(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
09 January 2025 (09.01.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/008965 A1

(51) International Patent Classification:
H04L 47/2441 (2022.01) *H04L 47/125* (2022.01)

(21) International Application Number:
PCT/IN2024/050952

(22) International Filing Date:
27 June 2024 (27.06.2024)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
202321044341 03 July 2023 (03.07.2023) IN

(71) Applicant: **JIO PLATFORMS LIMITED** [IN/IN]; OFFICE-101, SAFFRON, NR. CENTRE POINT, PANCHWATI 5 RASTA, AMBAWADI, GUJARAT, AHMEDABAD 380006 (IN).

(72) Inventors: **BHATNAGAR, Aayush**; Tower-7, 15B, Beverly Park, Sector-14 Koper Khairane, Maharashtra, Navi Mumbai 400701 (IN). **JHA, Adityakar**; 2 B1-305, G21 Avenue, Sector-83, Gurgaon, Haryana, Gurgaon 122 004 (IN). **RANJAN, Anu**; 3. S/O Kalendra Kumar Singh, Vill-Ghanshyamchak, Maheshpur, Bhagalpur, Bihar, Sanhoula 813205 (IN). **MALHOTRA, Pankaj**; 5/71 SUBHASH NAGAR, NEW DELHI, NEW DELHI 110027 (IN). **SENGUPTA, Swarup**; 5. I-1201A, The Coralwood, Sector 84, Gurgaon, Gurgaon 122004 (IN). **MAMGAIN, Ranjan**; 6. Flat No 35, Him Vihar Apartments, Plot No 8, I. P. Extension, Delhi, Patparganj 110092 (IN). **VASHISHTH, Yog**; 7. F-88A, FF, Sushant Lok 3, Sector 57, Haryana, Gurgaon 122001 (IN).

(74) Agent: **JAPHET, Chinthan**; K Law (Krishnamurthy and Co.), 4th Floor, Prestige Takt, No 23, Kasturba Road Cross, Bangalore, Bangalore 560 001 (IN).

(54) Title: SYSTEM AND METHOD FOR MANAGING FLOW RULES IN A NETWORK

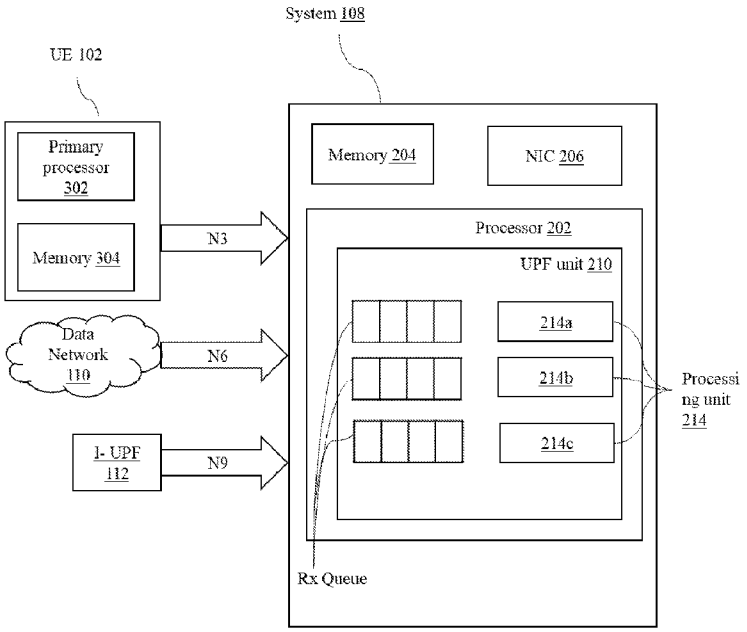


FIG. 3a

(57) Abstract: The present invention relates to method (400) and a system (108) for managing flow rules in a network (106) The method (400) includes step of creating of a plurality of flow rules utilizing at least one network interface unit. The plurality of flow rules includes at least one or more packet segregation rules and packet distribution rules. The method (400) further includes the step of applying one or more packet segregation rules for each of the received data packets to segregate the data packets and applying one or more packet distribution rules for each of the segregated data packets to distribute the data packets to a plurality of processing units based on a type of data packet pattern. Advantageously, the complexity and the repetition of the flow rules are minimized which results in concise implementation and obviates the need of defining multiple flow rules to resolve the conflicts.

WO 2025/008965 A1

[Continued on next page]

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

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, 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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

SYSTEM AND METHOD FOR MANAGING FLOW RULES IN A NETWORK

FIELD OF THE INVENTION

[0001] The present invention relates to the field of wireless communication system, more particularly relates to a system and method for managing flow rules in a network.

BACKGROUND OF THE INVENTION

[0002] A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. NIC is a circuit board installed in a computer that provides a dedicated network connection to the computer. NIC is also called network interface controller, network adapter or LAN adapter.

[0003] NIC allows both wired and wireless communications. NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP). NIC is both a physical layer and a data link layer device, i.e. NIC provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

[0004] An NIC provides a computer with a dedicated, full-time connection to a network. It implements the physical layer circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi. Each card represents a device and can prepare, transmit and control the flow of data on the network.

[0005] The IP 5-tuple identifies a Transmission Control Protocol (TCP)/IP connection and includes source IP address, source port, destination IP address, destination port, and transport protocol. A 5-tuple uniquely identifies a User Datagram Protocol (UDP)/TCP session. The NIC distributes packets by applying a filter to each packet that assigns it to one of a small number of logical flows. Packets for each flow are steered to a separate receive queue, which in turn can be processed by separate

Central Processing Units (CPUs). This mechanism is generally known as Receive Side Scaling (RSS). The goal of RSS and the other scaling techniques is to increase performance uniformly. Multi-queue distribution can also be used for traffic prioritization.

[0006] There are NICs which are capable of identifying the pattern. For example, a 2-tuple or 3 tuple may be used. Based upon the identified pattern, the NIC locates the information in the packet. Flow rules are required to be created for various patterns of the packet received on UPF data plane. For each and every possible pattern, flow rules are required to be defined and created.

[0007] To achieve high performance, high throughput processing and low latency, the UPF is generally designed on a multi-core CPU architecture. With multi-core CPU's, for optimal performance, it is desired that each of the CPU cores is equally loaded. This can be taken care of within the software. However, this requires a dedicated core that can be defined to receive the packets from the NIC hardware, and then further load distribute and assign them to rest of the cores for processing. This puts an undesired load on the core and consumes processor band width and uses the processor resources which could have been made available for the UPF packet processing tasks.

[0008] Besides, with flow rule definition in parallel for multiple interfaces like N3/N6/N9, and with N3 and N9 interfaces both using General Packet Radio Service Tunneling protocol (GTP) tunneled traffic, there is complexity in configuring the rules as the generic pattern matches for N3 and N9 conflict.

[0009] Therefore, there is a need for reducing the load on the core processor and optimization of the flow rules in a network which increases the processing speed and reduces the complexity of the rules and the memory required for storing the rules.

SUMMARY OF THE INVENTION

[0010] One or more embodiments of the present disclosure provide a method and system for managing flow rules in a network.

[0011] In one aspect of the present invention, a system for managing flow rules in a network is disclosed. The system includes a plurality of data packet sources and a User Plane Function (UPF) unit in communication with each of the plurality of data packet sources via a plurality of interface units. The UPF unit is configured to receive data packets from a plurality of data packet sources via a plurality of interface units. The UPF unit is further configured to create a plurality of flow rules utilizing at least one network interface unit, wherein the plurality of flow rules includes at least one or more packet segregation rules and packet distribution rules. The UPF unit is further configured to apply one or more packet segregation rules for each of the received data packets to segregate the data packets subsequent to satisfying one or more predefined conditions. The UPF unit is further configured to apply one or more packet distribution rules for each of the segregated data packets to distribute the data packets to a plurality of processing units based on a type of data packet pattern.

[0012] In one embodiment, the plurality of interface units includes at least one of, N3 interface, N6 interface and N9 interface.

[0013] In another embodiment, the plurality of data packet sources includes at least one of, User Equipment (UE), data network and Intermediate User Plane function (I-UPF).

[0014] In yet another embodiment. the UE is in communication with the UPF unit via the N3 interface, the data network is in communication with the UPF via the N6 interface and I-UPF is in communication with the UPF unit via the N9 interface.

[0015] In yet another embodiment, the packet segregation rules are arranged in a primary table.

[0016] In yet another embodiment, the UPF unit is further configured to route the data packet to one or more secondary tables from the primary table upon satisfying the one or more pre-defined conditions, the one or more pre-defined conditions are satisfied when a Virtual Local Area Network (VLAN) ID of the data packet corresponds to at least one of the plurality of interface units.

[0017] In yet another embodiment, the UPF unit is configured to equally distribute the data packets from at least one or more secondary tables to a plurality of processing units subsequent to satisfying the one or more pre-defined conditions utilizing the one or more packet distribution rules.

[0018] In yet another embodiment, the network interface unit is at least one of, a Network Interface Card (NIC).

[0019] In yet another embodiment, the plurality of flow rules includes one or more packet segregation rules and one or more packet distribution rules, the one or more packet segregation rules pertain to segregating the data packets based on receiving the data packets via a specific interface unit from the available plurality of interface units, and the one or more packet distribution rules pertain to distributing the data packets to a plurality of processing units based on load distribution.

[0020] In yet another embodiment, the plurality of flow rules are created for the data packets related to the type of data packet patterns using one or more features of the network interface unit, wherein the type of data packet patterns includes at least one of, Ethernet, Virtual Local Area Network (VLAN)-Id, Internet Protocol version 4 ((IP)v4)/ Internet Protocol version 6 (IPv6), General Packet Radio Service Tunneling protocol (GTP), Transaction Protocol Data Unit (TPDU), Internet Protocol (IP)/Subnet, GTP with and without Primary scrambling code (PSCs), Differentiated Services Code Point (DSCP) and Quality of Service Flow Identifier (QFI) marking

[0021] In another aspect of the present invention, a method for managing flow rules in a network is disclosed. The method includes the step of receiving data packets from

a plurality of data packet sources via a plurality of interface units. The method further includes the step of creating, a plurality of flow rules utilizing at least one network interface unit, wherein the plurality of flow rules includes at least one or more packet segregation rules and packet distribution rules. The method further includes the step of applying one or more packet segregation rules for each of the received data packets to segregate the data packets subsequent to satisfying one or more predefined conditions. The method further includes the step of applying one or more packet distribution rules for each of the segregated data packets to distribute the data packets to a plurality of processing units based on a type of data packet pattern.

[0022] Other features and aspects of this invention will be apparent from the following description and the accompanying drawings. The features and advantages described in this summary and in the following detailed description are not all-inclusive, and particularly, many additional features and advantages will be apparent to one of ordinary skill in the relevant art, in view of the drawings, specification, and claims hereof. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes and may not have been selected to delineate or circumscribe the inventive subject matter, resort to the claims being necessary to determine such inventive subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023] The accompanying drawings, which are incorporated herein, and constitute a part of this disclosure, illustrate exemplary embodiments of the disclosed methods and systems in which like reference numerals refer to the same parts throughout the different drawings. Components in the drawings are not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the present disclosure. Some drawings may indicate the components using block diagrams and may not represent the internal circuitry of each component. It will be appreciated by those skilled in the art that disclosure of such drawings includes disclosure of electrical

components, electronic components or circuitry commonly used to implement such components.

[0024] **FIG. 1** is an exemplary block diagram of an environment for managing flow rules in a network, according to one or more embodiments of the present invention;

[0025] **FIG. 2** is an exemplary block diagram of the system for managing flow rules in a network, according to one or more embodiments of the present invention;

[0026] **FIG. 3a** is an exemplary flow diagram of the system of **FIG. 2**, according to one or more embodiments of the present invention; and

[0027] **FIG. 4** is a flow diagram of a method for managing flow rules in a network**,** according to one or more embodiments of the present invention.

[0028] The foregoing shall be more apparent from the following detailed description of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0029] Some embodiments of the present disclosure, illustrating all its features, will now be discussed in detail. It must also be noted that as used herein and in the appended claims, the singular forms "a", "an" and "the" include plural references unless the context clearly dictates otherwise.

[0030] Various modifications to the embodiment will be readily apparent to those skilled in the art and the generic principles herein may be applied to other embodiments. However, one of ordinary skill in the art will readily recognize that the present disclosure including the definitions listed here below are not intended to be limited to the embodiments illustrated but is to be accorded the widest scope consistent with the principles and features described herein.

[0031] A person of ordinary skill in the art will readily ascertain that the illustrated steps detailed in the figures and here below are set out to explain the exemplary

embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments.

[0032] The present invention provides a system and method for managing flow rules in a network. The system utilizes the underlying Network Interface Card (NIC) feature for creation of plurality of flow rules which includes at least one or more packet segregation rules and packet distribution rules. The system normalizes and simplifies these flow rules by providing a primary table and one or more secondary tables. The present invention offers advantages which include avoiding the repetition of the flow rules and thus complexity in the rules is minimized.

[0033] Referring to **FIG. 1**, **FIG. 1** illustrates an exemplary block diagram of an environment **100** for managing flow rules in a network **106**, according to one or more embodiments of the present invention. The environment **100** includes, a User Equipment (UE) **102**, a server **104**, a network **106,** a system **108,** a data network **110** and an Intermediate User Plane function (I-UPF)**112**.

[0034] For the purpose of description and explanation, the description will be explained with respect to one or more user equipment's (UEs) **102**, or to be more specific will be explained with respect to a first UE **102a**, a second UE **102b**, and a third UE **102c**, and should nowhere be construed as limiting the scope of the present disclosure. Each of the at least one UE **102** namely the first UE **102a**, the second UE

102b, and the third UE **102c** is configured to connect to the server **104** via the network **106**.

[0035] In an embodiment, each of the first UE **102a**, the second UE **102b**, and the third UE **102c** is one of, but not limited to, any electrical, electronic, electro-mechanical or an equipment and a combination of one or more of the above devices such as virtual reality (VR) devices, augmented reality (AR) devices, laptop, a computer, desktop, personal digital assistant, tablet computer, mainframe computer, or any other computing device.

[0036] The network **106** includes, by way of example but not limitation, one or more of a wireless network, a wired network, an internet, an intranet, a public network, a private network, a packet-switched network, a circuit-switched network, an ad hoc network, an infrastructure network, a Public-Switched Telephone Network (PSTN), a cable network, a cellular network, a satellite network, a fiber optic network, or some combination thereof. The network **106** may include, but is not limited to, a Third Generation (3G), a Fourth Generation (4G), a Fifth Generation (5G), a Sixth Generation (6G), a New Radio (NR), a Narrow Band Internet of Things (NB-IoT), an Open Radio Access Network (O-RAN), and the like.

[0037] The network **106** may also include, by way of example but not limitation, at least a portion of one or more networks having one or more nodes that transmit, receive, forward, generate, buffer, store, route, switch, process, or a combination thereof, etc. one or more messages, packets, signals, waves, voltage or current levels, some combination thereof, or so forth. The network **106** may also include, by way of example but not limitation, one or more of a wireless network, a wired network, an internet, an intranet, a public network, a private network, a packet-switched network, a circuit-switched network, an ad hoc network, an infrastructure network, a Public-Switched Telephone Network (PSTN), a cable network, a cellular network, a satellite network, a fiber optic network, a VOIP or some combination thereof.

[0038] The environment **100** includes the server **104** accessible via the network **106**. The server **115** may include by way of example but not limitation, one or more of a standalone server, a server blade, a server rack, a bank of servers, a server farm, hardware supporting a part of a cloud service or system, a home server, hardware running a virtualized server, a processor executing code to function as a server, one or more machines performing server-side functionality as described herein, at least a portion of any of the above, some combination thereof. In an embodiment, the entity may include, but is not limited to, a vendor, a network operator, a company, an organization, a university, a lab facility, a business enterprise side, a defence facility side, or any other facility that provides service.

[0039] The environment **100** further includes a system **108** communicably coupled to the server **104** and each of the first UE **102a**, the second UE **102b**, and the third UE **102c** via the network **106**. The system **108** is adapted to be embedded within the server **104** or is embedded as the individual entity. However, for the purpose of description, the system **108** is described as an integral part of the server **104**, without deviating from the scope of the present disclosure. The system **108** is configured to manipulate message in the network **106**.

[0040] The data network **110** includes, by way of example but not limitation, one or more of a wireless network, a wired network, an internet, an intranet, a public network, a private network, a packet-switched network, a circuit-switched network, an ad hoc network, an infrastructure network, a Public-Switched Telephone Network (PSTN), a cable network, a cellular network, a satellite network, a fiber optic network, or some combination thereof. The network **106** may include, but is not limited to, a Third Generation (3G), a Fourth Generation (4G), a Fifth Generation (5G), a Sixth Generation (6G), a New Radio (NR), a Narrow Band Internet of Things (NB-IoT), an Open Radio Access Network (O-RAN), and the like.

[0041] The environment **100** further includes an Intermediate User Plane function (I-UPF) **112** communicably coupled to the system **108**. An I-UPF **112** performs the

role of an uplink classifier and communicates with the system **108** over the N9 interface.

[0042] Operational and construction features of the system **108** will be explained in detail with respect to the following figures.

[0043] **FIG. 2** is an exemplary block diagram of the system **108** for managing flow rules in a network **106**, according to one or more embodiments of the present invention.

[0044] As per the illustrated and preferred embodiment, the system **108** to manage flow rules in the network **106** is a User Plane function (UPF). The system **108** supports features and capabilities to facilitate a user plane operation. In order for the system **108** to manage flow rules in the network **106**, the system **108** includes one or more processors **202**, a memory **204**, and a Network Interface Card (NIC) **206.** The one or more processors **202** includes a User Plane Function (UPF) unit **210**. The one or more processors **202**, hereinafter referred to as the processor **202**, may be implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, state machines, logic circuitries, single board computers, and/or any devices that manipulate signals based on operational instructions. However, it is to be noted that the system **108** may include multiple processors as per the requirement and without deviating from the scope of the present disclosure. Among other capabilities, the processor **202** is configured to fetch and execute computer-readable instructions stored in the memory **204**.

[0045] As per the illustrated embodiment, the processor **202** is configured to fetch and execute computer-readable instructions stored in the memory **204** as the memory **204** is communicably connected to the processor **202**. The memory **204** is configured to store one or more computer-readable instructions or routines in a non-transitory computer-readable storage medium, which may be fetched and executed to create or share data packets over a network service. The memory **204** may include any non-

transitory storage device including, for example, volatile memory such as RAM, or non-volatile memory such as disk memory, EPROMs, FLASH memory, unalterable memory, and the like.

[0046] In an embodiment, the User Plane Function (UPF) unit **210** of the processor **202** is communicably connected with each of the plurality of data packet sources via a plurality of interface units which supports features and capabilities to facilitate user plane operation. The plurality of data packet sources includes at least one of, User Equipment (UE) **102** such as at least first UE **102a**, the second UE **102b**, and the third UE **102c**, data network **110** and Intermediate User Plane function (I-UPF) **112**. In one embodiment, the plurality of interface units includes at least one of, but not limited to, N3 interface, N6 interface and N9 interface. The UE **102** is in communication with the UPF unit **210** via the N3 interface, the data network **110** is in communication with the UPF unit **210** via the N6 interface and I-UPF **112** is in communication with the UPF unit **210** via the N9 interface. The UPF unit **210** of the processor **202** includes plurality of processing units **214** associated with the Rx queues.

[0047] The N3 interface is for communication between Next-Generation NodeB (gNB) and the UPF unit **210**. The N3 interface is primarily used for exchanging user plane traffic between the gNB and the UPF unit **210** which includes forwarding of data packets between a radio access network and a core network. The N6 interface is an interface which provides the communication between the UPF unit **210** and the at least one of, an external or an internal network such as the data network **110**, a service platform, such as an internet, a public cloud or a private cloud. The N6 interface forwards the data packets from the data network **110** to the UPF unit **210**. The N9 interface is the interface between the two UPFs such as the UPF unit **210** and the I-UPF **112**. The N9 interface is used for forwarding data packets from the I-UPF **112** to the UPF unit **210**.

[0048] Accordingly, the UPF unit **210** is configured to receive data packets from the plurality of data packet sources via the plurality of interface units. The UPF unit

210 is further configured to create a plurality of flow rules utilizing at least one network interface unit such as NIC **206**. The NIC **206** is a hardware component, typically a circuit board or a chip, installed in the system **108** in order to connect the UPF unit **210** to the network **106**. Modern NICs provide functionality to the system **108**, such as support for an input/output interrupt, a direct-memory access interfaces, data transmission, a network traffic engineering and partitioning. In one embodiment, the plurality of flow rules includes at least one or more packet segregation rules and packet distribution rules. The UPF unit **210** is further configured to apply one or more packet segregation rules for each of the received data packets to segregate the data packets subsequent to satisfying one or more predefined conditions. The UPF unit **206** is further configured to apply one or more packet distribution rules for each of the segregated data packets to distribute the data packets to a plurality of processing units **214** of the UPF unit **210** based on a type of data packet pattern.

[0049] In one embodiment, the one or more packet segregation rules are rules to segregate one or more packets received at the UPF unit **210** from the at least one of the UE **102**, the data network **110** and the I-UPF **112** via the specific interface units. In one embodiment, the one or more packet distribution rules are rules to distribute the segregated data packets to the plurality of processing units **214** of the UPF unit **210**.

[0050] In one embodiment, the primary table is a list which specifies packet segregation rules (for example, by Rule ID 1, 2, 3, etc.) and the one or more secondary tables includes an alternate list of the one or more packet distribution rules (for example, type of data packet pattern) which are used to distribute the segregated data packets to the plurality of processing units **214** of the UPF unit **210.**

[0051] Initially, at least one of the processing units **214** of the UPF unit **210** were dedicated to receive the packets from the NIC **206** hardware, and then the at least one of the processing units **214** is further configured to distribute load of the packets to rest of the processing units **214** for packet processing tasks. In this invention, the system **108** provides offloading the functionality of distributing load of the packets to

the hardware NIC **214**, so that the processing units **214** can be saved and optimally utilized for the packet processing tasks. Advantageously, the computational cost of the packet processing tasks like load balancing gets offloaded to the NIC. Further, efficient load distribution among the plurality of the processing units **214** is also achieved.

[0052] The NIC **206,** and the UPF unit **210** in an exemplary embodiment, are implemented as a combination of hardware and programming (for example, programmable instructions) to implement one or more functionalities of the processor **202**. In the examples described herein, such combinations of hardware and programming may be implemented in several different ways. For example, the programming for the processor **202** may be processor-executable instructions stored on a non-transitory machine-readable storage medium and the hardware for the processor may comprise a processing resource (for example, one or more processors), to execute such instructions. In the present examples, the memory **204** may store instructions that, when executed by the processing resource, implement the processor **202**. In such examples, the system **108** may comprise the memory **204** storing the instructions and the processing resource to execute the instructions, or the memory **204** may be separate but accessible to the system **108** and the processing resource. In other examples, the processor **202** may be implemented by electronic circuitry.

[0053] **FIG. 3a** illustrates an exemplary block diagram of an architecture for the system **108** of **FIG. 2,** according to one or more embodiments of the present invention. **FIG. 3b** illustrates an exemplary primary table and one or more secondary tables. More specifically, **FIG. 3** illustrates the system **108** configured for managing flow rules in the network **106**. It is to be noted that the embodiment with respect to **FIG. 3a** and **FIG. 3b** will be explained with respect to plurality of data packet sources for the purpose of description and illustration and should nowhere be construed as limited to the scope of the present disclosure. The **FIG. 3** includes the system **108** and the plurality of data packet sources such as UE **102,** the data network **110**, the I-UPF **112**.

[0054] For the purpose of description of the exemplary embodiment as illustrated in **FIG. 3**, the plurality of data packet sources communicates with the system **108** via the plurality of interface units including at least one of, N3 interface, N6 interface and N9 interface. For example, the data packets received at the system **108** are transmitted by at least one of the data packet sources which includes the UE **102** via the N3 interface**,** the data network **110** via the N6 interface, and the I-UPF **112** via the N9 interface, respectively. , .

[0055] In an embodiment, the UE **102** includes a primary processor **302**, and a memory **304**. In alternate embodiments, the UE **102** may include more than one primary processor **302** as per the requirement of the network **106**. The primary processor **302**, may be implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, state machines, logic circuitries, single board computers, and/or any devices that manipulate signals based on operational instructions.

[0056] In an embodiment, the primary processor **302** is configured to fetch and execute computer-readable instructions stored in the memory **304**. The memory **304** may be configured to store one or more computer-readable instructions or routines in a non-transitory computer-readable storage medium, which may be fetched and executed to create or share data packets over a network **106**. The memory **304** may include any non-transitory storage device including, for example, volatile memory such as RAM, or non-volatile memory such as disk memory, EPROMs, FLASH memory, unalterable memory, and the like.

[0057] Initially the data packets are received at system **108** from at least one of the plurality of data packet sources via the plurality of interface units. Based on the plurality of data packets received at the system **108**, the plurality of flow rules are required to be created by the system **108** utilizing at least one network interface unit (NIC) **206**. In an embodiment, the system **108** uses underlying NIC's feature for creation of flow rules. Flow rules are required to be created related to the interface

units and various patterns of the data packet received on system **108**. In order to avoid conflicts of pattern matches for interface units like N3 and N9, flow rules are created related to the interface units. For example, the data packets are received at the system **108** via the N3 and the N9 interfaces both using GPRS Tunnelling Protocol (GTP) tunneled traffic pattern, then there is complexity in configuring the rules as the pattern matches for N3 and N9 interfaces. The GPRS Tunnelling Protocol (GTP) is a group of IP-based communications protocols which are used to carry data packets within a Global System for Mobile Communication (GSM), a Universal Mobile Telecommunications System (UMTS), a Long-Term Evolution (LTE) and 5G radio networks. The traffic tunneling is a port redirection technique in which the network data packet traffic is received at one port and forwarded to another port. The plurality of flow rules created by the system **108** includes one or more packet segregation rules and one or more packet distribution rules. The one or more packet distribution rules pertain to distributing the data packets to a plurality of processing units **214** based on load of the data packets.

[0058] The packet segregation rules are arranged in a primary table as shown in **FIG. 3b**. The one or more packet segregation rules pertains to segregating the data packets based on receiving the data packets via a specific interface unit from the available plurality of interface units. For example, the data packets received by system **108** are segregated based on the plurality of interface units. Further based on the interface specific VLAN, the traffic pertaining to data packets are moved to the one or more secondary tables denoted as Jump Table 1 and Jump Table 2. For example, Rule 1 in the primary table relates to VLAN ID = N3_VLAN, then traffic flow pertaining to the data packets moves or routes to the secondary table 1 and for VLAN ID = N9_VLAN, then traffic flow moves to the secondary table 2. In an alternate embodiment, the plurality of flow rules are not limited to one primary table and two secondary tables. In another alternate embodiment, the system **108** may create more levels of tables after the secondary table as well so as to form a chain of tables.

[0059] Further, the system **108** utilizes NIC **206** in order to equally distribute the traffic pertaining to the data packets to the multiple Rx queues of the plurality of processing units **214** based on the one or more packet distribution rules and the type of the data packet pattern. The type of data packet pattern includes at least one of, Ethernet, Virtual Local Area Network (VLAN)-Id, Internet Protocol version 4 (IPv4)/ Internet Protocol version 6 (IPv6), General Packet Radio Service Tunneling protocol (GTP), Transaction Protocol Data Unit (TPDU), Internet Protocol (IP)/Subnet, GTP with and without Primary scrambling code (PSCs), Differentiated Services Code Point (DSCP) and Quality of Service Flow Identifier (QFI) marking. For example, the secondary table 1 includes Rule 1 that denotes action for the data packet pattern GTP/IP (SRC IP) such as Receive side scaling (RSS) on inner Source IP. The Source IP (SRC IP) address is the IP packet field containing the IP address of at least one of, the UE **102,** the data network **110**, and the I-UPF **112** from which the data packet is transmitted using the GTP. The RSS has an important role in deciding the criteria for distributing the traffic of the data packets over Rx queues of the plurality of processing units **214.** The RSS is a network driver technology that enables the efficient distribution of the traffic of the data packets across multiple processing units **214** in the system **108**.

[0060] In one embodiment, the one or more packet distribution rules pertain to distributing the data packets to the plurality of processing units **214** based on load distribution task done by the system **108** utilizing the NIC **206**. The NIC **206** equally distributes load pertaining to the traffic of data packets among each of the plurality of processing units **214a**, **214b** and **214c**. The system **108** enables NIC **206** for traffic distribution and a load balancing task which consequently contributes towards achieving an optimal performance of the system **108**.

[0061] In one embodiment, the data packets are distributed to the plurality of processing units **214** using the inner SRC IP and an Inner Destination IP (DST IP). The inner SRC IP and the inner DST IP includes the IP addresses for various units/modules included in the network **106**. In particular, an inner IP address is

specific to the network **106** which is used for communicating within the various units/modules of that network **106**.

[0062] **FIG. 4** is a flow diagram of a method **400** for managing flow rules in a network **106**, according to one or more embodiments of the present invention. For the purpose of description, the method **400** is described with the embodiments as illustrated in **FIG. 2** and should nowhere be construed as limiting the scope of the present disclosure.

[0063] At step **402**, the method **400** includes the step of receiving data packets from the plurality of data packet sources via the plurality of interface units. In one embodiment, UPF unit **210** of the processor **202** is configured to receive data packets from the plurality of data packet sources which includes at least one of, User Equipment (UE) **102,** data network **110** and I-UPF **112** via the plurality of interface units including at least one of, but not limited to, N3 interface, N6 interface and N9 interface.

[0064] At step **404**, the method **400** includes the step of creating a plurality of flow rules utilizing at least one network interface unit (NIC) **206**. In one embodiment, the UPF unit **210** of the processor **202** is configured to create the plurality of flow rules utilizing at least one underlying feature of the NIC **206**. The plurality of flow rules governs how the received data packets shall be handled and steered in the system **108**. The plurality of flow rules includes at least one or more packet segregation rules and packet distribution rules. The packet segregation rules are arranged in the primary table and one or more secondary tables. For example, the primary table specifies packet segregation rules (for example, by Rule ID 1, 2, 3, etc.) on the basis of the interface specific VLAN's. The packet distribution rules are created related to distributing the load of the data packets to the plurality of processing units **214** based on the type of data packet patterns. The arrangement of the packet segregation rules and the packet distribution rules in the table format results in a concise implementation by obviating the need of defining multiple specific flow rules, allowing each flow rule

to work independently, minimizing the repetition of flow rules and minimizing the complexity of the flow rules.

[0065] At **406**, the method **400** includes the step of applying one or more packet segregation rules for each of the received data packets to segregate the data packets subsequent to satisfying one or more predefined conditions. In one embodiment, UPF unit **210** of the processor **202** is configured to apply one or more packet segregation rules for each of the received data packets to segregate the data packets subsequent to satisfying one or more predefined conditions. The one or more predefined conditions includes segregating the data packets based on received data packets via a specific interface unit from the available plurality of interface units. For example, the data packets received from the N3 interface, N6 interface and N9 interface are segregated and are added to the primary table. Further, the data packets are routed to the one or more secondary tables from the primary table upon satisfying the one or more pre-defined conditions when a Virtual Local Area Network (VLAN) ID of the data packet corresponds to at least one of the plurality of interface units. For example, Rule 1 in the primary table relates to VLAN ID = N3_VLAN, then traffic flow pertaining to the data packets moves to the secondary table 1 and for VLAN ID = N9_VLAN, then traffic flow moves to secondary table 2.

[0066] At **408**, the method **400** includes the step of applying one or more packet distribution rules for each of the segregated data packets to distribute the data packets to a plurality of processing units based on the type of data packet pattern. For example, the type of the data packet pattern includes at least one of, but not limited to, GTP/IP (SRC IP) and GTP+PSC/IP (DST IP). The GTP+PSC/IP (DST IP) is the at least one type of the data packet pattern which provides the information such as the data packet is received by the UPF unit **210** via the GTP along with the Primary Synchronization Code (PSC) and the Destination IP address (DST IP) of a recipient of this specific data packet. In one embodiment, the UPF unit **210** of the processor **202** utilizing the NIC **206** is configured to equally distribute the data packets from the at least one or more secondary tables to the plurality of processing units **214** subsequent to satisfying the

one or more pre-defined conditions utilizing the one or more packet distribution rules. The one or more predefined conditions includes identifying the data packet pattern of the segregated data packets and then distributing the traffic of the segregated data packets to the plurality of processing units **214** based on the type of data packet pattern which includes at least one of, Ethernet, Virtual Local Area Network (VLAN)-Id, Internet Protocol version 4 (IPv4)/ Internet Protocol version 6 (IPv6), General Packet Radio Service Tunneling protocol (GTP), Transaction Protocol Data Unit (TPDU), Internet Protocol (IP)/Subnet, GTP with and without Primary scrambling code (PSCs), Differentiated Services Code Point (DSCP) and Quality of Service Flow Identifier (QFI) marking.

[0067] In an alternate embodiment, the traffic of the segregated data packet is distributed into multiple Rx queues of the corresponding plurality of processing units **214** due to which each of the plurality of processing units **214** are able to receive traffic independently.

[0068] The present invention further discloses a non-transitory computer-readable medium having stored thereon computer-readable instructions. The computer-readable instructions are executed by the processor **202**. The processor **202** is configured to receive data packets from the plurality of data packet sources via the plurality of interface units. The processor **202** is further configured to create a plurality of flow rules utilizing at least one network interface unit, the plurality of flow rules includes at least one or more packet segregation rules and packet distribution rules. The processor **202** is further configured to apply one or more packet segregation rules for each of the received data packets to segregate the data packets subsequent to satisfying one or more predefined conditions. The processor **202** is further configured to apply one or more packet distribution rules for each of the segregated data packets to distribute the data packets to a plurality of processing units **214** based on a type of data packet pattern.

[0069] A person of ordinary skill in the art will readily ascertain that the illustrated embodiments and steps in description and drawings (FIG.1-4) are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments.

[0070] The present disclosure provides technical advancement of offloading the flow rule processing to the NIC (206). Further, the processing units (214) are saved and optimally utilized for the packet processing tasks. Further, the computational cost of tasks like load balancing gets offloaded to the NIC (206). Further, efficient load distribution is also achieved by utilizing NIC (206) for distribution of packets. The invention provides concise implementation and reduces the number of flow rules to be defined. This also allows each flow group to work independently. There is no repetition of flow rules and thus the complexity of the rules decreases.

[0071] The present invention offers multiple advantages over the prior art and the above listed are few examples to emphasize on some of the advantageous features. The listed advantages are to be read in a non-limiting manner.

REFERENCE NUMERALS

[0072] Environment - 100;

[0073] User Equipment (UE) - 102;

[0074] Server - 104;

[0075] Network- 106;

[0076] System -108;

[0077] Data Network – 110;

[0078] I-UPF – 112;

[0079] Processor - 202;

[0080] Memory - 204;

[0081] NIC – 206;

[0082] UPF units – 210;

[0083] Processing units – 214

[0084] Primary processor – 302;

[0085] Memory – 304;

We Claim:

1. A system (108) for managing flow rules in a network (106), the system (108) comprising:

a plurality of data packet sources; and

a User Plane Function (UPF) unit (210) in communication with each of the plurality of data packet sources via a plurality of interface units, wherein the UPF unit (210) is configured to:

receive, data packets from the plurality of data packet sources via the plurality of interface units;

create, a plurality of flow rules utilizing at least one network interface unit (206), wherein the plurality of flow rules includes at least one or more packet segregation rules and packet distribution rules;

apply, one or more packet segregation rules for each of the received data packets to segregate the data packets subsequent to satisfying one or more predefined conditions; and

apply, one or more packet distribution rules for each of the segregated data packets to distribute the data packets to a plurality of processing units (214) based on a type of data packet pattern.

2. The system (108) as claimed in claim 1, wherein the plurality of interface units includes at least one of, N3 interface, N6 interface and N9 interface.

3. The system (108) as claimed in claim 1, wherein the plurality of data packet sources includes at least one of, User Equipment (UE) (102), data network (110) and Intermediate User Plane function (I-UPF) (112).

4. The system (108) as claimed in claim 3, wherein the UE (102) is in communication with the UPF unit (210) via the N3 interface, the data network (110) is in communication with the UPF unit (210) via the N6 interface and I-UPF (112) is in communication with the UPF unit (210) via the N9 interface.

5. The system (108) as claimed in claim 1, wherein the packet segregation rules are arranged in a primary table.

6. The system (108) as claimed in claim 5, wherein the UPF unit (210) is configured to:

route the data packet to one or more secondary tables from the primary table upon satisfying the one or more pre-defined conditions, wherein the one or more pre-defined conditions are satisfied when a Virtual Local Area Network (VLAN) ID of the data packet corresponds to at least one of the plurality of interface units.

7. The system (108) as claimed in claim 6, wherein the UPF unit (210) is configured to equally distribute the data packets from at least one or more secondary tables to a plurality of processing units subsequent to satisfying the one or more pre-defined conditions utilizing the one or more packet distribution rules.

8. The system (108) as claimed in claim 1, wherein the network interface unit (206) is at least one of, a Network Interface Card (NIC).

9. The system (108) as claimed in claim 1, wherein the plurality of flow rules includes one or more packet segregation rules and one or more packet distribution rules, the one or more packet segregation rules pertain to segregating the data packets based on receiving the data packets via a specific interface unit from the available plurality of interface units, and the one or more packet distribution rules pertain to distributing the data packets to a plurality of processing units (214) based on load distribution.

10. The system (108) as claimed in claim 1, wherein the plurality of flow rules are created for the data packets related to the type of data packet patterns using one or more features of the network interface unit, wherein the type of data packet patterns includes at least one of, Ethernet, Virtual Local Area Network (VLAN)-Id, Internet Protocol version 4 (IPv4)/ Internet Protocol version 6 (IPv6), General Packet Radio Service Tunneling protocol (GTP), Transaction Protocol Data Unit (TPDU), Internet Protocol (IP)/Subnet, GTP with and without Primary scrambling code (PSCs), Differentiated Services Code Point (DSCP) and Quality of Service Flow Identifier (QFI) marking.

11. A method (400) for managing flow rules in a network (106), the method (400) comprises the steps of:

receiving, by one or more processors (202), data packets from a plurality of data packet sources via a plurality of interface units;

creating, by the one or more processors (202), a plurality of flow rules utilizing at least one network interface unit (206), wherein the plurality of flow rules includes at least one or more packet segregation rules and packet distribution rules;

applying, by the one or more processors (202), one or more packet segregation rules for each of the received data packets to segregate the data packets subsequent to satisfying one or more predefined conditions; and

applying, by the one or more processors (202), one or more packet distribution rules for each of the segregated data packets to distribute the data packets to a plurality of processing units (214) based on a type of data packet pattern.

12. The method (400) as claimed in claim 11, wherein the plurality of interface units includes at least one of, N3 interface, N6 interface and N9 interface.

13. The method (400) as claimed in claim 11, wherein the plurality of data packet sources includes at least one of, User Equipment (UE) (102), data network (110) and Intermediate User Plane function (I-UPF) (112).

14. The method (400) as claimed in claim 13, wherein the UE (102) is in communication with the one or more processors (202)via the N3 interface, the data network (110) is in communication with the one or more processors (202) via the N6 interface and I-UPF (212) is in communication with the one or more processors (202)via the N9 interface.

15. The method (400) as claimed in claim 11, wherein the packet segregation rules are arranged in a primary table.

16. The method (400) as claimed in claim 15, wherein the one or more processors (202) is configured to:

route the data packet to one or more secondary tables from the primary table upon satisfying the one or more pre-defined conditions, wherein the one or more pre-defined conditions are satisfied when a Virtual Local Area Network (VLAN) ID of the data packet corresponds to at least one of the plurality of interface units.

17. The method (400) as claimed in claim 16, wherein the one or more processors (202) is configured to equally distribute the data packets from at least one or more secondary tables to a plurality of processing units (214) subsequent to satisfying the one or more pre-defined conditions utilizing the one or more packet distribution rules.

18. The method (400) as claimed in claim 11, wherein the network interface unit (206) is at least one of, a Network Interface Card (NIC).

19. The method (400) as claimed in claim 11, wherein the plurality of flow rules includes one or more packet segregation rules and one or more packet distribution rules, the one or more packet segregation rules pertain to segregating the data packets based on receiving the data packets via a specific interface unit from the available plurality of interface units, and the one or more packet distribution rules pertain to distributing the data packets to a plurality of processing units (214) based on load distribution.

20. The method (400) as claimed in claim 11, wherein the plurality of flow rules are created for the data packets related to the type of data packet patterns using one or more features of the network interface unit, wherein the type of data packet patterns includes at least one of, Ethernet, Virtual Local Area Network (VLAN)-Id, Internet Protocol version 4 (IPv4)/ Internet Protocol version 6 (IPv6), General Packet Radio Service Tunneling protocol (GTP), Transaction Protocol Data Unit (TPDU), Internet Protocol (IP)/Subnet, GTP with and without Primary scrambling code (PSCs), Differentiated Services Code Point (DSCP) and Quality of Service Flow Identifier (QFI) marking.

21. A non-transitory computer-readable medium having stored thereon computer-readable instructions that, when executed by a processor (502), causes the processor (502) to:

receive, data packets from the plurality of data packet sources via the plurality of interface units;

create, a plurality of flow rules utilizing at least one network interface unit (206), wherein the plurality of flow rules includes at least one or more packet segregation rules and packet distribution rules;

apply, one or more packet segregation rules for each of the received data packets to segregate the data packets subsequent to satisfying one or more predefined conditions; and

apply, one or more packet distribution rules for each of the segregated data packets to distribute the data packets to a plurality of processing units (214) based on a type of data packet pattern.

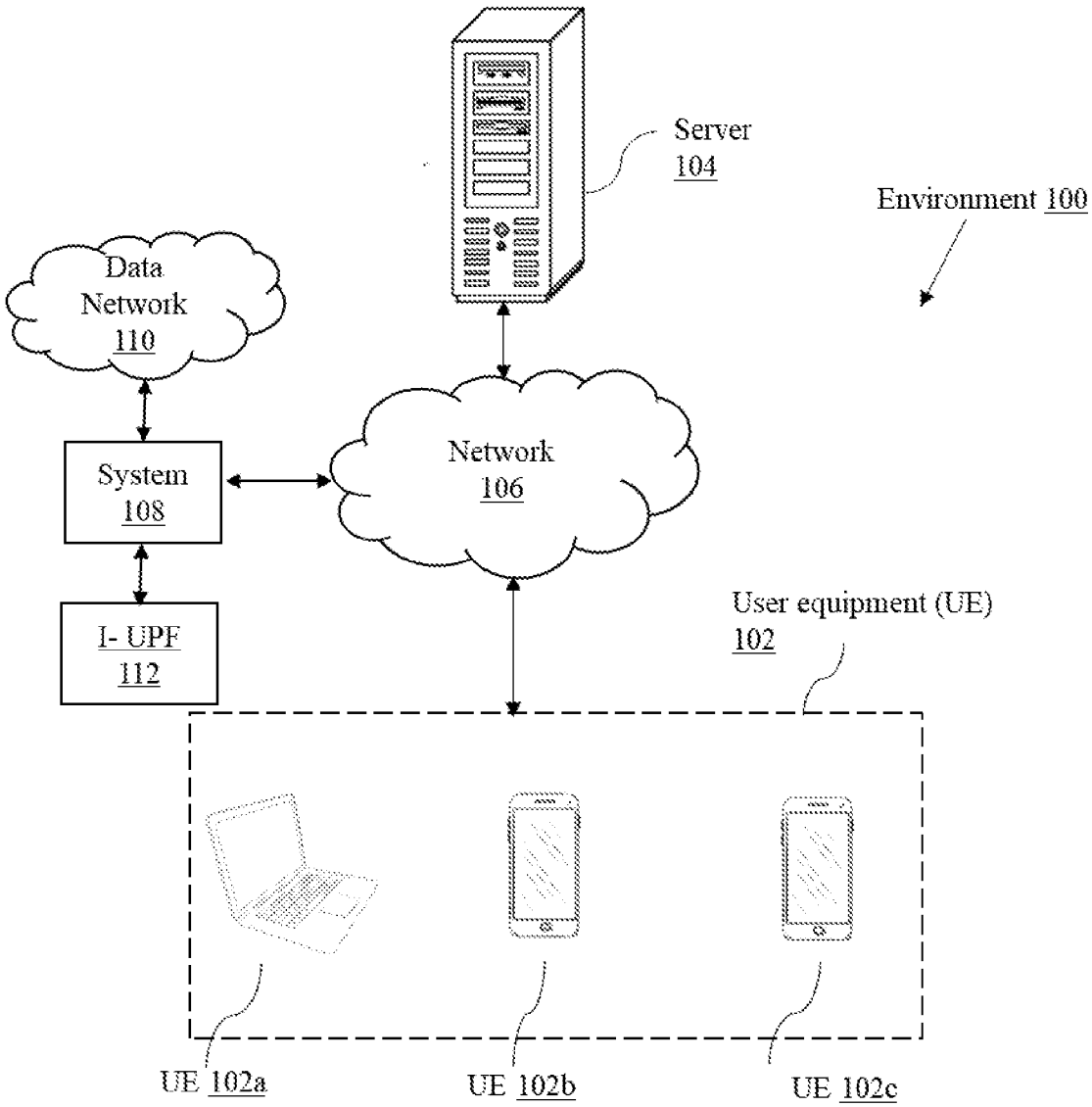

Server
104
Environment 100
Data
Network
110
System
108
Network
106
I- UPF
112
User equipment (UE)
102
UE 102a
UE 102b
UE 102c

FIG. 1

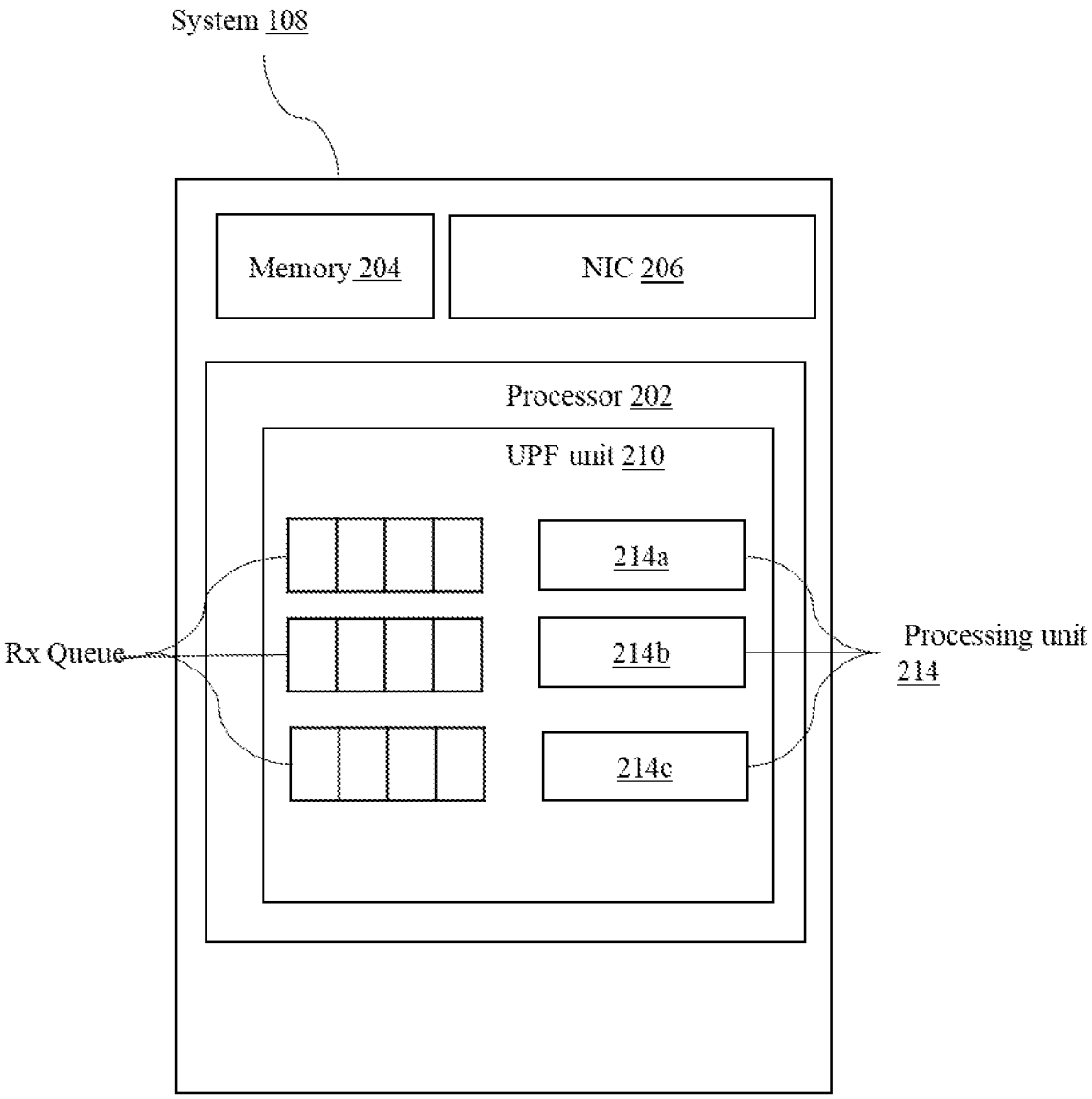

System 108
Memory 204
NIC 206
Processor 202
UPF unit 210
214a
214b
214c
Rx Queue
Processing unit 214

FIG. 2

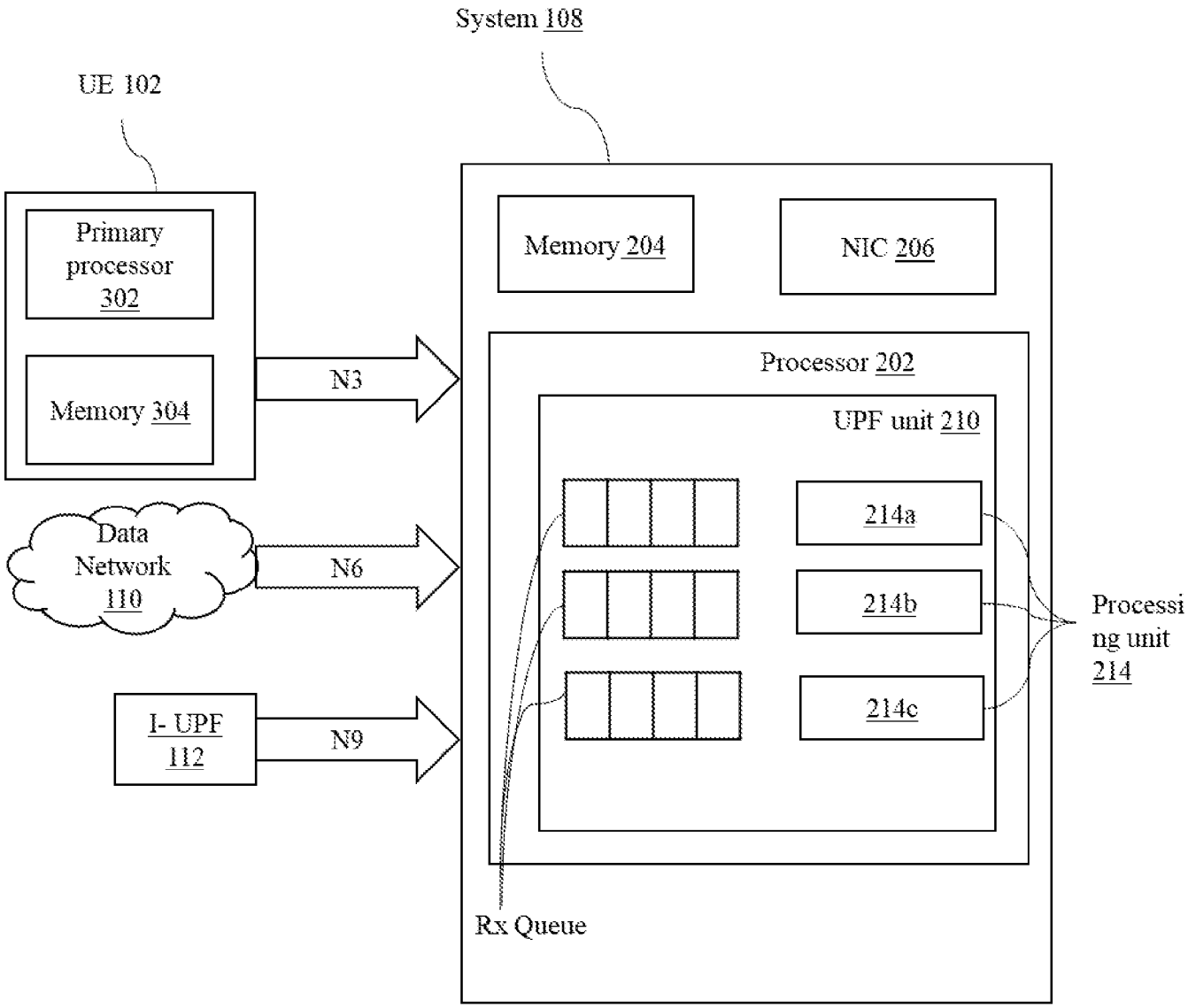

System 108
UE 102
Primary processor 302
Memory 304
N3
Data Network 110
N6
I- UPF 112
N9
Memory 204
NIC 206
Processor 202
UPF unit 210
214a
214b
214c
Processing unit 214
Rx Queue

FIG. 3a

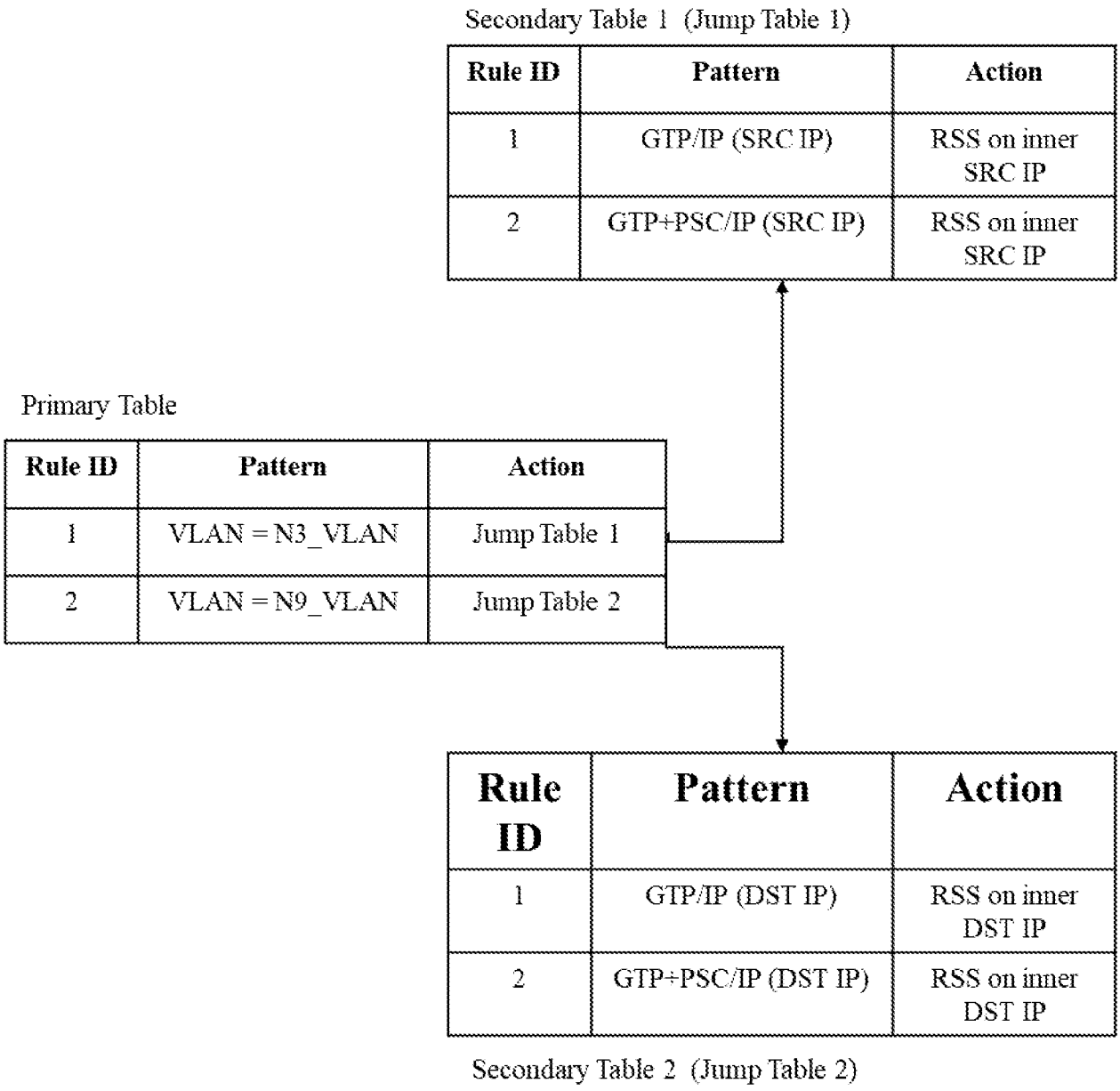

Secondary Table 1 (Jump Table 1)
Rule ID
Pattern
Action
1
GTP/IP (SRC IP)
RSS on inner SRC IP
2
GTP+PSC/IP (SRC IP)
RSS on inner SRC IP
Primary Table
Rule ID
Pattern
Action
1
VLAN = N3_VLAN
Jump Table 1
2
VLAN = N9_VLAN
Jump Table 2
Rule ID
Pattern
Action
1
GTP/IP (DST IP)
RSS on inner DST IP
2
GTP+PSC/IP (DST IP)
RSS on inner DST IP
Secondary Table 2 (Jump Table 2)

FIG. 3b

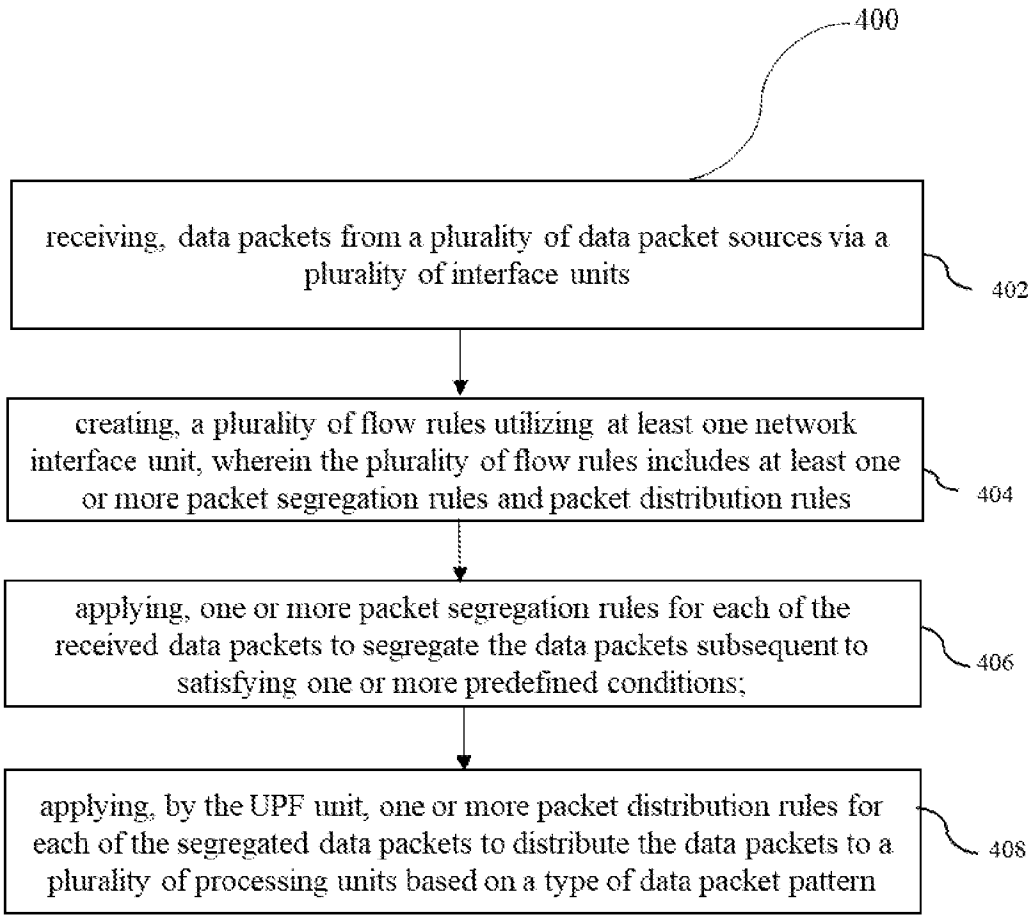

400
receiving, data packets from a plurality of data packet sources via a plurality of interface units
402
creating, a plurality of flow rules utilizing at least one network interface unit, wherein the plurality of flow rules includes at least one or more packet segregation rules and packet distribution rules
404
applying, one or more packet segregation rules for each of the received data packets to segregate the data packets subsequent to satisfying one or more predefined conditions;
406
applying, by the UPF unit, one or more packet distribution rules for each of the segregated data packets to distribute the data packets to a plurality of processing units based on a type of data packet pattern
408

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IN2024/050952

A. CLASSIFICATION OF SUBJECT MATTER
H04L47/2441,H04L47/125 Version=2024.01

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 database consulted during the international search (name of database and, where practicable, search terms used)

PatSeer, IPO Internal Database

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US20200128426A1 (ANTERIX INC) 23 Apr 2020 (23-04-2020) paragraphs [0008], [0027]-[0028], [0033]-[0034	1-21
Y	US2017318082A1 (QUALCOMM INC) 02 Nov 2017 (02-11-2017) abstract; paragraphs [0006]-[0007], [0039]-[0041]	1-21

☐ 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
"D" document cited by the applicant in the international application
"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
30-10-2024	30-10-2024
Name and mailing address of the ISA/ Indian Patent Office Plot No.32, Sector 14,Dwarka,New Delhi-110075 Facsimile No.	Authorized officer Ravi Kumar Telephone No. +91-1125300200