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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
03 March 2022 (03.03.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/046170 A1

(51) International Patent Classification:
H04L 29/08 (2006.01)

(21) International Application Number:
PCT/US2021/020122

(22) International Filing Date:
26 February 2021 (26.02.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
17/001,599 24 August 2020 (24.08.2020) US

(71) Applicant: **ORACLE INTERNATIONAL CORPORATION** [US/US]; 500 Oracle Parkway, Mail Stop 5OP7, Redwood Shores, CA 94065 (US).

(72) Inventor: **KRISHAN, Rajiv**; Flat No. 2-I, Fresh Winds, Munireddy Layout, Panathur Road, Bangalore 560 103 (IN).

(74) Agent: **HUNT, Gregory, A.**; Jenkins, Wilson, Taylor & Hunt, P.A., 3015 Carrington Mill Boulevard, Suite 550, Morrisville, NC 27560 (US).

(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, IT, 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,

(54) **Title:** METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR OPTIMIZED NETWORK FUNCTION (NF) DISCOVERY AND ROUTING USING SERVICE COMMUNICATIONS PROXY (SCP) AND NF REPOSITORY FUNCTION (NRF)

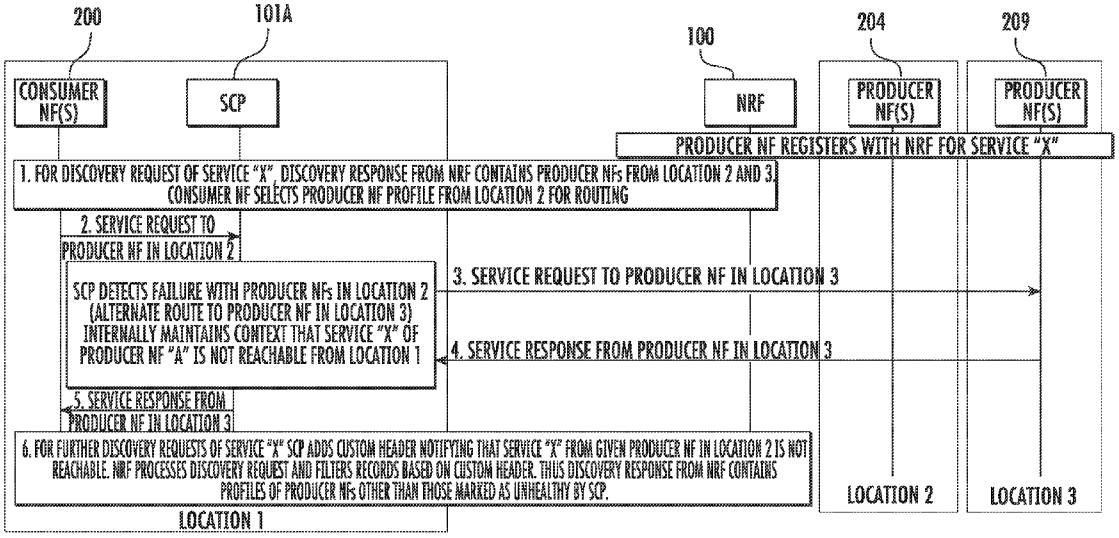

FIG. 3

(57) **Abstract:** A method for optimized NF discovery and routing includes, at an SCR, receiving a discovery request message or generating a discovery request message in response to a received service request message with a 3gpp-Sbi- Discovery header. The SCR modifies the discovery request message to identify as unhealthy at least one service endpoint and service name combination associated with at least one producer NF instance capable of providing a service identified in the discovery request message or the service request message The SCR forwards the discovery request message to the NRF. The NRF creates a list of service profiles of producer NF instances capable of providing the service identified in the discovery or service request message and excludes, from the list, at least one service profile of the at least one producer NF instance corresponding to the endpoint and service name combinations identified

WO 2022/046170 A1

[Continued on next page]

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, 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))*

METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR OPTIMIZED NETWORK FUNCTION (NF) DISCOVERY AND ROUTING USING SERVICE COMMUNICATIONS PROXY (SCP) AND NF REPOSITORY FUNCTION (NRF)

PRIORITY CLAIM

This application claims the priority benefit of U.S. Patent Application Serial No. 17/001,599, filed August 24, 2020, the disclosure of which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

The subject matter described herein relates to routing messages to producer NFs in 5G communications networks. More particularly, the subject matter described herein relates to methods, systems, and computer readable media for optimized NF discovery and routing using an SCP and an NRF.

BACKGROUND

In 5G telecommunications networks, the network node that provides service is referred to as a producer network function (NF). A network node that consumes services is referred to as a consumer NF. A network function can be both a producer NF and a consumer NF depending on whether it is consuming or providing service.

A given producer NF may have many service endpoints, where a service endpoint is the point of contact for one or more NF instances hosted by the producer NF. The service endpoint is identified by a combination of Internet protocol (IP) address and port number or a fully qualified domain name that resolves to an IP address and port number on a network node that hosts a producer NF. An NF instance is an instance of a producer NF that provides a service. A given producer NF may include more than one NF instance. It should also be noted that multiple NF instances can share the same service endpoint.

Producer NFs register with a network function repository function (NRF). The NRF maintains service profiles of available NF instances identifying the services supported by each NF instance. Consumer NFs can

subscribe to receive information about producer NF instances that have registered with the NRF.

In addition to consumer NFs, another type of network node that can subscribe to receive information about NF service instances is a service communications proxy (SCP). The SCP subscribes with the NRF and obtains reachability and service profile information regarding producer NF service instances. Consumer NFs connect to the service communications proxy, and the service communications proxy load balances traffic among producer NF service instances that provide the required service or directly routes the traffic to the destination producer NF instance.

In addition to the SCP, other examples of intermediate proxy nodes or groups of network nodes that route traffic between producer and consumer NFs include the security edge protection proxy (SEPP), the service gateway, and nodes in the 5G service mesh. The SEPP is the network node used to protect control plane traffic that is exchanged between different 5G public land mobile networks (PLMNs). As such, the SEPP performs message filtering, policing and topology hiding for all API messages.

The service gateway is a node that sits in front of a group of producer NFs that provide a given service. The service gateway may load balance incoming service requests among the producer NF instances that provide the service in a manner similar to the SCP.

The service mesh is a name for a group of intermediate proxy nodes that enable communications between producer and consumer NFs. The service mesh may include one or more SCPs, SEPPs, and service gateways.

One problem that occurs in 5G networks is that an NRF may indicate that a producer NF instance is available to provide a service; however, the producer NF instance may not be reachable from the consumer NF. For example, one of the most crucial jobs for the NRF is to receive service discovery requests from consumer NFs and return matching responses including service profiles of producer NF instances available to provide a service to a consumer NF. The NRF obtains this information through registration messages from the producer NFs. Even though the network between the producer NFs and the NRF may not be congested, there may be

network impairment between the consumer NF and the producer NFs. Thus, when a consumer NF requests from the NRF a list of service profiles producer NF instances capable of providing a service, the NRF may return a list of service profiles of producer NF instances, some of which may not be reachable from the consumer NF. As a result, when the consumer NF sends a service request message to a producer NF instance through the SCP, the SCP may determine that the service endpoint of the selected producer NF instance is not available and perform a reselection process to select a different NF instance of same or different producer NF. Performing the reselection process at the SCP is undesirable, as it increases latency in providing the service to the consumer NF.

In light of these difficulties, there exists a need for methods, systems, and computer readable media for optimized NF discovery and routing using an NRF and an SCP.

SUMMARY

A method for optimized network function (NF) discovery and routing using an NF repository function (NRF) and a service communications proxy (SCP) includes, at the SCP, receiving a discovery request message or generating a discovery request message in response to a received service request message with a 3gpp-Sbi-Discovery header, as defined in Section 5.2.3.2.7 of Third Generation Partnership Project (3GPP) Technical Specification (TS) 29.500. According to Section 5.2.3.2.7 of 3GPP TS 29.500, the 3gpp-Sbi-Discovery header is used to convey NF service discovery factors to the SCP in indirect communication models. The 3gpp-Sbi-Discovery header contains discovery parameters to be conveyed by the NF consumer to the SCP and is used for finding a suitable NF producer instance, e.g. by performing the NF service discovery procedure with the NRF on behalf of the NF consumer in case of indirect communication with the delegated discovery model.

The method further includes modifying, by the SCP, the discovery request message to identify as unhealthy at least one endpoint and service name combination associated with a producer network function (NF) instance

capable of providing a service identified in the discovery request message or the service request message with the 3gpp-Sbi-Discovery header. The method further includes forwarding, by the SCP, the discovery request message to the NRF. The method further includes at the NRF, creating a list of service profiles of producer NF instances capable of providing the service identified in the discovery or service request message. The method further includes excluding, by the NRF and from the list, at least one service profile of at least one producer NF instance corresponding to the at least one endpoint and service name combination identified as unhealthy in the discovery request message. The method further includes forwarding, by the NRF and to the SCP, a discovery response message including the list of service profiles of producer NF instances.

According to another aspect of the subject matter described herein, the method for optimized NF discovery and routing includes maintaining, at the SCP, an unhealthy endpoint database and modifying the discovery request message includes performing a lookup in the unhealthy endpoint database using service name included in or derived from the discovery request message or the service request message with the 3gpp-Sbi-Discovery header, locating a record in the unhealthy endpoint database corresponding to the service name included in or derived from the discovery or service request message, extracting the endpoint from the record, and inserting the endpoint and the service name into the discovery request message.

According to another aspect of the subject matter described herein, inserting the endpoint and service name into the discovery request message includes inserting the endpoint and the service name into a custom header of the discovery request message.

According to another aspect of the subject matter described herein, maintaining the unhealthy endpoint database includes, in response to a determination that a producer NF instances associated with an endpoint and service name combination is unhealthy: determining whether a record corresponding to the endpoint and service name combination exists in the unhealthy endpoint database; in response to determining that a record corresponding to the endpoint and service name combination does not exist

in the unhealthy endpoint database, adding a record corresponding to the endpoint and service name combination to the unhealthy endpoint database; inserting a timestamp in the record; and starting a cleanup timer for the record.

According to another aspect of the subject matter described herein, the method for optimized NF discovery and routing includes detecting expiration of the cleanup timer, and, in response, deleting the record corresponding to the endpoint and service name combination from the unhealthy endpoint database.

According to another aspect of the subject matter described herein, creating the list of service profiles of producer NF instances includes extracting a service name parameter from the discovery, identifying service profiles of producer NF instances capable of providing the service identified by the service name parameter, and including the service profiles of the producer NF instances capable of providing the service identified by the service name parameter in the list.

According to another aspect of the subject matter described herein, excluding the at least one service profile from the list includes removing, from the list, at least one service profile corresponding to the at least one endpoint and service name combination identified as unhealthy in the discovery request message received from the SCP.

According to another aspect of the subject matter described herein, the at least one service profile excluded from the list includes at least one service profile of at least one producer NF instance having connectivity with the NRF and being unreachable from the SCP.

According to another aspect of the subject matter described herein, receiving a discovery or service request message includes receiving a service request message indicating delegated discovery and further comprising, at the SCP, after receiving the discovery response message, forwarding the service request message to one of the producer NF instances having a service profile in the list.

According to another aspect of the subject matter described herein, a system for optimized NF discovery and routing comprises a service communications proxy (SCP) including at least one processor. The system

includes an NF repository function (NRF) including at least one processor. The system further includes an SCP discovery/service request handler and database manager implemented by the at least one processor of the SCP for receiving a discovery request message or generating a discovery request message in response to a received service request message, modifying, the discovery request message to identify as unhealthy at least one endpoint and service name combination associated with at least one producer NF instance capable of providing a service identified in the discovery or service request message, and forwarding, by the SCP, the discovery request message to the NRF. The system further includes an NRF discovery request handler implemented by the at least one processor of the NRF for creating a list of service profiles of producer NF instances capable of providing the service identified in the discovery request message, excluding, from the list, at least one service profile of at least one producer NF instance corresponding to the at least one endpoint and service name combination identified as unhealthy in the discovery request message, and forwarding, to the SCP, a discovery response message including the list of service profiles of producer NF instances.

According to another aspect of the subject matter described herein, the system for optimized NF discovery and routing includes an unhealthy endpoint database located at the SCP and the SCP discovery/service request handler and database manager is configured to modify the discovery request message by: performing a lookup in the unhealthy endpoint database using service name included in or derived from the discovery or service request message; locating a record in the unhealthy endpoint database corresponding to the service name identified in or derived from the discovery request message or the service request message with the 3gpp-Sbi-Discovery header; extracting the endpoint from the record; and inserting the endpoint and the service name into the discovery request message.

According to another aspect of the subject matter described herein, the SCP discovery/service request handler and database manager is configured to insert the endpoint and the service name into a custom header of the discovery request message.

According to another aspect of the subject matter described herein, the SCP discovery request handler is configured to follow model D in Section E1 of 3GPP TS 23.501 and generate a discovery request message using discovery parameters received in a service request with the 3gpp-Sbi-Discovery header from a consumer NF in delegated discovery mode and by: performing a lookup in the unhealthy endpoint database using service identifier included in or derived from the discovery parameters in the service request; locating a record in the unhealthy endpoint database corresponding to the service identified in or derived from the service request message; extracting an identifier for the endpoint from the record; and inserting identifier for the endpoint in the discovery request message.

According to another aspect of the subject matter described herein, the SCP discovery/service request handler and database manager is configured to, in response to a determination that a producer NF instance associated with an endpoint and service name combination is unhealthy: determine whether a record corresponding to the endpoint and service name combination exists in the unhealthy endpoint database; in response to determining that a record corresponding to the endpoint and service name combination does not exist in the unhealthy endpoint database, add a record corresponding to the endpoint and service name combination to the unhealthy endpoint database; insert a timestamp in the record; and start a cleanup timer for the record.

According to another aspect of the subject matter described herein, the SCP discovery/service request handler and database manager is configured to detect expiration of the cleanup timer, and, in response, delete the record corresponding to the endpoint and service name combination from the unhealthy endpoint database.

According to another aspect of the subject matter described herein, the NRF discovery request handler is configured to extract a service name parameter from the discovery request message, identify service profiles of service endpoints on producer NFs capable of providing the service identified by the service name parameter, and include the service profiles of the service endpoints on producer NFs capable of providing the service identified by the service name parameter in the list.

According to another aspect of the subject matter described herein, the service profiles excluded from the list include service or NF profiles of service endpoints on producer NFs having connectivity with the NRF but that are unreachable from the SCP.

According to another aspect of the subject matter described herein, the SCP discovery/service request handler and database manager is configured to receive the discovery response message, forward the discovery response message to a consumer NF, receive, from the consumer NF, a service request message addressed to one of the service endpoints in the list and forward the service request to the service endpoint.

According to another aspect of the subject matter described herein, a non-transitory computer readable medium having stored thereon executable instructions that when executed by a processor of a computer control the computer to perform steps is provided. The steps include, at a service communications proxy (SCP), receiving a discovery request message or generating a discovery request message in response to a received service request message with a 3gpp-Sbi-Discovery header. The steps further include modifying, by the SCP, the discovery request message to identify as unhealthy at least one endpoint service name combination corresponding to at least one producer NF instance capable of providing a service identified in the discovery or service request message. The steps further include forwarding, by the SCP, the discovery request message to an NF repository function (NRF). The steps further include, at the NRF, creating a list of service profiles of service endpoints on producer NFs capable of providing the service identified in the discovery or service request message. The steps further include excluding, by the NRF and from the list, at least one service profile of at least one producer NF instance associated with the endpoint and service name combination identified as unhealthy in the discovery request message. The steps further include forwarding, by the NRF and to the SCP, a discovery response message including the list of service profiles of producer NF instances.

The subject matter described herein may be implemented in hardware, software, firmware, or any combination thereof. As such, the terms “function”

"node" or "module" as used herein refer to hardware, which may also include software and/or firmware components, for implementing the feature being described. In one exemplary implementation, the subject matter described herein may be implemented using a computer readable medium having stored thereon computer executable instructions that when executed by the processor of a computer control the computer to perform steps. Exemplary computer readable media suitable for implementing the subject matter described herein include non-transitory computer-readable media, such as disk memory devices, chip memory devices, programmable logic devices, and application specific integrated circuits. In addition, a computer readable medium that implements the subject matter described herein may be located on a single device or computing platform or may be distributed across multiple devices or computing platforms.

BRIEF DESCRIPTION OF THE DRAWINGS

The subject matter described herein will now be explained with reference to the accompanying drawings of which:

Figure 1 is a network diagram illustrating an exemplary 5G network architecture;

Figure 2 is a network diagram illustrating a problem that occurs when a producer NF has connectivity with an NRF but the connectivity between the producer NF and a consumer NF may be down or unavailable;

Figure 3 is a message flow diagram illustrating exemplary messaging between consumer NFs, an SCP, an NRF for optimized routing using an SCP and an NRF;

Figure 4A is a flow chart illustrating an exemplary SCP algorithm for marking service endpoints as unhealthy and utilizing service endpoints health information in making routing decisions;

Figure 4B is a flow chart illustrating an exemplary SCP algorithm for maintaining a list of unhealthy service endpoints;

Figure 5 is a flow chart illustrating an exemplary SCP process for adding a custom header carrying health information to a discovery request;

Figure 6 is a flow chart illustrating an exemplary NRF algorithm for processing discovery requests received from an SCP;

Figure 7 is a block diagram illustrating an SCP and a NRF including components for optimized routing as subscribed herein; and

Figure 8 is a flow chart illustrating an exemplary process for optimized routing using an NRF and an SCP.

DETAILED DESCRIPTION

The subject matter described herein relates to methods, systems, and computer readable media for optimized service discover and routing using an SCP and an NRF. The subject matter may be implemented in a 5G system network architecture or a network architecture that includes both 5G and non-5G network elements. Figure 1 is a block diagram illustrating an exemplary 5G system network architecture. The architecture in Figure 1 includes NRF **100** and SCP **101**, which may be **located** in the same home public land mobile network (HPLMN). As described above, NRF **100** may maintain profiles of available producer NF service instances and their supported services and allow consumer NFs or SCPs to subscribe to and be notified of the registration of new/updated producer NF service instances. SCP **101** may also support service discovery and selection of producer NF instances. SCP **101** may perform load balancing of connections between consumer and producer NFs. In addition, using the methodologies described herein, SCP **101** may perform preferred NF location based selection and routing.

NRF **100** is a repository for NF or service profiles of producer NF instances. In order to communicate with a producer NF instance, a consumer NF or an SCP must obtain the NF or service profile or the producer NF instance from NRF **100**. The NF or service profile is a JavaScript object notation (JSON) data structure defined in Third Generation Partnership Project (3GPP) Technical Specification (TS) 29.510. The NF or service profile definition includes at least one of a fully qualified domain name (FQDN), an Internet protocol (IP) version 4 (IPv4) address or an IP version 6 (IPv6) address. In Figure 1, any of the nodes (other than NRF **100**) can be either consumer NFs or producer NFs, depending on whether they are requesting or providing services. In the illustrated example, the nodes include a policy control function (PCF) **102** that performs policy related operations in a

network, a user data management (UDM) function **104** that manages user data, and an application function (AF) **106** that provides application services. The nodes illustrated in Figure 1 further include a session management function (SMF) **108** that manages sessions between access management function (AMF) **110** and PCF **102**. AMF **110** performs mobility management operations similar to those performed by a mobility management entity (MME) in 4G networks. An authentication server function (AUSF) **112** performs authentication services for user equipment (UEs), such as user equipment (UE) **114**, seeking access to the network.

A network slice selection function (NSSF) **116** provides network slicing services for devices seeking to access specific network capabilities and characteristics associated with a network slice. A network exposure function (NEF) **118** provides application programming interfaces (APIs) for application functions seeking to obtain information about Internet of things (IoT) devices and other UEs attached to the network. NEF **118** performs similar functions to the service capability exposure function (SCEF) in 4G networks.

A radio access network (RAN) **120** connects user equipment (UE) **114** to the network via a wireless link. Radio access network **120** may be accessed using a g-Node B (gNB) (not shown in Figure 1) or other wireless access point. A user plane function (UPF) **122** can support various proxy functionality for user plane services. One example of such proxy functionality is multipath transmission control protocol (MPTCP) proxy functionality. UPF **122** may also support performance measurement functionality, which may be used by UE **114** to obtain network performance measurements. Also illustrated in Figure 1 is a data network (DN) **124** through which UEs access data network services, such as Internet services.

SEPP **126** filters incoming traffic from another PLMN and performs topology hiding for traffic exiting the home PLMN. SEPP **126** may communicate with an SEPP in a foreign PLMN which manages security for the foreign PLMN. Thus, traffic between NFs in different PLMNs may traverse two SEPP functions, one for the home PLMN and the other for the foreign PLMN.

As stated above, one problem that occurs in 5G networks is that an NRF will report when a discovery response message that a producer NF instance is available to provide a service when the network between the NRF and the producer NF instance is uncongested. However, a consumer NF may not be able to reach the producer NF instance because the network between the consumer NF and the producer NF instance is congested or unavailable. Figure 2 illustrates this problem in more detail. In Figure 2, an SCP **101A** serves location 1, an SCP **101B** serves location 2, and an SCP **101C** serves location 3. The NRF **100** responds to the discovery requests in each of locations 1, 2, and 3. In this example, consumer NFs **200** and **202** reside in location 1. Producer NFs **204** reside in location 2, and producer NFs **206** and **208** reside in location 3. In the illustrated example, producer NFs **204** in location 2 register with NRF **100**, and NRF **100** marks producer NFs **204** as registered (which indicates that producer NFs **204** are available). This is possible because producer NFs **204** have good connectivity with NRF **100**.

However, consumer NFs **200** and **202** residing in location 1 may lack good connectivity with location 2, indicated by the X marks on the lines between SCP **101A** and producer NFs **204** and between SCP **101A** and SCP **101B**. Accordingly, when a consumer NF **200** or **202** sends a discovery request to NRF **100** requesting service provided by producer NFs **204**, NRF **100** will return a list including service profiles of producer NF instances on producer NFs **204** to the requesting consumer NFs **200** or **202**. Consumer NF **200** or **202**, upon receiving a response to the discovery request, will send service requests to their local SCP **101A**. SCP **101A** may determine that producer NF instances on producer NFs **204** are unreachable and may perform a reselection process to select an alternate producer NF instance to handle the service request. For example, SCP **101A** may select an alternate producer NF instance in location 2 or may select one of the producer NF instances on producer NFs **206** and **208** in location 3. Such reselection is undesirable as it adds latency in processing service requests. There is currently no mechanism in 3GPP to provide feedback to the NRF where producer NF availability can be restricted to a set of consumer NFs. 3GPP allows producers to limit discovery based on domain, network slice selection

assistance identifier (NSSAI), NF type, etc. However, this does not solve the problem of restricting the set of producer NF instances based on connectivity or producer NF instance health.

Figure 3 is a message flow diagram illustrating exemplary messaging for optimized routing using an SCP and an NRF. Referring to Figure 3, in line 1, one of consumer NFs **200** sends a discovery request for a service X to NRF **100**. NRF **100** responds to the discovery request with a list of service profiles of producer NF instances from location 2 and location 3 capable of providing the service. Consumer NF **200** selects a service endpoint from a producer NF in location 2 for providing the service.

In line 2 of the message flow diagram, the consumer NF that sent the discovery request sends a service request to SCP **101A** requesting service from a producer NF in location 2. SCP **101A** determines the selected service endpoint of producer NF in location 2 is unavailable, for example, due to lack of connectivity, and determines that there is a producer NF instance in location 3 that is capable of providing the service. Accordingly, in line 3 of the message flow diagram, SCP **101A** forwards the service request to one of the producer NF instances on producer NFs **208** in location 3 that is capable of providing the service.

SCP **101A** maintains internally a service context that a service X of producer NF **204** is not reachable from location 1. As will be described in more detail below, SCP **101A** may maintain an unhealthy endpoint database that includes a list of service endpoints that are not reachable from the location of SCP **101A**.

In line 4 of the message flow diagram, the producer NF instance on producer NF **208** in location 3 that received the service request message responds to the service request. For example, if producer NF **208** is a PCF and the service request is a request for policy service, the producer NF instance on producer NF **208** may respond to the service request by providing policy instructions to requesting consumer NF **200**.

In line 5 of the message flow diagram, SCP **101A** receives the service response and forwards the response to the requesting consumer NF **200**.

Because SCP **101A** maintains context about the health or reachability of producer NF instances on producer NFs **204**, SCP **101A** can utilize this context to facilitate optimized routing by communicating the context to NRF **100**. Such utilization is illustrated by line 6 of the message flow diagram where, when SCP **101A** receives further discovery requests for service X, SCP **101A** adds a custom header notifying or indicating to NRF **100** that service X from a given producer NF in location 2 is not reachable from the location of SCP **101A**. SCP **101A** forwards this discovery request to NRF **100**. NRF **100** processes the discovery request and filters the service profiles in the list of service profiles that is returned in response to the discovery request based on the custom header. The discovery response from NRF **100** will contain the profiles of producer NF instances on producer NFs that are reachable from location 1. In the example illustrated in Figure 3, the discovery response would include service profiles of producer NF instances on producer NFs from location 3, but not service profiles of producer NF instances of producer NFs from location 2. Utilizing such a system, the consumer NFs can send a service request to producer NF instances on producer NFs that are reachable by the consumer NFs and the SCP was not required to provide a re-selection service, which could result in processing delay of the service request.

One issue that should be considered is whether the NRF should blacklist all producer NFs in a given location when the SCP notifies the NRF that a service endpoint in that location is not reachable. In one exemplary implementation, the NRF will not blacklist all service endpoints when it receives an indication that one endpoint in a given location is unavailable. The problem being faced by an SCP instance may be for a specific service instance only. Thus, limiting traffic to all producer NFs from that location is not an ideal choice. When the SCP detects that a given endpoint is down, the NRF may exclude the service profile of producer NF instances associated with that endpoint from discovery response messages to the SCP in the region from which the endpoint is unreachable, but not from other regions.

In some implementations, more than one service may share a given endpoint (i.e., when NF services have common application programming

interface (API) gateway as their exposure point). Should the NRF restrict discovery of all service instances that share a given endpoint when the SCP determines that one service that shares or exposes a given endpoint is down? In an ideal implementation, the answer is no, because some of the other services that share or expose the same endpoint may be available (assuming the problem is with the one service and not the network between the endpoint and the consumer NFs. When the SCP detects that a given service that shares an endpoint with other services is down, the SCP should notify the NRF about the service instance that is impacted on that endpoint. The NRF avoids discovery of that service instance from consumer NFs having location served by SCP that notified the NRF about service instance unavailability.

Two main components of the subject matter described herein are the SCP and the NRF. Their functions in providing optimized routing as described herein are as follows:

SCP

For given service names (service name is identified from the registered uniform resource indicator (RURI), the SCP maintains list of endpoints that have unhealthy network status. An endpoint can be unhealthy due to reachability or congestion or any other criteria being monitored by SCP. Endpoints can be identified by fully qualified domain name (FQDN), Internet protocol (IP) address, or both.

The SCP starts a cleanup timer for each service endpoint that is marked as unhealthy. On expiry of the cleanup timer, the SCP marks service instance as healthy again by removing the record for the endpoint from the unhealthy endpoint database. For case of network unreachability, “ping” or other network tools can be used to track the endpoint reachability. For a simplified implementation, the subject matter described herein uses timer based options to determine when to mark an endpoint identified as unhealthy as healthy again.

The SCP adds custom headers to a discovery request message where the custom header identifies endpoints that have been marked by the SCP as unhealthy. This is to provide guidance to the NRF on which service profiles should be excluded from the discovery response.

NRF

Based on parameters in a received discovery request message, the NRF generates a list of viable service profiles of producer NF instances capable of providing each service identified in the discovery request message. The NRF removes or excludes from the list the profiles of service instances that match with endpoints indicated as unhealthy by the SCP in the custom header. The NRF returns the service profiles in a discovery response.

SCP Algorithm

Figure 4A illustrates exemplary behavior of an SCP for an endpoint whose network status is determined to be unhealthy. Referring to Figure 4A, in step **400**, SCP **101** determines that a given service endpoint is unhealthy. This determination may be made in any suitable manner, such as failing to receive a response from the endpoint to a service request or an http heartbeat message. The service endpoint may be identified by a service name and an endpoint identifier. In step **402**, if the service endpoint is already marked as unhealthy, control proceeds to step **404** where the timestamp for the service name and endpoint is updated in an unhealthy endpoint database maintained by SCP **101**. Table 1 shown below illustrates an example of an unhealthy endpoint database that may be maintained by SCP **101**.

Unhealthy endpoints		
Service Name	Endpoint(s)	Timestamp
nudm-sdm	sdm1.udm1.com	<in secs>
nudm-sdm	sdm2.oracle.com	<in secs>
nudm-sdm	100.10.2.4	<in secs>
nudm-uecm	100.10.2.5	<in secs>

Table 1: Unhealthy Endpoint Database Example

In Table 1, endpoint and service name combinations that have been determined to be unhealthy are identified by service name and endpoint identifier. The service name specifies the 3GPP service provided by the endpoint. In Table 1, the identified services are nudm-sdm, which is used by consumer NFs to retrieve subscription information for a UE, and nudm-uecm service, which is used by consumer NFs to obtain context information

regarding transactions being performed by a UE. The endpoints providing the services are identified by fully qualified domain names (FQDNs) or IP addresses. Each entry in Table 1 further includes a timestamp, which is the time that the entry was added to the unhealthy endpoint database. It should also be noted that endpoints, rather than entire services, are marked as unhealthy. Marking endpoints rather than services as unhealthy enables consumer NFs to obtain services from healthy endpoints that provide a service even when other endpoints that provide the same service are unhealthy or not reachable.

It should also be noted that SCP **101** marks an endpoint and service name combination as unhealthy when SCP **101** cannot obtain the identified service from the producer NF instance that exposes the endpoint. An unhealthy status recorded for an endpoint and service name combination in the unhealthy endpoint database could be caused by the producer NF instance being unreachable by the SCP, even if the producer NF instance is capable of registering with the NRF, as is the case with producer NF instances located on producer NFs **204** illustrated in Figure 2. It should also be noted that because SCPs maintain health status information regarding producer NFs that the SCPs can reach, the unhealthy endpoint database maintained by SCPs in different regions, such as SCPs **101A**, **101B**, and **101C** in Figure 2 may be different. Because each SCP maintains its own region or location-specific unhealthy endpoint database of service instances on producer NFs that are unreachable from that SCP, and the NRF returns service profiles of producer NF instances that are reachable by that SCP, the efficiency of the network is increased over a solution where unhealthy producer NF instance status is not SCP-specific. Stated differently, the subject matter described herein enables the NRF to formulate and return SCP-region-specific lists of service profiles of producer NF instances that are reachable from each SCP.

Returning to Figure 4A, after updating the timestamp for the service name and endpoint pair in step **404**, control proceeds to step **406**, where the SCP restarts the cleanup timer for the service name and endpoint pair. The cleanup timer is a timer maintained by the SCP for each entry in the unhealthy endpoint database. The SCP starts the cleanup timer when an entry is added

to the unhealthy endpoint database. When the timer reaches a predetermined value, the SCP removes the entry from the unhealthy endpoint database.

In step **408**, the SCP performs alternate routing to select a different service endpoint or producer NF in response to receiving a service request for an endpoint that is marked as unhealthy.

Returning to step **402**, if the endpoint is not already marked as unhealthy, control proceeds to step **410** where the service name and endpoint identifier are added to the unhealthy endpoint database. In step **412**, the cleanup timer is started for the service name and endpoint identifier pair. Control then proceeds to step **410** where alternate routing is used to route the service request to a producer NF instance on a producer NF that is not listed in the unhealthy endpoint database.

Figure 4B illustrates an exemplary process performed by SCP **101** to clean up entries in the unhealthy endpoint database. The purpose of the cleanup process is to mark producer NF instances as healthy by default and only mark them as unhealthy if they are detected as unhealthy and for a short time thereafter. Referring to Figure 4B, in step **414**, the cleanup timer for a service name and endpoint pair expires. In step **416**, the SCP determines whether the endpoint and service name combination is still in the unhealthy list or database. If the endpoint and service name combination is still in the unhealthy list or database, control proceeds to **418** where the service name and endpoint are deleted from the unhealthy endpoint database. If the service name and endpoint combination is not still in the unhealthy list or database, the process ends. It should be noted that a single timer or individual timers can be used to manage unhealthy service instances. Using individual timers for each service name and endpoint pair is just an example implementation of the subject matter described herein. The implementation can be changed to a single timer for all endpoint and service name pairs without departing from the scope of the subject matter described herein.

Figure 5 is a flow chart illustrating an exemplary process performed by SCP **101** in response to receiving a discovery request or a service request with a 3gpp-Sbi-Discovery header, from a consumer NF. For example, SCP **101** may receive a discovery request form a consumer NF when the consumer

NF is performing service discovery. SCP **101** may receive a service request from a consumer NF in the case where the consumer NF implements delegated discovery, and SCP **101** supports delegated discovery, as illustrated by model D in Section E1 of 3GPP TS 23.501. Figure 5 also illustrates the same unhealthy endpoint database **500** illustrated in Table 1. Referring to Figure 5, in step **502**, SCP **101** receives a discovery request or a service request with a 3gpp-Sbi-Discovery header (indicating delegated discovery) from a consumer NF. In step **504**, SCP **101** determines whether the discovery or service request includes a service names parameter. If the discovery parameter includes a service names parameter, control proceeds to step **506** where SCP **101** begins iterating for each service name in the service names parameter. In step **508**, SCP **101** determines whether iteration is complete for the service name currently being checked. In step **510**, SCP **101** performs a lookup in unhealthy endpoint database **500** for the service name. In step **512**, it is determined whether a service name is found. If a service name is found, control proceeds to step **514** where SCP **101** adds unhealthy endpoint information for the endpoint corresponding to the entry in unhealthy endpoint database **500** to the discovery request. In one implementation, SCP **101** may insert the unhealthy endpoint information into a discovery request by adding a custom header to the discovery request. The custom header indicates the service name and endpoint that are marked as unhealthy in unhealthy endpoint database **500**. In the example illustrated in Figure 5, the custom header is of the format "X-SCP-UH-<service name>:<endpoint>", wherein X-SCP-UH is the prefix for the header, <service name> is the name of the service provided by the endpoint marked as unhealthy, and <endpoint> is the identifier of the service endpoint marked as unhealthy.

Returning to step **504**, if the service request does not contain a service names parameter, control proceeds to step **516** where SCP **101** creates a list of service names as defined by 3GPP TS 23.501 section 7.2. Creating a list of service names is also described in Table 6.1.6.3.11 of 3GPP TS 29.510. After the list is created, control proceeds to step **518** where SCP **101** iterates through the process of determining whether each service name is located in

the unhealthy endpoint database and, if so, adds a custom header identifying the endpoint as unhealthy to the discovery request.

Returning to step **508**, once SCP **101** completes iterating through the service names in the service names parameter list or the list of service names generated by SCP **101**, control proceeds to step **520** where SCP **101** forwards the discovery request to NRF **100**. In the example illustrated in Figure 5, if a consumer NF is requesting nudm-sdm service,. SCP **101** will add the following custom header values to the discovery request message:

X-SCP-UH-nudm-sdm: sdm1.udm1.com
X-SCP-UH-nudm-sdm: sdm2.oracle.com
X-SCP-UH-nudm-sdm: 100.10.2.4

In the example above, each of the custom header values that is added to the discovery request are for the endpoints that provide nudm-sdm service and that are identified as unhealthy in unhealthy endpoint database **500**. As will be described in detail below, NRF **100** utilizes the endpoints identified in the custom headers to filter the list of service profiles returned in the discovery response and exclude from the list the service profiles of endpoints that are marked as unhealthy in unhealthy endpoint database **500**.

Figure 6 is a flow chart illustrating an exemplary algorithm performed by NRF **100** in processing a discovery request. Referring to Figure 6, in step **600**, NRF **100** receives the discovery request. The discovery request may be from SCP **101** or directly from a consumer NF. In the case where the NRF receives the discovery request directly from the consumer NF, the custom headers may be missing. However, the consumer NF may implement the application logic described herein for the SCP and add custom headers identifying unhealthy endpoints to the discovery request.

In step **602**, NRF **100**, based on the discovery request parameters, creates a list of potential service profiles with service instance information that can be provided in a discovery response. A service or NF profile is a data structure defined in 3GPP TS 29.510 and maintained by the NRF for each producer NF instance that has registered with the NRF. The service profile

includes parameters, such as the nfInstanceID, which uniquely identifies an NF instance, the NF type, which identifies the type of network function, etc. The consumer NF that receives a list of service profiles will utilize the information in the service profiles to select a producer NF instance to provide a given service and send a service request to the producer NF instance.

In step **604**, NRF **100** determines whether the custom headers indicating unhealthy endpoint and service name combinations are present in the discovery request. If the custom headers indicating unhealthy endpoint and service name combinations are present, control proceeds to step **606** where NRF **100** iterates through all headers with the prefix "X-SCP-UH", which indicates that the header includes information identifying an unhealthy endpoint and service name combination. The information included in the custom header may include the service name and endpoint for each combination determined by the SCP that send the discovery request to be unhealthy.

In step **608**, if the NRF is not finished iterating through all of the custom headers, control proceeds to step **610** where NRF **100** determines whether there are any service profiles in the service profile list created in step **602** that match the current endpoint being examined in the custom headers. If a matching endpoint is located, control proceeds to step **612** where NRF **100** removes the service instance from the service profile list. Removing the service profile from the list includes the deleting the service profile for the producer NF instance from the list of service profiles that will be provided to the SCP or consumer NF in the discovery response.

Returning to step **604**, if there are no custom headers present in the discovery request message, control proceeds to step **614** where NRF **100** applies its local policy to order or sort the list of service profiles, update priority or other parameters, and apply scoping to limit the number of service profiles returned in a discovery response. In step **616**, the discovery response is sent to the consumer NF or SCP.

Returning to step **608**, if NRF **100** determines that it has iterated through all of the custom headers in the discovery request message, control proceeds to step **618** where NRF **100** determines whether the discovery

request includes a service name parameter. If the discovery request does not include a service name parameter, control returns or proceeds to step **614** where NRF **100** applies local NRF policy to sort the list of possible service profiles, applies scoping parameters, etc. and step **616** where NRF **100** sends the discovery response to the requester.

Returning to step **618**, if a service name parameter is present in the discovery request message, control proceeds to step **620** where NRF **100** removes empty service profiles from the potential list of profiles that will be returned to the requester. Control then proceeds to step **614** and **616** where the list of profiles is sorted and the discovery response is sent to the requester.

In step **608**, once NRF **100** has completed iterating through the list of service profiles, control proceeds to steps **614**, **616**, **618**, and **620** where NRF **100** sorts the list of service profiles of producer NF instances capable of providing a service identified in the discovery request with unhealthy service profiles removed from the list and sends the discovery response to the requesting SCP or consumer NF.

Figure 7 is a block diagram illustrating an exemplary SCP and NRF capable of performing the steps described herein for optimized NF discovery and routing. Referring to Figure 7, SCP **101** and NRF **100** each include at least one processor **700** and a memory **702**. SCP **101** further includes unhealthy endpoint database **500** that stores the list of endpoints that have been marked as unhealthy by SCP **101**. Unhealthy endpoint database **500** may reside in memory **702** of SCP **101**. SCP **101** further includes an SCP discovery/service request handler and database manager **704** that processes discovery requests and service requests with 3gpp-Sbi-Discovery headers from consumer NFs. In the case of discovery request received from consumer NFs, SCP discovery/service request handler and database manager **704** may modify the discovery request to include unhealthy endpoint and service name information. In the case of delegated discovery where SCP **101** formulates a discovery request on behalf of a consumer NF, SCP discovery/service request handler and database manager **704** may receive a service request with a 3gpp-Sbi-Discovery header, formulate a discovery request on behalf of the consumer NF and modify the discovery request to include the unhealthy

endpoint and service name information. SCP discovery/service request handler and database manager **704** also maintains the list of unhealthy service name and endpoint combinations in database **500**. SCP discovery/service request handler and database manager **704** may be implemented by computer executable instructions stored in memory **702** of SCP **101** and that are executed by processor **700** of SCP **101**.

As stated above, SCP **101** maintains a local list of unhealthy endpoint and service name combinations and different SCPs may maintain different lists of unhealthy endpoint and service name combinations. As a result, the problems described above with regard to Figure 2 where producer NFs could register with the NRF as available but not be reachable by a particular consumer NF is avoided. In addition, producer NF instances that appear as being unhealthy to some SCPs may appear as healthy to other SCPs. The endpoint and service name combinations are only marked as unhealthy by the SCPs to which the endpoint and service name combinations appear as unhealthy. Other SCPs who do not see the producer NF instances as unhealthy can still reach the producer NF instances. As are result, producer NF utilization is improved over an implementation where producer NF instances are marked as being unhealthy globally.

NRF **100** includes NRF discovery request handler **706** that receives discovery requests, parses the discovery requests for unhealthy endpoint and service name combinations, and formulates discovery response messages to exclude service profiles of producer NF instances corresponding to the endpoint and service name combinations that have been marked as unhealthy by SCP **101**. Thus, NRF discovery request handler **706** generates lists of service profiles that are SCP-region specific in terms of reachability of the producer NF instances corresponding to the service profiles. NRF discovery request handler **706** may be implemented by computer executable instructions that are stored in memory **702** of NRF **100** and executed by processor **700** of NRF **100**.

Figure 8 is a flow chart illustrating an exemplary process performed by SCP **101** and NRF **100** in performing optimized routing as described herein. Referring to Figure 8, in step **800**, a discovery request or a service request

with a 3gpp-Sbi-Discovery header is received from a consumer NF. The discovery or service request may identify at least one service for which NF discovery is being requested (either directly by the consumer NF or indirectly in the case of delegated discovery).

In step **802**, a lookup is performed in the unhealthy endpoint database. For example, SCP **101** may perform a lookup in database **500** for each service identified in the discovery or service request or generated based on the discovery or service request.

In step **804**, unhealthy endpoint and service name combinations resulting from the lookup are added to the existing or new discovery request. For example, SCP **101** may add custom headers to the discovery request that identify each endpoint and service name combination identified as unhealthy based on the lookup in unhealthy endpoint database **500**.

In step **806**, the discovery request with the unhealthy endpoint and service name identification information is forwarded to the NRF. For example, SCP **101** may forward the modified discovery request to NRF **100**.

In step **808**, a list of service profiles is created at the NRF using the unhealthy endpoint and service name identification information provided in the discovery request. For example, in NRF **100** may generate an initial list of service profiles of endpoints based on the service identifier (outside of the custom headers in the discovery request message) and exclude or remove service profiles of endpoints from the list service profiles that have service name and endpoint combinations that are indicated by SCP **101** as being unhealthy.

In step **810**, the discovery response with the list of service profiles is transmitted to the SCP. For example, NRF **100** may send a list of service profiles that has been filtered to remove service profiles of producer NF instances corresponding to endpoint and service name combinations identified as unhealthy to SCP **101**.

In step **812**, the process includes providing the list to a consumer NF. Step **812** would only occur in the case of non-delegated discovery where the SCP receives a discovery request from a consumer NF and forwards the discovery request to the NRF. In the case of delegated discovery where the

SCP does not receive a discovery request from the consumer NF but instead receives a service request, step 812 is not performed. In step 812, for the case of non-delegated discovery, SCP **101** may forward the discovery response including the list of service profiles of producer NF instances to a consumer NF that sent the initial discovery request to SCP **101**.

In step **814**, process includes forwarding a service request to a producer NF instance. The service request may be the same service request received in step **800** in the case of delegated discovery. The service request may be a new service request received from a consumer NF in the case of non-delegated discovery. In either case, SCP **101** forwards the request to one of the producer NF instances whose service profile is in the filtered list of service profiles, and the likelihood of the SCP having to perform producer NF re-selection is reduced.

The disclosure of each of the following references is hereby incorporated herein by reference in its entirety:

References

1. 3GPP TS 23.501; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2 (Release 16) V16.4.0 (2020-03)
2. 3GPP TS 23.502; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Procedures for the 5G System (5GS); Stage 2 (Release 16) (2020-03) V16.4.0 (2020-03)
3. 3GPP TS 29.510; 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Network Function Repository Services; Stage 3 (Release 16), V16.4.0 (2020-07)
4. 3GPP TS 29.500; 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Technical Realization of Service Based Architecture; Stage 3 (Release 16), V16.4.0 (2020-06)

It will be understood that various details of the presently disclosed subject matter may be changed without departing from the scope of the

presently disclosed subject matter. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation.

CLAIMS

What is claimed is:

1. A method for optimized network function (NF) discovery and routing using an NF repository function (NRF) and a service communications proxy (SCP), the method comprising:

at the SCP, receiving a discovery request message or generating a discovery request message based on a received service request message with a 3gpp-Sbi-Discovery header;

modifying, by the SCP, the discovery request message to identify as unhealthy at least one endpoint and service name combination associated with a producer NF instance capable of providing a service identified in the discovery or service request message;

forwarding, by the SCP, the discovery request message to the NRF;

at the NRF, creating a list of service profiles of producer NF instances capable of providing the service identified in the discovery or service request message;

excluding, by the NRF and from the list, at least one service profiles of at least one producer NF instance corresponding to the at least one endpoint and service name combination identified as unhealthy in the discovery request message; and

forwarding, by the NRF and to the SCP, a discovery response message including the list of service profiles of producer NF instances.

2. The method of claim 1 comprising, at the SCP, maintaining an unhealthy endpoint database and wherein modifying the discovery request message includes:

performing a lookup in the unhealthy endpoint database using a service name included in or derived from the service or discovery request message;

locating a record in the unhealthy endpoint database corresponding to the service name identified in or derived from the service or discovery request message;

extracting the endpoint from the record; and

inserting the endpoint and the service name into the discovery request message.

3. The method of claim 2 wherein inserting the endpoint and service name into the discovery request message includes inserting the endpoint and service name into a custom header of the discovery request message.

4. The method of claim 2 or claim 3 wherein maintaining the unhealthy endpoint database includes, in response to a determination that a producer NF instance associated with an endpoint and service name combination is unhealthy:

determining whether a record corresponding to the service name and endpoint combination exists in the unhealthy endpoint database;

in response to determining that a record corresponding to the endpoint and service name combination does not exist in the unhealthy endpoint database, adding a record corresponding to the endpoint and service name combination to the unhealthy endpoint database;

inserting a timestamp in the record; and

starting a cleanup timer for the record.

5. The method of claim 4 comprising, detecting expiration of the cleanup timer, and, in response, deleting the record corresponding to the endpoint and service name combination from the unhealthy endpoint database.

6. The method of any of the preceding claims wherein creating the list of service profiles of producer NF instances includes extracting, by the NRF, a service name parameter from the discovery request message, identifying service profiles of producer NF instances capable of providing the service identified by the service name parameter, and including the service profiles of the producer NF instances capable of providing the service identified by the service name parameter in the list.

7. The method of claim 6 wherein excluding the at least one service profile of the at least one producer NF instances from the list includes removing, from the list, at least one service profile corresponding to the at least one service name and endpoint combinations identified as unhealthy in the discovery request message received from the SCP.

8. The method of any of the preceding claims wherein the at least one service profile excluded from the list includes at least one service profiles of at least one producer NF instance having connectivity with the NRF and being unreachable from the SCP.

9. The method of any of the preceding claims wherein, at the SCP, in response to the discovery response message, forwarding the discovery response message to a consumer NF.

10. The method of any of claims 1 to 8 wherein receiving a discovery or service request message includes receiving a service request message indicating delegated discovery and further comprising, at the SCP, after receiving the discovery response message, forwarding the service request message to one of the producer NF instances having a service profile in the list.

11. A system for optimized network function (NF) discovery and routing, the system comprising:

a service communications proxy (SCP) including at least one processor;

an NF repository function (NRF) including at least one processor;

an SCP discovery/service request handler and database manager implemented by the at least one processor of the SCP for receiving a discovery request message or generating a discovery request message based on a received service request message with a 3gpp-Sbi-Discovery header, modifying the discovery request message to identify as unhealthy at least one endpoint and service name combination associated with at least one producer NF capable of providing a service identified in the discovery or service request

message, and forwarding, by the SCP, the discovery request message to the NRF; and

an NRF discovery request handler implemented by the at least one processor of the NRF for receiving the discovery request message, creating a list of service profiles of producer NF instances capable of providing the service identified in the discovery request message, excluding, from the list, at least one service profiles of at least one producer NF instance corresponding to the at least one endpoint and service name combination identified as unhealthy in the discovery request message, and forwarding, to the SCP, a discovery response message including the list of service profiles of producer NF instances.

12. The system of claim 11 comprising an unhealthy endpoint database located at the SCP and wherein the SCP discovery/service request handler and database manager is configured to modify the discovery request message by:

performing a lookup in the unhealthy endpoint database using a service name included in or derived from the discovery request or the service request message with the 3gpp-Sbi-Discovery header;

locating a record in the unhealthy endpoint database corresponding to the service identified in or derived from the discovery request message or the service request message with the 3gpp-Sbi-Discovery header;

extracting the endpoint from the record; and

inserting the service name and the endpoint into the discovery request message.

13. The system of claim 12 wherein the SCP discovery/service request handler and database manager is configured to insert the endpoint and the service name into a custom header of the discovery request message.

14. The system of claim 12 or claim 13 wherein the SCP discovery/service request handler and database manager is configured to, in response to a determination that a producer NF instance associated with an endpoint and service name combination is unhealthy:

determine whether a record corresponding to the endpoint and service name combination exists in the unhealthy endpoint database;

in response to determining that a record corresponding to the service name and endpoint combination does not exist in the unhealthy endpoint database, add a record corresponding to the service name and endpoint combination to the unhealthy endpoint database;

insert a timestamp in the record; and

start a cleanup timer for the record.

15. The system of claim 14 wherein the SCP discovery/service request handler and database manager is configured to detect expiration of the cleanup timer, and, in response, delete the record corresponding to the service name and endpoint combination from the unhealthy endpoint database.

16. The system of any of claims 11 to 15 wherein the NRF discovery request handler is configured to extract a service name parameter from the discovery request message, identify service profiles of producer NF instances capable of providing the service identified by the service name parameter, and include the service profiles of the producer NF instances capable of providing the service identified by the service name parameter in the list.

17. The system of claim 16 wherein excluding the at least one service profile corresponding to the at least one endpoint and service name combination identified as unhealthy from the list includes removing the at least one service profile from the list.

18. The system of any of claims 11 to 17 wherein the at least one service profile excluded from the list includes at least one service profile of at least one producer NF instance having connectivity with the NRF but that are unreachable from the SCP.

19. The system of any of claims 11 to 18 wherein the SCP discovery/service request handler and database manager is configured to receive the discovery response message, forward the discovery response message to a consumer NF, or, in response to receiving the service request message and the service request message indicating

delegated discovery, the SCP discovery/service request handler is configured to forward the service request message to one of the producer NF instances having a service profile identified in the list.

20. A non-transitory computer readable medium having stored thereon executable instructions that when executed by a processor of a computer control the computer to perform steps comprising:

at a service communications proxy (SCP), receiving a discovery request message or generating a discovery request message based on a received service request message with a 3gpp-Sbi-Discovery header;

modifying, by the SCP, the discovery request message to identify as unhealthy at least one endpoint and service name combination associated with at least one producer network function (NF) instance capable of providing a service identified in the discovery or service request message with the 3gpp-Sbi-Discovery header;

forwarding, by the SCP, the discovery request message to an NF repository function (NRF);

at the NRF, creating a list of service profiles of producer NF instances capable of providing the service identified in the discovery or service request message;

excluding, by the NRF and from the list, at least one service profile of at least one producer NF instance corresponding to the at least one endpoint and service name combination identified as unhealthy in the discovery request message; and

forwarding, by the NRF and to the SCP, a discovery response message including the list of service profiles of producer NF instances.

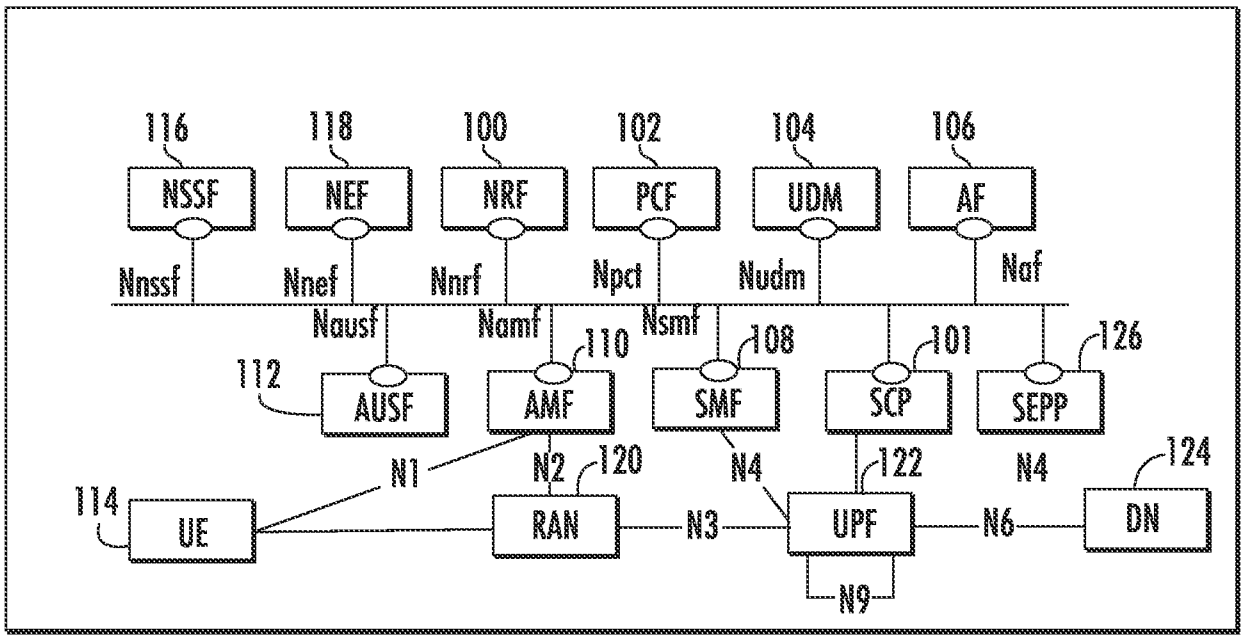
116
118
100
102
104
106
NSSF
NEF
NRF
PCF
UDM
AF
Nnssf
Nnef
Nnrf
Npcf
Nudm
Naf
Nausf
Namf
Nsmf
110
108
101
126
112
AUSF
AMF
SMF
SCP
SEPP
N1
N2
120
N4
122
N4
124
114
UE
RAN
N3
UPF
N6
DN
N9

FIG. 1

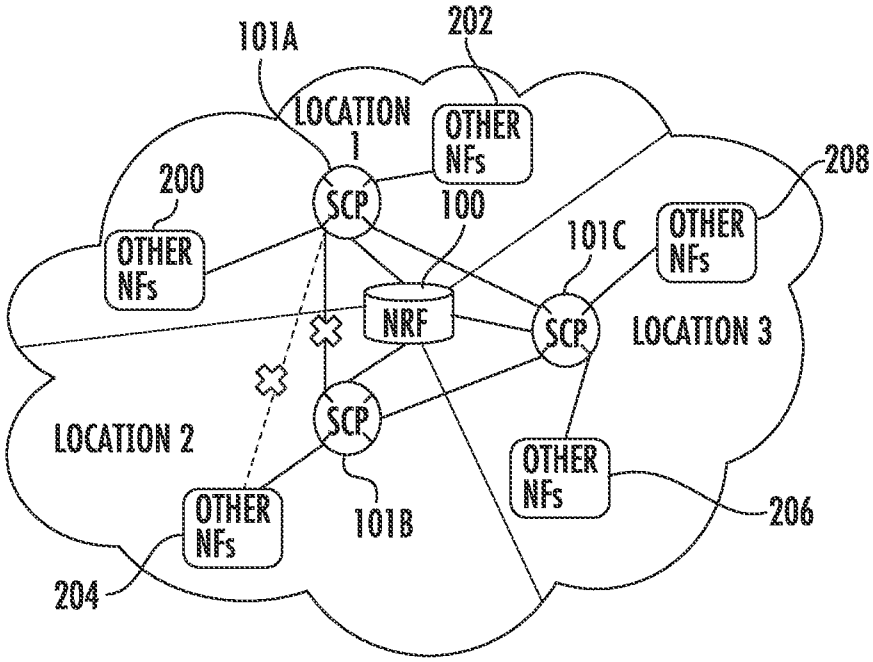
101A
202
LOCATION 1
OTHER NFs
208
200
SCP
100
OTHER NFs
101C
OTHER NFs
NRF
SCP
LOCATION 3
LOCATION 2
SCP
OTHER NFs
206
OTHER NFs
101B
204

FIG. 2

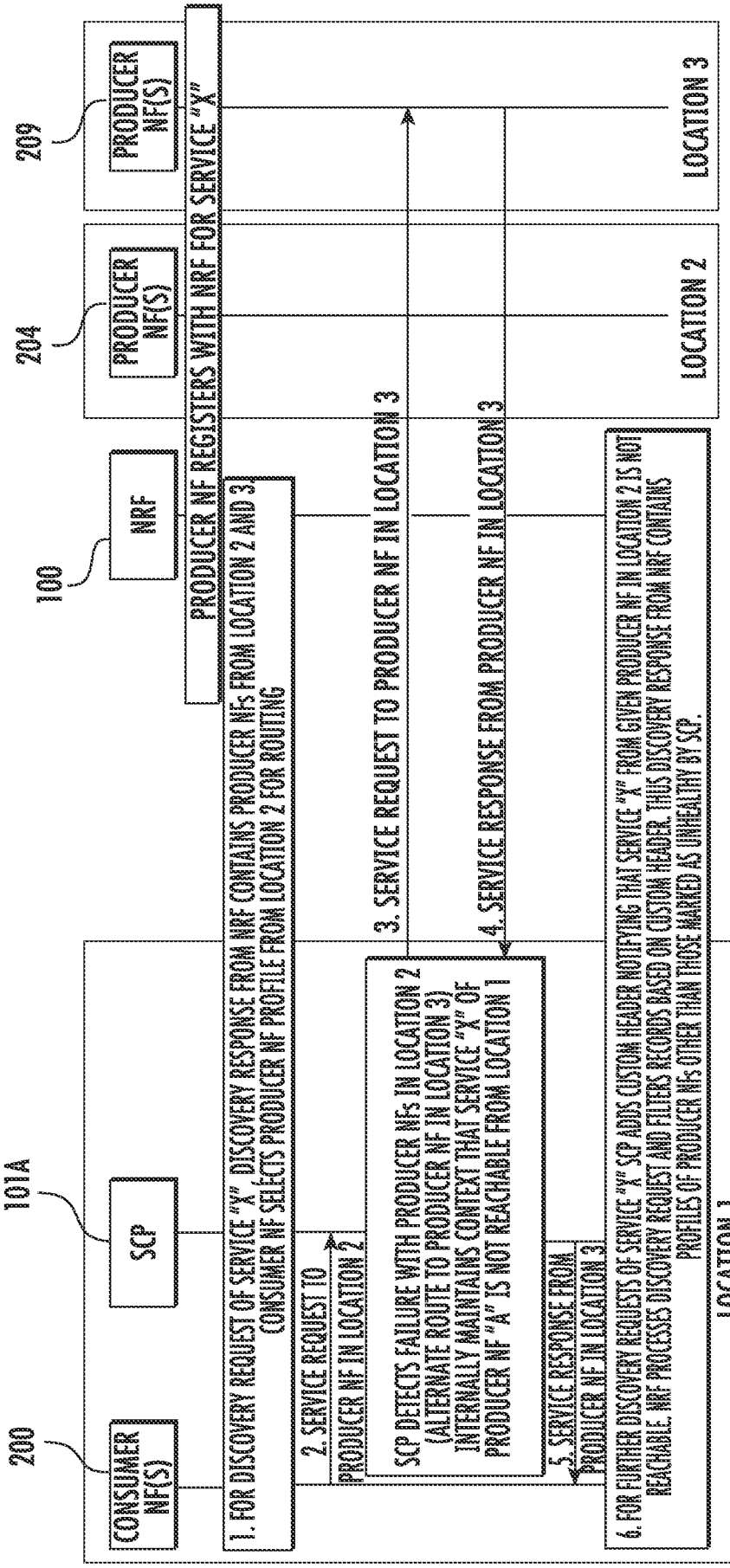
200
CONSUMER NF(S)
101A
SCP
100
NRF
204
PRODUCER NF(S)
209
PRODUCER NF(S)
LOCATION 1
LOCATION 2
LOCATION 3
PRODUCER NF REGISTERS WITH NRF FOR SERVICE "X"
1. FOR DISCOVERY REQUEST OF SERVICE "X", DISCOVERY RESPONSE FROM NRF CONTAINS PRODUCER NFs FROM LOCATION 2 AND 3
CONSUMER NF SELECTS PRODUCER NF PROFILE FROM LOCATION 2 FOR ROUTING
2. SERVICE REQUEST TO PRODUCER NF IN LOCATION 2
SCP DETECTS FAILURE WITH PRODUCER NFs IN LOCATION 2
(ALTERNATE ROUTE TO PRODUCER NF IN LOCATION 3)
INTERNALLY MAINTAINS CONTEXT THAT SERVICE "X" OF
PRODUCER NF "A" IS NOT REACHABLE FROM LOCATION 1
3. SERVICE REQUEST TO PRODUCER NF IN LOCATION 3
4. SERVICE RESPONSE FROM PRODUCER NF IN LOCATION 3
5. SERVICE RESPONSE FROM
PRODUCER NF IN LOCATION 3
6. FOR FURTHER DISCOVERY REQUESTS OF SERVICE "X" SCP ADDS CUSTOM HEADER NOTIFYING THAT SERVICE "X" FROM GIVEN PRODUCER NF IN LOCATION 2 IS NOT
REACHABLE. NRF PROCESSES DISCOVERY REQUEST AND FILTERS RECORDS BASED ON CUSTOM HEADER. THUS DISCOVERY RESPONSE FROM NRF CONTAINS
PROFILES OF PRODUCER NFs OTHER THAN THOSE MARKED AS UNHEALTHY BY SCP.

FIG. 3

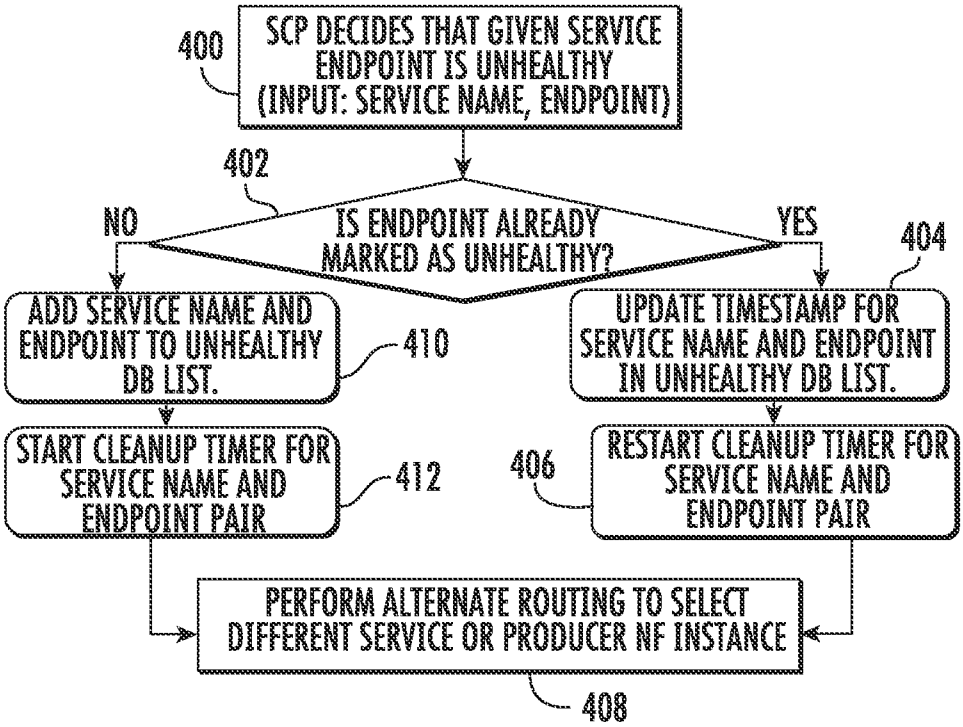
400
SCP DECIDES THAT GIVEN SERVICE ENDPOINT IS UNHEALTHY (INPUT: SERVICE NAME, ENDPOINT)
402
IS ENDPOINT ALREADY MARKED AS UNHEALTHY?
NO
YES
404
ADD SERVICE NAME AND ENDPOINT TO UNHEALTHY DB LIST.
410
UPDATE TIMESTAMP FOR SERVICE NAME AND ENDPOINT IN UNHEALTHY DB LIST.
START CLEANUP TIMER FOR SERVICE NAME AND ENDPOINT PAIR
412
406
RESTART CLEANUP TIMER FOR SERVICE NAME AND ENDPOINT PAIR
PERFORM ALTERNATE ROUTING TO SELECT DIFFERENT SERVICE OR PRODUCER NF INSTANCE
408

FIG. 4A

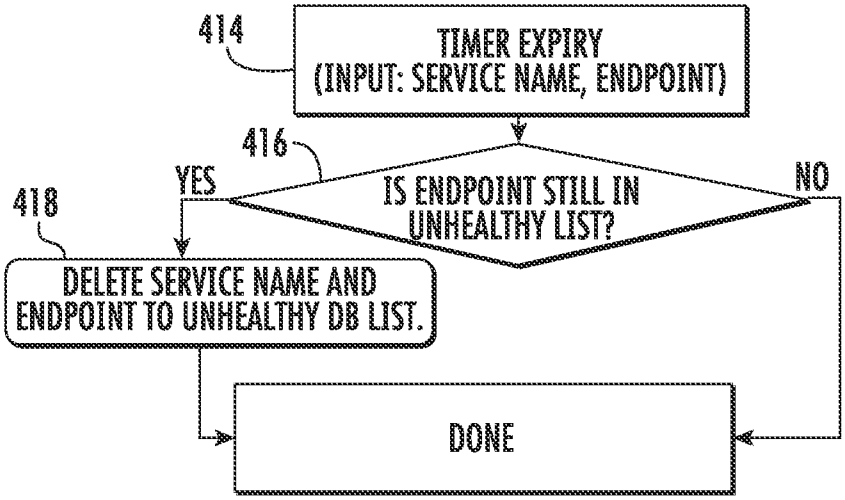
414
TIMER EXPIRY
(INPUT: SERVICE NAME, ENDPOINT)
416
IS ENDPOINT STILL IN UNHEALTHY LIST?
YES
NO
418
DELETE SERVICE NAME AND ENDPOINT TO UNHEALTHY DB LIST.
DONE

FIG. 4B

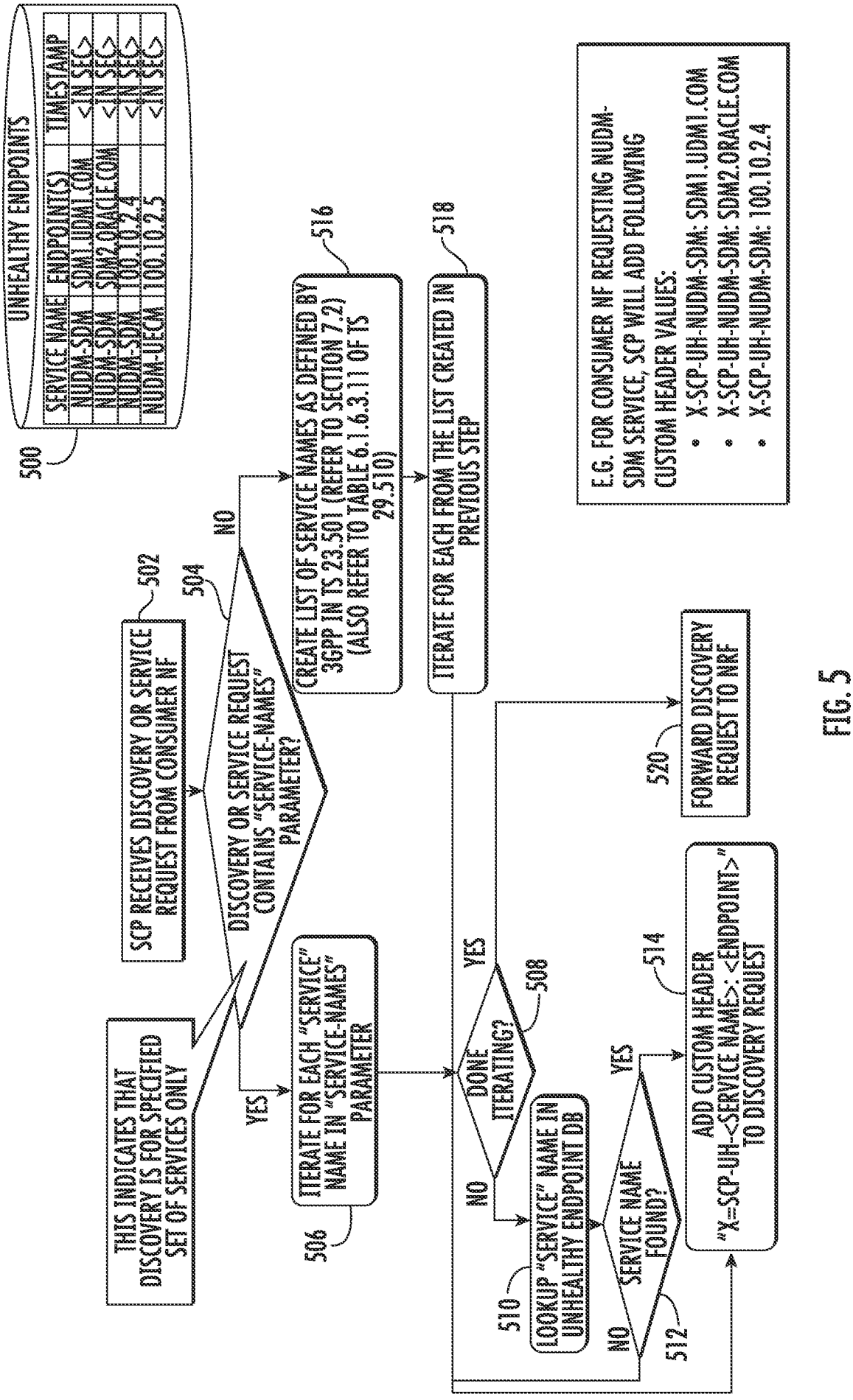
UNHEALTHY ENDPOINTS
SERVICE NAME | ENDPOINT(S) | TIMESTAMP
NUDM-SDM | SDM1.UDM1.COM | <IN SEC>
NUDM-SDM | SDM2.ORACLE.COM | <IN SEC>
NUDM-SDM | 100.10.2.4 | <IN SEC>
NUDM-UECM | 100.10.2.5 | <IN SEC>
500
SCP RECEIVES DISCOVERY OR SERVICE REQUEST FROM CONSUMER NF
502
DISCOVERY OR SERVICE REQUEST CONTAINS "SERVICE-NAMES" PARAMETER?
504
NO
YES
CREATE LIST OF SERVICE NAMES AS DEFINED BY 3GPP IN TS 23.501 (REFER TO SECTION 7.2) (ALSO REFER TO TABLE 6.1.6.3.11 OF TS 29.510)
516
ITERATE FOR EACH FROM THE LIST CREATED IN PREVIOUS STEP
518
THIS INDICATES THAT DISCOVERY IS FOR SPECIFIED SET OF SERVICES ONLY
ITERATE FOR EACH "SERVICE" NAME IN "SERVICE-NAMES" PARAMETER
506
DONE ITERATING?
508
NO
YES
LOOKUP "SERVICE" NAME IN UNHEALTHY ENDPOINT DB
510
SERVICE NAME FOUND?
512
NO
YES
ADD CUSTOM HEADER "X-SCP-UIH-<SERVICE NAME>: <ENDPOINT>" TO DISCOVERY REQUEST
514
FORWARD DISCOVERY REQUEST TO NRF
520
E.G. FOR CONSUMER NF REQUESTING NUDM-SDM SERVICE, SCP WILL ADD FOLLOWING CUSTOM HEADER VALUES:
• X-SCP-UIH-NUDM-SDM: SDM1.UDM1.COM
• X-SCP-UIH-NUDM-SDM: SDM2.ORACLE.COM
• X-SCP-UIH-NUDM-SDM: 100.10.2.4

FIG. 5

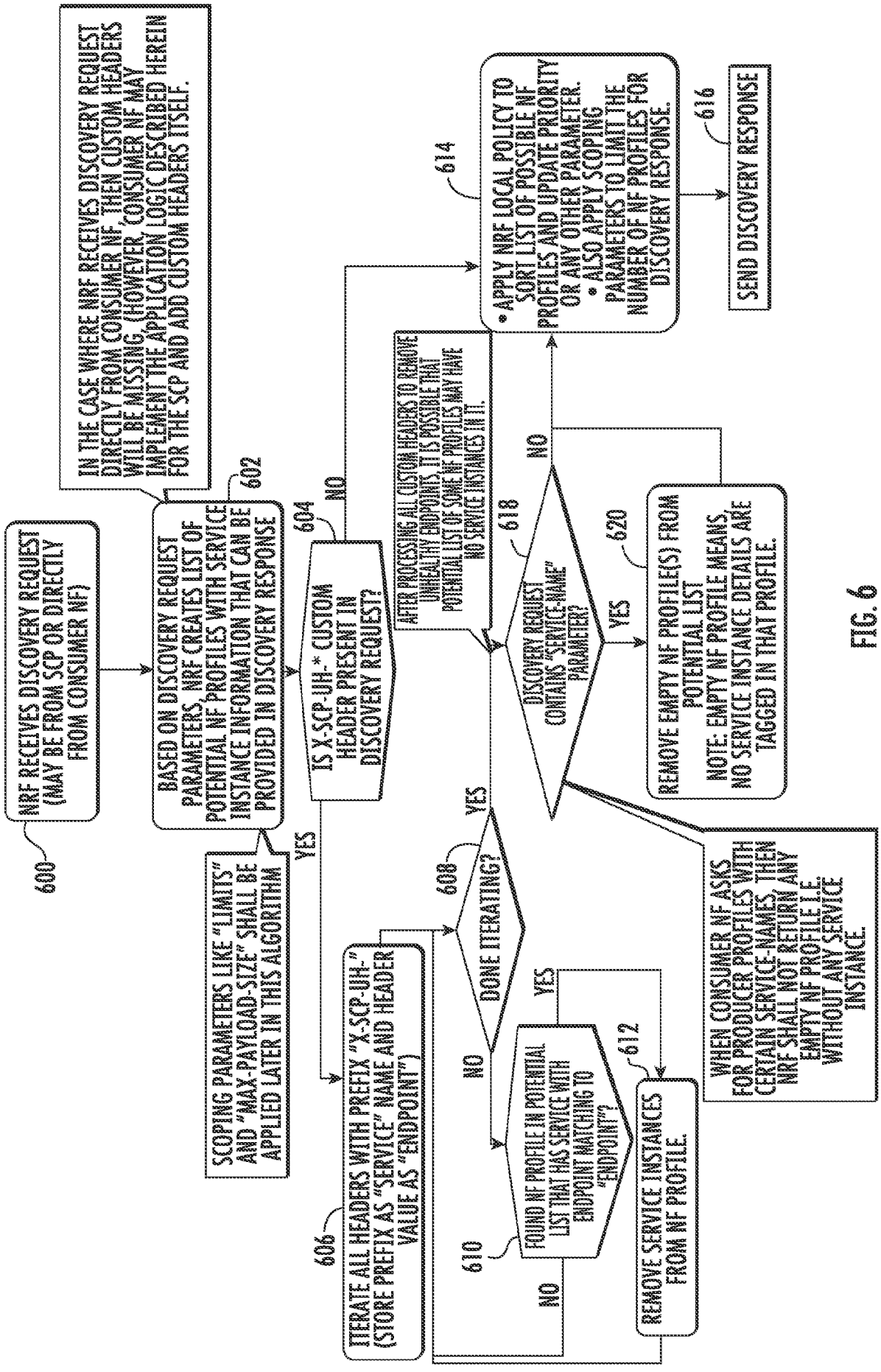
IN THE CASE WHERE NRF RECEIVES DISCOVERY REQUEST DIRECTLY FROM CONSUMER NF, THEN CUSTOM HEADERS WILL BE MISSING, (HOWEVER, CONSUMER NF MAY IMPLEMENT THE APPLICATION LOGIC DESCRIBED HEREIN FOR THE SCP AND ADD CUSTOM HEADERS ITSELF.
NRF RECEIVES DISCOVERY REQUEST (MAY BE FROM SCP OR DIRECTLY FROM CONSUMER NF)
600
BASED ON DISCOVERY REQUEST PARAMETERS, NRF CREATES LIST OF POTENTIAL NF PROFILES WITH SERVICE INSTANCE INFORMATION THAT CAN BE PROVIDED IN DISCOVERY RESPONSE
602
SCOPING PARAMETERS LIKE "LIMITS" AND "MAX-PAYLOAD-SIZE" SHALL BE APPLIED LATER IN THIS ALGORITHM
IS X-SCP-UH-* CUSTOM HEADER PRESENT IN DISCOVERY REQUEST?
604
NO
YES
ITERATE ALL HEADERS WITH PREFIX "X-SCP-UH-" (STORE PREFIX AS "SERVICE" NAME AND HEADER VALUE AS "ENDPOINT")
606
DONE ITERATING?
608
NO
YES
FOUND NF PROFILE IN POTENTIAL LIST THAT HAS SERVICE WITH ENDPOINT MATCHING TO "ENDPOINT"?
610
NO
YES
REMOVE SERVICE INSTANCES FROM NF PROFILE.
612
AFTER PROCESSING ALL CUSTOM HEADERS TO REMOVE UNHEALTHY ENDPOINTS, IT IS POSSIBLE THAT POTENTIAL LIST OF SOME NF PROFILES MAY HAVE NO SERVICE INSTANCES IN IT.
DISCOVERY REQUEST CONTAINS "SERVICE-NAME" PARAMETER?
618
NO
YES
REMOVE EMPTY NF PROFILE(S) FROM POTENTIAL LIST
NOTE: EMPTY NF PROFILE MEANS, NO SERVICE INSTANCE DETAILS ARE TAGGED IN THAT PROFILE.
620
WHEN CONSUMER NF ASKS FOR PRODUCER PROFILES WITH CERTAIN SERVICE-NAMES, THEN NRF SHALL NOT RETURN ANY EMPTY NF PROFILE I.E. WITHOUT ANY SERVICE INSTANCE.
• APPLY NRF LOCAL POLICY TO SORT LIST OF POSSIBLE NF PROFILES AND UPDATE PRIORITY OR ANY OTHER PARAMETER.
• ALSO APPLY SCOPING PARAMETERS TO LIMIT THE NUMBER OF NF PROFILES FOR DISCOVERY RESPONSE.
614
SEND DISCOVERY RESPONSE
616

FIG. 6

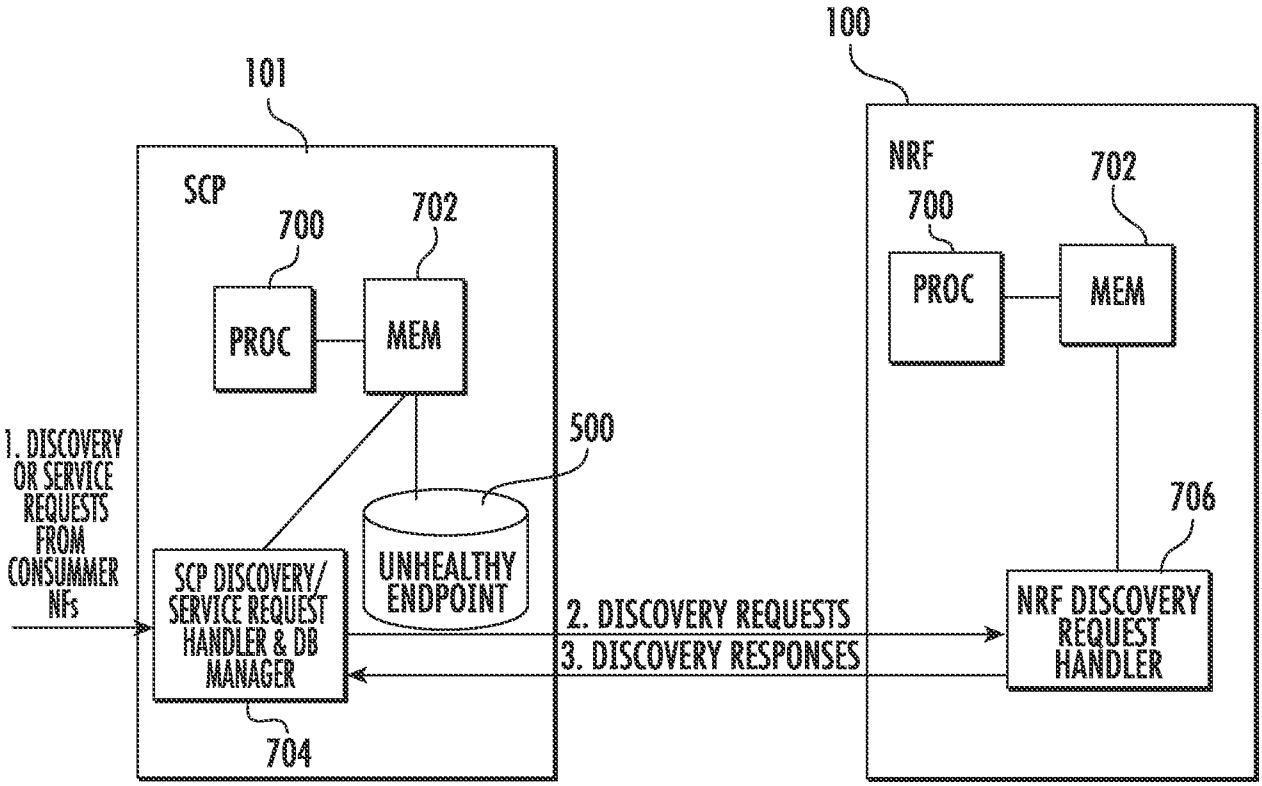
100
101
SCP
700
702
PROC
MEM
500
1. DISCOVERY OR SERVICE REQUESTS FROM CONSUMMER NFs
SCP DISCOVERY/ SERVICE REQUEST HANDLER & DB MANAGER
UNHEALTHY ENDPOINT
704
2. DISCOVERY REQUESTS
3. DISCOVERY RESPONSES
NRF
700
702
PROC
MEM
706
NRF DISCOVERY REQUEST HANDLER

FIG. 7

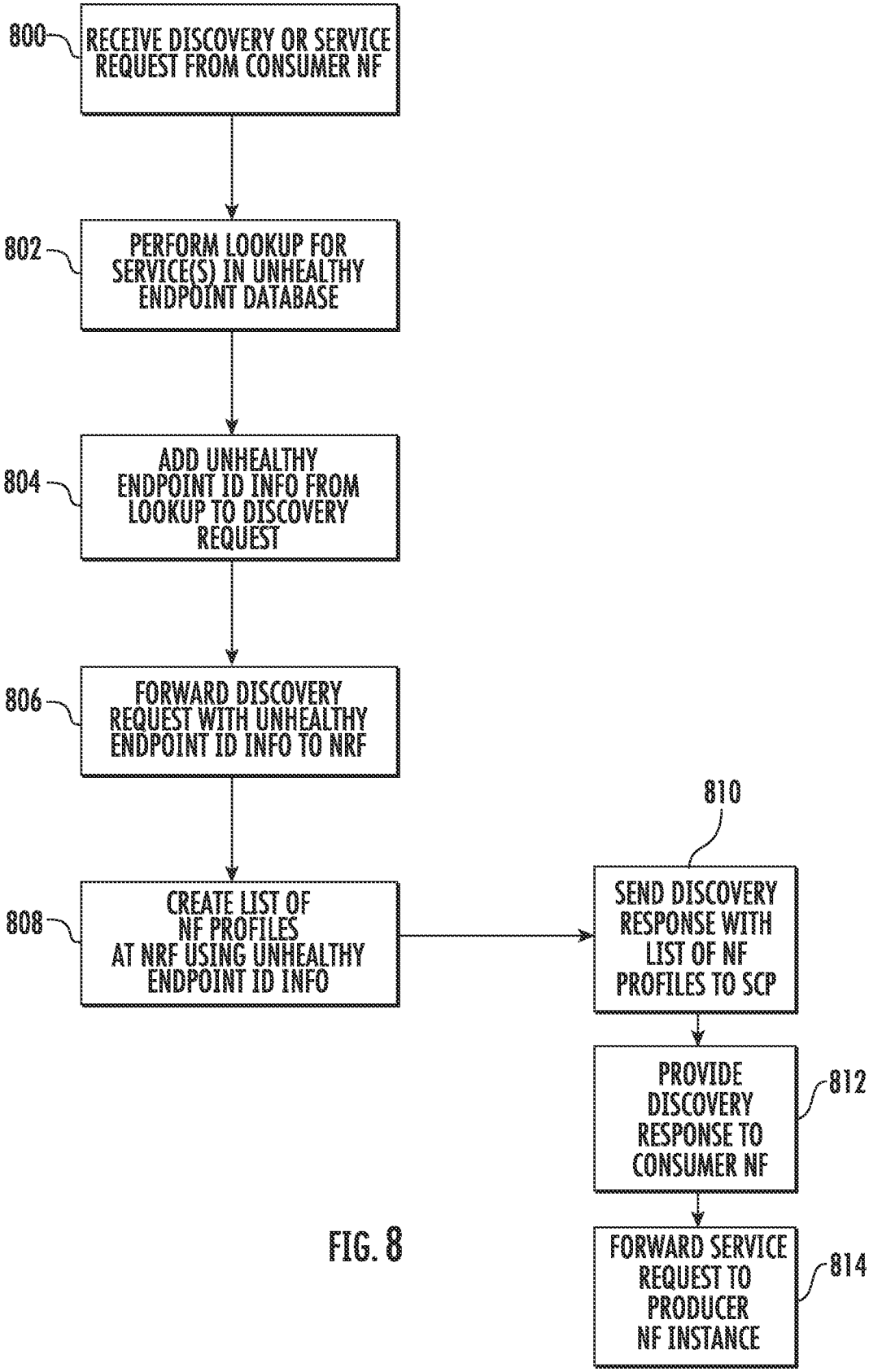
800
RECEIVE DISCOVERY OR SERVICE REQUEST FROM CONSUMER NF
802
PERFORM LOOKUP FOR SERVICE(S) IN UNHEALTHY ENDPOINT DATABASE
804
ADD UNHEALTHY ENDPOINT ID INFO FROM LOOKUP TO DISCOVERY REQUEST
806
FORWARD DISCOVERY REQUEST WITH UNHEALTHY ENDPOINT ID INFO TO NRF
808
CREATE LIST OF NF PROFILES AT NRF USING UNHEALTHY ENDPOINT ID INFO
810
SEND DISCOVERY RESPONSE WITH LIST OF NF PROFILES TO SCP
PROVIDE DISCOVERY RESPONSE TO CONSUMER NF
812
FORWARD SERVICE REQUEST TO PRODUCER NF INSTANCE
814

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2021/020122

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/08
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	HUAWEI ET AL: "eSBA: reselection of producer instance", 3GPP DRAFT; S2-1903559 ESBA RESELECTION OF PRODUCER INSTANCE_V1.0, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRAN , vol. SA WG2, no. Xi'an, China; 20190408 - 20190412 2 April 2019 (2019-04-02), XP051719707, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg%5Fsa/WG2%5FArch/TSGS2%5F132%5FXiAn/Docs/S2%2D1903559%2Ezip [retrieved on 2019-04-02] section 2 ----- -/--	1-20

[X] Further documents are listed in the continuation of Box C.

[ ] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 May 2021	01/06/2021

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Gutiérrez García, J

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2021/020122

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	NTT DOCOMO: "Update Solution 4 for implicit registration", 3GPP DRAFT; S2-1811294-WAS1810700, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. SA WG2, no. Dongguan, China; 20181015 - 20181019 17 October 2018 (2018-10-17), XP051540135, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg%5Fsa/WG2%5FArch/TSGS2%5F129%5FDongguan/Docs/S2%2D1811294%2Ezip [retrieved on 2018-10-17] section 2 -----	1-20