



(51) International Patent Classification:

H04W 28/08 (2009.01) H04W 28/02 (2009.01)
H04W 48/14 (2009.01) H04W 92/24 (2009.01)

(21) International Application Number:

PCT/EP2017/064915

(22) International Filing Date:

19 June 2017 (19.06.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

16177248.8 30 June 2016 (30.06.2016) EP

(71) Applicant: **BRITISH TELECOMMUNICATIONS
PUBLIC LIMITED COMPANY** [GB/GB]; 81 Newgate
Street, London EC1A 7AJ (GB).

(72) Inventor: **PUTHUSSEY, Pradeep**; Ground Floor, Faraday Building, 1 Knightrider Street 1 Kightrider Street, London EC4V 5BT (GB).

(74) Agent: **CARDUS, Alan**; BT Legal, Ground Floor, Faraday Building 1, Knightrider Street, London EC4V 5BT (GB).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: TRAFFIC STEERING IN ACCESS NETWORKS

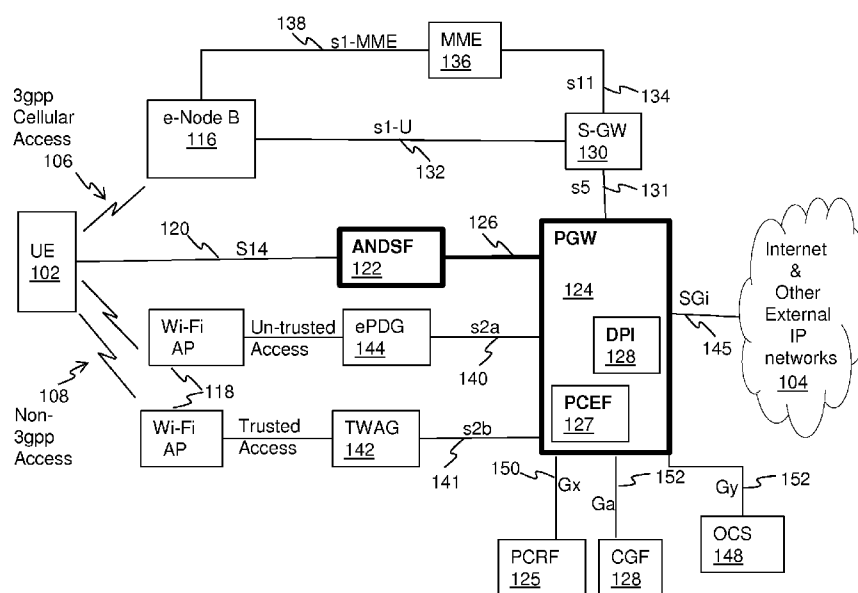


Figure 1

(57) **Abstract:** A server configured in a communications network to: receive information specific to an individual traffic flow between the communications network and a user equipment over a first access network of a first access network type; in which the information received comprises information relating to the traffic type of the individual traffic flow and information relating to the first access network type; in which the server is further configured to: instigate a determination of a specific one of the first access network and a second access network of a second access network type for selection for carrying the individual traffic flow between the communications network and the user equipment; in which the determination is based on the information received regarding the traffic flow and the first access network type and pre-programmed information on the second access network type; and in which the server is further configured to: communicate to the user equipment the identity of the specific one of the first and second access networks for selection for carrying



(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, 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).

Published:

— *with international search report (Art. 21(3))*

Traffic Steering In Access Networks

Field of the Invention

The present invention relates to communications networks in general and to access network selection in a communications network.

5 Background

Mobile Operators are challenged with demand for increasingly higher data rates. There is, accordingly, a need to improve selection between available access networks.

Summary of the Invention

10 The present invention accordingly provides, in a first aspect, a first server for operation in a communications network; in which the first server is configured to receive information specific to an individual traffic flow between the communications network and a user equipment over a first access network of a first access network type; in which the information received comprises information relating to the traffic type of the individual traffic flow and information relating to the first access network type; in which the
15 information specific to an individual traffic flow is detected by a second server; in which the second server is arranged in communication with the user equipment and is configured to create managed data sessions with the user equipment; in which the information specific to an individual traffic flow is received at the first server over a direct link between the first server and the second server; in which the first server is further
20 configured to instigate a determination of a specific one of the first access network and a second access network of a second access network type for selection for carrying the individual traffic flow between the communications network and the user equipment; in which the determination is based on the information received regarding the traffic flow and the information received regarding the first access network type and pre-programmed information on the second access network type; and in which the first server
25 is further configured to communicate to the user equipment the identity of the specific one of the first and second access networks for selection for carrying the individual traffic flow between the communications network and the user equipment.

30 According to an embodiment, the determination is carried out on the basis of a request made before the individual traffic flow commences; in which the information is received in the request.

According to an embodiment, the server is an Access Network Discovery and Selection Function or ANDSF.

According to an embodiment, the access networks comprise at least one 3GPP network and at least one non-3GPP network.

The invention accordingly provides in a second aspect, a method for operating a first server in a communications network; in which the method comprises the first server:
5 receiving over a direct link between the first server and a second server, information specific to an individual traffic flow between the communications network and a user equipment over a first access network of a first access network type; in which the information received comprises information relating to the traffic type of the individual traffic flow and information relating to the first access network type; in which the second
10 server is arranged in communication the user equipment and is configured to create a managed data session with the user equipment; in which the information specific to an individual traffic flow is detected by the second server; in which the method further comprises the first server: instigating a determination of a specific one of the first access network and a second access network of a second access network type for selection for
15 carrying the individual traffic flow between the communications network and the user equipment; in which the determination is based on the information received regarding the traffic flow, the information received regarding the first access network type and pre-programmed information on the second access network type; and in which the method further comprises the first server: communicating to the user equipment the identity of
20 the specific one of the first and second access networks for selection for carrying the individual traffic flow between the communications network and the user equipment.

According to an embodiment, the determination is carried out on the basis of a request made before the individual traffic flow commences; in which the information is received in the request.

25 According to an embodiment, the server is an Access Network Discovery and Selection Function or ANDSF.

According to an embodiment, the method further comprises the server obtaining from a data storage, at least one rule for determining a specific access network for selection for carrying a traffic flow between the communications network and the user equipment.

30 According to an embodiment, the method further comprises the server providing to the user equipment a policy derived from the rule.

According to an embodiment, the rule is an IFOM rule.

According to an embodiment, the method further comprises the server obtaining the at least one rule from the data storage in response to providing to the data storage, the information received regarding the individual traffic flow and the access network type.

According to an embodiment, the determination is based on a data type associated with the traffic flow.

According to an embodiment, the determination is based on a data-rate associated with the traffic flow.

According to an embodiment, where a plurality of traffic flows comprise different bandwidths, the server is configured to communicate to the user equipment the identity of a WLAN access network in relation to a higher-bandwidth traffic flow.

The present invention accordingly provides, in a third aspect, a computer program element comprising computer program code to, when loaded into a computer system and executed thereon, cause the computer to perform the steps of the method set out above.

Brief Description of the Figures

In order that the present invention may be better understood, embodiments thereof will now be described, by way of example only, with reference to the accompanying drawings in which:

Figure 1 is a block diagram of a communications system suitable for the operation of embodiments of the present invention;

Figures 2 to 3 show typical signal flows in the communications system of Figure 1; and

Figure 4 is a block diagram of a data processing system suitable for the operation of embodiments of the present invention.

Detailed Description of Embodiments

The arrangement proposed here improves current access-network selection by providing new functionality at a network server which receives information specific to an individual traffic flow between the communications network and a single user equipment over a first access network; instigates a determination of a specific one of the first and second access networks for selection for carrying the individual traffic flow and communicates to the user equipment the identity of the specific one of the first and second access networks for selection for carrying the traffic flow.

This solution can provide the user with improved data and voice traffic flows over various access technologies thereby improving user satisfaction. Network operators may be able to reduce capital and operational expenditure as fewer radio sites may be required to serve a given population of users. The solution described here can improve network efficiency by enabling automatic and seamless offloading of traffic based on traffic type and enhancing the operator's influence over the access network selection.

Embodiments of the invention enhance the operator's influence over the access network selection by providing information, detected at a server in a mobile network, on an individual traffic flow, i.e. a traffic flow specifically involving a single user equipment. For example, by detecting, within the mobile network, high-bandwidth network traffic flows impinging on the user equipment and by monitoring, within the mobile network, the availability of Wi-Fi access-network connections to a specific user equipment, the network operator is able to influence access network selection at the user equipment, so that high-bandwidth network traffic may be diverted, as appropriate, away from an overloaded mobile access network, for example to an alternative access network better able to cope with the traffic. In so doing, load on the mobile network can be reduced, and faster data-transfer facilitated by moving the data to a higher-bandwidth WLAN connection, where appropriate, and may in this way reduce mobile-related costs to the user. According to a further embodiment, this is achieved automatically, without action being required by the user.

In Figure 1, a user equipment 102, such as a mobile phone, mobile computing device or similar having wireless mobile telephony and data connections is in communication with a remote communications network 104 (e.g. a core IP network such as the Internet or a communications provider's public or proprietary core network) via a plurality of access networks. That is, the communications network is able to communicate with a user equipment via at least a first access network of a first type and via a second access network of a second type accessible to the user equipment. Suitable wireless access networks include WWAN 106 and WLAN 108. That is, user equipment 102 has two or more wireless communications interfaces that allow it to communicate with the core network 104 using a choice of different protocols over functionally separated access networks 106, 108. Each access network will have a different wireless termination point on the network side. For example, for the WWAN 106 this can be e-Node B 116, while for WLAN 108, this can be Wi-Fi access point (AP) 118.

PGW 124 connects the Evolved Packet Core (which includes the following elements from Figure 1: MME 136, SGW 130, PCRF 125, PGW 124, TWAG 142, Epdg 144 and ANDSF 122) to the remote communications network 104 via SGi interface 145. PGW 124 supports connection from access networks, such as WWAN 106 and WLAN 108. An exemplary embodiment is shown in Figure 1. According to this embodiment, PGW 124 connects to the WWAN access network 106 over s5 link 131 and Serving Gateway (S-GW) 130. S-GW 130 can be a function within the PGW 124. In more detail, PGW 124 connects to the WWAN access network 106 for control plane/signalling over Serving Gateway (S-GW) 130, connection s11 134, Mobility Management Node (MME) 136 and connection s1-MME 138 and PGW 124 connects to the WWAN access network 106 for user plane/user payload over S-GW 130 and connection S1-U 132. According to an embodiment, PGW 124 connects to the WLAN access network 108 over s2b connection 141 through Trusted Wi-Fi Access Gateway (TWAG) 142 to trusted WLAN access networks and over an s2a connection 140 and ePDG 144 to untrusted WLAN access networks.

The PGW 124 creates managed data sessions from user equipments such as user equipment 102. The PGW 124 receives requests for data sessions/bearer setup from user equipments and can accept or reject a request based on certain conditions. Before allowing a request, checks are performed, as described below, by the PGW 124, some of which can involve the PGW 124 interfacing with other nodes such as the PCRF 125 and the charging system (CGF 146 and OCS 148). The Gx interface 152 towards the PCRF is used for policy control. The Gy interface towards online charging system is used for real-time billing in which the credit balance of a user may be checked before allowing a data session. If the request is allowed, the data exchange (i.e. the user plane) is carried over the S1-U link 132 using GPRS Tunneling Protocol GTP-U.

According to an embodiment of the invention, the user equipment 102 is also connected, via S14 link 120, over the Mobile access network with ANDSF 122. ANDSF 122 is a network element in the 3GPP Evolved Packet Core (EPC) and is an enabler of selection between access networks using different technologies (e.g. 3GPP and non-3GPP access networks). The ANDSF 122 provides a user equipment with operational information and operator-defined policies. According to an embodiment of the invention, ANDSF 122 uses a standardized S14 interface 120 to distribute network selection information and policies to user equipments in the mobile network. The S14 interface enables IP-level communication between the user equipment 102 and ANDSF 122 via pull or push mechanisms as defined in 3GPP TS 23.402. A combination of pull and push

mechanisms may also be supported. The ANDSF is provided with information specific to each individual traffic flow between the individual user equipment and the network, to allow improved access network selection.

According to an aspect of the invention, information on access-network traffic monitored using DPI, is processed at the ANDSF 122 to inform decisions as to the most advantageous access network for an individual user equipment 102 to use for a specific network traffic flow (i.e. data or voice traffic). The information is provided by the PGW 124 to the ANDSF 122 by means of a new interface. The new interface enables the PGW 124 to provide the ANDSF 122 with information on requested and detected real-time traffic flow of the individual user equipment in one or more access networks 106, 108 (i.e. traffic flowing in the access networks between user equipment 102 and core network 104). According to a first embodiment, the new interface comprises a new connection, not found in conventional enhanced packet core, between the PGW 124 and the ANDSF 122 to facilitate sharing of the information processed by the PGW 124 from monitoring of network traffic at an individual user equipment 102 level. According to the first embodiment the new interface may be implemented as a DIAMETER-based interface.

The ANDSF 122 can then communicate with the user equipment 102 (e.g. by pushing an ISRP rule) to share with the user equipment a determination, based on the information received from the PGW 124, as to the preferred access network for an individual traffic flow. Rules related to various traffic types can be pre provisioned in the ANDSF 122 by the mobile operator. The information and policies provided by ANDSF 122 are used by the user equipment 102 to select a suitable network for the specific type of traffic.

According to an embodiment, access network selection information and policies provided to the user equipment 102 by the ANDSF 122 takes precedence over any information affecting selection of access network pre-set by the operator on the user equipment 102. The information and policies provided by ANDSF 122 to the user equipment 102 may comprise ISMP or ISRP information.

According to an embodiment of the invention, a secure connection is established over a connection s14 between the user equipment and the ANDSF using PSK TLS, which is a shared key-based mutual authentication scheme. PSK TLS supports a push model, where the ANDSF 122 is able to push data to the user equipment 102 over the PSK TLS connection. Information and policies provided to the user equipment 102 by the ANDSF regarding access networks that are available to the user equipment include:

- the access technology type (e.g. WLAN, LTE);
- the radio access network identifier (e.g. the SSID of a WLAN);
- other technology-specific information, e.g. one or more carrier frequencies;
- validity conditions, i.e. conditions indicating when the provided access network discovery information is valid (such conditions may include e.g. a location).

Turning again to **Figure 1**, a server (packet data network gateway – PGW 124) receives information about user equipment network traffic passing over different wireless networks. i.e.: wireless wide area networks (WWAN), which could include 3GPP, HSPA, LTE, etc. mobile wide area access networks – for example 3GPP cellular access-network connections 106 from eNodeB 116 to the user equipment 102; and wireless local area networks (WLAN), which could include Wi-Fi, WiMAX, CDMA, etc. - for example, Wi-Fi access-network connections 108 from Wi-Fi access points 118 to the user equipment 102. The invention uses a server (e.g. PGW 124) to extract detailed access-network traffic information specific to each individual traffic flow impinging on each individual user equipment 102. For example, detailed information on the characteristics of traffic flowing to and from a specific user equipment 102 via various access networks may be obtained through deep packet inspection (DPI). DPI 128 is shown as a function of the PGW but can, alternatively, be implemented as a separate network element: i.e. a traffic detection function (TDF) – not shown. DPI allows certain types of user traffic or IP flows to be detected and such information can be used in selecting and in applying certain policies. The detailed information on individual user equipment-specific access-network traffic flows is exploited to improve communications efficiency through the access-networks. The invention provides a new network connection, i.e. a new interface between the network server (e.g. PGW 124) and a network selection function (e.g. access network discovery and selection function – ANDSF 122) for sharing information relating to access network traffic flows.

PGW 124 is a component of the evolved packet Core network (EPC). The PGW 124 connects the EPC to the Internet and to IP networks that are external to the EPC. The PGW 124 supports connection from 3GPP WWAN networks and non-3GPP WLAN networks. The PGW 124 connects to the 3GPP access network through the S-GW (Serving Gateway) 130 which can be a function within the PGW or an external node and the MME (Mobility Management Node) 136. The PGW 124 connects to the non-3GPP access network over the s2a 140 and TWAG 142 for trusted network connection. The PGW 124 connects to the non-3GPP access network over the s2b for untrusted network

connection through the evolved packet data gateway ePDG 144. The main role of the ePDG is to provide security mechanisms such as IPsec tunnelling of connections with the user equipment over an untrusted non-3GPP access. The PGW 124 creates and manages data sessions from the user equipments, such as user equipment 102. The PGW 124 receives requests from the user equipments for bearer setup in the form of Create Bearer requests over the GTP-C GPRS tunnelling protocol control plane. A request may be received through either the S5 or S2A/S2B link, depending on the access being used by the user equipment at the time of requesting a bearer. The PGW 124 can accept or reject a request based on certain conditions. Before allowing a bearer request, the PGW performs several actions to decide the acceptability of the Create Bearer request. These actions are performed by various functions within the PGW 124 and by interfacing with other external EPC nodes like the PCRF 125 and the Charging System 148. Once the bearer is established the user data is carried over GTP-U. According to an embodiment of the invention, the PGW 124 also connects to the ANDSF 122 through opening a new connection over which to share detailed traffic flow information relating to traffic flows to and from an individual, single user equipment to enable the ANDSF to communicate to the user equipment, the identity of specific access networks for selection for carrying individual traffic flows between the communications network and the user equipment.

To ensure that subscriber packets receive the appropriate quality of service (QoS), charging, and gating control, a PCC rule may be defined for a subscriber or for a corresponding bearer in the access network. The PCC rules contain the QoS parameters to be applied, the pre-conditions that need to be met etc. If a PCC rule is defined for a bearer then it is applied whenever a request is received for that bearer from any subscriber. If the PCC rule is defined for a subscriber then it is only applied when a bearer request is received from that particular subscriber. PCC rules are checked at the time of setting up a bearer and then in the interim when there is a modification of the bearer for example when there are any changes to the conditions of the access such as radio access change etc. PCC definition is performed by a part of the PGW known as the policy and charging enforcement function (PCEF) 127. PCEF has the function of enforcing on user equipment, policies received over the Gx interface from the policy and charging rules function (PCRF) 124. Such policies can be related to QoS, PLMN change, access network (e.g. WWAN or WLAN), etc. When the PCRF 125 provides details about active PCC rules to the PCEF, the PCEF determines if an existing bearer in the access network can be used. If no bearer exists with the corresponding combination of QoS

Class Identifier (QCI) and allocation retention priority (ARP) values specified in the PCC rules, then the PCEF initiates the creation of new bearers.

As we have seen, the PGW 124 may host the important functions of PCEF 127 and DPI 128. Other functions of the PGW normally include IP address allocation, where the PGW allocates IP addresses to the user equipment to establish packet data connections; packet routing and forwarding, where the PGW performs the required routing and forwarding of packets to and from the user equipment and the external IP network or Internet; on-line and off-line charging where the PGW triggers the on-line charging system (OCS) 148 over the Gy interface 154 for real-time charging and generating CDR's for off-line billing.

Figure 2 shows signalling flows 21-26 and payload (user plane) flows 27, 28 impinging on PGW 124 and ANDSF 122. A request 21 for a specific Access Point Name (APN) arrives at the PGW from the user equipment 102 using any of the WWAN and WLAN access networks. The interface 202 shown in the Figure is a representational amalgamation of both 3GPP and non 3GPP access interfaces, including S2b, S2a, and S5. The PGW does DPI on the request 21 and applies policy enforcement functions to the request 21, as appropriate. Based on the information obtained through DPI, the PGW sends 22 a DIAMETER message over the new interface 126 between the PGW and ANDSF. Access network selection criteria are contained in an ANDSF rules database 204. PCC rules which are not used for access selection are contained in a PCRF rules database (not shown). The ANDSF checks the information on the request against the rules database 204 and selects an appropriate IFOM rule from the rules database. The ANDSF sends 23 the selected IFOM rule to the user equipment over the S14 interface. The ANDSF responds 24 to the PGW DIAMETER message (22). The PGW informs 25 the user equipment about the preferred access network for the requested traffic. In response, the user equipment switches access network and sends 26 the payload over the preferred access network to the destination (i.e. the desired APN) via the PGW and the SGi interface 145. A response message 27 from the APN is received by the PGW and passed to the user equipment.

Figure 3 shows in more detail the signalling flows using the proposed new interface 126 between PGW 124 and ANDSF 122. Pre-requisites for these flows are that user equipment 102 is IFOM-capable to establish a Packet Data Network (PDN) connection over multiple (e.g. WWAN and WLAN) access networks. The PGW needs to also act as

a Home Agent (HA) and support bearer binding and Evolved Packet System (EPS) bearer modification requests raised by the user equipment.

During establishment of the first PDN connection, the PGW assigns to the user equipment, the home IP address (HoA) (i.e. the IP address for the WWAN session over 3GPP access 106) and the Home Network Prefix (HNP). The user equipment uses the HNP to identify whether it is on the home network or not. It is to be noted that 3GPP access is always considered the home network in IFOM. When a user equipment with a 3GPP PDN connection comes into the coverage of a WLAN, the user equipment uses WLAN selection policies (WLANSF) to select the particular WLAN and, after completing an EAP-SIM-AKA authentication process, the user equipment registers to the WLAN. WLANSF are the policies used by the user equipment to select a particular WLAN when more than one WLAN is available. A mobile operator may, for example, have an agreement with certain ISP operators for use of their Wi-Fi hotspots. User equipments with a subscription to that mobile operator may, as a result, have free access to Wi-Fi hotspots on that operator's WLAN, which will therefore be indicated as the preferred WLAN set in the WLANSF. The WLANSF could also be influenced by other factors, such as load on the Wi-Fi network. Using the HNP, the user equipment discovers that it is on a foreign network (i.e. not the home network) and sends a binding update message to the PGW-HA (i.e. the PGW acting as Home Agent) with the Care of Address (CoA), i.e. the IP address on the WLAN. The user equipment sends, in the binding update message, the IP address it receives for the WLAN session along with route filters, which are used to identify certain routes that can only be used via certain access networks. The user equipment also indicates, in the binding update message, that it already has a HoA. This information is sent to the PGW-HA. The binding update message also comprises indications that there is one binding associated with the HoA and another one associated with CoA and that the connection on the HoA is active. The PGW then binds the CoA with the HoA and sends a Binding Acknowledgement. With the signalling complete, the user equipment has essentially two data flows on the same PDN Connection: one over WWAN and another over WLAN. IFOM requires support of the PGW for selective offload of data traffic between WWAN and WLAN access networks for certain data flows in a given PDN connection and thereafter for continuing the data flows simultaneously over WWAN and WLAN access networks. Support for IFOM is negotiated between the user equipment and ANDSF during the initial registration process of the user equipment. The user equipment and network will be aware of the IFOM capabilities at either side. The invention supports handover between WWAN and WLAN systems in a seamless manner

while maintaining the data sessions. IFOM support is configured by the service provider dynamically using the ANDSF. The configuration is implemented for a specific flow within the same APN or PDN connection. The PGW can be configured with a specific APN that supports access from 3GPP and non 3GPP access networks and also supports IFOM.

5 Where IFOM rules need to be applied on a per-subscriber basis, the IFOM rules and related routing filters may be provisioned in the ANDSF by the service provider's business support system (BSS).

10 A DPI rule for detecting the specific content, application or URL targeted in a request from the UE may be configured on the PCRF or directly on the PGW. In either case, the DPI rule is enforced by a part of the PGW known as the PCEF.

The flows in Figure 3 will now be described in more detail:

1. As a starting point, the IFOM capable user equipment is connected simultaneously to 3GPP and non 3GPP access networks and multiple bindings and multiple IP flows are registered at the PGW-HA, as mentioned above.

15 2. PGW supports PDN connection to a specific APN over both types of access network. PGW allocates a HoA and CoA addresses and binds the two addresses together. PGW uses the HNP to identify the non-3GPP access network so that the user equipment is ready to seamlessly transfer access between these connections.

20 3. The user equipment sends to PGW, a request for a specific content, application or URL.

4. The PGW performs DPI on the request and detects the specific APN.

25 5. As part of the Gx interface procedure between the PGW and PCRF, the PGW sends to the PCRF, as a Gx modification request, a diameter CCR message indicating the detected APN, together with subscriber details, access network currently being used, etc., as per the configured DPI rule.

6. PCRF responds to the CCR message of step 5 with a diameter CCA message to the PGW comprising the user capabilities appropriate to the specific request and a policy that triggers the PGW to initiate communication with the ANDSF.

30 7. Upon the receiving the CCA from the PCRF, the PGW sends over the new interface 126 to the ANDSF a diameter CCR message comprising subscriber information, the currently used access network and the specific APN requested. This information is transferred in the CCR in the form of AVPs. The main Attribute-Value Pairs (AVP) include

as Event Trigger AVP, Application Start, Application Identifier-AVP, Radio Access Technology (RAT)-type AVP, Application-Instance Identifier and Flow Information AVP along with other AVP's as per RFC 3588.

5 8. Based on the information received from the PGW, the ANDSF decides whether an access switch is required for that specific traffic or not. The ANDSF checks the current access network indicated in the CCR RAT-type AVP and takes a decision (communicated in the CCA message in step 12, below) on a preferred access network (i.e. WWAN or WLAN). If the specific traffic is already flowing over the preferred access network, then the ANDSF does not need to communicate to the user equipment and will
10 respond to the CCR indicating no change required to the access network. The ANDSF has access to a database with IFOM rules configured by the operator. The IFOM rules specify, among other things, a preferred access network. The ANDSF checks the IFOM rules to select, based on the information provided in the CCR (see 7), the appropriate IFOM rule specifying the preferred access network (i.e. WWAN or WLAN) for the request.

15 9. The ANDSF sends the selected IFOM rule to the user equipment with an identifier derived from the Application Identifier-AVP for the APN requested by the user equipment in step 3 and the preferred access network type for that application.

20 10. The user equipment receives the IFOM rule and checks the rule against any known user preferences (e.g. whether to allow use of Wi-Fi or not). If no incompatibility is found between the received IFOM rule and any known user preferences, the user equipment accepts the IFOM rule, otherwise the IFOM rule is rejected. The user equipment initiates data-flow mobility procedures towards the PGW-HA in accordance with the IFOM rule.

11. Depending on the decision taken in step 10, user equipment sends IFOM rule acceptance or rejection ACK to the ANDSF.

25 12. ANDSF sends to the PGW, a diameter CCA, which is the response to the CCR message received in step 7. A successful CCA message indicates that the user equipment has accepted the IFOM rule in step 11. If the user equipment does not accept the IFOM rule then the CCA will contain a reject message with a cause code.

30 13. The user equipment sends, using the access network over which the user equipment is currently trying to access the specific APN, a bearer modification request to the PGW-HA with details of the user and the type of session.

14. The user equipment also sends to the PGW-HA over the same access network, a binding update with a modified routing rule to associate a particular traffic flow ID (FID)

with a modified access binding ID (BID). This is a binding update message to request association of a specific traffic flow (as identified by the FID) to a specific access network (as identified by the BID).

15. The PGW-HA updates to PCRF over the Gx interface to notify the PCRF, as appropriate, of the IP flow modification. If an on-line charging system (OCS) 148 update is required, the PGW also updates the OCS over the Gy interface in a diameter CCR message.

16. The PCRF (and OCS, as appropriate) sends to the PGW-HA a CCA in response to the modification request. If the PGW-HA receives a rejection in the CCA response from either PCRF or OCS, then the flow modification request will be rejected.

17. The PGW-HA sends to the user equipment, over the current access network, in a binding acknowledgment, acceptance or rejection of the modification request, as appropriate.

18A. In the case of rejection of the modification request, the PGW-HA will send, over the current access network, a rejection back to the user equipment. The access to the specific APN proceeds without modification of the IP flow so as to reduce the end-user impact. On receipt of the rejection of the modification request in the binding acknowledgment, the user equipment does not retry modification and takes no further action in this regard.

18B. If the IP flow modification is accepted then, on receipt of the binding acknowledgment, the user equipment transfers the traffic for the specific APN to the new access network type as per the IFOM rule and the session continues seamlessly without any interruption or user intervention.

Insofar as embodiments of the invention described are implementable, at least in part, using a software-controlled programmable processing device, such as a microprocessor, digital signal processor or other processing device, data processing apparatus or system, it will be appreciated that a computer program for configuring a programmable device, apparatus or system to implement the foregoing described methods is envisaged as an aspect of the present invention. The computer program may be embodied as source code or undergo compilation for implementation on a processing device, apparatus or system or may be embodied as data object code, for example.

Figure 4 is a block diagram of a data processing system 40 suitable for the operation of embodiments of the present invention. A central processor unit (CPU) 410 is

communicatively connected to communications interface 408, a memory 412, a storage 414 and an input/output (I/O) interface 416 via a data bus 520. The memory 412 can be any read/write storage device such as a random access memory (RAM) or a non-volatile storage device suitable for storing data for use by processor 412. The storage 414 can be any read-only or read/write storage device such as a random access memory (RAM) or a non-volatile storage device suitable for the computer program for controlling the operation of processor 410. Memory 412 and storage 414 may comprise the same device or devices. The implementing computer program may be stored on a carrier medium in machine or device readable form, for example in solid-state memory, magnetic memory such as disk or tape, optically or magneto-optically readable memory such as compact disk or digital versatile disk etc., and the processing device utilises the program or a part thereof to configure it for operation. The computer program may be supplied from a remote source embodied in a communications medium such as an electronic signal, radio frequency carrier wave or optical carrier wave. Such carrier media are also envisaged as aspects of the present invention. The user interface 416 is an interface to devices for the input or output of data provided to or received from a user or operator of computer system 40. Examples of input/output devices connectable to user interface 416 include a keyboard, a mouse, a display (such as a monitor) and a network connection. Communications interface 408 is an interface to other devices and may comprise one or more radio transmit interfaces and one or more wired or wireless core network interfaces.

Summary

We have described a solution that enables real-time, per user responsiveness required for a truly seamless and consistently high-performance user experience across 3GPP and Wi-Fi in a dynamic network environment. The solution described here allows access selection policies to be deployed in the network and enforced by the network based on analysis of real-time traffic impinging on the user equipment 102. This solution is user equipment 102 agnostic and is not reliant on any specific user equipment 102 decision-making capabilities for access selection. This solution improves network efficiency. It is intended to switch the traffic between available access networks as a network function, which is transparent to the user. As a result user does not experience any interruption in the traffic during access switchover but provides the user with un-interrupted data and voice traffic over various access technologies thereby improving user satisfaction. Operators may be able to reduce CAPEX and OPEX as fewer radio sites may be required

as a result of implementing the invention. The solution described here provides service providers better control of the selection of access network.

It will be understood by those skilled in the art that, although the present invention has been described in relation to the above described example embodiments, the invention is not limited thereto and that there are many possible variations and modifications which fall within the scope of the invention. Although described, above, with reference to wireless access networks, the invention is equally applicable to other types of access network, including wired and optical fibre-based networks. Although DPI is described as yielding an APN, other traffic-related information may be detected through the DPI and may trigger the diameter CCR message to the PCRF indicating the detected traffic information as per the configured DPI rule.

The scope of the present invention includes any novel features or combination of features disclosed herein. The applicant hereby gives notice that new claims may be formulated to such features or combination of features during prosecution of this application or of any such further applications derived therefrom. In particular, with reference to the appended claims, features from dependent claims may be combined with those of the independent claims and features from respective independent claims may be combined in any appropriate manner and not merely in the specific combinations enumerated in the claims.

Glossary

	ANDSF	Access Network Discovery and Selection Function
	APN	Access Point Name
5	ARP	Allocation and Retention Priority
	AVP	Attribute-Value Pair
	BCM	bearer control mode
	BID	Binding ID
	CCA	(Diameter) credit control application?
10	CCR	(Diameter) credit control request?
	CGF	Charging Gateway Function
	CoA	Care of Address
	DPI	Deep Packet Inspection
	EPC	Evolved Packet Core
15	EPS	Evolved Packet System
	FID	Flow ID
	GBR	Guaranteed Bit Rate
	GTP	GPRS Tunneling Protocol
20	Gx	provides transfer of (QoS) policy and charging rules from PCRF to Policy and Charging Enforcement Function (PCEF) in the PDN GW.
	HA	Home Agent
	HNP	Home Network Prefix.
	HoA	Home Address
	HPLMN	Home Public Land Mobile Network
25	IARP	Inter APN Routing Policy
	IFOM networks)	IP Flow Mobility (only apply at user equipment) (guides IP flows between networks)
	ISMP	Inter-System Mobility Policy [a set of operator-defined rules that affect access network selection decisions taken by the user equipment.]
30	ISRP	Inter System Routing Policy [network selection rules for a user equipment with potentially more than one active access network connection (e.g., both LTE and Wi-Fi). Such user equipment may employ IP flow mobility (IFOM)]
	MME	Mobility Management Entity
35	OCS	On-line Charging System
	PCC	Policy and Charging Control
	PCEF	Policy and Charging Enforcement Function (in PGW)

	PCRF	Policy and Charging Rule Function
	P-CSCF	Proxy-Call Session Control Function
	PDN	Packet Data Network
	PGW	Packet Data Network (PDN) Gateway
5	PSK TLS	???
	RAN	Radio Access Network
	RAT	Radio Access Technology
	S1-MME	eNodeB - MME interface for control plane traffic.
	S1-U	eNodeB - SGW interface for user plane traffic.
10	S14	The ANDSF communicates with the user equipment over the S14 reference point.
	S5	S5 provides user plane tunnelling and tunnel management between SGW and PGW.
	SGW	Serving Gateway
15	TWAG	Trusted Wi-Fi Access Gateway
	UE	User Equipment

CLAIMS

1. A first server for operation in a communications network;
in which the first server is configured to receive information specific to an individual traffic flow between the communications network and a user equipment over a first access network of a first access network type;
in which the information received comprises information relating to the traffic type of the individual traffic flow and information relating to the first access network type;
in which the information specific to an individual traffic flow is detected by a second server;
in which the second server is arranged in communication with the user equipment and is configured to create managed data sessions with the user equipment;
in which the information specific to an individual traffic flow is received at the first server over a direct link between the first server and the second server;
in which the first server is further configured to instigate a determination of a specific one of the first access network and a second access network of a second access network type for selection for carrying the individual traffic flow between the communications network and the user equipment; in which the determination is based on the information received regarding the traffic flow and the information received regarding the first access network type and pre-programmed information on the second access network type; and
in which the first server is further configured to communicate to the user equipment the identity of the specific one of the first and second access networks for selection for carrying the individual traffic flow between the communications network and the user equipment.
2. The first server of claim 1, in which the determination is carried out on the basis of a request made before the individual traffic flow commences; in which the information is received in the request.

3. The first server of any above claim, in which, the first server is an Access Network Discovery and Selection Function or ANDSF.
4. The first server of any above claim in which the access networks comprise at least one 3GPP network and at least one non-3GPP network.
5. The first server of any above claim, in which the information specific to an individual traffic flow is detected by a DPI rule enforced by the second server.
6. The first server of any above claim, in which the second server is a Packet Data Network Gateway.

7. A method for operating a first server in a communications network;

in which the method comprises the first server:

receiving over a direct link between the first server and a second server, information specific to an individual traffic flow between the communications network and a user equipment over a first access network of a first access network type; in which the information received comprises information relating to the traffic type of the individual traffic flow and information relating to the first access network type;

in which the second server is arranged in communication the user equipment and is configured to create a managed data session with the user equipment;

in which the information specific to an individual traffic flow is detected by the second server;

in which the method further comprises the first server:

instigating a determination of a specific one of the first access network and a second access network of a second access network type for selection for carrying the individual traffic flow between the communications network and the user equipment; in which the determination is based on the information received regarding the traffic flow, the information received regarding the

first access network type and pre-programmed information on the second access network type; and

in which the method further comprises the first server:

communicating to the user equipment the identity of the specific one of the first and second access networks for selection for carrying the individual traffic flow between the communications network and the user equipment.

8. The method of claim 7, in which the determination is carried out on the basis of a request made before the individual traffic flow commences; in which the information is received in the request.

9. The method of any of claims 7 to 8, in which, the first server is an Access Network Discovery and Selection Function or ANDSF.

10. The method of any of claims 7 to 9 further comprising the first server obtaining from a data storage, at least one rule for determining a specific one of the first and second access networks for selection for carrying a traffic flow between the communications network and the user equipment.

11. The method of claim 10 further comprising the first server providing to the user equipment a policy derived from the rule.

12. The method of any of claims 10 to 11, in which the rule is an IP flow mobility rule.

13. The method of any of claims 10 to 12, further comprising the first server obtaining the at least one rule from the data storage in response to providing to the data storage, the information received regarding the individual traffic flow and the information received regarding the access network type.

14. The method of any of claims 7 to 13, in which the determination is based on at least one of a data type associated with the traffic flow and a data-rate associated with the traffic flow.

15. The method of any of claims 7 to 14, in which, where a plurality of traffic flows comprise different bandwidths, the first server is configured to

communicate to the user equipment the identity of a WLAN access network in relation to a higher-bandwidth traffic flow.

- 5
16. The method of any of claims 7 to 15, in which the information specific to an individual traffic flow is detected by a DPI rule enforced by a second server.
17. The method of any of claims 7 to 16, in which the second server is a Packet Data Network Gateway.
- 10
18. A computer program element comprising computer program code to, when loaded into a computer system and executed thereon, cause the computer to perform the steps of the method set out in any of claims 7 to 17.

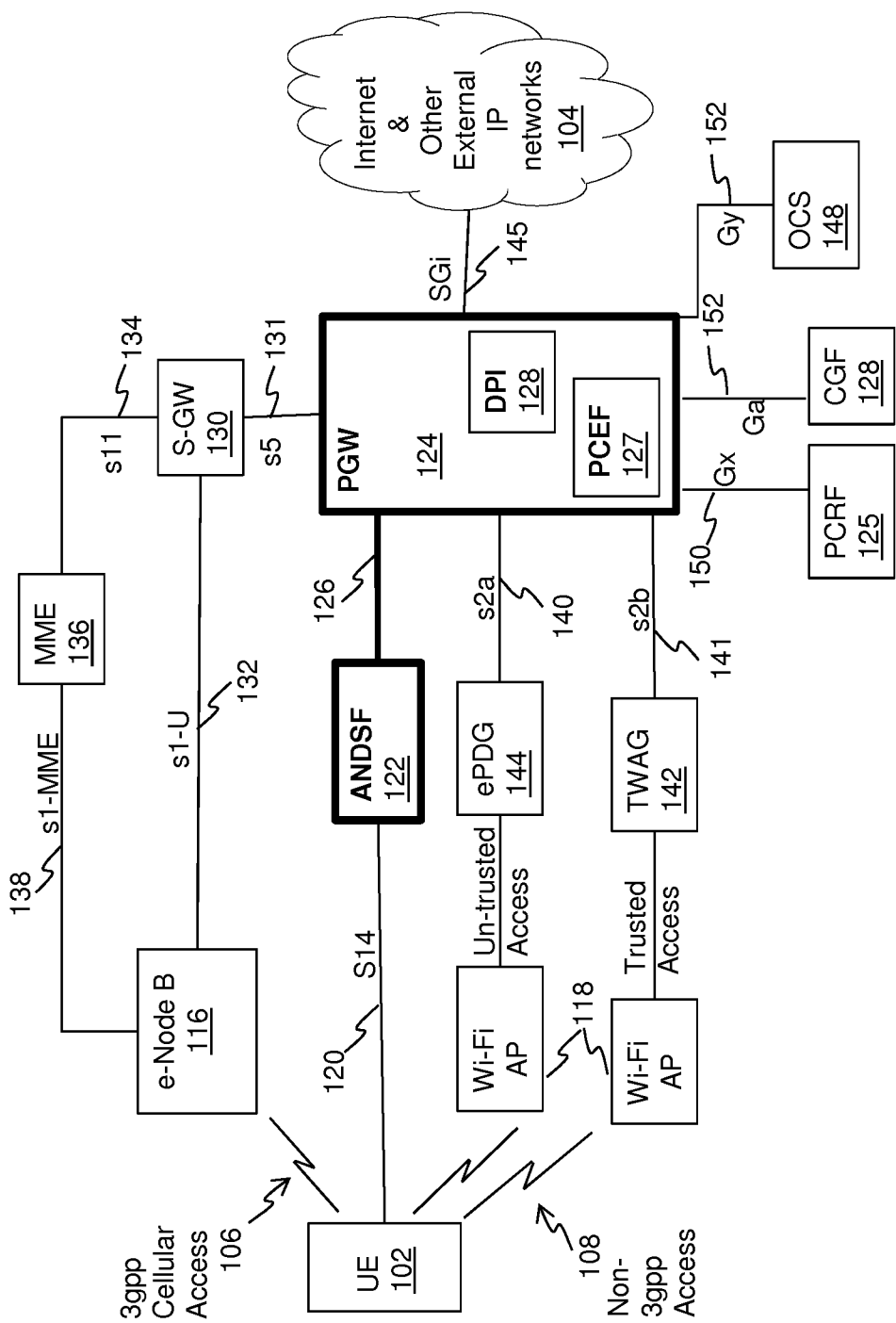


Figure 1

2 / 4

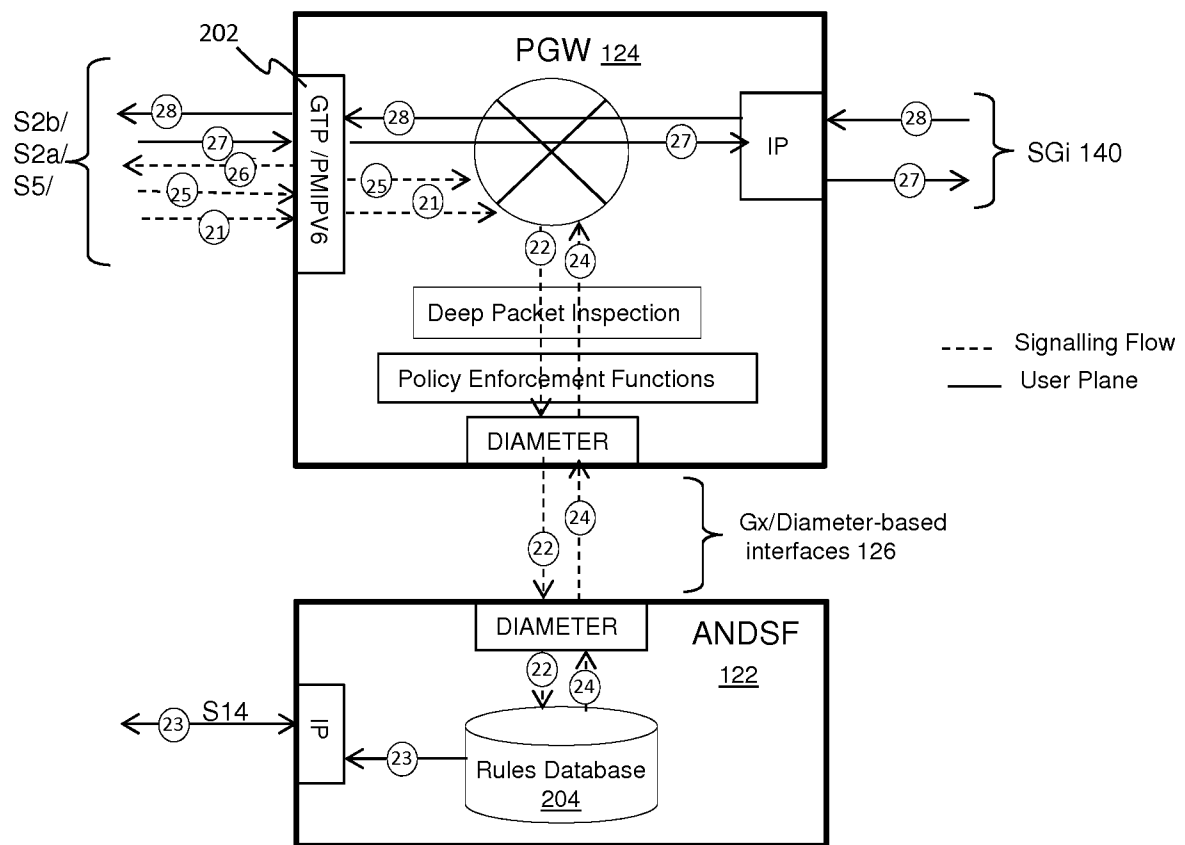


Figure 2

3 / 4

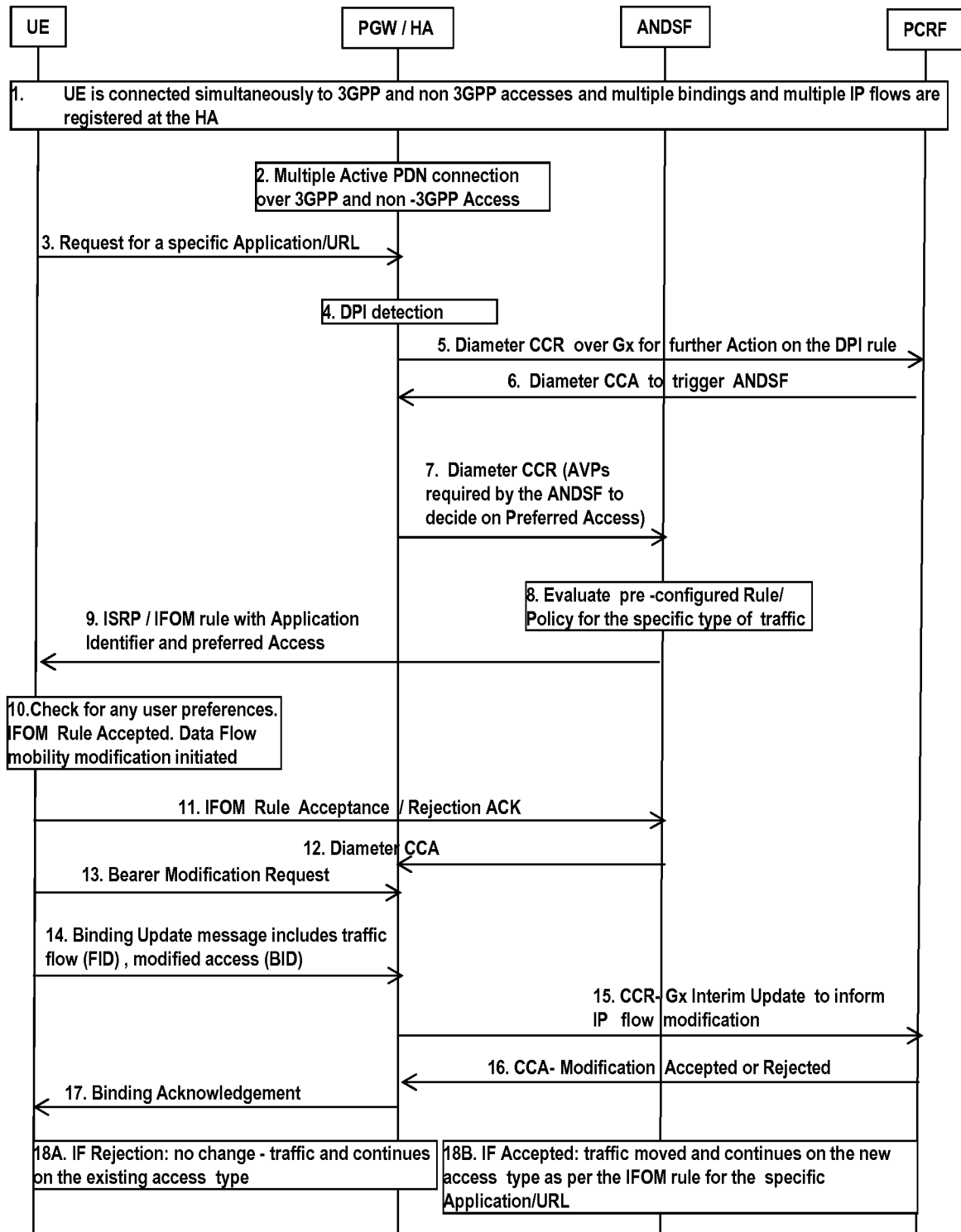


Figure 3

4 / 4

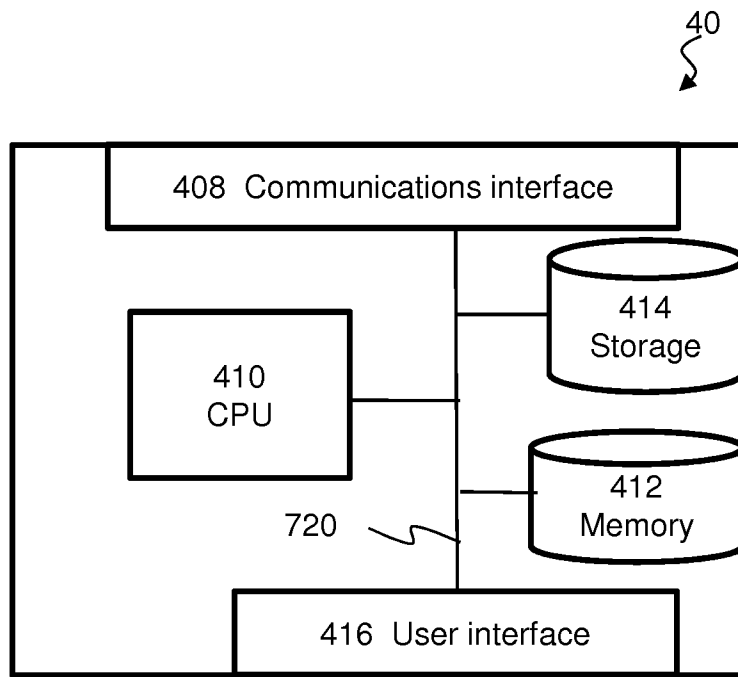


Figure 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/064915

A. CLASSIFICATION OF SUBJECT MATTER INV. H04W28/08 ADD. H04W48/14 H04W28/02 H04W92/24		
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) H04W		
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	US 2013/310030 A1 (VENTIMIGLIA MARK THOMAS [US] ET AL) 21 November 2013 (2013-11-21) paragraphs [0010], [0020] paragraph [0029] - paragraph [0045] paragraphs [0057], [0064] figures 1-3 -----	1-18
X	EP 2 445 266 A1 (ALCATEL LUCENT [FR]) 25 April 2012 (2012-04-25) paragraph [0011] - paragraph [0033] paragraphs [0063], [0069]; figures 1,2,3 -----	1-18
A	EP 2 852 223 A1 (ALCATEL LUCENT [FR]) 25 March 2015 (2015-03-25) paragraph [0020] - paragraph [0049] ----- -/-	1-18
☒ 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 4 August 2017		Date of mailing of the international search report 11/08/2017
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Allot, Corentin

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2017/064915

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
T	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses (Release 13)", 3GPP STANDARD; 3GPP TS 23.402, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. V13.6.0, 22 June 2016 (2016-06-22), pages 1-299, XP051123283, page 56 - page 75 -----	1-18
T	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 13)", 3GPP STANDARD; 3GPP TS 23.203, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. V13.8.0, 22 June 2016 (2016-06-22), pages 1-245, XP051123382, page 35 - page 95 -----	1-18
T	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2 (Release 13)", 3GPP STANDARD; 3GPP TS 23.261, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, vol. SA WG2, no. V13.0.0, 15 December 2015 (2015-12-15), pages 1-22, XP051047181, the whole document -----	1-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2017/064915

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
US 2013310030	A1	21-11-2013	CN	104335638 A		04-02-2015
			EP	2859757 A1		15-04-2015
			JP	6109302 B2		05-04-2017
			JP	2015524194 A		20-08-2015
			US	2013310030 A1		21-11-2013
			WO	2013177182 A1		28-11-2013

EP 2445266	A1	25-04-2012	CN	103181221 A		26-06-2013
			EP	2445266 A1		25-04-2012
			JP	5800908 B2		28-10-2015
			JP	2013546243 A		26-12-2013
			KR	20130086048 A		30-07-2013
			US	2013322300 A1		05-12-2013
			WO	2012055769 A1		03-05-2012

EP 2852223	A1	25-03-2015	CN	105580442 A		11-05-2016
			EP	2852223 A1		25-03-2015
			JP	2016536814 A		24-11-2016
			KR	20160060089 A		27-05-2016
			US	2016234760 A1		11-08-2016
			WO	2015040057 A1		26-03-2015
