(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 030 164**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **14 62364**

(51) Int Cl[8] : ***H 04 L 12/24*** *(2016.01), H 04 L 12/701*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 12.12.14.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 17.06.16 Bulletin 16/24.

(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 :**

( ) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *WORLDLINE Société anonyme* — FR.

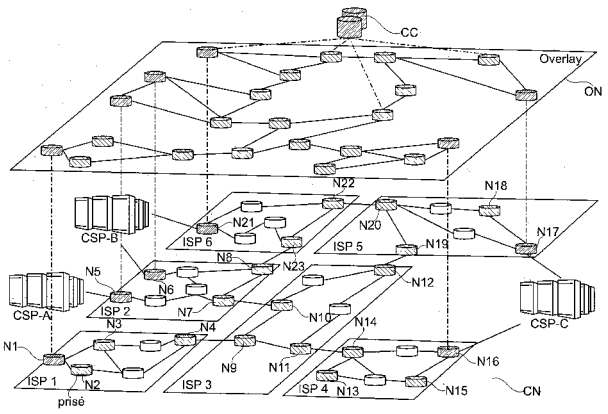
(72) **Inventeur(s) :** FRESSANCOURT ANTOINE et GAGNAIRE MAURICE.

(73) **Titulaire(s) :** WORLDLINE Société anonyme.

(74) **Mandataire(s) :** NOVAGRAAF TECHNOLOGIES.

(54) RESEAU SUPERPOSE POUR RESEAU DE COMMUNICATION CONNECTANT DES CENTRES DE DONNEES D'UN FOURNISSEUR DE SERVICES EN NUAGE.

(57) L'invention concerne un réseau superposé (ON) à un réseau de communication (CN) destiné à connecter des centres de données (CSP-A, CSP-B, CSP-C, CSP-D) d'un fournisseur de services en nuage, ce réseau superposé comportant une pluralité de noeuds particuliers (N1, N2, N3... N22) paramétrés de sorte à former des chemins reliant les centres de données, et le réseau superposé étant associé à un dispositif de contrôle (CC) ; les noeuds particuliers étant en outre prévus pour transmettre des mesures locales au dispositif de contrôle, et celui-ci étant prévu pour, en cas de détermination d'une anomalie à partir des mesures locales, calculer un nouveau chemin au sein du réseau superposé et provisionner ce nouveau chemin auprès d'un ensemble de noeuds particulier de ladite pluralité.



FR 3 030 164 - A1

RESEAU SUPERPOSE POUR RESEAU DE COMMUNICATION CONNECTANT DES CENTRES DE DONNEES D'UN FOURNISSEUR DE SERVICES EN NUAGE

DOMAINE DE L'INVENTION

L'invention est relative au domaine de l'informatique en nuage, communément appelée « *cloud computing* » selon la terminologie en langue anglaise. Elle concerne plus particulièrement la gestion d'une infrastructure réseau permettant d'assurer la connectivité entre plusieurs centres de données et permettant un haut degré de résilience.

CONTEXTE DE L'INVENTION

L'informatique en nuage permet d'abstraire les services offerts par une infrastructure de traitement de données de son architecture et de ses mécanismes technologiques sous-jacents. Elle permet notamment d'utiliser les puissances de calcul et/ou de stockage de serveurs informatiques distants et connectés par un réseau de communication, généralement le réseau Internet.

Un fournisseur de services en nuage, CSP (pour « Cloud Service Provider » en langue anglaise) peut ainsi offrir à ses clients ces puissances de calcul et/ou de stockage.

L'essor de ce type de modèle ces dernières années provoque un accroissement des exigences des clients sur la qualité de service attendue. Ainsi est apparue une demande importante pour que le service soit résiliant, c'est-à-dire qu'il ait la capacité de continuer à fournir le service demandé en cas de panne d'un équipement au sein du nuage.

Afin d'assurer cette exigence, les fournisseurs CSP déploient leurs services au sein de plusieurs centres de données, ou « datacenters » selon la terminologie en langue anglaise, redondants et distants les uns des autres. Ces centres de données sont interconnectés, généralement par des liens privés et dédiés au sein du réseau de communication reliant les centres de données. Ces liens peuvent être également redondants.

Toutefois, cette solution d'implémentation pose d'assez importants problèmes.

Notamment, elle oblige à sur-provisionner les ressources, puisque les redondances sont nécessairement fixées de façon statique. En outre, le temps de paramétrage est long.

RESUME DE L'INVENTION

Le but de la présente invention est de fournir une solution palliant au moins partiellement les inconvénients précités.

A cette fin, la présente invention propose un réseau superposé à un réseau de communication destiné à connecter des centres de données d'un fournisseur de services en nuage, ledit réseau superposé comportant une pluralité de nœuds particuliers, paramétrés de sorte à former des chemins reliant lesdits centres de données, et ledit réseau superposé étant associé à un dispositif de contrôle ; lesdits nœuds particuliers étant en outre prévus pour transmettre des mesures locales audit dispositif de contrôle, et ledit dispositif de contrôle étant prévu pour, en cas de détermination d'une anomalie à partir desdites mesures locales, calculer un nouveau chemin au sein dudit réseau superposé et provisionner ledit nouveau chemin auprès d'un ensemble de nœuds particulier de ladite pluralité

Suivant des modes de réalisation préférés, l'invention comprend une ou plusieurs des caractéristiques suivantes qui peuvent être utilisées séparément ou en combinaison partielle entre elles ou en combinaison totale entre elles :

- les données transmises d'un premier centre de données vers un second centre de données sont acheminées en utilisant un mécanisme de routage par segments, lesdits segments étant fournis par ledit dispositif de contrôle ;
- les communications entre ledit dispositif de contrôle et lesdits nœuds particuliers sont conformes au mécanisme « Openflow » ;
- ledit dispositif de contrôle est prévu pour construire à partir desdites mesures locales, une série temporelle et pour comparer ladite série temporelle à des informations témoins afin de déterminer ladite anomalie, lesdites informations témoins étant préalablement établies dans une phase d'apprentissage ;
- chacun desdits centres de données est connecté à au moins deux domaines du réseau de communication ;
- ledit nouveau chemin est calculé en fonction des besoins opérationnels d'une application utilisant lesdits centres de données.

Un autre objet de l'invention concerne un réseau de communication pour connecter des centres de données d'un fournisseur de services en nuage, ledit réseau de communication comportant au moins un domaine, une pluralité de nœuds particuliers formant un réseau superposé dudit réseau de communication et paramétrés de sorte à former des chemins reliant lesdits centres de données, et ledit réseau de communication étant associé à un dispositif de contrôle ; lesdits nœuds particuliers étant en outre prévus pour transmettre des mesures locales audit dispositif de contrôle, et ledit dispositif de contrôle étant prévu pour, en cas de détermination d'une anomalie à partir desdites mesures locales, calculer un nouveau chemin au sein dudit réseau de communication et provisionner ledit nouveau chemin auprès d'un ensemble de nœuds particulier de ladite pluralité.

Suivant des modes de réalisation préférés, l'invention comprend une ou plusieurs des caractéristiques suivantes qui peuvent être utilisées séparément ou en combinaison partielle entre elles ou en combinaison totale entre elles :

- les données transmises d'un premier centre de données vers un second centre de données sont acheminées en utilisant un mécanisme de routage par segments, lesdits segments étant fournis par ledit dispositif de contrôle ;
- les communications entre ledit dispositif de contrôle et lesdits nœuds particuliers sont conformes au mécanisme « Openflow » ;
- ledit dispositif de contrôle est prévu pour construire à partir desdites mesures locales, une série temporelle et pour comparer ladite série temporelle à des informations témoins afin de déterminer ladite anomalie, lesdites informations témoins étant préalablement établies dans une phase d'apprentissage ;
- chacun desdits centres de données est connecté à au moins deux domaines du réseau de communication ;
- ledit nouveau chemin est calculé en fonction des besoins opérationnels d'une application utilisant lesdits centres de données.

Un autre objet de l'invention concerne un procédé de gestion d'un réseau superposé à un réseau de communication connectant des centres de données d'un fournisseur de services en nuage, ledit réseau comportant une pluralité de nœuds particuliers paramétrés de sorte à former des chemins reliant lesdits centres de données, et ledit réseau superposé étant associé à un dispositif de contrôle ; dans lequel lesdits nœuds particuliers transmettent des mesures

locales audit dispositif de contrôle, et ledit dispositif de contrôle, en cas de détermination d'une anomalie à partir desdites mesures locales, calcule un nouveau chemin au sein dudit réseau de communication et provisionne ledit nouveau chemin auprès d'un ensemble de nœuds particulier de ladite pluralité.

Suivant des modes de réalisation préférés, l'invention comprend une ou plusieurs des caractéristiques suivantes qui peuvent être utilisées séparément ou en combinaison partielle entre elles ou en combinaison totale entre elles :

- chacun dudit au moins domaine est associé à un opérateur de services internet.
- chacun desdits centres de données est connecté à au moins deux domaines dudit réseau de communication (CN) ;
- ledit nouveau chemin est calculé en fonction des besoins opérationnels d'une application utilisant lesdits centres de données.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui suit d'un mode de réalisation préféré de l'invention, donnée à titre d'exemple et en référence aux dessins annexés.

BREVE DESCRIPTION DES DESSINS

La figure 1 représente schématiquement un exemple de mise en œuvre d'un réseau superposé associé à un dispositif de contrôle selon l'invention.

DESCRIPTION DETAILLEE DE L'INVENTION

La figure 1 représente un exemple de réseau de communication CN connectant des centres de données CSP-A, CSP-B, CSP-C et CSP-D. Ces centres de données peuvent appartenir à un même fournisseur de services en nuage (CSP pour « Cloud Service Provider » en langue anglaise) ou bien à plusieurs fournisseurs distincts mais ayant choisi de fédérer leur offre de service.

Ce réseau de communication CN est typiquement le réseau Internet. Il permet de connecter des centres de données situées en des localisations distantes les unes des autres.

La multiplicité des centres de données permet d'apporter une caractéristique de résilience au service en nuage : une panne locale sur un centre de données particulier n'impacte pas durablement le service fourni car celui-ci peut alors être déployé sur un autre centre de données. Un avantage de disposer de centres de données distants est d'éviter qu'une panne locale (alimentation…) impacte plusieurs centres de données.

Le réseau de communication CN est également prévu pour répondre à cette exigence de résilience. Pour ce faire, selon l'invention, il est à même de s'adapter rapidement à une panne locale afin que les communications entre les centres de données CSP-A, CSP-B, CSP-C et CSP-D ne soient pas interrompues mais se poursuivent avec la meilleure qualité de service possible (QoS pour « Quality of Service »).

Le réseau de communication CN comporte au moins un domaine mais préférablement plusieurs domaines. Chacun de ces domaines (ISP 1, ISP 2, ISP 3, ISP 4, ISP 5, ISP 6) peut être associé à un fournisseur de service internet distinct.

De la sorte, une panne impactant un fournisseur de service Internet n'affectera qu'un domaine, soit une partie du réseau de communication CN. Comme on le verra plus loin, celui-ci est prévu, selon l'invention, pour réagir à une telle panne et réallouer ses ressources pour que les communications passant par ce domaine et concernant le service en nuage soient réacheminées pour passer par d'autres domaines.

De façon connue en soi, le réseau de communication CN est composé d'un grand nombre de nœuds (par exemple des routeurs, en technologie « IP »…).

Selon l'invention, sur la base de ce réseau de communication CN, on constitue un réseau superposé, ou « overlay » selon la terminologie en langue anglaise plus commune, auquel on associe un dispositif de contrôle CC. Plus précisément, on considère un sous-ensemble de nœuds, N1, N2, N3… N22, que l'on appelle ici « nœuds particuliers » et qui forment ce réseau superposé.

Sur la figure 1, ce réseau superposé ON est représenté comme une surcouche du réseau de communication CN. Il s'agit toutefois d'une vue de l'esprit, dans la mesure où il ne s'agit que d'une abstraction qui permet de faire comprendre que d'un point de vue extérieur, et de celui d'un dispositif de contrôle CC, seul cette sous-partie du réseau de communication CN

est considéré (ou « vue »). Les nœuds figurants dans la couche d' « overlay » ON sont les mêmes que les nœuds particuliers figurants en grisé dans la couche du réseau de communication CN.

Selon un mode de réalisation de l'invention, les nœuds particuliers sont de deux sortes :

- Des nœuds d'inflexion du routage, en grisé clair
- Des nœuds de bordure, en grisé très sombre.

En outre, le réseau superposé ON est associé à un dispositif de contrôle CC. Ce dispositif est central et est unique pour le fournisseur de service en nuage, tout du moins d'un point de vue fonctionnel (il peut lui-même être réparti sur plusieurs systèmes redondants).

Les nœuds particuliers sont paramétrés de sorte à former des chemins reliant les centres de données. Ces chemins peuvent être déterminés par le dispositif de contrôle CC. Ainsi, ce dernier n'ayant que la vue du réseau superposé OC, les chemins ne sont établis qu'au sein du sous-ensemble des nœuds particuliers.

D'un point de vue pratique, l'acheminement des données entre deux nœuds particuliers au sein du réseau de communication est donc lié au fonctionnement propre du réseau de communication et sort donc du cadre de l'invention. Par exemple sur la figure 1, deux chemins existent entre les nœuds particuliers N3 et N4, et le choix du chemin est donc laissé à la technologie propre au réseau de communication CN.

En ne traitant que les nœuds particuliers, le dispositif de contrôle a à sa disposition une vue globale mais réduite du réseau de communication. Le nombre de nœuds particuliers peut être important mais substantiellement moindre que celui des nœuds du réseau de communication, de sorte qu'il est à même de traiter les informations et d'établir, comme il sera vu plus tard, des nouveaux chemins de façon dynamique.

En outre, d'une façon générale, le dispositif de contrôle CC peut ne pas avoir accès à l'ensemble des nœuds d'un domaine géré par un fournisseur de service Internet. Par l'usage du réseau superposé ON, il a accès à une partie des nœuds qui échappent au contrôle du fournisseur de service Internet, ce qui lui permet de s'abstraire en partie de la politique de routage du fournisseur de service Internet. Notamment, les nœuds particuliers peuvent être situés dans les zones frontalières entre les domaines sur lesquels les fournisseurs de service Internet n'ont pas de contrôle direct et exclusif.

Le dispositif de contrôle CC peut donc établir la politique de routage de façon centralisée pour l'ensemble du réseau de communication CN. Celle-ci peut donc être

indépendante des opérateurs de télécommunication et des fournisseurs de service Internet (ISP, « *Internet Service Providers* »), dans la mesure où il n'est pas assujetti à un SLA (« Service Level Agreement »), dont la mise en place et la gestion sont des opérations très complexes.

Par exemple, cette politique de routage peut utiliser un mécanisme de routage par segments, ou « *segment routing* » selon la terminologie en langue anglaise. Ce mécanisme est actuellement en cours de standardisation à l'IETF (« Internet Engineering Task Force »). D'autres mécanismes de routage sont également possibles dans le cadre de l'invention, tels, notamment, la mise en place de tunnels.

Avec le routage par segments, un nœud achemine un datagramme à l'aide d'une liste ordonnée d'instructions ou étiquettes appelées « segment », qui peuvent avoir des valeurs locales à un nœud ou globales à l'intérieur d'un domaine. Une liste de segments peut être fournie pour chaque flot de datagrammes.

Ainsi, le dispositif de contrôle CC peut déterminer, pour un flot donné entre deux centres de données, une liste de segments formant un chemin entre ces deux centres de données à travers le réseau de communication CN.

Ces segments peuvent correspondre aux nœuds d'inflexion de routage, qui ont donc un rôle très important puisque ce sont ceux-ci qui acheminent les flots de données selon la politique générale établie par le dispositif de contrôle centralisé CC.

Ces segments peuvent également correspondre à un lien entre les nœuds d'inflexion de routage, voire à un groupe de nœuds d'inflexion de routage.

Il est possible de ne donner que peu de segments, de sorte que le chemin réel pris par le flot de données n'est que peu contraint par la politique générale établie par le dispositif de contrôle CC. En dehors de ces contraintes, comme il a été vu plus haut, les mécanismes de routage propres au domaine concerné s'appliquent.

Il est également possible de fournir un très grand nombre de segments, de sorte que le chemin est fortement contraint par la politique générale.

Il est également possible d'établir des tunnels entre chaque nœud particulier N1, N2, N3… N22 d'un chemin donné.

Les nœuds de bordure ont pour rôle d'acheminer les flots de données entre les centres de données CSP-A, CSP-B, CSP-C, CSP-D et les domaines ISP 1, ISP 2, ISP 3, ISP 4, ISP 5, ISP 6.

Il peut être choisi de n'associer un nœud de bordure qu'à un unique couple centre de données / domaine. En outre, il peut être choisi que chacun des centres de données est connecté à au moins deux domaines. Ainsi, sur la figure 1, le centre de données CSP-A est connecté au domaine ISP 1 via le nœud de bordure N1, et au domaine ISP 2 via le nœud de bordure N5. De la sorte, on établit une redondance dans les moyens de connexion des centres de données avec le réseau de communication CN.

En outre, les nœuds de bordure ont pour rôle de faire le pont entre les mécanismes de routage interne au réseau au réseau superposé ON et le routage internet aux centres de données. Dans l'exemple d'une mise en œuvre utilisant un routage par segments, les nœuds de bordure écoutent continument les annonces de segment transmises par l'algorithme de routage de leur domaine (par exemple le protocole IGP pour « Interior Gateway routing Protocol), et transmet cette information au dispositif de contrôle CC. Ils annoncent aussi les segments afin d'être atteints depuis l'intérieur des centres de données. Ces mêmes segments peuvent également être utilisés par le dispositif de contrôle CC pour le routage au sein du réseau superposé ON.

Par ailleurs, les nœuds particuliers sont prévus pour transmettre des mesures locales au dispositif de contrôle CC. Tant les nœuds d'inflexion de routage que les nœuds de bordure peuvent être concernés par cette tâche de remontée d'informations. Les mesures locales transmises par les nœuds de bordure permettent au dispositif de contrôle d'acquérir une connaissance de ce qui se passe à l'intérieur de chaque centre de données.

Les mesures locales peuvent être effectuées par le nœud particulier lui-même sur le trafic de données qui transite par lui. Différents types de mesures peuvent être effectués et transmis vers le dispositif de contrôle : gigue, latence, perte de paquets, etc.

Le dispositif de contrôle CC étant centralisé, il reçoit par conséquent des mesures locales provenant des différents nœuds particuliers (potentiellement de l'ensemble des nœuds particulier du réseau superposé ON). Il peut ainsi obtenir une vision d'ensemble du

comportement du réseau superposé ON, et déterminer une anomalie dès sa survenance au sein de ce réseau ON.

Une anomalie peut par exemple être un changement, éventuellement brutal, dans une des caractéristiques d'un nœud particulier. Il peut par exemple s'agir d'un accroissement du taux de perte de paquets, d'une augmentation de la gigue ou de la latence, etc.

Il peut alors réagir en déclenchant le calcul d'un (ou plusieurs) nouveau chemin au sein du réseau de communication. Ce nouveau chemin remplace le chemin impacté par l'anomalie. Si plusieurs chemins sont impactés par une anomalie, alors autant de nouveaux chemins peuvent être calculés par le dispositif de contrôle CC.

Par exemple, si l'anomalie est liée à un nœud particulier par lequel passe un chemin entre deux centres de données, un nouveau chemin reliant ces deux centres de données peut être calculé pour éviter le nœud particulier incriminé.

La transmission des mesures locales ainsi que le provisionnement d'informations relatives à un nouveau chemin vers les nœuds particuliers du réseau superposé ON peuvent être effectuées selon différents modes de réalisation. Notamment, le protocole Openflow, défini par l'« Open Networking Foundation » (ONF) peut être utilisé. Au sein d'un réseau de communication, ce protocole permet de séparer le contrôle de la transmission (« forwarding »). Il permet ainsi de déporter la couche de contrôle en dehors des équipements matériels des fabricants de routeurs et de commutateurs vers des équipements distants supportant des moyens logiciels.

Le dispositif de contrôle CC a pour rôle de s'assurer que les flots de données transmis entre les centres de données correspondent aux requis de qualité spécifiés par le fournisseur de services en nuage. Notamment, il est prévu pour détecter une anomalie dans le réseau de communication, via le réseau superposé ON, et réagir en déterminant un nouveau chemin pour contourner l'anomalie.

Comme on l'a vu, pour ce faire, il reçoit des mesures locales de la part des nœuds particuliers qui lui donnent une information complète du trafic au sein du réseau superposé ON et des centres de données CSP-A, CSP-B, CSP-C, CSP-D.

Plusieurs mécanismes peuvent être mis en œuvre par le dispositif de contrôle et entre celui-ci et les nœuds particuliers.

Une première mise en œuvre se base sur la détection de déviation des caractéristiques mesurées par les nœuds particuliers.

Selon cette mise en œuvre, le dispositif de contrôle CC met en œuvre un algorithme passif, c'est-à-dire basé uniquement sur des informations remontées depuis le réseau de communication.

Plus précisément, le dispositif de contrôle CC construit, à partir des mesures locales reçues des nœuds particuliers, une série temporelle. Cette série temporelle est représentative de l'évolution d'une caractéristique (gigue, latence, perte de paquet… par exemple) pour un nœud donné. En comparant cette série temporelle à des informations témoins, il peut déterminer une anomalie. Ces informations témoins peuvent avoir été préalablement établies dans une phase d'apprentissage.

Un exemple de phase d'apprentissage peut consister à :

- fournir au dispositif de contrôle CC une série de mesures de gigue, latence, pertes de paquets… collectées et remontées par les nœuds particuliers pendant une période de référence.
- Associer des observations de panne aux mesures fournies afin que le dispositif de contrôle CC associe les mesures collectées et les pannes constatées ;
- Analyser les mesures afin d'en déduire des règles permettant d'associer des pannes aux mesures collectées.
- Fournir ces règles à un moteur de règles inclus dans le dispositif de contrôle CC.

Dans une phase de traitement, le moteur de règles peut alors utiliser les règles préalablement établies pour déterminer les anomalies.

Par exemple de façon périodique, les nœuds particuliers du réseau superposé ON transmettent des mesures locales au dispositif de contrôle CC.

Celui-ci peut les stocker et les mettre en relation avec les mesures locales précédemment collectées de sorte à construire des séries temporelles. Ces séries temporelles (constituées de mesures historisées) sont fournies au moteur de règles.

Si le moteur de règles reconnait, dans les séries temporelles, un signal ou empreinte qui a été associé à une panne lors de la phase d'apprentissage, alors une anomalie est déterminée.

Cette anomalie correspondant à un nœud particulier ou à un lien associé à ce nœud particulier. Pour tout chemin passant par ce nœud ou ce lien, le dispositif de contrôle CC peut alors calculer un nouveau chemin qui l'évite. Ce nouveau chemin remplace alors le chemin précédent et les informations correspondant à ce nouveau chemin sont alors provisionnées sur les nœuds particuliers concernés du réseau superposé ON.

Par exemple, si le nœud particulier N7 est victime d'une panne, et si le chemin reliant les centres de données CSP-A et CSP-B passe par ce nœud N7, le dispositif de contrôle CC doit calculer un nouveau chemin. Un tel nouveau chemin peut par exemple passer par les nœuds N2, N4, N9, N10, N12, N19, N20, N22 et N21. Il peut alors provisionner ce nouveau chemin auprès d'un ensemble de nœuds particuliers concernés. Notamment, il peut définir ce chemin en établissant la liste appropriée de segments correspondants aux nœuds particuliers qui doivent être traversés selon ce nouveau chemin.

Ainsi, le trafic correspondant aux flots de données entre les centres de données CSP-A et CSP-B évite le nœud N7 impacté d'une panne, et la qualité de service globale n'est pas impactée par l'anomalie détectée.

Une autre mise en œuvre se base sur la détection de la perte de paquets par les nœuds particuliers et sur un algorithme actif/passif mis en place par le dispositif de contrôle CC.

Comme précédemment, le dispositif de contrôle CC reçoit passivement les mesures locales provenant des nœuds particuliers.

Dans un mode de réalisation, il s'intéresse au taux de perte de paquets et déclenche un traitement particulier uniquement si ce taux dépasse un certain seuil pour un nœud spécifique.

En ce cas, le dispositif de contrôle CC marque le nœud cible du flot de paquets comme potentiellement défaillant. On nomme dans la suite le nœud à l'origine de la remontée de l'information « nœud de signalement ».

Le dispositif de contrôle CC demande alors (c'est la phase active de l'algorithme) aux nœuds voisins du nœud potentiellement défaillant au sein du réseau superposé ON (y compris le nœud de signalement) d'émettre des paquets de sonde vers ce nœud potentiellement défaillant.

Ces paquets de sonde requièrent une réponse de la part du nœud potentiellement défaillant destinataire.

Il y a alors 3 possibilités :

- Les paquets de sonde envoyés sont sans réponse. On a affaire à une panne du nœud potentiellement défaillant. Le dispositif de contrôle CC détermine une anomalie sur ce nœud et calcule des nouveaux chemins évitant ce nœud.
- Seule une partie des paquets de sonde reste sans réponse (dont normalement le paquet de sonde envoyé par le nœud de signalement). On a donc affaire à une panne de lien(s). Le dispositif de contrôle CC détermine une anomalie sur ce ou ces liens et calcule des nouveaux chemins évitant ces liens.
- Aucun paquet de sonde ne reste sans réponse. On peut alors considérer qu'il s'agit d'un « faux positif ». Le dispositif de contrôle CC ne détermine pas de nouveaux chemins et la politique générale de routage reste inchangée.

On peut prévoir que le dispositif de contrôle CC place le lien entre le nœud de signalement et le nœud potentiellement défaillant sous une surveillance particulière. Notamment, si des futures mesures locales remontent le même problème, alors il pourra être décidé de déterminer une anomalie sur ce lien. Le dispositif de contrôle CC peut alors déterminer un nouveau chemin contournant l'anomalie.

Comme décrit précédemment, le (ou les) nouveau chemin est provisionné dans les nœuds particuliers concernés du réseau superposé ON.

Selon ces deux modes de réalisation décrits, le réseau de communication CN s'est adapté de façon transparente pour les utilisateurs et peut être automatique pour le gestionnaire du fournisseur de services en nuage. D'autres algorithmes peuvent être mis en place par le dispositif de contrôle CC, de sorte à fournir cette même capacité de résilience adaptative.

De la même façon, si une panne touche globalement un fournisseur de service internet (ISP), le domaine correspondant peut être évité et calculant les chemins appropriés le contournant et reliant les différents centres de données. Le fournisseur de services en nuage est ainsi totalement indépendant des fournisseurs de services internet.

En conséquence, il n'est plus nécessaire pour les fournisseurs de services en nuage de négocier et acheter des contrats particuliers de fournitures de service SLA (« Service Level Agreement »).

Il est en outre possible de gérer plusieurs chemins reliant deux centres de données. Le dispositif de contrôle CC peut alors effectuer une gestion des chemins en fonction de chaque flot de datagrammes, et attribuer des qualités de service différentes correspondant à des

chemins différents, en fonction des flots. Il est ainsi possible de régler un degré de résilience souhaité selon les flots de datagrammes (et donc, par exemple, en fonction du type d'application, du contrat entre le client et le fournisseur de services en nuage, etc.)

Le nouveau chemin à provisionner peut donc aussi dépendre de l'application utilisant les centres de données, et notamment de ses besoins opérationnels : qualité de service (QoS), degré de résilience, bande passante, gigue…

Il est à noter que dans le cadre d'une solution conforme à l'état de la technique utilisant le réseau Internet, une adaptation du réseau de communication peut s'effectuer également mais à un rythme lent, de l'ordre d'environ 5 mn. Pendant ce temps d'adaptation, il n'y a aucune assurance que les flots de données soient correctement acheminés.

L'invention permet d'écourter cette période d'adaptation durant laquelle le réseau se reconfigure, grâce à la combinaison, notamment, du réseau superposé ON et du dispositif de contrôle CC agencés tels que décrits précédemment.

Bien entendu, la présente invention n'est pas limitée aux exemples et au mode de réalisation décrits et représentés, mais elle est susceptible de nombreuses variantes accessibles à l'homme de l'art.

REVENDICATIONS

1. Réseau superposé (ON) à un réseau de communication (CN) destiné à connecter des centres de données (CSP-A, CSP-B, CSP-C, CSP-D) d'un fournisseur de services en nuage, ledit réseau superposé comportant une pluralité de nœuds particuliers (N1, N2, N3… N22), paramétrés de sorte à former des chemins reliant lesdits centres de données, et ledit réseau superposé étant associé à un dispositif de contrôle (CC) ; lesdits nœuds particuliers étant en outre prévus pour transmettre des mesures locales audit dispositif de contrôle, et ledit dispositif de contrôle étant prévu pour, en cas de détermination d'une anomalie à partir desdites mesures locales, calculer un nouveau chemin au sein dudit réseau superposé et provisionner ledit nouveau chemin auprès d'un ensemble de nœuds particulier de ladite pluralité.

2. Réseau superposé selon la revendication précédente, dans lequel les données transmises d'un premier centre de données vers un second centre de données sont acheminées en utilisant un mécanisme de routage par segments, lesdits segments étant fournis par ledit dispositif de contrôle (CC).

3. Réseau superposé selon l'une des revendications précédentes, dans lequel les communications entre ledit dispositif de contrôle (CC) et lesdits nœuds particuliers sont conformes au mécanisme « Openflow ».

4. Réseau superposé selon l'une des revendications précédentes, dans lequel ledit dispositif de contrôle (CC) est prévu pour construire à partir desdites mesures locales, une série temporelle et pour comparer ladite série temporelle à des informations témoins afin de déterminer ladite anomalie, lesdites informations témoins étant préalablement établies dans une phase d'apprentissage.

5. Réseau superposé selon l'une des revendications précédentes, dans lequel chacun desdits centres de données est connecté à au moins deux domaines du réseau de communication (CN).

6. Réseau superposé selon l'une des revendications précédentes, dans lequel ledit nouveau chemin est calculé en fonction des besoins opérationnels d'une application utilisant lesdits centres de données.

7. Réseau de communication (CN) pour connecter des centres de données (CSP-A, CSP-B, CSP-C, CSP-D) d'un fournisseur de services en nuage, ledit réseau de communication comportant au moins un domaine (ISP 1, ISP 2, ISP 3, ISP 4, ISP 5, ISP 6), une pluralité de nœuds particuliers (N1, N2, N3… N22), formant un réseau superposé (ON) dudit réseau de communication (CN) et paramétrés de sorte à former des chemins reliant lesdits centres de données, et ledit réseau de communication étant associé à un dispositif de contrôle (CC) ; lesdits nœuds particuliers étant en outre prévus pour transmettre des mesures locales audit dispositif de contrôle, et ledit dispositif de contrôle étant prévu pour, en cas de détermination d'une anomalie à partir desdites mesures locales, calculer un nouveau chemin au sein dudit réseau de communication et provisionner ledit nouveau chemin auprès d'un ensemble de nœuds particulier de ladite pluralité.

8. Procédé de gestion d'un réseau superposé (ON) à un réseau de communication (CN) connectant des centres de données (CSP-A, CSP-B, CSP-C, CSP-D) d'un fournisseur de services en nuage, ledit réseau comportant une pluralité de nœuds particuliers (N1, N2, N3… N22), paramétrés de sorte à former des chemins reliant lesdits centres de données, et ledit réseau superposé étant associé à un dispositif de contrôle (CC) ; dans lequel lesdits nœuds particuliers transmettent des mesures locales audit dispositif de contrôle, et ledit dispositif de contrôle, en cas de détermination d'une anomalie à partir desdites mesures locales, calcule un nouveau chemin au sein dudit réseau de communication et provisionne ledit nouveau chemin auprès d'un ensemble de nœuds particulier de ladite pluralité.

9. Procédé de gestion selon la revendication précédente, dans lequel chacun dudit au moins domaine est associé à un opérateur de services internet.

10. Procédé de gestion selon la revendication précédente, dans lequel chacun desdits centres de données est connecté à au moins deux domaines dudit réseau de communication (CN).

5

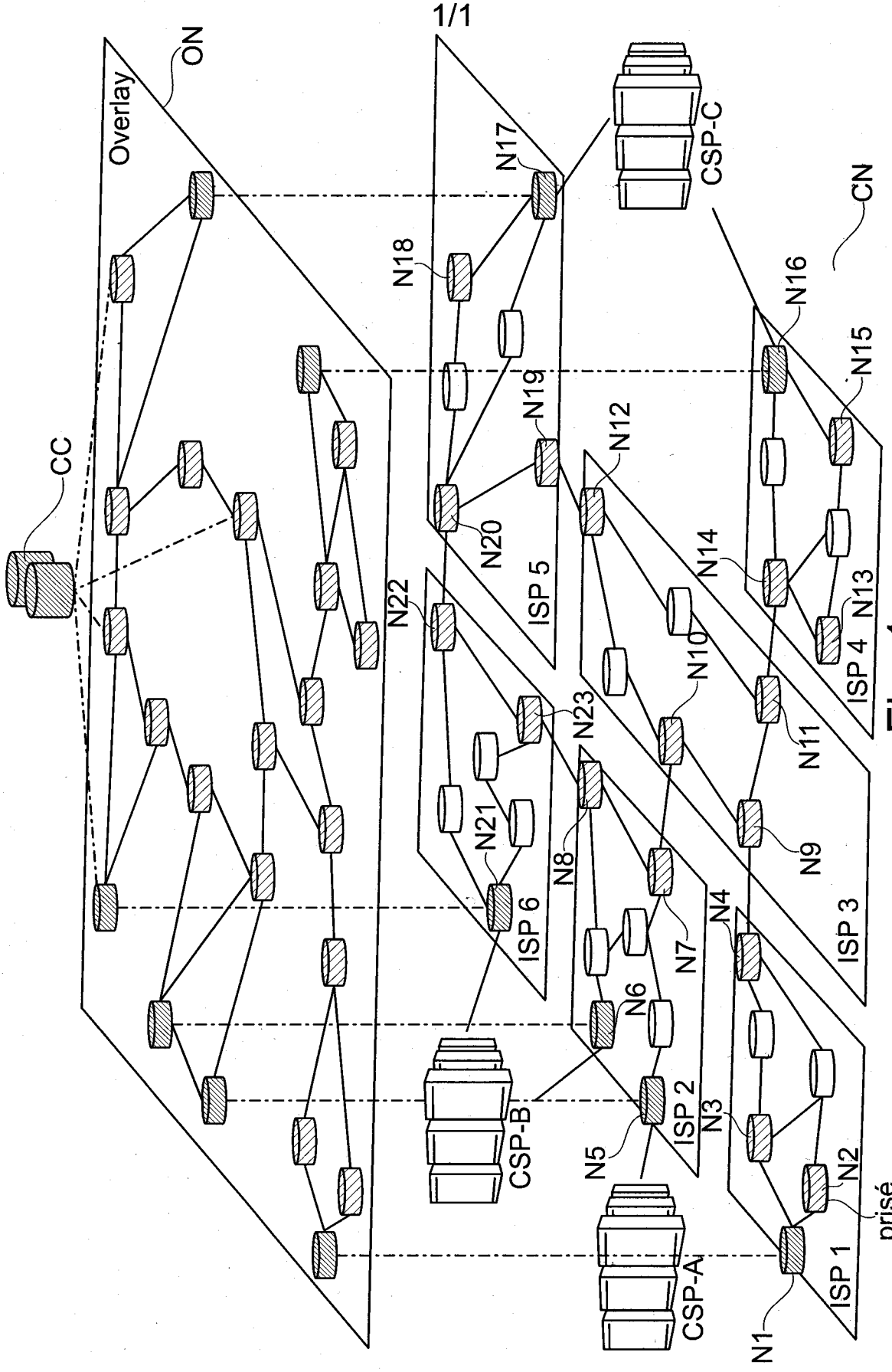

Overlay
ON
CC
CSP-C
CSP-B
CSP-A
CN
ISP 1
ISP 2
ISP 3
ISP 4
ISP 5
ISP 6
prisé
N1
N2
N3
N4
N5
N6
N7
N8
N9
N10
N11
N12
N13
N14
N15
N16
N17
N18
N19
N20
N21
N22
N23

Fig. 1

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 803801
FR 1462364

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	RENUGA KANAGAVELU ET AL: "OpenFlow based control for re-routing with differentiated flows in Data Center Networks", NETWORKS (ICON), 2012 18TH IEEE INTERNATIONAL CONFERENCE ON, IEEE, 12 décembre 2012 (2012-12-12), pages 228-233, XP032376784, DOI: 10.1109/ICON.2012.6506562 ISBN: 978-1-4673-4521-7 * le document en entier *	1-10	H04L12/24 H04L12/701
X	CN 103 514 245 A (JUNIPER NETWORKS INC) 15 janvier 2014 (2014-01-15) * le document en entier *	1-10	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)

H04L
G06F

Date d'achèvement de la recherche	Examinateur
21 octobre 2015	Aura Marcos, F

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1462364 FA 803801

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 21-10-2015
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
CN 103514245 A	15-01-2014	AUCUN	

EPO FORM P0465