(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
02 janvier 2025 (02.01.2025)

WIPO | PCT

(10) Numéro de publication internationale
WO 2025/003097 A1

(51) Classification internationale des brevets :
H04L 45/302 (2022.01)

(21) Numéro de la demande internationale :
PCT/EP2024/067744

(22) Date de dépôt international :
25 juin 2024 (25.06.2024)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR2306885 29 juin 2023 (29.06.2023) FR

(71) Déposant : **ORANGE** [FR/FR] ; 111, quai du Président Roosevelt, 92130 Issy-les-Moulineaux (FR).

(72) Inventeurs : **BOUCADAIR, Mohamed Boucadair** ; ORANGE - Intellectual Property and Licensing, Orange Gardens - 44 Avenue de la République, CS 50010, 92326 Chatillon (FR). **JACQUENET, Christian** ; ORANGE - Intellectual Property and Licensing, Orange Gardens - 44 Avenue de la République, CS 50010, 92326 Chatillon (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH,

(54) Title: METHODS FOR ACCESSING A SERVICE, METHOD FOR PROVIDING SERVICES, CONTROL METHOD, MANAGEMENT METHOD, AND CORRESPONDING TERMINAL, SERVICE FUNCTION INSTANCE, CONTROLLER, BORDER NODE AND COMPUTER PROGRAMS

(54) Titre : PROCÉDÉS D'ACCÈS À UN SERVICE, PROCÉDÉ DE FOURNITURE DE SERVICES, PROCÉDÉ DE CONTRÔLE, PROCÉDÉ DE GESTION, TERMINAL, INSTANCE DE SERVICE, CONTRÔLEUR, NŒUD DE BORDURE ET PROGRAMMES D'ORDINATEUR CORRESPONDANTS

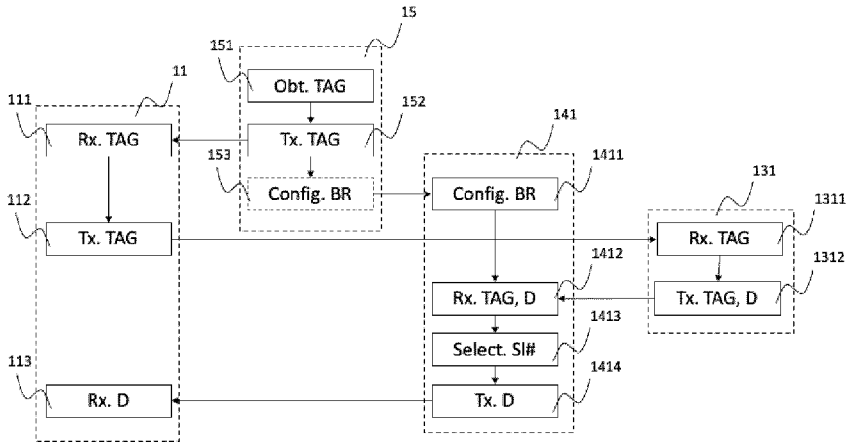


Fig. 2

(57) Abstract: The invention relates to a method for accessing at least one service by a terminal (11) via a communication network using network slices, the method involving: • obtaining (111) at least one identifier for classifying the traffic to said terminal, said at least one identifier being associated with at least one network slice or one type of network slice, • transmitting (112) the at least one identifier to at least one first service function instance (131) that is able to provide said at least one service to the terminal, • receiving (113) a message comprising data associated with the at least one service routed via at least one network slice that is associated with the at least one identifier and is selected by a border node (141) in the communication network by applying at least one traffic classification rule known to said border node.

(57) Abrégé : L'invention concerne un procédé d'accès à au moins un service par un terminal (11), via un réseau de communication mettant en œuvre des tranches réseau, comprenant : • l'obtention (111) d'au moins un identifiant destiné à la classification du trafic à destination dudit terminal, ledit au moins un identifiant étant associé à au moins une tranche réseau ou un type de tranche réseau, • la transmission (112) dudit au moins un identifiant à au moins une première instance de service (131) apte à fournir ledit au moins

[Suite sur la page suivante]

WO 2025/003097 A1

TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

— *avec rapport de recherche internationale (Art. 21(3))*

un service audit terminal, • la réception (113) d'un message comportant des données associées audit au moins un service acheminées via au moins une tranche réseau associée audit au moins un identifiant, sélectionnée par un nœud de bordure (141) dudit réseau de communication en appliquant au moins une règle de classification de trafic connue dudit nœud de bordure.

Description

Titre de l'invention : Procédés d'accès à un service, procédé de fourniture de services, procédé de contrôle, procédé de gestion, terminal, instance de service, contrôleur, nœud de bordure et programmes d'ordinateur correspondants.

1. Domaine technique

[0001] Le domaine de l'invention est celui des communications au sein d'au moins un réseau de communication, et notamment celui des services IP à valeur ajoutée.

[0002] Plus précisément, l'invention concerne l'accès à au moins un service en utilisant les ressources de tranches réseau (« network slice » ou « slice » en anglais) d'un réseau de communication.

[0003] En particulier, l'invention propose une solution pour la sélection d'une ou plusieurs tranches réseau à utiliser pour tout ou partie du trafic à destination d'un terminal.

2. Art antérieur

[0004] Une tranche réseau peut être définie comme une partition du réseau telle qu'un réseau privé virtuel (RPV, ou VPN pour « Virtual Private Network » en anglais) déployé sur une infrastructure fixe, mobile, ou une combinaison des deux.

[0005] Les caractéristiques d'une tranche réseau sont principalement exprimées en termes de capacité (bande passante) et de qualité de service (par exemple latence, temps de transit unidirectionnel, etc.), voire de sécurité (par exemple préservation de la confidentialité des informations transmises au sein du RPV moyennant l'utilisation de techniques de chiffrement) et de fonctions service (« Service Functions » ou SF).

[0006] Les caractéristiques d'une tranche réseau sont par exemple présentées dans le document « A Framework for IETF Network Slices » de A. Farrel et al., version 21 publiée le 15 juin 2023.

[0007] Un exemple d'utilisation de tranches réseau déployées dans une infrastructure mobile 5G est présenté dans le document « A Realization of IETF Network Slices for 5G Networks Using Current IP/MPLS Technologies » de K. G. Szarkowicz et al., version 9 publiée le 23 mai 2023.

[0008] Classiquement, le trafic susceptible d'être acheminé au sein d'une tranche réseau fait l'objet d'une habilitation (aussi appelée contrôle d'accès) à emprunter les chemins établis au sein de ladite tranche réseau. Une telle habilitation repose typiquement sur l'application de règles de classification de trafic. Ces règles sont en général appliquées par un point d'accès au réseau au sein duquel des tranches réseau ont été déployées. Ce point d'accès est un nœud situé en périphérie du réseau et qui est généralement déployé en frontal des accès clients ou bien utilisé pour connecter un réseau à d'autres réseaux

voisins. Par exemple, un tel point d'accès peut être situé à l'interface de raccordement d'une passerelle qui permet d'accéder au réseau Internet. Cette passerelle est désignée « packet gateway » pour les générations (4G, 5G) les plus récentes des réseaux mobiles. Dans ce cas, la fonction de classification de trafic pourrait être localisée à l'interface de raccordement d'une « packet gateway » au réseau Internet. Le point d'accès peut également se situer à l'interface de raccordement d'un terminal mobile (ou « User Equipment » ou UE en anglais) au réseau d'accès radio (ou « Radio Access Network » ou RAN en anglais), de façon notamment à optimiser l'usage des ressources radio en fonction du type de la tranche réseau et du profil du trafic qu'elle est susceptible d'acheminer. Un profil de trafic est l'ensemble des caractéristiques propres au trafic. Ces caractéristiques peuvent refléter la sensibilité des applications à la latence, au délai de transit ou à la perte de paquets, mais également des pratiques d'usage, par exemple un trafic qui ne serait généré que sur une période donnée (par exemple un trafic de gestion lié à l'exécution d'une opération de maintenance d'un équipement programmée pendant la nuit). Les règles de classification et de contrôle d'admission de trafic sont donc appliquées à la périphérie du réseau.

[0009] On rappelle par ailleurs que l'organisme 3GPP a défini différents types de tranches réseau, selon leurs caractéristiques :

- un premier type de tranches réseau permettant d'offrir un service mobile large bande amélioré (« Enhanced Mobile BroadBand » ou EMBB en anglais) ;
- un deuxième type de tranches réseau permettant d'offrir un service dans le cadre d'un déploiement (massif) de l'Internet des Objets (« massive Internet of Things » ou mIoT en anglais) ; et
- un troisième type de tranches réseau permettant d'offrir un service de communication ultra fiable et à faible latence (« Ultra Reliable Low Latency Communications ou URLLC en anglais).

[0010] Le choix de concevoir et de déployer l'un ou l'autre de ces types de tranche réseau est conditionné par la nature du trafic caractéristique des applications ou services utilisés ou souscrits par un utilisateur. Par exemple, un service dit « immersif » qui exploite des techniques de réalité augmentée ou virtuelle est généralement très exigeant en termes de latence et de fiabilité des échanges de données : l'utilisation de tranches de type URLLC est donc privilégiée pour un service immersif de ce type.

[0011] On note par ailleurs que les règles de classification de trafic peuvent être complexes, car le niveau de granularité associé à l'ingénierie et au déploiement d'une tranche réseau peut être macroscopique (par exemple une tranche réseau déployée pour acheminer le trafic à destination de l'Internet), ou bien microscopique (par exemple une tranche réseau déployée pour le trafic applicatif échangé entre deux terminaux mobiles).

[0012] Cette granularité génère une complexité globale de l'ingénierie des tranches réseau, par exemple une difficulté à optimiser l'usage des ressources mises en œuvre par une tranche réseau, par un ensemble de tranches réseau, ou par toutes les tranches réseau, ou une difficulté à garantir strictement l'isolation du trafic acheminé au sein d'une tranche réseau, ou encore une difficulté à garantir strictement le niveau de qualité ou de sécurité associé à une tranche réseau, voire le niveau de disponibilité et de résilience d'une tranche réseau donnée, etc.

[0013] En particulier, la complexité de la configuration et de l'application de règles de classification de trafic associées à la mise en place d'une tranche réseau donnée évolue avec la diversité des trafics, la richesse de l'organisation de la structure qui exploite la tranche réseau (par exemple un service de comptabilité, un service de R&D, un service de production) ou encore le mode d'usage de la tranche réseau (par exemple, gestion des surcharges de trafic lors des heures chargées, principes de répartition de la charge de trafic). Cette complexité peut notamment être aggravée par l'évolution des règles de classification de trafic au cours du temps (par exemple, dans le contexte du déploiement d'une tranche réseau pour la retransmission d'un événement sportif ou culturel, les règles de classification de trafic peuvent évoluer avec le nombre et le profil des utilisateurs de la tranche réseau).

[0014] Il existe donc un besoin pour une nouvelle technique d'accès à un service cherchant à améliorer l'utilisation des ressources de tranches réseau, notamment pour l'acheminement du trafic retour vers le terminal.

3. Exposé de l'invention

[0015] L'invention propose une solution ne présentant pas l'ensemble des inconvénients de l'art antérieur sous la forme d'un procédé d'accès à au moins un service par un terminal, via un réseau de communication mettant en œuvre des tranches réseau, comprenant :

- l'obtention d'au moins un premier identifiant destiné à la classification du trafic à destination dudit terminal, ledit au moins un premier identifiant étant associé à au moins une tranche réseau ou un type de tranche réseau,
- la transmission dudit au moins un premier identifiant à au moins une première instance de service apte à fournir ledit au moins un service audit terminal,
- la réception d'un message comportant des données associées audit au moins un service acheminées via au moins une tranche réseau associée audit au moins un premier identifiant, sélectionnée par un nœud de bordure dudit réseau de communication en appliquant au moins une règle de classification de trafic connue dudit nœud de bordure.

[0016] Un tel procédé peut notamment être mis en œuvre par un terminal connecté au réseau de communication.

[0017] Un tel terminal obtient au cours d'une première étape au moins un premier identifiant destiné à la classification du trafic à destination du terminal. Un tel premier identifiant, également appelé tag par la suite, est par exemple noté « inbound_flow_map » dans un mode de réalisation de l'invention. Il peut être associé à une tranche réseau ou à un type de tranche réseau (par exemple EMBB, mIoT ou URLLC si l'on considère un réseau 5G). Un tel premier identifiant du trafic à destination du terminal est différent d'un identifiant de tranche réseau utilisé par un équipement pour se connecter à une tranche réseau : cet autre identifiant de tranche réseau est par exemple de type NSSAI 3GPP. Un tel premier identifiant du trafic à destination du terminal est par exemple généré par un gestionnaire du réseau, mettant par exemple en œuvre une fonction de gestion de session (« Session Manager Function » ou SMF en anglais) ou un contrôleur réseau.

[0018] Le premier identifiant destiné à la classification du trafic à destination du terminal peut notamment être reçu directement du gestionnaire SMF ou d'un contrôleur réseau, ou via à routeur intermédiaire, par exemple un CPE (« Customer Premises Equipment ») ou un autre équipement de raccordement au réseau. Notamment, un tel premier identifiant peut être inséré dans un en-tête dédié (par exemple un en-tête HTTP, une trame QUIC) ou décrit dans des messages formatés selon des protocoles comme SIP (« Session Initiation Protocol »), SDP (« Session Description Protocol ») ou WebRTC.

[0019] Au cours d'une deuxième étape, le terminal transmet ledit au moins un premier identifiant à au moins une première instance de service (« Service Function Instance », en anglais, par exemple un serveur d'application), par exemple en utilisant une tranche réseau configurée à cet effet, ou un chemin par défaut. En particulier, un tel premier identifiant peut faire l'objet d'un paramètre appelé par la suite SOLACE, pour « Slicing Optimisé A LA CartE ». Le terminal fournit ainsi à au moins une première instance de service un ou plusieurs premiers identifiants à utiliser pour faciliter l'identification de la tranche réseau que les données associées audit au moins un service à destination du terminal sont habilitées à emprunter. On note qu'une instance de service peut être embarquée dans un terminal distant.

[0020] Au cours d'une troisième étape, le terminal peut ainsi recevoir un message comportant les données associées audit au moins un service. De telles données sont acheminées via au moins une tranche réseau sélectionnée par un nœud de bordure du réseau de communication en appliquant au moins une règle de classification de trafic connue du nœud de bordure (par exemple préalablement configurée dans le nœud de bordure suite à la réception de ladite au moins une règle en provenance d'un contrôleur).

[0021] De cette façon, le terminal communique à une instance de service une clé prenant la forme d'un premier identifiant destiné à la classification du trafic. Par exemple,

l'instance de service peut insérer cette clé dans le trafic retour à destination du terminal, directement ou sous une forme modifiée. Cette clé peut être extraite du trafic retour par un nœud de bordure du réseau de communication par lequel transite le trafic retour, lorsqu'elle est directement insérée dans le trafic retour à destination du terminal ou lorsqu'un protocole de signalisation est utilisé entre une instance de service et le réseau de communication via un nœud de bordure typiquement, ou bien être déduite ou reconstruite par le nœud de bordure, lorsqu'elle est insérée sous une forme modifiée dans le trafic retour à destination du terminal (par exemple sous la forme d'un condensé). Le nœud de bordure peut ainsi identifier au moins une tranche réseau ou un type de tranche réseau associée à cette clé, sans avoir à inspecter les données (par exemple le contenu du service considéré, qui peut être chiffré) et sélectionner la tranche réseau ou un type de tranche réseau à utiliser pour acheminer les données vers le terminal. Par exemple, le nœud de bordure est un nœud qui annonce les préfixes IP alloués aux différents équipements du réseau de communication. On utilise ici et dans toute la suite du document le terme « nœud de bordure » pour désigner un nœud en bordure du réseau, par exemple de type « Autonomous System Border Router », ou ASBR, ou un nœud en périphérie du réseau, par exemple de type « Provider Edge (router) », ou PE, dans un réseau IP/MPLS.

[0022] Le réseau de communication (ou plus précisément le nœud de bordure du réseau) sait ainsi quelle(s) tranche(s) réseau il peut utiliser pour acheminer le trafic vers le terminal.

[0023] On note que les règles de classification de trafic peuvent être décrites dans une table de classification de trafic, ou algorithmiquement par exemple. Aucune hypothèse n'est faite quant à la manière dont les règles de classification de trafic sont décrites.

[0024] Dans un mode de réalisation particulier, ladite au moins une tranche réseau ou ledit type de tranche réseau est associé à un mode de transmission appartenant au groupe comprenant :

- l'acheminement de données à destination du terminal,
- l'acheminement de données en provenance du terminal,
- l'acheminement de données à destination du terminal et en provenance du terminal.

[0025] Par exemple, cette classification des tranches réseau ou des types de tranches réseau associés au trafic aller et/ou retour peut reposer sur une logique du service (qui peut être intégrée dans l'applicatif embarqué dans le terminal) et/ou décidée par le réseau (par exemple par un équipement du réseau). La classification peut également faire l'objet d'une décision prise par le terminal (par exemple, selon les choix et instructions de l'utilisateur du terminal).

[0026] Le mode de transmission peut être négocié lors de la phase d'établissement d'une

connexion à une tranche réseau entre le terminal et le réseau de communication.

[0027] Dans un mode de réalisation particulier, le procédé met en œuvre la transmission, par le terminal, d'un premier indicateur signalant que le terminal est apte à mettre en œuvre une procédure collaborative pour l'acheminement des données associées audit au moins un service et à destination dudit terminal reposant sur le traitement dudit au moins un premier identifiant. Cette procédure collaborative est appelée SOLACE.

[0028] Par exemple, un tel premier indicateur est noté « Collaborative-Solace-Capable » par la suite. La valorisation de ce paramètre à « 1 » indique par exemple que le terminal supporte le procédé décrit ci-dessus.

[0029] En particulier, un tel premier indicateur peut être fourni globalement (par exemple lorsque le terminal se connecte au réseau) ou lors de l'activation d'une tranche réseau.

[0030] Dans un mode de réalisation particulier, le terminal met en œuvre la réception d'un deuxième indicateur signalant que le fournisseur des tranches réseau est apte à mettre en œuvre une procédure collaborative SOLACE pour l'acheminement des données associées audit au moins un service et à destination dudit terminal reposant sur le traitement dudit au moins un premier identifiant (SOLACE).

[0031] Par exemple, un tel deuxième indicateur est également noté « Collaborative-Solace-Capable » par la suite. La valorisation de ce paramètre à « 1 » indique par exemple que ledit réseau supporte le procédé décrit ci-dessus.

[0032] Selon une caractéristique particulière, ladite obtention comprend l'obtention d'au moins un premier identifiant par réseau auquel ledit terminal est connecté.

[0033] Par exemple, si le terminal est connecté à une instance de service via différents réseaux (par exemple en 5G et en Wi-Fi®), un premier identifiant différent par réseau peut être obtenu (par exemple un premier tag TAG1 pour le traitement des données envoyées vers le terminal par l'instance de service via le réseau 5G, et un deuxième tag TAG2 pour le traitement de données envoyées vers le terminal par l'instance de service via le réseau Wi-Fi®).

[0034] Dans un mode de réalisation particulier, ledit procédé comprend la transmission, à la première instance de service, d'au moins une règle de classification de trafic.

[0035] Par exemple, dans un contexte de « multihoming » selon lequel le terminal est connecté à plusieurs réseaux, le terminal indique explicitement l'adresse destination correspondant à chaque réseau auquel il est connecté. En d'autres termes, le terminal peut transmettre plusieurs premiers identifiants correspondant chacun à au moins une adresse du terminal dans le réseau concerné. L'application des règles de classification de trafic permet que les données associées au service auquel le terminal souhaite accéder soient correctement acheminées via le réseau dans lequel le terminal est identifié par l'adresse destination correspondante. L'utilisation d'un identifiant différent de celui associé à un réseau donné implique une mauvaise application de la

règle de classification des données envoyées par une instance de service. Les données envoyées par l'instance de service risquent alors d'être rejetées au lieu d'être acheminées vers le terminal.

[0036] Dans un autre exemple, les règles de classification peuvent également tenir compte d'un numéro de port destination.

[0037] Dans un mode de réalisation particulier, le procédé met en œuvre une sélection préalable de ladite moins une première instance de service habilitée à recevoir ledit au moins un premier identifiant.

[0038] Le terminal peut ainsi mettre en place une procédure de sélection pour choisir le service ou l'instance de service habilitée à recevoir le premier identifiant destiné à la classification du trafic à destination du terminal.

[0039] Dans un autre mode de réalisation, l'invention concerne un terminal adapté à mettre en œuvre le procédé d'accès à au moins un service décrit précédemment. Un tel terminal peut bien sûr présenter les différentes caractéristiques relatives au procédé d'accès à au moins un service selon l'invention, qui peuvent être combinées ou considérées isolément. Ainsi, les caractéristiques et avantages de ce terminal sont les mêmes que ceux du procédé et ne sont pas détaillés plus amplement.

[0040] L'invention concerne par ailleurs un procédé de contrôle de la fourniture d'au moins un service à un terminal, via un réseau de communication mettant en œuvre des tranches réseau, comprenant :

- l'obtention d'au moins un premier identifiant destiné à la classification du trafic à destination dudit terminal, ledit au moins un premier identifiant étant associé à au moins une tranche réseau ou un type de tranche réseau,
- la transmission dudit au moins un premier identifiant audit terminal, directement ou via au moins un routeur intermédiaire,
- la transmission, à au moins un nœud de bordure dudit réseau de communication, d'au moins une règle de classification de trafic pour la sélection d'au moins une tranche réseau destinée à acheminer vers ledit terminal des données associées audit au moins un service.

[0041] Un tel procédé peut notamment être mis en œuvre par un contrôleur réseau, par exemple un contrôleur SDN (« Software-Defined Networking »).

[0042] Au cours d'une première étape, un tel contrôleur obtient au moins un premier identifiant du trafic à destination du terminal. Comme indiqué précédemment, un tel premier identifiant peut être généré par une SMF (« Session Manager Function »). Éventuellement, le premier identifiant peut être généré par le contrôleur.

[0043] Au cours d'une deuxième étape, le contrôleur transmet le premier identifiant au terminal, directement ou via au moins un routeur intermédiaire, par exemple un CPE.

[0044] Le contrôleur (premier contrôleur), ou un autre contrôleur (deuxième contrôleur),

peut également transmettre à au moins un nœud de bordure du réseau de communication au moins une règle de classification de trafic, permettant par exemple d'associer ledit au moins un premier identifiant à au moins une tranche réseau. Le deuxième contrôleur peut notamment recevoir ladite au moins une règle de classification de trafic en provenance du premier contrôleur. Par exemple, de telles règles peuvent être configurées dans le nœud de bordure, ou transmises sous la forme d'un algorithme destiné à être mis en œuvre par le nœud de bordure.

[0045] Selon un mode de réalisation particulier, le contrôleur peut également transmettre au(x) nœud(s) de bordure des consignes spécifiant si le ou les identifiants (premier identifiant ou deuxième identifiant) qu'un nœud de bordure reçoit en provenance d'une instance de service doivent être retirés ou maintenus dans le message comportant les données qui seront transmises via la tranche réseau sélectionnée.

[0046] Dans un mode de réalisation particulier, le procédé comprend la transmission dudit au moins un premier identifiant à au moins un autre terminal connecté audit réseau de communication.

[0047] De cette façon, un même premier identifiant peut être négocié avec plusieurs terminaux. Il est ainsi possible de mutualiser les règles de classification de trafic maintenues par les nœuds de bordure.

[0048] Dans un autre mode de réalisation, l'invention concerne un contrôleur adapté à mettre en œuvre le procédé de contrôle de la fourniture d'au moins un service décrit précédemment. Un tel contrôleur peut bien sûr présenter les différentes caractéristiques relatives au procédé de contrôle de la fourniture d'au moins un service selon l'invention, qui peuvent être combinées ou considérées isolément. Ainsi, les caractéristiques et avantages de ce contrôleur sont les mêmes que ceux du procédé et ne sont pas détaillés plus amplement.

[0049] L'invention concerne par ailleurs un procédé de fourniture d'au moins un service à un terminal, via un réseau de communication mettant en œuvre des tranches réseau, comprenant :

- la réception d'au moins un premier identifiant destiné à la classification du trafic à destination dudit terminal, ledit au moins un premier identifiant étant associé à au moins une tranche réseau ou un type de tranche réseau,
- la transmission, via au moins un nœud de bordure dudit réseau de communication, d'un message comportant au moins un deuxième identifiant et des données associées audit au moins un service,

[0050] lesdites données étant destinées à être acheminées via au moins une tranche réseau associée audit au moins un premier identifiant,

[0051] ladite au moins une tranche réseau étant sélectionnée par ledit nœud de bordure en appliquant au moins une règle de classification de trafic connue dudit nœud de

bordure, et

[0052] ledit au moins un deuxième identifiant étant fonction dudit au moins un premier identifiant.

[0053] Un tel procédé peut notamment être mis en œuvre par une instance de service, qui fournit le service auquel souhaite accéder le terminal. Par exemple, une telle instance de service est un serveur applicatif hébergé par le fournisseur de services ou une autre infrastructure.

[0054] Ainsi, au cours d'une première étape, une telle instance de service, dite première instance de service, reçoit au moins un premier identifiant, en provenance du terminal (directement ou via un routeur intermédiaire).

[0055] La première instance de service peut alors renvoyer, à destination du terminal, un message comportant les données associées au service et au moins un deuxième identifiant, fonction dudit premier identifiant.

[0056] En d'autres termes, un deuxième identifiant correspond soit à un premier identifiant reçu du terminal, soit à un nouvel identifiant obtenu à partir d'un premier identifiant reçu du terminal. Par exemple, un deuxième identifiant est obtenu en appliquant une fonction de hachage (« hash » en anglais) à un premier identifiant. D'autres fonctions peuvent être utilisées, tant qu'elles permettent de lier les deux identifiants : le deuxième identifiant doit pouvoir être obtenu à partir du premier identifiant, et le premier identifiant retrouvé à partir du deuxième identifiant.

[0057] Ce message transite via un nœud de bordure qui permet d'accéder au terminal. Le nœud de bordure extrait le ou les deuxièmes identifiants. Si le deuxième identifiant correspond à un premier identifiant, le nœud de bordure identifie la ou les tranches réseau, ou type(s) de tranches réseau, associé(e)s à ce premier identifiant. Si le deuxième identifiant est obtenu en appliquant une fonction distincte d'une fonction identité à un premier identifiant, le nœud de bordure retrouve le premier identifiant, et identifie la ou les tranches réseau associée(s) à ce premier identifiant, et les règles de classification de trafic correspondantes.

[0058] Le nœud de bordure peut alors relayer les données au terminal via la ou les tranches réseau, ou type(s) de tranches réseau ainsi sélectionnée(s) selon l'application de règles de classification de trafic. Éventuellement, le nœud de bordure peut supprimer le ou les deuxièmes identifiants du message avant de transmettre les données au terminal.

[0059] Dans un mode de réalisation particulier, le procédé comprend la réception d'au moins une règle de classification de trafic pour l'acheminement des données associées audit au moins un premier identifiant, et le stockage de ladite au moins une règle de classification de trafic et dudit au moins un premier identifiant associé.

[0060] Une telle étape est notamment mise en œuvre lorsque plusieurs premiers identifiants sont communiqués à l'instance de service, par exemple un premier identifiant A

correspondant à une première adresse du terminal et une premier identifiant B correspondant à une deuxième adresse du même terminal.

[0061] Dans un mode de réalisation particulier, la première instance de service reçoit au moins deux premiers identifiants associés chacun à au moins une tranche réseau et applique au moins une règle de classification de trafic pour sélectionner l'un des premiers identifiants.

[0062] Par exemple, si le service est de type immersif, l'instance de service peut sélectionner un premier identifiant associé à une tranche réseau de type URLLC, plutôt qu'un premier identifiant associé à une tranche réseau EMBB.

[0063] Dans un mode de réalisation particulier, la première instance de service met en œuvre la transmission du message comportant ledit au moins un deuxième identifiant et des données associées audit au moins un service à au moins une deuxième instance de service apte à fournir ledit au moins un service.

[0064] Un même service peut ainsi impliquer une pluralité d'instances de service, sans pour autant nécessiter la transmission, par le terminal, du ou des premiers identifiants du trafic à destination des instances de service. On évite de cette façon de consommer inutilement des ressources du réseau de communication.

[0065] Les règles de classification de trafic issues de la complétude de la procédure SOLACE peuvent ainsi être synchronisées entre plusieurs instances de service.

[0066] Dans un autre mode de réalisation, l'invention concerne une instance de service capable de mettre en œuvre le procédé de fourniture d'au moins un service décrit précédemment. Une telle instance de service peut bien sûr présenter les différentes caractéristiques relatives au procédé de fourniture d'au moins un service selon l'invention, qui peuvent être combinées ou considérées isolément. Ainsi, les caractéristiques et avantages de cette instance de service sont les mêmes que ceux du procédé et ne sont pas détaillés plus amplement.

[0067] L'invention concerne encore un procédé de gestion de l'accès à au moins un service par un terminal, via un réseau de communication, comprenant :

- la réception d'au moins un message en provenance d'au moins une première instance de service apte à fournir ledit au moins un service, ledit message comportant au moins un deuxième identifiant, fonction d'au moins un premier identifiant destiné à la classification du trafic à destination dudit terminal et des données associées audit au moins un service,

[0068] ledit au moins un premier identifiant étant associé à au moins une tranche réseau ou un type de tranche réseau,

- la sélection d'au moins une tranche réseau associée audit au moins un premier identifiant en appliquant au moins une règle de classification de trafic connue (reçue d'un contrôleur),

– la transmission desdites données associées audit au moins un service sur ladite au moins une tranche réseau sélectionnée.

[0069] Un tel procédé peut notamment être mis en œuvre dans un nœud de bordure du réseau de communication.

[0070] Comme indiqué précédemment, un tel nœud de bordure peut ainsi recevoir au moins un deuxième identifiant et des données associées au service auquel le terminal souhaite accéder. Le nœud de bordure peut notamment extraire le ou les deuxièmes identifiants, correspondant soit au(x) premier(s) identifiant(s), soit à une fonction du ou des premiers identifiants. Dans ce dernier cas, le nœud de bordure peut mettre en œuvre une fonction inverse pour retrouver le ou les premiers identifiants. Le nœud de bordure peut ensuite appliquer une règle de classification de trafic pour vérifier si une tranche réseau, ou un type de tranche réseau, est associé(e) à ce ou ces premiers identifiants. Si oui, les données peuvent être transmises au terminal via la tranche réseau ou le type de tranche réseau ainsi identifié(e). Sinon, les données ne sont pas transmises au terminal ou alors elles sont transmises via un chemin par défaut, ou une route déterminée selon un schéma de routage IP classique par exemple, qui ne repose pas nécessairement sur l'utilisation de tranches réseau.

[0071] Ainsi, le message reçu de l'instance de service peut comporter le ou les premiers identifiants, encodés dans un seul champ ou dans plusieurs champs, explicitement ou implicitement. Dans le mode explicite, le message transporte directement le ou les premiers identifiants. Dans le mode implicite, le message transporte des informations (deuxièmes identifiants) permettant de retrouver le ou les premiers identifiants.

[0072] Éventuellement, le nœud de bordure peut supprimer le ou les deuxièmes identifiants du message avant de transmettre les données au terminal.

[0073] Dans un autre mode de réalisation, l'invention concerne un nœud de bordure adapté à mettre en œuvre le procédé de gestion de l'accès à au moins un service décrit précédemment. Un tel nœud de bordure peut bien sûr présenter les différentes caractéristiques relatives au procédé de gestion de l'accès à au moins un service selon l'invention, qui peuvent être combinées ou considérées isolément. Ainsi, les caractéristiques et avantages de ce nœud de bordure sont les mêmes que ceux du procédé et ne sont pas détaillés plus amplement.

[0074] Dans les différents modes de réalisation envisagés, ledit au moins un premier identifiant est associé à une durée de validité. Par exemple, un tel premier identifiant peut évoluer au cours du temps. De même, ledit au moins un deuxième identifiant peut être associée à une durée de validité, identique ou différente de celle associée au premier identifiant à partir duquel le deuxième identifiant est construit.

[0075] En particulier, ledit au moins un premier identifiant peut être associé à une clé de sécurité, par exemple un jeton (« token ») ou un nombre aléatoire (« nonce »).

[0076] Par exemple, un nombre aléatoire ou pseudo-aléatoire, unique pour un terminal, est également communiqué au terminal avec le ou les premiers identifiants / tags. Une telle clé de sécurité peut être utilisée à des fins d'autorisation. On améliore ainsi la robustesse du procédé et évite qu'un terminal utilise un identifiant communiqué à un autre terminal.

[0077] Dans les différents modes de réalisation envisagés, au moins une desdites tranches réseau peut être composée d'au moins une tranche réseau locale déployée dans au moins un sous-réseau du réseau de communication (par exemple dans un réseau d'accès, un réseau de collecte, un réseau cœur, un réseau de transit).

[0078] L'invention concerne en outre au moins un programme d'ordinateur comportant des instructions pour la mise en œuvre d'au moins un des procédés décrits ci-dessus, lorsque ce ou ces programmes sont exécutés par un processeur, ainsi qu'au moins un support d'informations lisible par un ordinateur comportant des instructions d'au moins un programme d'ordinateur tel que mentionné ci-dessus.

[0079] Le procédé selon l'invention peut être mis en œuvre de diverses manières, notamment sous forme câblée ou sous forme logicielle.

4. Liste des figures

[0080] D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation particulier, donné à titre d'exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la [Fig.1] représente un système dans lequel l'invention peut être mise en œuvre ;
- la [Fig.2] illustre les principales étapes des procédés selon au moins un mode de réalisation de l'invention ;
- la [Fig.3] illustre les principaux messages échangés lors de la mise en œuvre des procédés selon la [Fig.2] ;
- la [Fig.4] illustre un exemple de réseau de communication composé de plusieurs sous-réseaux ;
- la [Fig.5] illustre un exemple d'agrégation de plusieurs services au sein d'une même tranche réseau ;
- la [Fig.6] illustre un exemple de déploiement de plusieurs instances de service ;
- la [Fig.7] présente les différentes entités intervenant dans le déroulement du mode collaboratif de la procédure SOLACE ;
- la [Fig.8] illustre un exemple d'association de trafic à des tranches réseau et arrivant à un nœud de bordure et à destination du terminal ;
- la [Fig.9] illustre un exemple de problème empêchant l'association de trafic à des tranches réseau et arrivant à un nœud de bordure ;

- la [Fig.10] illustre un exemple d'activation de la procédure SOLACE en présence d'un CPE ;
- la [Fig.11] présente un exemple d'option PCP (« Port Control Protocol ») mis en œuvre par un terminal pour obtenir au moins un premier identifiant destiné à la classification du trafic à destination du terminal et habilité à être acheminé via une tranche donnée ;
- la [Fig.12] présente la structure simplifiée des différentes entités selon un mode de réalisation particulier.

[0081] **5. Description d'un mode de réalisation de l'invention**

5.1 Principe général

[0082] Le principe général de l'invention repose sur l'utilisation d'un ou plusieurs premiers identifiants (tags, en anglais) destinés à la classification du trafic à destination d'un terminal, pour identifier la tranche réseau qu'un trafic à destination d'un terminal est habilité à emprunter. Ce principe s'inscrit dans un contexte où un terminal souhaite accéder à au moins un service via un réseau de communication mettant en œuvre des tranches réseau. De cette façon, un nœud de bordure du réseau de communication peut identifier la ou les tranches réseau via lesquelles le trafic retour (i.e. à destination du terminal) doit être acheminé, sans avoir à inspecter les données associées au service considéré.

[0083] Ainsi, la solution proposée offre, selon au moins un mode de réalisation, un mécanisme de découverte automatique et sécurisée de tranches réseau déployées (ou instanciées) sur une infrastructure fixe et/ou mobile et réservées à un certain usage, par exemple la retransmission d'un évènement sportif ou musical.

[0084] En particulier, la plupart des solutions existantes suppose que le trafic aller entre le terminal et le fournisseur de service, et le trafic retour entre le fournisseur de service et le terminal sont acheminés via une même tranche réseau. Selon l'art antérieur, le terminal ne contrôle pas l'accès à la ou aux tranches réseau utilisée(s) pour acheminer les données associées au service considéré et ne permet pas de bénéficier ainsi des ressources de la tranche réseau qui optimise la qualité du service considéré, telle qu'elle peut être perçue par l'utilisateur du terminal, notamment. Le terminal ne dispose donc pas de moyens de vérifier que la tranche réseau à laquelle l'instance de service se raccorde est celle qui met en place une politique d'acheminement de trafic optimisée pour le service considéré et tel que souscrit par le client.

[0085] L'invention, selon au moins un mode de réalisation, propose une solution à ce problème.

[0086] La [Fig.1] illustre un exemple de système dans lequel l'invention peut être mise en œuvre. Un tel système comprend un terminal UE 11 (« User Equipment » en anglais) souhaitant accéder à au moins un service via un réseau de communication SSP 12 («

Slice Service Provider » en anglais, ou fournisseur de services reposant sur des tranches réseau) mettant en œuvre des tranches réseau, par exemple deux tranches réseau Sl. #1 161 et Sl. #2 162 (« Slice » en anglais).

[0087] Le terminal 11 peut éventuellement être connecté au réseau 12 via un routeur intermédiaire, par exemple un CPE.

[0088] Le service peut être fourni par au moins une instance de service, par exemple par deux instances de services SFI #1 131 et SFI #2 132. Une instance de service peut être connectée au réseau 12 par l'intermédiaire d'un nœud de bordure du réseau. Par exemple, la première instance 131 est connectée au réseau 12 par l'intermédiaire du premier nœud de bordure BR 141 (« Border Router » en anglais), et la deuxième instance 132 est connectée au réseau 12 par l'intermédiaire du deuxième nœud de bordure BR 142. Les instances de service ne sont pas nécessairement directement connectées aux nœuds de bordure.

[0089] Au moins un contrôleur réseau 15 peut être utilisé pour transmettre à au moins un nœud de bordure du réseau 12 (par exemple dans les nœuds de bordure 141 et 142) des règles de classification de trafic (par exemple sous forme algorithmique, ou sous la forme d'au moins une table de classification de trafic, ou sous toute autre forme). Le contrôleur 15 peut également transmettre au terminal 11 le ou les premiers identifiants (également appelés « tags ») du trafic à destination du terminal. Le contrôleur 15, ou le nœud de bordure, peut maintenir au moins une règle de classification du trafic, permettant d'associer un premier identifiant du trafic à au moins une tranche réseau. On note que la configuration des nœuds de bordure et des terminaux peut être effectuée par des entités réseau distinctes.

[0090] On présente désormais, en relation avec la [Fig.2], les principales étapes mises en œuvre par les différents procédés selon un mode de réalisation de l'invention.

[0091] On considère que le contrôleur 15 obtient au cours d'une étape 151 au moins un premier identifiant TAG destiné à la classification du trafic à destination du terminal 11. Un tel premier identifiant est associé à au moins une tranche réseau ou un type de tranche réseau. Par exemple, le contrôleur maintient une règle de classification de trafic selon laquelle le premier identifiant TAG #1 est associé à la tranche réseau Sl #1.

[0092] Au cours d'une étape 152, ledit au moins un premier identifiant TAG est transmis au terminal 11, directement ou via au moins un routeur intermédiaire.

[0093] Au cours d'une étape 153, le contrôleur 15 transmet, à au moins un nœud de bordure du réseau de communication, par exemple le nœud BR1 141, au moins une règle de classification de trafic pour la sélection d'au moins une tranche réseau destinée à acheminer vers le terminal des données associées audit au moins un service. Par exemple, de telles règles peuvent être configurées dans le nœud de bordure, ou mises en œuvre par l'exécution d'un algorithme connu du nœud de bordure (reçu d'un

contrôleur).

[0094] On note que l'étape 153 peut être mise en œuvre avant les étapes 151 et/ou 152.En d'autres termes, la transmission des règles de classification de trafic au nœud de bordure peut être mise en œuvre avant ou après avoir transmis ledit au moins un premier identifiant TAG au terminal 11. Eventuellement, l'étape 153 peut être mise en œuvre par un autre contrôleur.

[0095] Au cours d'une étape 111, le terminal 11 reçoit donc ledit au moins un premier identifiant TAG, en provenance du contrôleur 15, directement ou via au moins un routeur intermédiaire.

[0096] Au cours d'une étape 112, le terminal 11 transmet ledit au moins un premier identifiant TAG à au moins une première instance de service apte à fournir le service considéré, par exemple à la première instance de service SFI #1 131.

[0097] Au cours d'une étape 1311, la première instance de service 131 reçoit donc ledit au moins un premier identifiant TAG.

[0098] Au cours d'une étape 1312, la première instance de service 131 transmet, via au moins un nœud de bordure, par exemple le premier nœud de bordure BR 141, un message MSG1 comportant au moins un deuxième identifiant et des données D associées au service considéré. Ces données D sont destinées au terminal 11. Par exemple, le deuxième identifiant est égal au premier identifiant TAG. Dans une variante, le premier identifiant est utilisé pour calculer un deuxième identifiant qui peut être inclus dans ledit message. Par exemple, le deuxième identifiant est obtenu en appliquant une fonction de hachage « Hash » au premier identifiant.

[0099] Dans l'exemple illustré, on considère que le deuxième identifiant est égal au premier identifiant TAG. Le message MSG1 émis par la première instance de service 131 comporte donc ledit au moins un premier identifiant TAG et les données D.

[0100] Au cours d'une étape 1412, le premier nœud de bordure 141 reçoit donc le message MSG1 en provenance de la première instance de service 131 comportant ledit au moins un premier identifiant TAG et les données D.

[0101] Au cours d'une étape 1413, le premier nœud de bordure 141 vérifie si au moins une tranche réseau est associée audit au moins un premier identifiant TAG en appliquant au moins une règle de classification de trafic connue du premier nœud de bordure 141 (par exemple configurée au cours d'une étape 1411), et sélectionne ladite au moins une tranche réseau correspondante.

[0102] Au cours d'une étape 1414, le premier nœud de bordure 141 transmet les données D associées au service considéré sur ladite au moins une tranche réseau sélectionnée. Le premier nœud de bordure 141 peut retransmettre au terminal 11 le message MSG1 comportant ledit au moins un premier identifiant TAG et les données D tels que reçus de la première instance de service 131, ou supprimer ledit au moins un premier

identifiant TAG pour n'envoyer que les données D au terminal 11 dans un message MSG1'.

[0103] Au cours d'une étape 113, le terminal 11 reçoit donc le message MSG1' comportant les données D acheminées via au moins une tranche réseau associée audit au moins un premier identifiant TAG.

[0104] La [Fig.3] est un diagramme de flux illustrant les messages échangés selon les principales étapes décrites en [Fig.2].

[0105] De manière plus générale, on considère qu'une tranche réseau du réseau de communication peut être associée à d'autres tranches réseau pour fournir des services à valeur ajoutée. Par exemple, un fournisseur de service peut s'appuyer sur des tranches mises en place dans différents sous-réseaux pour fournir un service dont le trafic est destiné à être acheminé dans la tranche réseau « globale » composée des tranches déployées dans les différents sous-réseaux. On parle alors de « tranche multi-domaines » (ou « stitched slices » ou « hierarchical slices » en anglais). Une telle tranche réseau peut en effet refléter une structure hiérarchique.

[0106] Par exemple, comme illustré par la [Fig.4], le réseau SSP 12 peut être composé de plusieurs sous-réseaux 121, 122 et 123. Chaque sous-réseau peut supporter une ou plusieurs tranches réseau. Par exemple, le premier sous-réseau 121 supporte quatre tranches réseau, le deuxième sous-réseau 122 supporte trois tranches réseau, et le troisième sous-réseau 123 supporte quatre tranches réseau. La première tranche réseau Sl. #1 161 du réseau de communication est par exemple composée des tranches réseau Sl. #3 déployée sur le sous-réseau 121, Sl. #2 déployée sur le sous-réseau 122 et Sl. #2 déployée sur le sous-réseau 123. Les interfaces de raccordement entre tranches adjacentes (« Attachment Circuits » en anglais) sont par exemple gérées en utilisant les mécanismes décrits dans le document « YANG Data Models for 'Attachment Circuits'-as-a-Service (ACaaS) » de M. Boucadair et al., version 6 publiée le 3 mai 2023.

[0107] Par exemple, chaque sous-réseau peut être associé à un domaine distinct (par exemple, un réseau de communication peut être composé d'un réseau d'accès, d'un réseau de collecte, d'un réseau cœur et d'un réseau de transit). Chacun de ces domaines supporte des tranches réseau dont l'ingénierie et l'exploitation sont caractéristiques du domaine (par exemple, une tranche déployée sur un réseau cœur mobile 5G peut faire appel à des fonctions de traitement de trafic et d'exploitation caractéristiques d'un réseau cœur mobile 5G). Ainsi, chaque domaine (accès, collecte, cœur, transit, etc.) peut exploiter différentes technologies déployées dans ce domaine pour la réalisation des tranches réseau.

[0108] Ainsi, la réalisation d'une tranche réseau qui s'étend sur plusieurs domaines n'est pas conditionnée par la disponibilité ou l'activation des mêmes technologies utilisées pour

la réalisation des tranches « locales » à chaque domaine.

[0109] Par exemple, en référence à la [Fig.4], un premier domaine associé au premier sous-réseau 121 met en place des tunnels IPsec qui sont exploités pour acheminer le trafic dans les tranches déployées dans ce domaine, alors qu'un deuxième domaine associé au deuxième sous-réseau 122 utilise une ingénierie de réseau privé virtuel de niveau réseau (Layer 3 VPN ou L3VPN en anglais) combiné avec des mécanismes d'ingénierie de trafic (« Traffic Engineering » ou TE en anglais) pour acheminer le trafic dans les tranches déployées dans ce domaine, tandis qu'un troisième domaine associé au troisième sous-réseau 123 utilise les ressources du routage par segments reposant sur le protocole IPv6 (« Segment Routing IPv6 » ou SRv6 en anglais) pour acheminer le trafic dans les tranches déployées dans ce domaine.

[0110] Selon un autre exemple, une tranche réseau dans un réseau mobile (5G par exemple) peut reposer sur la mise en place de tranches réseau dans les différents sous-réseaux/segments suivants : réseau d'accès radio (« Radio Access Network » ou RAN), réseau cœur (« Core Network » ou CN) et réseau de transport (« Transport Network » ou TN).

[0111] L'association entre une tranche réseau, par exemple une tranche réseau 5G dans le cas d'un réseau mobile de dernière génération, et les tranches réseau déployées dans chacun des segments / sous-réseaux composant le réseau mobile 5G est réalisée dans le plan de contrôle et à la périphérie de chacun des réseaux RAN, CN et TN. La tranche réseau déployée dans le réseau TN est parfois appelée « IETF Network Slice ».

[0112] Selon l'invention, aucune hypothèse n'est faite quant à la nature des tranches réseau, leur nombre, et le « mapping » entre des tranches réseau de domaines voisins (par exemple RAN et TN, TN et CN).

[0113] Par exemple, les mécanismes décrits dans le document « A Realization of IETF Network Slices for 5G Networks Using Current IP/MPLS Technologies » précédemment cité sont mis en œuvre pour la réalisation des tranches réseau dans un réseau IP/MPLS (qui est un exemple de réseau de transport au sens du 3GPP).

[0114] On note par ailleurs qu'une même tranche réseau peut être utilisée pour agréger le trafic d'un ou plusieurs services. Ainsi, comme illustré par la [Fig.5], un premier service S1 servi par une ou plusieurs instances de service 51 peut être fourni à un premier client UE1 via une tranche réseau Sl. #3 du réseau SSP, un deuxième service S2 servi par une ou plusieurs instances de service 52 peut être fourni à un deuxième client UE2 via la même tranche réseau Sl. #3 du réseau SSP, un troisième service S3 servi par une ou plusieurs instances de service 53 peut être fourni au deuxième client UE2 via la même tranche réseau Sl. #3 du réseau SSP.

[0115] De plus, une tranche réseau peut impliquer une ou plusieurs fonctions service (ou « Service Functions » en anglais, selon la terminologie utilisée par le document

RFC7665 – « Service Function Chaining (SFC) Architecture » de J. Halpern et al. publié en octobre 2015, ou « Network Functions » comme gNB (« gNodeB ») ou des fonctions UPF (« User Plane Functions ») selon la terminologie utilisée par le 3GPP). Une même fonction service peut être fournie par une ou plusieurs instances de service.

[0116] La [Fig.6] illustre un exemple de déploiement d'instances de service. En particulier, une instance de service peut être hébergée par le SSP (par exemple les instances de service 63 et 64) ou au sein d'une autre infrastructure (par exemple l'instance de service 65).

[0117] Dans un mode de réalisation particulier, des chaînes de service (« Service Function Chain » ou SFC en anglais) peuvent être mises en place afin de faciliter l'acheminement de trafics de différente nature et présentant des profils différents pour les besoins de la réalisation d'une tranche réseau ou au sein d'une tranche réseau (par exemple les instances de service 611, 612 et 613 de la [Fig.6]).

5.2 Exemples de mise en œuvre

[0118] On présente désormais des exemples de mise en œuvre de l'invention. Par souci de simplification, on considère ci-après que le premier identifiant et le deuxième identifiant sont identiques. On utilise donc simplement le terme « identifiant ».

[0119] En se référant de nouveau à la [Fig.1], on considère que le terminal 11 négocie avec le SSP 12 une liste d'au moins une tranche réseau que le terminal 11 est susceptible d'utiliser pour envoyer ou recevoir du trafic. Le terminal 11 peut indiquer le cas échéant le mode de transmission envisagé pour chacune des tranches réseau de ladite liste :

- l'acheminement de données à destination du terminal 11 (« receive-only »),
- l'acheminement de données en provenance du terminal 11 (« send-only »),
- l'acheminement de données associées à destination du terminal 11 et en provenance du terminal 11 (« send-receive »).

[0120] Selon cet exemple de mise en œuvre de l'invention, le terminal 11 et le SSP 12 échangent des messages pour s'assurer qu'ils supportent bien l'un et l'autre la procédure SOLACE (« Slicing Optimisé A LA CartE ».

[0121] Par exemple, le terminal 11 valorise un premier indicateur ou paramètre noté « Collaborative-Solace-Capable » à une valeur donnée, par exemple « 1 », pour indiquer au SSP 12 qu'il est apte à mettre en œuvre une procédure collaborative pour l'acheminement des données associées à au moins un service auquel le terminal souhaite accéder et à destination du terminal, reposant sur le traitement d'au moins un identifiant (tag) destiné à la classification du trafic à destination du terminal.

[0122] Cette indication de support de la procédure SOLACE peut être fournie globalement ou lors de l'activation de chaque tranche réseau.

[0123] Si le SSP 12 supporte la procédure SOLACE, il retourne un deuxième indicateur ou

paramètre « Collaborative-Solace-Capable » valorisé à une valeur donnée, par exemple « 1 », pour indiquer au terminal 11 qu'il est apte à mettre en œuvre une procédure collaborative pour l'acheminement des données associées à au moins un service auquel le terminal souhaite accéder et à destination du terminal, reposant sur le traitement d'au moins un identifiant (tag).

[0124] Le deuxième indicateur peut être retourné au terminal 11 en réponse à la réception du premier indicateur. En variante, c'est le premier indicateur qui est retourné par le terminal 11 en réponse à la réception du deuxième indicateur.

[0125] Le mode collaboratif de la procédure SOLACE est alors activé par le terminal 11 et le SSP 12.

[0126] A l'inverse, si le deuxième indicateur ou paramètre « Collaborative-Solace-Capable » retourné par le SSP 12 est égal à « 0 », alors le terminal 11 désactive le mode collaboratif de la procédure SOLACE.

[0127] On suppose par la suite que le mode collaboratif de la procédure SOLACE est activé.

[0128] Comme illustré par la [Fig.7], un contrôleur réseau 15 peut transmettre au terminal 11 au moins un identifiant (tag) destiné à la classification du trafic à destination du terminal 11. Un tel tag, noté par exemple « Inbound-Flow-Map », peut être retourné pour chaque tranche réseau négociée avec le terminal 11. Le contrôleur réseau 15 peut notamment maintenir à jour au moins une règle de classification de trafic associant au moins un identifiant du trafic à destination du terminal, ou tag, avec au moins une tranche réseau.

[0129] Ainsi, l'absence du tag et/ou du deuxième indicateur « Collaborative-Solace-Capable » est une indication implicite du non-support du mode collaboratif de la procédure SOLACE par le SSP 12.

[0130] En particulier, le mode collaboratif SOLACE peut être négocié avec chacun des réseaux auxquels le terminal peut se connecter. Dans ce cas, le terminal 11 peut récupérer des tags distincts par réseau auquel le terminal 11 est connecté.

[0131] Dans un mode de réalisation particulier, une durée de validité ou une échéance peut être associée au tag. Dans ce cas, un nouveau tag (« Inbound-Flow-Map ») peut être renégocié avec le réseau à ladite échéance ou à l'expiration de ladite durée de validité.

[0132] Dans une autre variante, une clé de sécurité peut être associée au tag. Par exemple, un nombre aléatoire ou pseudo-aléatoire, ou « nonce », unique pour un terminal, est également communiqué au terminal avec le ou les tags. Une telle clé de sécurité peut être utilisée à des fins d'autorisation.

[0133] Le contrôleur réseau 15 (ou un autre contrôleur réseau) peut également transmettre aux nœuds de bordure, par exemple au premier nœud de bordure BR 141 et au deuxième nœud de bordure BR 142, des règles de classification de trafic pour associer le trafic entrant sur le nœud de bordure à la ou aux tranches réseau négociées avec le

terminal 11 (et donc associer l'identifiant du trafic à destination du terminal associé, ou tag, à la ou aux tranches réseau négociées avec le terminal 11).

[0134] On note qu'un même tag peut être négocié avec plusieurs terminaux pour optimiser la taille des tables de classification de trafic lorsque les règles de de classification de trafic sont stockées dans des tables maintenues par les nœuds de bordure.

[0135] Le terminal 11 peut ainsi associer le trafic retour de chaque service éligible à l'exploitation de tranches avec au moins une tranche réseau, grâce à au moins un tag. Le trafic retour d'un même service peut être associé à plusieurs tranches réseau selon la nature du service. La classification de chacune de ces catégories selon un type de tranche réseau peut être définie par la logique du service (par exemple intégrée dans l'applicatif embarqué dans le terminal 11) ou fournie par le réseau SSP 12. La classification des différents trafics peut également faire l'objet d'une décision prise par le terminal 11 (par exemple, selon les choix et instructions de l'utilisateur du terminal 11).

[0136] Pour ce faire, le terminal 11 peut transmettre un ou plusieurs tags à au moins une instance de service apte à fournir le service auquel le terminal souhaite accéder. Par exemple, le terminal 11 utilise un nouveau paramètre appelé ci-après « Solace », pour transmettre le ou les tags dans un message qu'il envoie à une instance de service, par exemple à la première instance de service SFI #1 131.

[0137] Si le paramètre Solace ne contient qu'un seul tag « Inbound-Flow-Map », alors ce tag s'applique pour tout le trafic émis par l'instance de service.

[0138] Si ce paramètre Solace contient une liste de tags « Inbound-Flow-Map », alors des règles de classification de trafic sont également fournies par le terminal 11 à l'instance de service, de façon à pouvoir identifier le trafic émis par l'instance de service et le tag associé.

[0139] Dans un contexte où le terminal 11 est connecté à plusieurs réseaux de communication (contexte de « multihoming » par exemple), le terminal 11 s'assure que les règles de classification de trafic ainsi générées permettent d'associer le trafic avec le tag du réseau destiné à acheminer ledit trafic.

[0140] Par exemple, comme illustré en [Fig.8], le terminal 11 peut être connecté à un premier réseau de communication SSP1 et à un deuxième réseau de communication SSP2. Le terminal 11 peut indiquer explicitement, par exemple via le paramètre Solace, son adresse destination dans chaque réseau de communication comme règle de classification de trafic, correspondant ici à un paramètre de démultiplexage.

[0141] Ainsi, le paramètre Solace contient par exemple une liste de tags dont un premier tag TAG1 correspondant à l'adresse du terminal via le premier réseau SSP1 (notée dst@1), et un deuxième tag TAG2 correspondant à l'adresse du terminal via le deuxième réseau SSP2 (notée dst@2) : Solace {dst@1=TAG1, dst@2=TAG2}.

[0142] En particulier, le nouveau paramètre Solace peut être inséré dans un en-tête dédié (par exemple en-tête HTTP, trame QUIC) ou décrit dans des messages caractéristiques de protocoles tels que SDP (« Session Description Protocol ») ou WebRTC.

[0143] L'exemple suivant illustre l'usage d'un nouvel attribut SDP pour la transmission du paramètre Solace entre le terminal 11 et une instance de service, appelé ci-après « a=slice-tag » :

```
v=0
o=-25678753849INIP62001:db8::1
s=
c=INIP62001:db8::1
t=00
m=audio12340RTP/AVP08
a=slice-tag:156IP62001:db8::145678
a=slice-tag:651IP62001:db8::12312340
```

[0144] Selon cet exemple, le tag « 156 » (i.e. l'identifiant destiné à la classification du trafic à destination du terminal) peut être utilisé par l'instance de service si l'adresse destination utilisée pour envoyer le trafic vers le terminal 11 est « 2001:db8::1 », alors que le tag « 651 » peut être utilisé par l'instance de service si l'adresse destination utilisée pour envoyer le trafic vers le terminal 11 est « 2001:db8::123 ».

[0145] Il est bien entendu que cet exemple n'est fourni qu'à titre d'illustration ; d'autres paramètres pour caractériser le trafic associé à chaque tag peuvent être indiqués dans une offre/réponse SDP par exemple.

[0146] En revenant à la [Fig.7], le message comportant le paramètre « Solace » envoyé vers une instance de service est acheminé depuis le terminal 11 en utilisant une tranche réseau configurée à cet effet ou en utilisant un chemin par défaut si aucune tranche réseau n'est disponible ou activée pour acheminer le trafic à destination de cette instance de service.

[0147] Sur réception du message comportant le paramètre « Solace », l'instance de service vérifie la présence d'au moins un tag (« Inbound-Flow-Map »).

[0148] Par exemple, l'instance de service extrait puis enregistre localement la ou les règles de classification de trafic transmises par le terminal, ainsi que le ou les tags associés.

[0149] Le cas échéant, ces tags remplacent ceux déjà présents pour les mêmes règles de classification de trafic.

[0150] De façon optionnelle, l'instance de service confirme la bonne mise en place des règles de classification de trafic. Cette confirmation peut être communiquée au terminal 11 en utilisant un paramètre d'acquittement dédié (par exemple en-tête HTTP, trame QUIC) ou décrite explicitement dans des messages caractéristiques de protocoles

tels que SIP, SDP ou WebRTC. Pour certains services, l'absence de message d'erreur peut aussi être interprétée comme un acquittement et une confirmation implicites.

[0151] Si un trafic sortant (issu d'au moins une instance de service et à destination du terminal 11) est associé à une règle de classification de trafic communiquée par le terminal, alors l'instance de service marque le trafic avec le tag correspondant. En d'autres termes, l'instance de service peut émettre un message MSG1 comportant un ou plusieurs tags « tag » et, pour chaque tag, les données associées au service auquel le terminal souhaite accéder selon les règles de classification de trafic communiquées par le terminal. Par exemple, le ou les tags peuvent être insérés dans une option UDP, un en-tête HTTP, un en-tête SIP, le champ « Flow Label » d'un entête de paquet IPv6, un entête d'extension IPv6, etc.

[0152] Par exemple, comme illustré par la [Fig.7], la première instance de service SFI #1 131 peut transférer le message MSG1 à d'autres instances de service impliquées dans la fourniture du service, telles que la deuxième instance de service SFI #2 132. Ceci est avantageux car un même service peut impliquer une pluralité d'instances de service sans pour autant devoir réitérer la phase de communication des tags par le terminal avec toutes les instances de service. Cette synchronisation est notamment avantageuse pour les services qui utilisent un adressage anycast (c'est-à-dire, les instances de service sont joignables depuis une même adresse IP).

[0153] Le trafic retour (issu d'au moins une instance de service et à destination du terminal 11) est reçu par au moins un nœud de bordure, par exemple le premier nœud de bordure BR 141 et/ou deuxième nœud de bordure BR 142. Sur réception du message MSG1 envoyé par l'instance de service, le nœud de bordure BR inspecte, puis extrait le cas échéant le ou les tags.

[0154] Si aucun tag n'est présent, alors le trafic est traité selon une règle d'acheminement par défaut. Par exemple, le trafic est acheminé au terminal 11 via une route par défaut (par exemple une route qui n'est pas établie dans l'une quelconque des tranches réseau déployées, ou une tranche réseau dédiée au trafic dit « Best Effort »).

[0155] Si un tag est présent, le nœud de bordure BR applique les règles de classification de trafic ad hoc (par exemple en consultant une table de classification de trafic qu'il maintient localement) pour identifier la tranche réseau associée au tag :

- si aucune entrée dans la table de classification de trafic n'est trouvée, alors le trafic peut être acheminé vers le terminal 11 via une route par défaut, ou bien bloqué. Par exemple, en [Fig.7], le nœud de bordure BR 142 ne dispose pas, dans la table de classification de trafic, d'une entrée descriptive de la tranche réseau associée au tag reçu dans le message MSG1. Les données sont donc acheminées selon une route par défaut, qui ne repose pas nécessairement sur l'utilisation de tranches réseau.

- si une entrée dans la table de classification de trafic est identifiée par le nœud de bordure BR, alors celui-ci achemine le trafic selon le contenu de cette entrée, c'est-à-dire via la tranche réseau identifiée à partir du tag. Par exemple, en [Fig.7], le nœud de bordure BR 141 reconnaît que le tag reçu dans le message MSG1 est associé à la tranche réseau Sl. #2. Il peut donc transmettre les données au terminal 11 via la tranche réseau Sl. #2.

[0156] En revenant à la [Fig.8], le nœud de bordure BR 141 du premier réseau SSP1 reçoit des données D1 et l'identifiant TAG1 en provenance de l'instance de service 131, et peut sélectionner, à partir de la lecture de la table de classification de trafic, la tranche réseau associée à l'identifiant TAG1 pour l'acheminement des données D1 via le premier réseau SSP1, par exemple la tranche réseau Sl. #3. Le nœud de bordure BR 842 du deuxième réseau SSP2 reçoit des données D2 et l'identifiant TAG2 en provenance de l'instance de service 131, et peut sélectionner, à partir de la lecture de la table de classification de trafic, la tranche réseau associée à l'identifiant TAG2 pour l'acheminement des données D2 via le deuxième réseau SSP2, par exemple la tranche SL. #1. Les données D1 et D2 peuvent être identiques ou différentes.

[0157] En revanche, comme illustré par la [Fig.9], si le nœud de de bordure BR 141 du premier réseau SSP1 reçoit des données D1 et l'identifiant TAG2 en provenance de l'instance de service 131, aucune entrée n'est trouvée dans la table de classification de trafic. Les données D1 sont donc acheminée vers le terminal 11 en utilisant une route par défaut, ou une route déterminée selon un schéma de routage IP classique par exemple.

[0158] De façon optionnelle, le nœud de bordure BR peut retirer le ou les tags avant de retransmettre les données vers le terminal.

[0159] Dans une variante, le nœud de bordure BR vérifie la présence d'une clé de sécurité, par exemple la présence d'un paramètre « nonce » valide associé au terminal considéré, avant d'injecter le trafic dans une tranche réseau. La vérification de la validation du « nonce » peut être effectuée localement ou en faisant intervenir un contrôleur réseau, par exemple le contrôleur 15. La vérification n'est pas nécessairement effectuée systématiquement pour tous les paquets du message MSG1 qui transportent un tag et une clé de sécurité.

[0160] Dans une variante, le nœud de bordure BR peut calculer un condensé (« hash ») sur la base d'un premier paquet du message MSG1, et ce « hash » peut ensuite être utilisé pour valider les paquets suivants sans solliciter l'intervention d'un contrôleur réseau.

[0161] Si le terminal 11 détecte une anomalie/incohérence entre la tranche réseau utilisée pour un trafic retour d'un service donné et les indications communiquées à l'instance de service, notamment le tag destiné à la classification du trafic retour et/ou la clé de sécurité, le terminal peut procéder comme suit :

- renvoyer les instructions de marquage à l'instance de service, i.e. renvoyer le paramètre Solace,
- négocier une nouvelle procédure SOLACE avec le réseau, i.e. renégocier la liste de tranches réseau que le terminal est susceptible d'utiliser pour envoyer ou recevoir du trafic,
- ajuster les règles de classification de trafic.

[0162] Dans un autre mode de réalisation, le terminal 11 n'est pas connecté directement au réseau de communication, mais par l'intermédiaire d'un équipement de raccordement (par exemple un CPE ou autre routeur intermédiaire). Dans ce mode de réalisation, l'équipement de raccordement peut mettre en œuvre la procédure SOLACE comme si le terminal était directement connecté au réseau.

[0163] En variante, le CPE peut négocier avec le terminal l'activation de la procédure SOLACE. Par exemple, la communication des tags aux instances de service est effectuée par le terminal.

[0164] Dans une autre variante, le CPE insère les tags selon des règles locales au CPE. Ces règles peuvent être configurées par l'utilisateur ou communiquées par le terminal via un mécanisme dédié (PCP, par exemple).

[0165] Ainsi, comme illustré par la [Fig.10], le contrôleur 15 peut transmettre le ou les tags au CPE 10. Le terminal 11 peut contacter le CPE 10 pour récupérer les tags associés à chaque tranche réseau. Par exemple, le terminal 11 utilise de nouvelles options qui peuvent être supportées par différents protocoles tels que PCP (Port Control Protocol), DHCP (Dynamic Host Configuration Protocol), RA (message « Router Advertisement » en environnement IPv6), etc., pour obtenir les tags.

[0166] Un exemple d'option PCP utilisée à cet effet est proposé en [Fig.11]. Selon cet exemple, le champ « Tag count » indique le nombre de tags inclus dans l'option PCP. De manière optionnelle, le champ « Traffic Selector » peut être renseigné pour un tag. Ce champ décrit par exemple la règle de classification de trafic éligible au marquage avec ledit tag (par exemple adresse IP destination, numéro de port destination, identifiant de protocole), par une instance de service, des données associées au service considéré. Si aucune règle n'est indiquée, alors le marquage des données avec un tag est applicable à tout le trafic entrant sur l'instance de service (i.e. à destination du terminal).

[0167] Si le mode collaboratif de la procédure SOLACE est désactivé, le terminal peut notamment indiquer dans un message à destination d'une instance de service la liste des tranches réseau négociées avec le réseau. Sur réception de ce message, l'instance de service peut choisir d'invoquer une tranche distincte de celle utilisée pour acheminer ce message, pour tout ou partie du trafic à destination du terminal.

[0168] On a décrit ci-dessus différents exemples de mise en œuvre de l'invention. Bien

entendu, ces exemples sont purement illustratifs et non limitatifs. En particulier, comme déjà indiqué, aucune hypothèse n'est faite selon l'invention quant à la nature des tranches réseau, leur nombre, et le « mapping » éventuel entre des tranches réseau de domaines voisins (par exemple RAN et TN, TN et CN). Notamment, une tranche réseau peut être déployée sur une infrastructure fixe, mobile, ou une combinaison des deux.

[0169] **5.3 Structure simplifiée des entités correspondantes**

[0170] On présente finalement, en relation avec la [Fig.12], les structures simplifiées d'une entité, par exemple un terminal, un contrôleur, une instance de service, ou un nœud de bordure selon au moins un mode de réalisation décrit ci-dessus.

[0171] Comme illustré par la [Fig.12], une telle entité comprend au moins une mémoire 121 comprenant une mémoire tampon, au moins une unité de traitement 122, équipée par exemple d'une machine de calcul programmable ou d'une machine de calcul dédiée, par exemple un processeur P, et pilotée par le programme d'ordinateur 123, mettant en œuvre des étapes d'au moins un procédé selon au moins un mode de réalisation de l'invention.

[0172] A l'initialisation, les instructions de code du programme d'ordinateur 123 sont par exemple chargées dans une mémoire RAM avant d'être exécutées par le processeur de l'unité de traitement 122.

[0173] Si l'entité est un terminal, le processeur de l'unité de traitement 122 met en œuvre des étapes du procédé d'accès à au moins un service décrit précédemment, selon les instructions du programme d'ordinateur 123, pour :

- obtenir au moins un premier identifiant destiné à la classification du trafic à destination dudit terminal,

[0174] ledit au moins un premier identifiant étant associé à au moins une tranche réseau ou un type de tranche réseau,

- transmettre dit au moins un premier identifiant à au moins une première instance de service apte à fournir ledit au moins un service audit terminal,
- recevoir un message comportant des données associées audit au moins un service acheminées via au moins une tranche réseau associée audit au moins un premier identifiant, ladite au moins une tranche réseau étant sélectionnée par un nœud de bordure dudit réseau de communication en appliquant au moins une règle de classification de trafic connue dudit nœud de bordure.

[0175] Si l'entité est un contrôleur, le processeur de l'unité de traitement 122 met en œuvre des étapes du procédé de contrôle de la fourniture d'au moins un service décrit précédemment, selon les instructions du programme d'ordinateur 123, pour :

- obtenir au moins un premier identifiant destiné à la classification du trafic à destination dudit terminal,

[0176] ledit au moins un premier identifiant étant associé à au moins une tranche réseau ou un type de tranche réseau,

- transmettre ledit au moins un premier identifiant audit terminal, directement ou via au moins un routeur intermédiaire,
- transmettre, à au moins un nœud de bordure dudit réseau de communication, au moins une règle de classification de trafic pour la sélection d'au moins une tranche réseau destinée à acheminer vers ledit terminal des données associées audit au moins un service.

[0177] Si l'entité est une instance de service, le processeur de l'unité de traitement 122 met en œuvre des étapes du procédé de fourniture d'au moins un service décrit précédemment, selon les instructions du programme d'ordinateur 123, pour :

- recevoir au moins un premier identifiant destiné à la classification du trafic à destination dudit terminal,

[0178] ledit au moins un premier identifiant étant associé à au moins une tranche réseau ou un type de tranche réseau,

- la transmission, via au moins un nœud de bordure dudit réseau de communication, d'un message comportant au moins un deuxième identifiant, fonction dudit au moins un premier identifiant, et des données associées audit au moins un service, lesdites données étant destinées à être acheminées via au moins une tranche réseau associée audit au moins un premier identifiant,

[0179] ladite au moins une tranche réseau étant sélectionnée par ledit nœud de bordure en appliquant au moins une règle de classification de trafic connue dudit nœud de bordure.

[0180] Si l'entité est un nœud de bordure, le processeur de l'unité de traitement 122 met en œuvre des étapes du procédé de gestion de l'accès à au moins un service décrit précédemment, selon les instructions du programme d'ordinateur 123, pour :

- recevoir au moins un message en provenance d'au moins une première instance de service apte à fournir ledit au moins un service, ledit message comportant au moins un deuxième identifiant, fonction d'au moins un premier identifiant destiné à la classification du trafic à destination dudit terminal, et des données associées audit au moins un service,

[0181] ledit au moins un premier identifiant étant associé à au moins une tranche réseau ou un type de tranche réseau,

- sélectionner au moins une tranche réseau associée audit au moins un premier identifiant en appliquant au moins une règle de classification de trafic connue,
- transmettre lesdites données associées audit au moins un service sur ladite au moins une tranche réseau sélectionnée.

Revendications

[Revendication 1] Procédé d'accès à au moins un service par un terminal (11), via un réseau de communication mettant en œuvre des tranches réseau, comprenant :

- l'obtention(111)d'aumoinsunpremieridentifiantdestinéàlacl assificationdutraficàdestinationduditterminal,leditaumoinsu npremieridentifiantétantassociéàaumoinsunetrancheréseauo uuntypedetrancheréseau,
- latransmission(112)duditaumoinsunpremieridentifiantàaum oinsunepremièreinstancedeservice(131)apteàfournirleditau moinsunserviceauditterminal,
- laréception(113)d'unmessagecomportantdesdonnéesassocié esauditaumoinsunserviceacheminéesviaaumoinsunetranche réseauassociéeauditaumoinsunpremieridentifiant,sélectionn éeparunnœuddebordure(141)duditréseaudecommunicatione nappliquantaumoinsunerègledeclassificationdetraficconnue duditnœuddebordure.

[Revendication 2] Procédé selon la revendication 1, caractérisé en ce que ladite au moins une tranche réseau ou ledit type de tranche réseau est associé à un mode de transmission appartenant au groupe comprenant :

- l'acheminementdedonnéesàdestinationduditterminal,
- l'acheminementdedonnéesenprovenanceduditterminal,
- l'acheminementdedonnéesàdestinationduditterminaletenpro venanceduditterminal.

[Revendication 3] Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que ladite obtention comprend l'obtention d'au moins un premier identifiant par réseau auquel ledit terminal est connecté.

[Revendication 4] Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend la transmission, à ladite première instance de service, d'au moins une règle de classification de trafic.

[Revendication 5] Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il met en œuvre une sélection préalable de ladite moins une première instance de service habilitée à recevoir ledit au moins un premier identifiant.

[Revendication 6] Procédé de contrôle de la fourniture d'au moins un service à un

terminal (11), via un réseau de communication mettant en œuvre des tranches réseau, comprenant :

- l'obtention(151)d'aumoinsunpremieridentifiantdestinéàlaclassificationdutraficàdestinationduditterminal,leditaumoinsunpremieridentifiantétantassociéàaumoinsunetrancheréseauouuntypedetrancheréseau,
- latransmission(152)duditaumoinsunpremieridentifiantauditterminal,directementouviaaumoinsunrouteurintermédiaire,
- latransmission(153),àaumoinsunnœuddebordure(141)duditréseaudecommunication,d'aumoinsunerègledeclassificationdetraficpourlasélectiond'aumoinsunetrancheréseaudestinéeàacheminerversleditterminaldesdonnéesassociéesauditaumoinsunservice.

[Revendication 7] Procédé selon la revendication 6, caractérisé en ce qu'il comprend la transmission dudit au moins un premier identifiant à au moins un autre terminal connecté audit réseau de communication.

[Revendication 8] Procédé de fourniture d'au moins un service à un terminal (11), via un réseau de communication mettant en œuvre des tranches réseau, comprenant :

- laréception(1311)d'aumoinsunpremieridentifiantdestinéàlaclassificationdutraficàdestinationduditterminal,leditaumoinsunpremieridentifiantétantassociéàaumoinsunetrancheréseauouuntypedetrancheréseau,
- latransmission(1312),viaaumoinsunnœuddebordure(141)duditréseaudecommunication,d'unmessagecomportantaumoinsundeuxièmeidentifiant,fonctionduditaumoinsunpremieridentifiant,etdesdonnéesassociéesauditaumoinsunservice,lesditesdonnéesétantdestinéesàêtreacheminéesviaaumoinsunetrancheréseauassociéeauditaumoinsunpremieridentifiant,sélectionnéeparleditnœuddebordureenappliquantaumoinsunerègledeclassificationdetraficconnueduditnœuddebordure.

[Revendication 9] Procédé selon la revendication 8, caractérisé en ce qu'il comprend la réception d'au moins une règle de classification de trafic pour l'acheminement des données associées audit au moins un premier identifiant, et le stockage de ladite au moins une règle de classification de trafic et dudit au moins un premier identifiant

associé.

[Revendication 10] Procédé selon l'une quelconque des revendications 8 et 9, caractérisé en ce que ladite réception comprend la réception d'au moins deux premiers identifiants associés chacun à au moins une tranche réseau et l'application d'au moins une règle de classification de trafic pour sélectionner l'un desdits premiers identifiants.

[Revendication 11] Procédé selon l'une quelconque des revendications 8 à 10, caractérisé en ce qu'il comprend la transmission dudit message comportant ledit au moins un deuxième identifiant et des données associées audit au moins un service à au moins une deuxième instance de service apte à fournir ledit au moins un service.

[Revendication 12] Procédé de gestion de l'accès à au moins un service par un terminal, via un réseau de communication, comprenant :

- laréception(1412)d'aumoinsunmessageenprovenanced'aum oinsunepremièreinstancedeservice(131)apteàfournirleditau moinsunservice,leditmessagecomportantaumoinsundeuxiè meidentifiant,fonctiond'aumoinsunpremieridentifiantdestin éàlaclassificationdutraficàdestinationduditterminal,etdesdon néesassociéesauditaumoinsunservice, leditaumoinsunpremieridentifiantétantassociéàaumoinsunet rancheréseauouuntypedetrancheréseau,
- lasélection(1413)d'aumoinsunetrancheréseauassociéeaudita umoinsunpremieridentifiantenappliquantaumoinsunerègled eclassificationdetraficconnue,
- latransmission(1414)desditesdonnéesassociéesauditaumoin sunservicesurladiteaumoinsunetrancheréseausélectionnée.

[Revendication 13] Procédé selon l'une quelconque des revendications 1 à 12 caractérisé en ce que ledit au moins un premier identifiant est associé à une durée de validité.

[Revendication 14] Procédé selon l'une quelconque des revendications 1 à 13 caractérisé en ce que ledit au moins un premier identifiant est associé à une clé de sécurité.

[Revendication 15] Procédé selon l'une quelconque des revendications 1 à 14 caractérisé en ce qu'au moins une desdites tranches réseau est composée d'au moins une tranche réseau locale déployée dans au moins un sous-réseau dudit réseau de communication.

[Revendication 16] Terminal (11) apte à accéder à au moins un service, via un réseau de

communication mettant en œuvre des tranches réseau, comprenant au moins un processeur configuré pour :

- obteniraumoinsunpremieridentifiantdestinéàlaclassification dutraficàdestinationduditterminal,leditaumoinsunpremierid entifiantétantassociéàaumoinsunetrancheréseauouuntypedet rancheréseau,
- transmettreditaumoinsunpremieridentifiantàaumoinsunepre mièreinstancedeserviceapteàfournirleditaumoinsunservicea uditterminal,
- recevoirunmessagecomportantdesdonnéesassociéesauditau moinsunserviceacheminéesviaaumoinsunetrancheréseauass ociéeauditaumoinsunpremieridentifiant,sélectionnéeparunn œuddebordureduditréseaudecommunicationenappliquantau moinsunerègledeclassificationdetraficconnueduditnœuddeb ordure.

[Revendication 17] Contrôleur (15) apte à contrôler la fourniture d'au moins un service à un terminal, via un réseau de communication mettant en œuvre des tranches réseau, comprenant au moins un processeur configuré pour :

- obteniraumoinsunpremieridentifiantdestinéàlaclassification dutraficàdestinationduditterminal,leditaumoinsunpremierid entifiantétantassociéàaumoinsunetrancheréseauouuntypedet rancheréseau,
- transmettreleditaumoinsunpremieridentifiantauditterminal,d irectementouviaaumoinsunrouteurintermédiaire,
- transmettre,àaumoinsunnœuddebordureduditréseaudecomm unication,aumoinsunerègledeclassificationdetraficpourlasél ectiond'aumoinsunetrancheréseaudestinéeàacheminerversle ditterminaldesdonnéesassociéesauditaumoinsunservice.

[Revendication 18] Instance de service (131, 132) apte à fournir au moins un service à un terminal, via un réseau de communication mettant en œuvre des tranches réseau, comprenant au moins un processeur configuré pour :

- recevoiraumoinsunpremieridentifiantdestinéàlaclassificatio ndutraficàdestinationduditterminal,leditaumoinsunpremieri dentifiantétantassociéàaumoinsunetrancheréseauouuntyped etrancheréseau,
- latransmission,viaaumoinsunnœuddebordureduditréseaudec

ommunication,d'unmessagecomportantaumoinsundeuxièmeidentifiant,fonctionduditaumoinsunpremieridentifiant,etdesdonnéesassociéesauditaumoinsunservice,lesditesdonnéesétantdestinéesàêtreacheminéesviaaumoinsunetrancheréseauassociéeauditaumoinsunpremieridentifiant,sélectionnéeparleditnœuddebordureenappliquantaumoinsunerègledeclassificationdetraficconnueduditnœuddebordure.

[Revendication 19] Nœud de bordure (141, 142) apte à gérer l'accès à au moins un service par un terminal, via un réseau de communication, comprenant au moins un processeur configuré pour :

- recevoiraumoinsunmessageenprovenanced'aumoinsunepremièreinstancedeserviceapteàfournirleditaumoinsunservice,leditmessagecomportantaumoinsundeuxièmeidentifiant,fonctiond'aumoinsunpremieridentifiantdestinéàlaclassificationdutraficàdestinationduditterminal,etdesdonnéesassociéesauditaumoinsunservice,
leditaumoinsunpremieridentifiantétantassociéàaumoinsunetrancheréseauouuntypedetrancheréseau,
- sélectionneraumoinsunetrancheréseauassociéeauditaumoinsunpremieridentifiantenappliquantaumoinsunerègledeclassificationdetraficconnue,
- transmettrelesditesdonnéesassociéesauditaumoinsunservice surladiteaumoinsunetrancheréseausélectionnée.

[Revendication 20] Programme d'ordinateur comportant des instructions pour la mise en œuvre d'un procédé selon l'une quelconque des revendications 1 à 15 lorsque ce programme est exécuté par un processeur.

[Fig. 1]

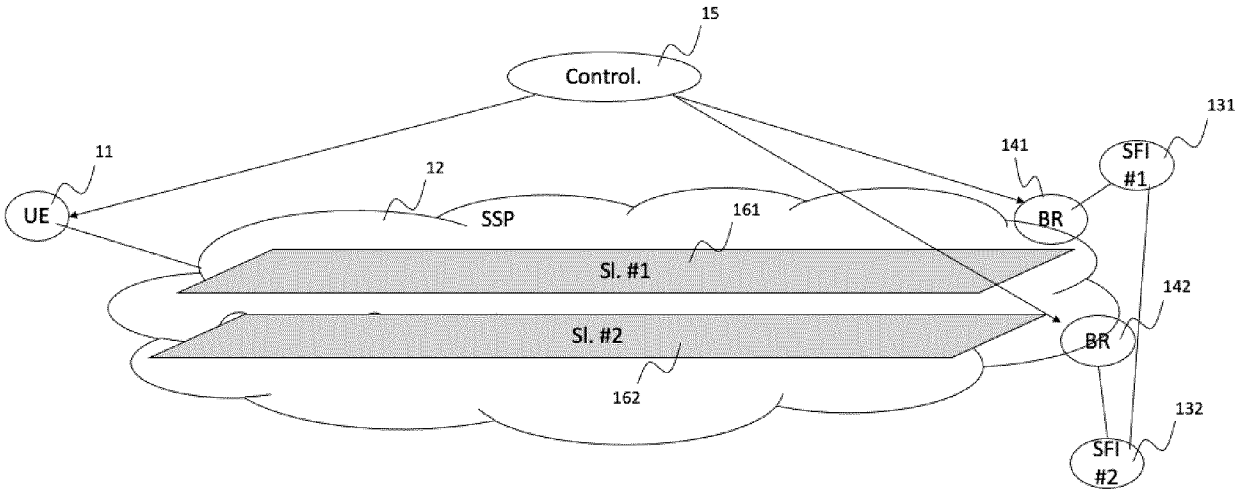


Fig. 1

[Fig. 2]

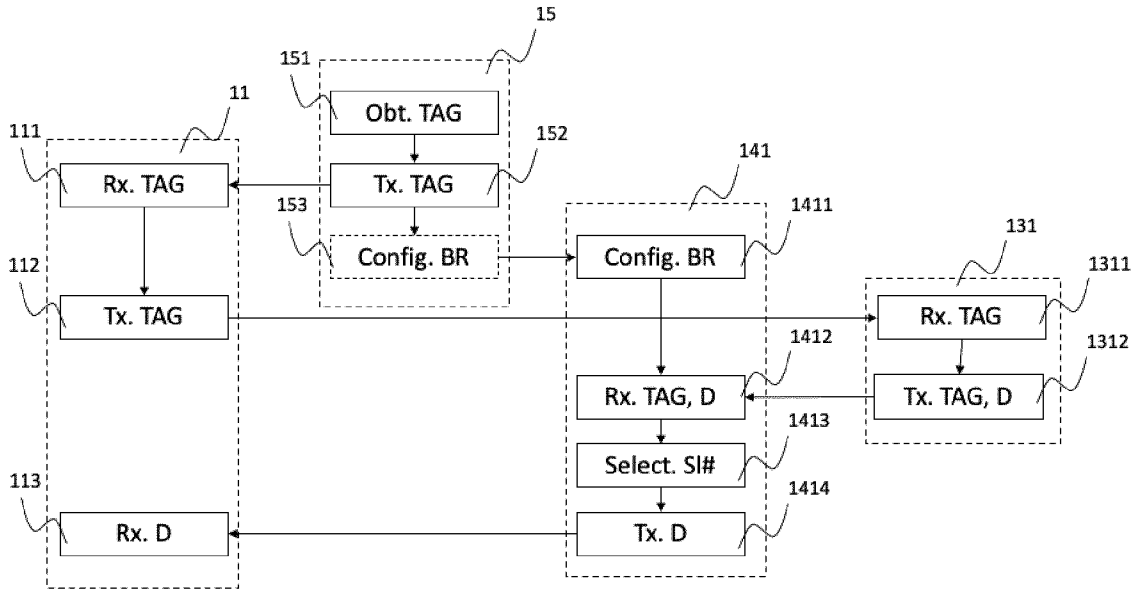


Fig. 2

[Fig. 3]

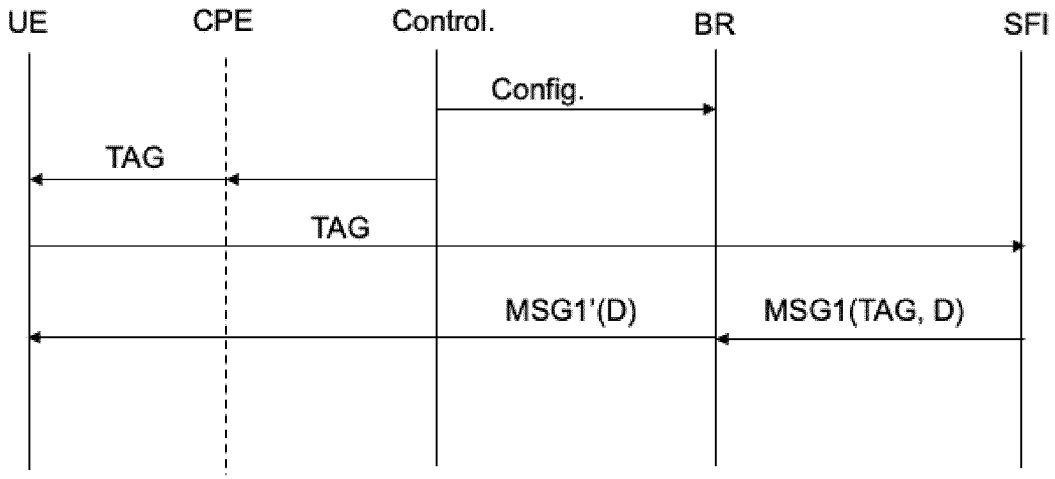


Fig. 3

[Fig. 4]

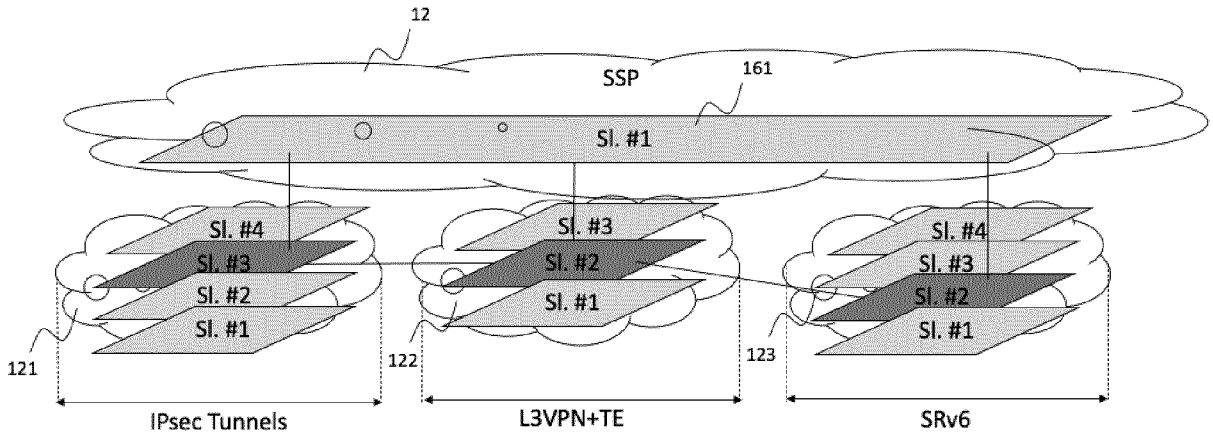


Fig. 4

[Fig. 5]

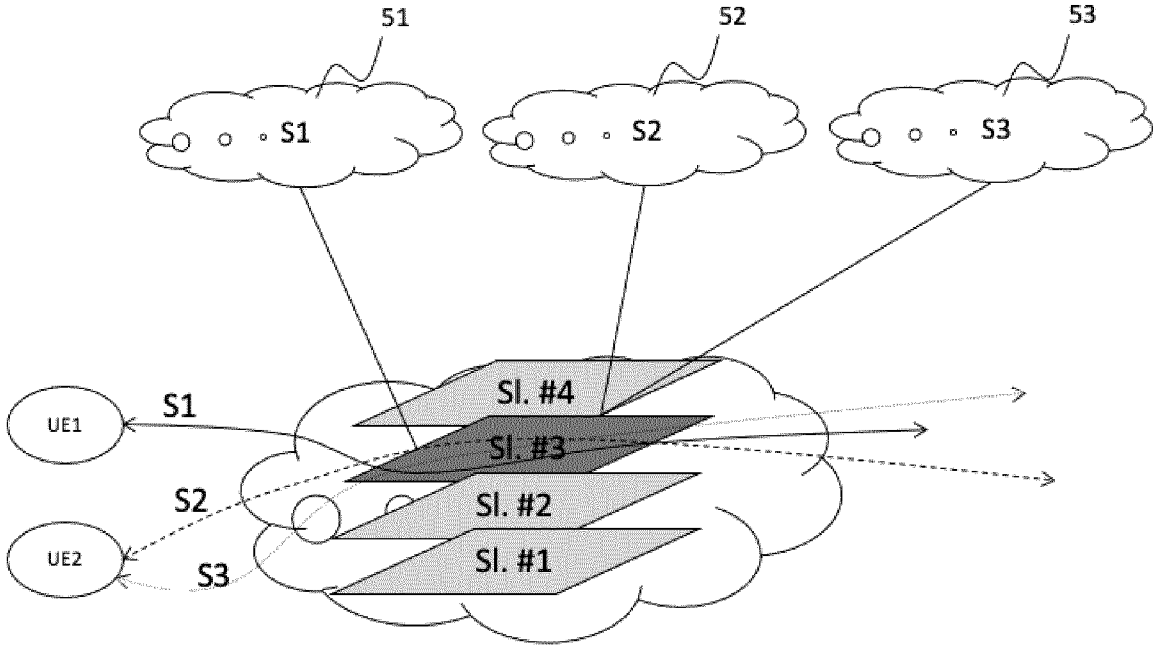


Fig. 5

[Fig. 6]

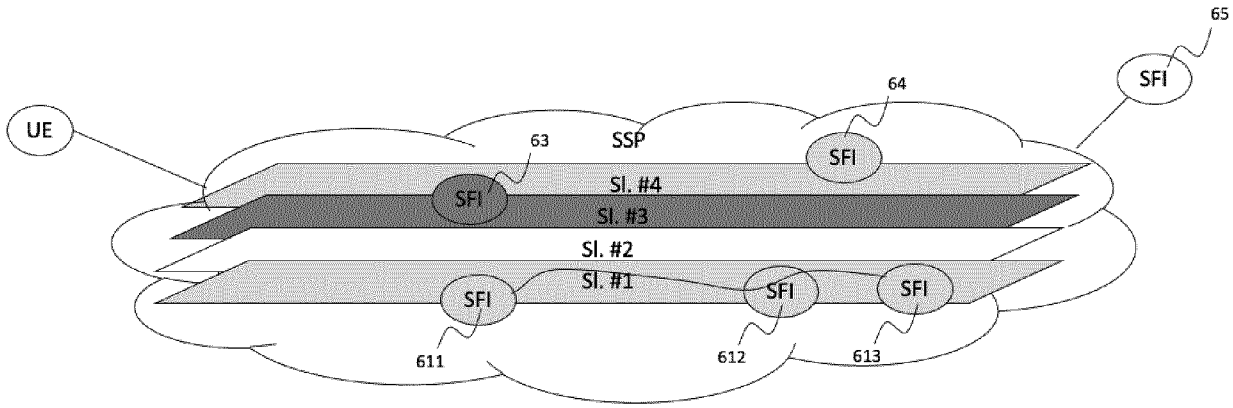


Fig. 6

[Fig. 7]

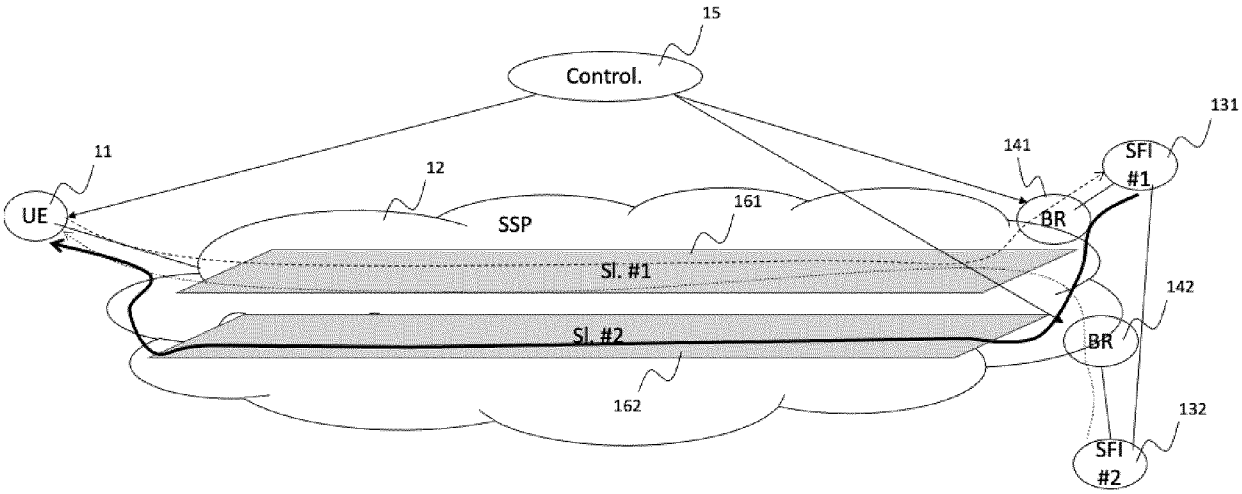


Fig. 7

[Fig. 8]

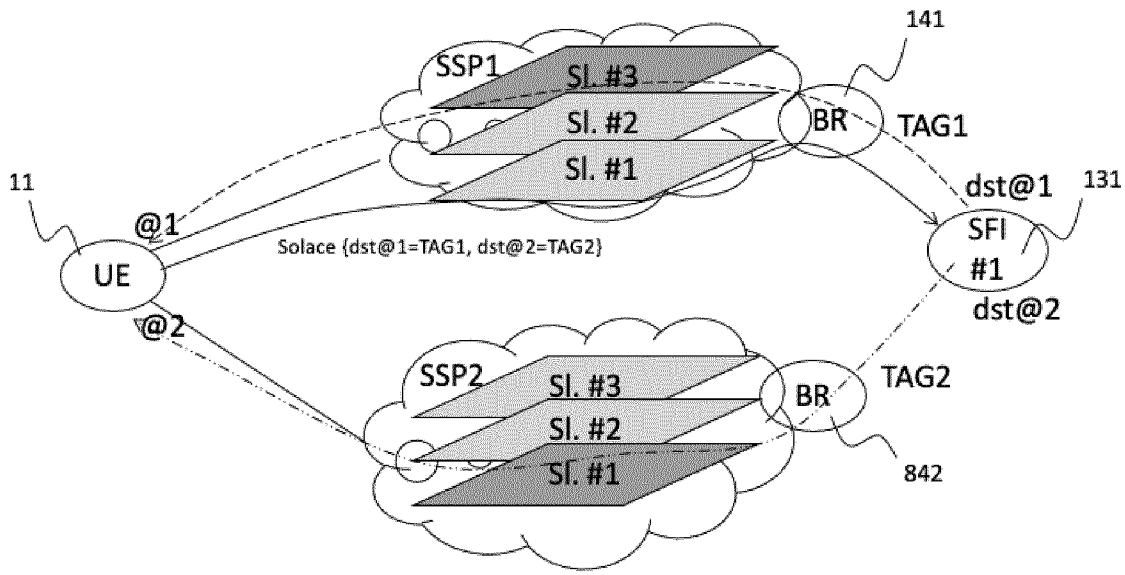


Fig. 8

[Fig. 9]

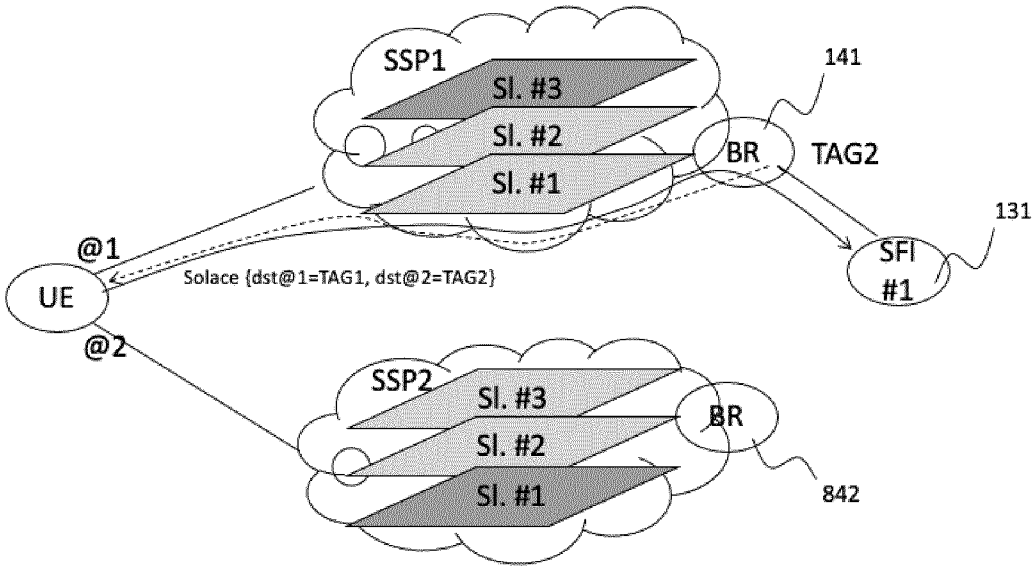


Fig. 9

[Fig. 10]

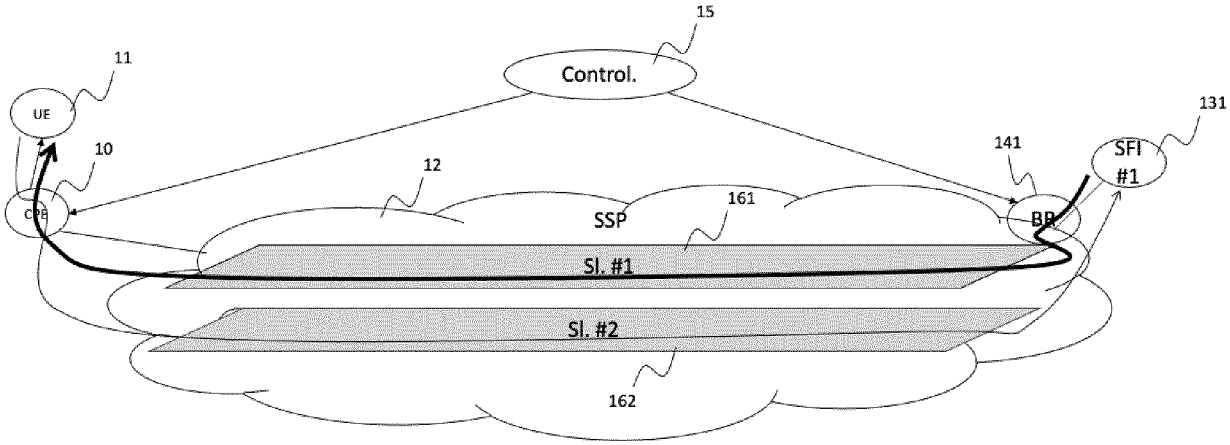


Fig. 10

[Fig. 11]

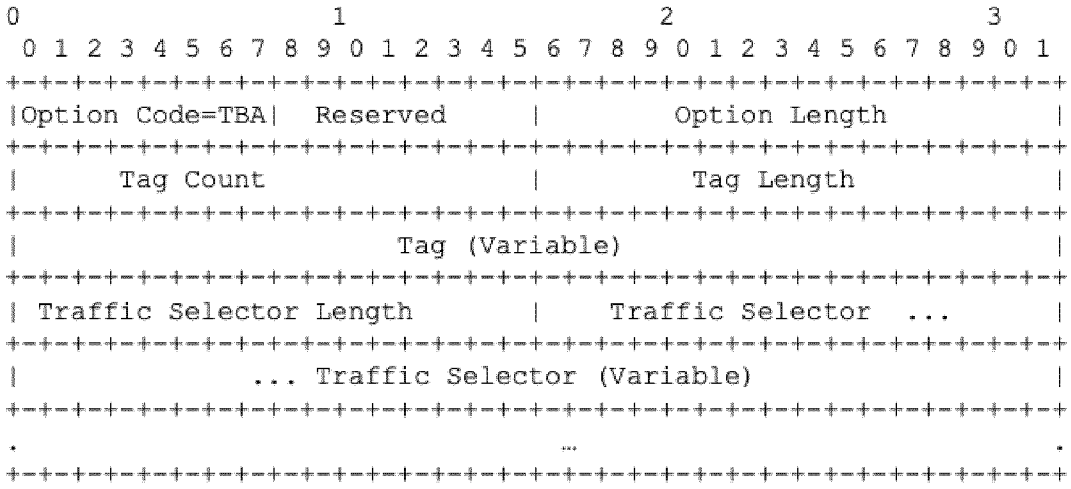


Fig. 11

[Fig. 12]

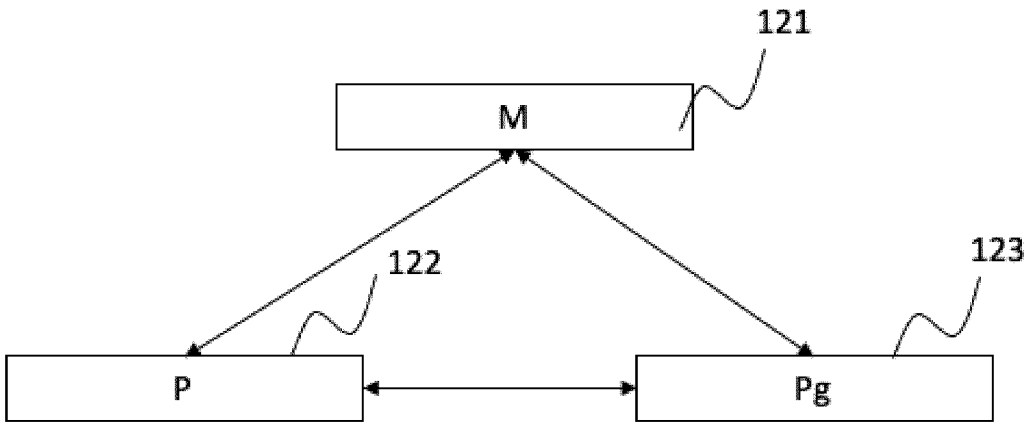


Fig. 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2024/067744

A. CLASSIFICATION OF SUBJECT MATTER

H04L 45/302(2022.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2017200978 A1 (IDAC HOLDINGS INC [US]) 23 November 2017 (2017-11-23) paragraph [0100] paragraph [0271] - paragraph [0282]; figures 2,4	1-20
A	WEI Y ET AL. "Network Service Header (NSH) Metadata Type 2 Variable-Length Context Headers ;rfc9263.txt" 09 August 2022 (2022-08-09), pages 1-9, NETWORK SERVICE HEADER (NSH) METADATA TYPE 2 VARIABLE-LENGTH CONTEXT HEADERS ;RFC9263.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARD, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, Retrieved from the Internet: https://tools.ietf.org/html/rfc9263 [retrieved on 2022-08-09] XP015154231 the whole document	1-20
A	US 10785652 B1 (RAVINDRANATH RAMMOHAN [IN] ET AL) 22 September 2020 (2020-09-22) the whole document	1-20

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 September 2024	**23 September 2024**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands (Kingdom of the)** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Perrier, Samuel** Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2024/067744

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2022141713 A1 (JAGANNATHA DEEPA [US] ET AL) 05 May 2022 (2022-05-05) the whole document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2024/067744

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2017200978 A1	23 November 2017	NONE	
US 10785652 B1	22 September 2020	NONE	
US 2022141713 A1	05 May 2022	US 2022141713 A1	05 May 2022
		US 2022264374 A1	18 August 2022

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2024/067744

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L45/302
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 2017/200978 A1 (IDAC HOLDINGS INC [US]) 23 novembre 2017 (2017-11-23) alinéa [0100] alinéa [0271] - alinéa [0282]; figures 2,4	1-20

-/--

[x] Voir la suite du cadre C pour la fin de la liste des documents

[x] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
6 septembre 2024	23/09/2024

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Perrier, Samuel

1

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2024/067744

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WEI Y ET AL: "Network Service Header (NSH) Metadata Type 2 Variable-Length Context Headers ;rfc9263.txt", NETWORK SERVICE HEADER (NSH) METADATA TYPE 2 VARIABLE-LENGTH CONTEXT HEADERS ;RFC9263.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARD, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, , 9 août 2022 (2022-08-09), pages 1-9, XP015154231, Extrait de l'Internet: URL:https://tools.ietf.org/html/rfc9263 [extrait le 2022-08-09] le document en entier	1-20

A	US 10 785 652 B1 (RAVINDRANATH RAMMOHAN [IN] ET AL) 22 septembre 2020 (2020-09-22) le document en entier	1-20

A	US 2022/141713 A1 (JAGANNATHA DEEPA [US] ET AL) 5 mai 2022 (2022-05-05) le document en entier	1-20

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2024/067744

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2017200978 A1	23-11-2017	AUCUN	
US 10785652 B1	22-09-2020	AUCUN	
US 2022141713 A1	05-05-2022	US 2022141713 A1	05-05-2022
		US 2022264374 A1	18-08-2022