600	12	TCP	24	4000	100
192.3.2.4	1	156.100.140.24	8.2.3.1	7000	12	TCP	24	4000	100
192.3.2.4	1	156.100.140.25	4.3.2.1	12	8000	TCP	24	10000	10
192.3.2.4	1	156.100.140.12	7.2.3.7	161	1730	UDP	24	8000	10
192.3.2.5	1	140.100.140.12	9.2.3.7	3400	12	TCP	24	4000	100
192.3.2.5	1	140.100.140.9	23.2.3.7	6500	12	TCP	24	4000	100
192.3.2.5	1	140.100.140.67	45.2.3.7	3200	12	TCP	24	4000	100
192.3.2.5	1	140.100.140.43	78.2.3.7	2000	12	TCP	24	4000	100
192.3.2.5	1	140.100.140.12	9.2.3.7	2000	12	TCP	24	4000	100
192.3.2.5	1	140.100.140.9	23.2.3.7	2000	12	TCP	24	4000	100
192.3.2.5	1	140.100.140.67	45.2.3.7	2000	12	TCP	24	4000	100
192.3.2.5	1	140.100.140.48	86.2.3.7	2000	12	TCP	24	4000	100
192.3.2.5	1	140.100.140.43	78.2.3.7	2000	12	TCP	24	4000	100
192.3.2.4	1	139.100.140.12	9.76.3.7	3400	12	TCP	24	4000	100
192.3.2.4	1	139.100.140.9	48.2.3.7	6500	12	TCP	24	4000	100
192.3.2.4	1	139.100.140.67	46.2.3.7	3200	12	TCP	24	4000	100
192.3.2.4	1	139.100.140.48	35.2.3.7	5400	12	TCP	24	4000	100
192.3.2.4	1	139.100.140.43	98.2.3.7	2000	12	TCP	24	4000	100
192.3.2.4	1	139.100.140.12	9.76.3.7	2000	12	TCP	24	4000	100
192.3.2.4	1	139.100.140.9	48.2.3.7	2000	12	TCP	24	4000	100
192.3.2.4	1	139.100.140.67	46.2.3.7	2000	12	TCP	24	4000	100
192.3.2.4	1	139.100.140.48	35.2.3.7	2000	12	TCP	24	4000	100
192.3.2.4	1	139.100.140.43	98.2.3.7	2000	12	TCP	24	4000	100

Tableau VII

Exporter	Aggr ID	I f I n d e x	DstAddr	Nbf lux	Src Port	Sens	Proto col	Dst Mask	bytes	pkts
192.3.2.4	Ag1	1	156.100.140.0	3	12	1	TCP	24	12000	300
192.3.2.4	Ag1	1	156.100.140.0	1	12	0	TCP	24	10000	10
192.3.2.4	Ag1	1	156.100.140.0	1	161	0	UDP	24	8000	10
192.3.2.5	Ag1	1	140.100.140.0	9	12	1	TCP	24	36000	900
192.3.2.4	Ag1	1	139.100.140.0	9	12	1	TCP	24	40000	1000

Tableau VIII: Activité vers des serveurs externes au réseau client

AggrI D	Client network	Src Mask	Port server	Proto col	out Nb	Out Bytes	Out Pkts	In Nb	In Bytes	In Pkts
Ag1	156.100.140.0	24	12	TCP	1	2500	5	3	10000	10
Ag1	156.100.140.0	24	161	UDP	1	5400	10	1	8000	10
Ag2	140.100.140.0	24	162	UDP	1	300	1	0	0	0

Tableau IX: Activité des serveurs dans le réseau client

AggrI D	Client network	Src Mask	Port server	Proto col	out Nb	Out Bytes	Out Pkts	In Nb	In Bytes	In Pkts
Ag1	156.100.140.0	24	12	TCP	3	1500	30	3	12000	300
Ag2	140.100.140.0	24	12	TCP	9	4500	90	10	36000	900
Ag2	139.100.140.0	24	12	TCP	10	5000	100	10	40000	1000

REVENDICATIONS

1. Procédé de collecte de descriptions de flux portant sur des flux relatifs à au moins un réseau client (2, 3), le réseau client (2, 3) étant rattaché à un réseau d'interconnexion (1), ledit procédé comprenant:

- une première étape de réception de descriptions de flux (E3), lesdites descriptions de flux portant sur des flux en provenance du réseau client (2,3) ;
- une première étape d'agrégation des descriptions de flux (E62) portant sur les flux en provenance du réseau client (2,3) en fonction d'un critère d'agrégation ;
- une première étape de transmission (E63) des descriptions de flux agrégées vers un équipement de collecte (60, 70) ;

caractérisé en ce qu'il comprend en outre:

- une étape d'analyse des descriptions des flux (E4) portant sur les flux en provenance du réseau client (2,3) afin de déterminer au moins une caractéristique de flux propre au réseau client ;
- une deuxième étape de réception de descriptions de flux (E81), lesdites descriptions de flux portant sur des flux en provenance du réseau d'interconnexion (1) ;
- une étape de filtrage des descriptions de flux (E82) portant sur les flux en provenance du réseau d'interconnexion (1), dans laquelle sont éliminées les descriptions de flux portant sur des flux dépourvus de ladite au moins une caractéristique de flux propre au réseau client déterminée ;
- une deuxième étape de transmission (E85) des descriptions de flux filtrées vers l'équipement de collecte (60, 70).

2. Procédé selon la revendication 1, dans lequel, avant la deuxième étape de transmission (E85), le procédé comprend en outre une deuxième étape d'agrégation (E84) des descriptions de flux filtrées en fonction du critère d'agrégation.

3. Procédé selon la revendication 1 ou 2, dans lequel la première étape d'agrégation (E62) comprend en outre une sous-étape d'affectation aux descriptions de flux agrégées d'un paramètre d'identification d'une demande d'agrégation et l'étape de filtrage des descriptions de flux (E82) comprend une sous-étape d'affectation aux descriptions de flux filtrées du même paramètre d'identification de la demande d'agrégation.
4. Procédé selon la revendication 2 ou 3, ledit procédé comprenant en outre une troisième étape d'agrégation (E9), ladite étape consistant à agréger les descriptions de flux agrégées portant sur des flux en provenance du réseau client (2,3) et les descriptions de flux agrégées en provenance du réseau d'interconnexion (1) afin d'obtenir des descriptions de flux agrégées bi-directionnelles avant transmission vers l'équipement de collecte (60, 70).
5. Procédé selon les revendications 2 à 4, dans lequel
- il est en outre prévu une étape d'affectation (E61) aux descriptions de flux portant sur les flux en provenance du réseau client (2,3) et aux descriptions de flux portant sur les flux en provenance du réseau d'interconnexion (1) d'un paramètre représentatif d'un sens de transmission entre un client et un serveur, sens montant du client vers le serveur et sens descendant du serveur vers le client, en fonction des valeurs respectives des ports source et de destination contenues dans lesdites descriptions de flux, et
 - lors des première et deuxième étapes d'agrégation (E62, E84), les descriptions de flux sont agrégées en fonction dudit paramètre représentatif du sens de transmission et du critère d'agrégation.
6. Procédé selon l'une quelconque des revendications précédentes, dans lequel il est en outre prévu une étape d'affectation (E62) aux descriptions de flux agrégées portant sur les flux en provenance du réseau client (2, 3) et aux descriptions de flux agrégées portant sur les flux en provenance du réseau d'interconnexion (1)

d'un paramètre temporel représentatif de la répartition dans le temps des descriptions de flux qui ont été agrégées.

- 5 7. Système de collecte de descriptions de flux portant sur des flux relatifs à au moins un réseau client, le réseau client (2, 3) étant rattaché à un réseau d'interconnexion (1), ledit système comprenant:
- au moins un module de réception de descriptions de flux (510) agencé pour recevoir des descriptions de flux portant sur des flux en provenance de l'un des deux réseaux d'interconnexion (1) et client (2,3) ;
 - 10 - au moins un module d'agrégation de descriptions de flux (512), agencé pour agréger des descriptions de flux reçues en fonction d'un critère d'agrégation ;
 - un module d'analyse de descriptions de flux (511), agencé pour analyser des descriptions de flux portant sur des flux en provenance du réseau client (2,3) afin de déterminer au moins une caractéristique de flux propre au réseau client ;
 - 15 - un module de filtrage de descriptions de flux (515), agencé pour éliminer, dans les descriptions de flux reçues, celles portant sur des flux dépourvus de ladite au moins caractéristique de flux déterminée ;
 - un module de transmission de descriptions de flux (513), agencé pour transmettre des descriptions de flux filtrées à un module de collecte (60, 70).
- 20 8. Système selon la revendication 7 comprenant en outre un module d'agrégation (602) agencé pour agréger des descriptions de flux agrégées portant sur des flux en provenance du réseau client (2, 3) et des descriptions de flux agrégées en provenance du réseau d'interconnexion (1).
- 25 9. Système selon la revendication 7 ou 8, dans lequel il est prévu un module d'affectation à une description de flux d'un paramètre représentatif d'un sens de transmission entre un client et un serveur (516), sens montant du client vers le serveur et sens descendant du serveur vers le client en fonction des valeurs respectives des ports source et de destination contenues dans ladite description de
- 30

flux et le module d'agrégation (512) est agencé pour agréger les descriptions de flux en fonction dudit paramètre représentatif du sens de transmission et du critère d'agrégation.

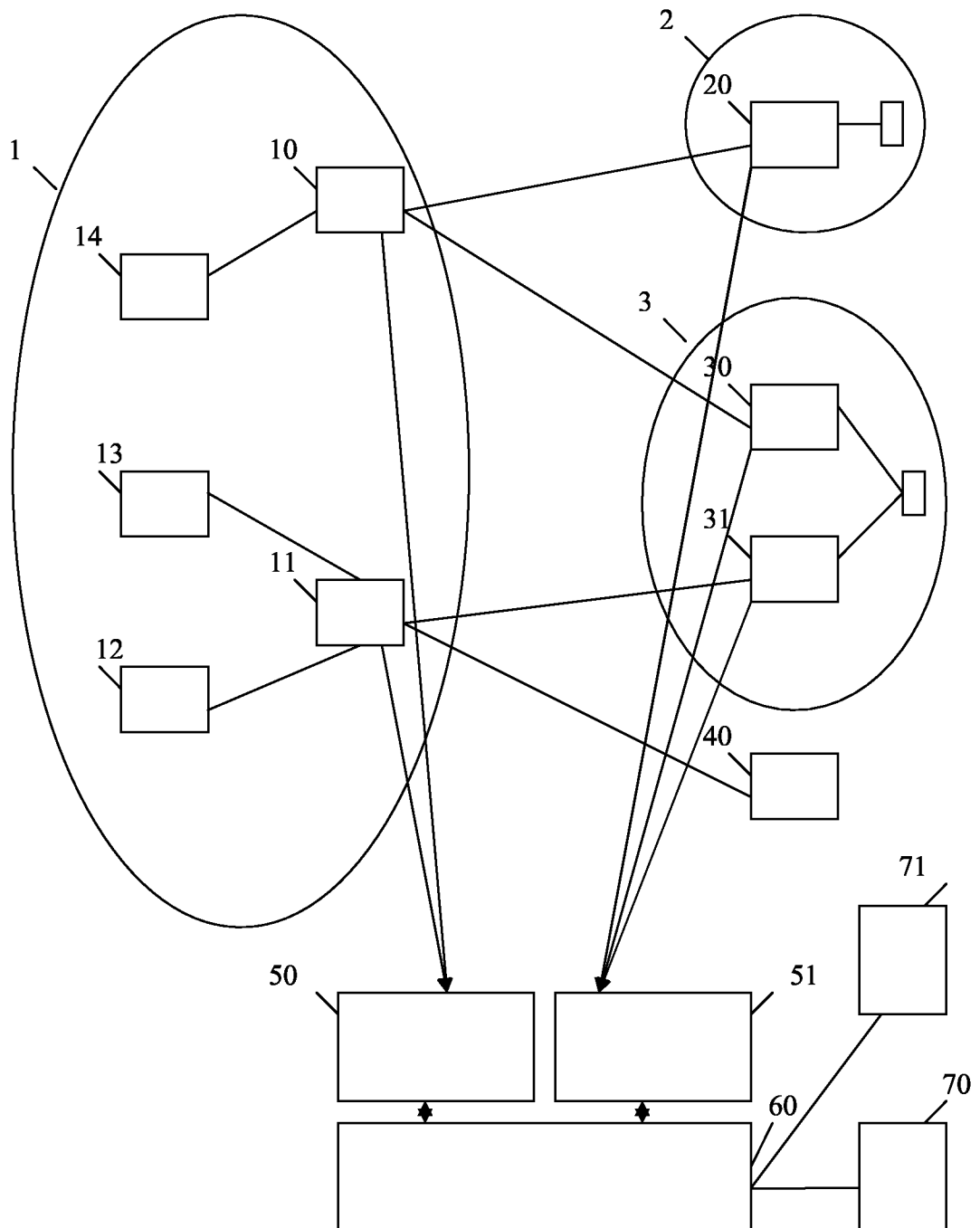


Figure 1

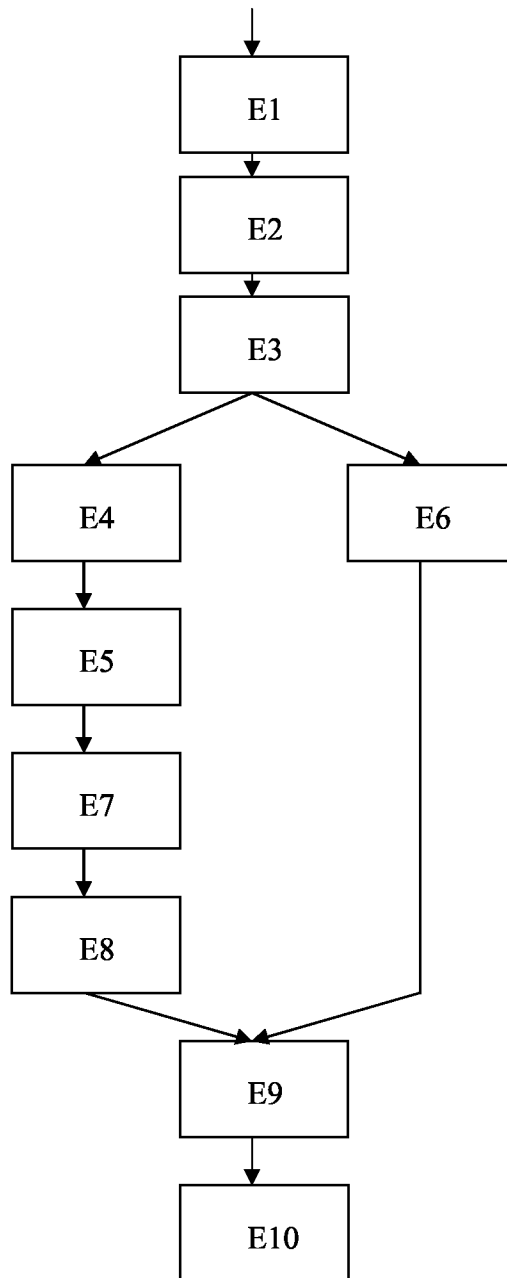


Figure 2

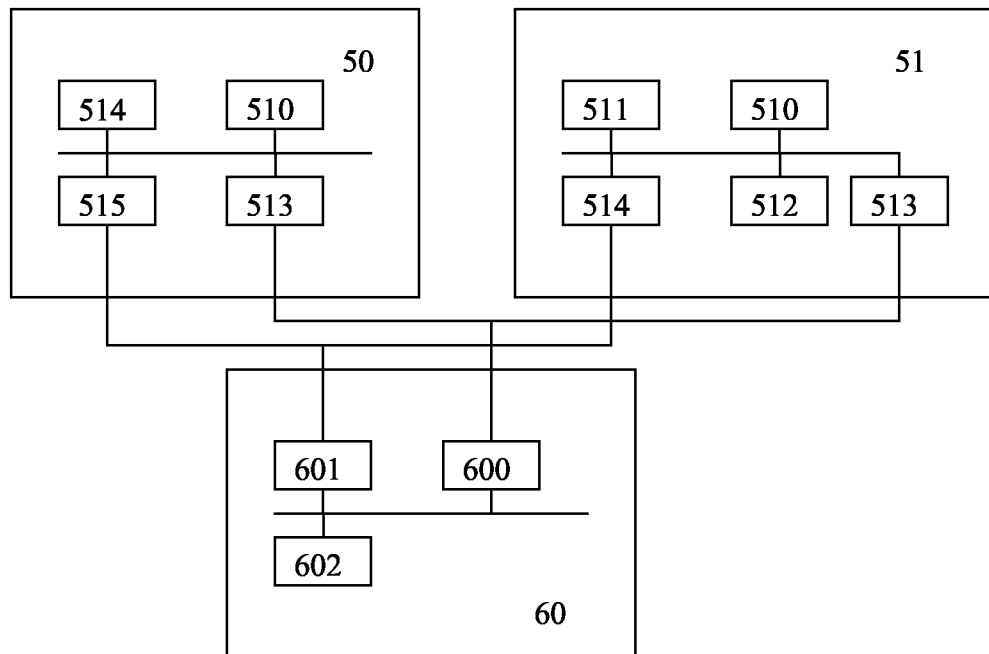


Figure 3