



(51) International Patent Classification:
H04L 29/12 (2006.01)

(21) International Application Number:
PCT/US2020/035004

(22) International Filing Date:
28 May 2020 (28.05.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/555,817 29 August 2019 (29.08.2019) US

(71) Applicant: **ORACLE INTERNATIONAL CORPORATION** [US/US]; 500 Oracle Parkway, Mail Stop 50P7, Redwood Shores, CA 94065 (US).

(72) Inventor: **GOEL, Yesh**; Flat No - B 905, N D Passion Apartments, Harlur Main Road, Bangalore 560 068 (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, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(54) Title: METHOD, SYSTEM, AND COMPUTER READABLE MEDIA FOR DISCOVERING AND TRACKING ADDRESSES

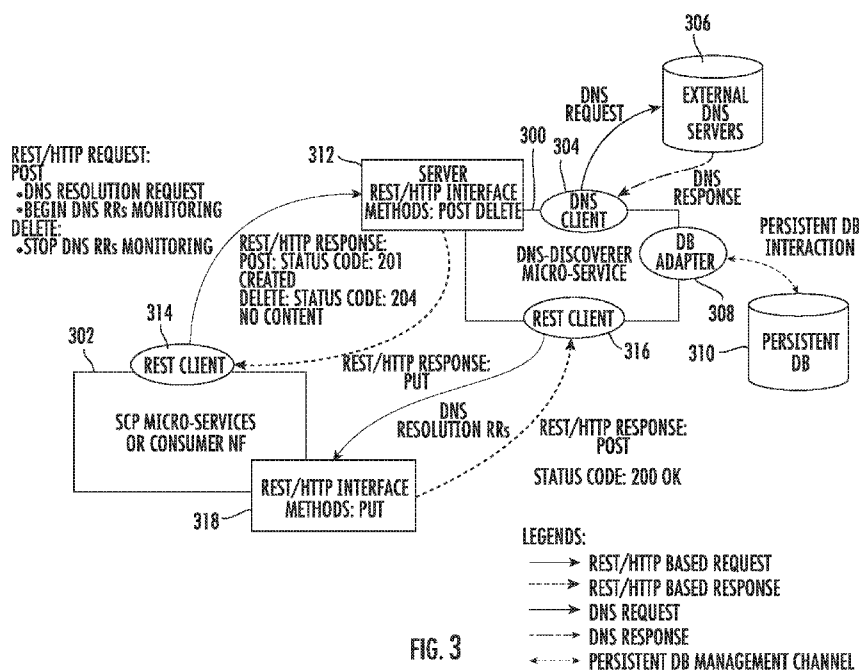


FIG. 3

(57) Abstract: A method for discovering and tracking addresses associated with producer network function (NF) service endpoints includes receiving a first domain name system (DNS) resolution request from a requesting node. The method further includes querying a DNS server using a fully qualified domain name (FQDN) extracted from the first DNS resolution request. The method further includes receiving a first response from the DNS server, the first response including an associated with a producer NF service endpoint associated with the FQDN and storing the address associated with the producer NF service endpoint in a database. The method further includes communicating the address associated with the producer NF service endpoint to the requesting node. The method further includes monitoring the FQDN for changes in address associated with the FQDN. The method further includes notifying the requesting node of the changes in address associated with the FQDN.

(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))*

DESCRIPTION

METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR ACTIVELY DISCOVERING AND TRACKING ADDRESSES ASSOCIATED WITH 5G AND NON-5G SERVICE ENDPOINTS

5

PRIORITY CLAIM

This application claims the priority benefit of U.S. Patent Application Serial No. 16/555,817, filed August 29, 2019, the disclosure of which is incorporated herein by reference in its entirety.

10

TECHNICAL FIELD

The subject matter described herein relates to discovering address information associated with service endpoints in a telecommunications network. More particularly, the subject matter described herein relates to methods, systems, and computer readable media for actively discovering and tracking addresses associated with 5G and non-5G service endpoints.

15

BACKGROUND

In telecommunications networks, a service endpoint is an address on a network node that uniquely identifies an entity that provides service to service consumers. The service endpoint can include an Internet protocol (IP) address or a combination of IP address and transport layer port number, which is also referred to as an IP endpoint.

20

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.

25

A given producer NF may have many service endpoints. Producer NFs register with a network function repository function (NRF). The NRF maintains an NF profile of available NF instances and their supported services. Consumer NFs can subscribe to receive information about producer NF instances that have registered with the NRF.

30

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 destined producer NF.

One problem with the existing 3GPP service architecture is that a consumer NF or an SCP may have insufficient information to load balance traffic among service endpoints exposed by a producer NF service instance. In one scenario, a producer NF may only register its FQDN at the NF service level without individually registering domain names, IP addresses, or IP endpoints of producer NF services. In another scenario, a producer NF may only register its FQDN at the NF instance level without individually registering IP addresses or IP endpoints of services or FQDNs at the NF service level.

In either of these scenarios, the consumer NF or SCP must obtain the IP addresses or IP endpoints associated with the service endpoints to contact the individual service endpoints. In general, IP addresses or IP endpoints corresponding to domain names can be determined using the domain name system (DNS). In the 5G network architecture described above, service consumers need to be notified of service endpoint IP addresses whenever an NF registers or updates its profile. Another scenario in which the consumer NF or SCP needs to be updated with the IP addresses or IP endpoints of the service is when the IP addresses or IP endpoints change without a corresponding NF profile or service update. Even though IP addresses or IP endpoints are discoverable through DNS, there is no automated process for notifying service consumers when an IP address or IP endpoint associated with a service changes.

Accordingly, there exists a need for methods, systems, and computer readable for actively discovering and tracking addresses associated with 5G and non-5G service endpoints.

SUMMARY

A method for discovering and tracking addresses associated with producer network function (NF) service endpoints includes receiving a first domain name system (DNS) resolution request from a requesting node. The method further includes querying a DNS server using a fully qualified domain name (FQDN) extracted from the first DNS resolution request. The method further includes receiving a first response from the DNS server, the first response including an address associated with a producer NF service endpoint associated with the FQDN. The method further includes storing the address associated with the producer NF service endpoint in a database. The method further includes communicating the address associated with the producer NF service to the requesting node. The method further includes monitoring the FQDN for changes in address associated with the FQDN. The method further includes notifying the requesting node of the changes in address associated with the FQDN.

According to an aspect of the subject matter described herein, receiving the first DNS resolution request includes receiving the first DNS resolution request from a service communications proxy (SCP).

According to another aspect of the subject matter described herein, receiving the first DNS resolution request includes receiving the first DNS resolution request from a consumer NF or a non-5G service consumer.

According to yet another aspect of the subject matter described herein, receiving the first DNS resolution request includes receiving the first DNS resolution request at a representational state transfer (REST) server interface provided by a DNS discoverer micro-service.

According to yet another aspect of the subject matter described herein, querying the DNS server includes querying the DNS server from a DNS discoverer micro-service separate from the consumer NF or SCP and the DNS server. In this context, "separate from" means that the DNS discoverer micro-service is implemented on a computing platform separate from a consumer NF or SCP that needs to resolve a domain name and also separate from a computing platform that hosts the DNS server. In an alternate

implementation, the DNS discoverer micro-service may be implemented on the same computing platform as a consumer NF or an SCP.

According to yet another aspect of the subject matter described herein, storing the address associated with the producer NF service comprises storing
5 the address in a database local to the DNS discoverer micro-service along with the time to live of each address received from the DNS Server.

According to yet another aspect of the subject matter described herein, for every address received from the DNS server along with a time to live value when stored in a record in the database, a timer is started for the time period
10 received in time to live field.

According to yet another aspect of the subject matter described herein, monitoring the FQDN comprises: detecting expiration of a record storing the address associated with the producer NF service in the database; in response to detecting expiration of the record, querying the DNS server using the
15 FQDN; receiving a second response from the DNS server; comparing an address in the second response to the address stored in the record in the database; and determining that a change in address associated with the FQDN has occurred in response to the address in the second response being different from the address stored in the record in the database.

According to yet another aspect of the subject matter described herein, the address associated with the producer NF service instance comprises an Internet protocol (IP) address or an IP endpoint.
20

According to yet another aspect of the subject matter described herein, monitoring the FQDN for changes address includes continually monitoring the
25 FQDN for changes in address until stopped in response to a message from the requesting node to cease monitoring the FQDN.

According to yet another aspect of the subject matter described herein, the message from the requesting node to cease monitoring the FQDN comprises a second DNS resolution request including a DELETE method
30 type, and, in response, ceasing monitoring the FQDN.

According to yet another aspect of the subject matter described herein, the DNS discoverer micro-service includes a representational state transfer

(REST) server interface to cease the monitoring of FQDN from the requesting node.

According to yet another aspect of the subject matter described herein, a system for discovering and tracking producer network function (NF) service endpoints, comprises a computing platform including at least one processor. The system further includes a domain name system (DNS) discover micro-service located on the computing platform and implemented by the at least one processor for receiving a first domain name system (DNS) resolution request, querying a DNS server using a fully qualified domain name (FQDN) extracted from the first DNS resolution request, receiving a first response from the DNS server, the first response including an address associated a producer NF service endpoint associated with the FQDN, storing the address associated with the producer NF service endpoint in a database, communicating the address associated with the producer NF service endpoint to the requesting node, monitoring the FQDN for changes in address associated with the FQDN, and notifying the requesting node of the changes in address associated with the FQDN.

According to yet another aspect of the subject matter described herein, the DNS discoverer micro-service is configured to receive the first DNS resolution request from a service communications proxy (SCP).

According to yet another aspect of the subject matter described herein, the DNS discoverer micro-service is configured to the first DNS resolution request from a consumer NF or a non-5G service consumer.

According to yet another aspect of the subject matter described herein, the DNS discoverer micro-service includes a representational state transfer (REST) server interface for receiving the first DNS resolution request from the requesting node.

According to yet another aspect of the subject matter described herein, the computing platform and the DNS discoverer micro-service are separate from the requesting node and the DNS server.

According to yet another aspect of the subject matter described herein, the database is local to the DNS discoverer micro-service.

According to yet another aspect of the subject matter described herein, the DNS discoverer micro-service includes a DNS records change discoverer for performing the monitoring of the FQDN by: detecting expiration of a record storing the address associated with the producer NF service endpoint in the database; in response to detecting expiration of the record, querying the DNS server using the FQDN; receiving a second response from the DNS server; and comparing an address in the second response to the address stored in the record in the database; determining that a change in address associated with the FQDN has occurred in response to the address in the second response being different from the address or stored in the record in the database.

According to yet another aspect of the subject matter described herein, the address associated with the producer NF service endpoint comprises an Internet protocol (IP) address or an IP endpoint.

According to yet another aspect of the subject matter described herein, the DNS record change discoverer is configured to continually monitor the FQDN for changes address associated with the FQDN until stopped in response to a message from the requesting node to cease monitoring the FQDN.

According to yet 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 receiving a first domain name system (DNS) resolution request from a requesting node. The steps include querying a DNS server using a fully qualified domain name (FQDN) extracted from the first DNS resolution request. The steps further include receiving a first response from the DNS server, the response including an address associated with a producer NF service endpoint associated with the FQDN. The steps further include storing the address associated with the producer NF service endpoint in a database. The steps further include communicating the address associated with the producer NF service endpoint to the requesting node. The steps further include monitoring the FQDN for changes in address associated with the FQDN. The steps further include

notifying the requesting node of the changes in address associated with the FQDN.

The subject matter described herein may be implemented in hardware, software, firmware, or any combination thereof. As such, the terms “function”
5 “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
10 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
15 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

20 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 load balancing by a service
25 communications proxy among 5G producer NF service instances and service endpoints exposed by the 5G producer NF service instances;

Figure 3 is a network diagram illustrating a DNS discoverer micro-service that enables a consumer NF or SCP to discover address information associated with producer NF service endpoints;

30 Figure 4 is a call flow diagram illustrating exemplary messaging for obtaining address information for producer NF service endpoints using a DNS discoverer micro-service;

Figure 5 is a call flow diagram illustrating a DNS change monitor and control flow using the DNS discoverer micro-service;

Figure 6 is a call flow diagram illustrating a stop DNS call flow using a DNS discoverer micro-service;

Figure 7 is a block diagram illustrating a network node implementing a DNS discoverer micro-service; and

- 5 Figure 8 is a flow chart illustrating an exemplary process for discovering and monitoring address information associated with 5G and non-5G service endpoints using the DNS discoverer micro-service.

DETAILED DESCRIPTION

- 10 The subject matter described herein relates to methods, systems, and computer readable media for discovering and actively tracking address information associated with 5G and non-5G service endpoints. 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
15 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
20 of producer NFs. In addition, SCP **101** may perform load balancing of connections between consumer and producer NFs.

- NRF **100** is a repository for NF profiles. In order to communicate with a producer NF, a consumer NF or an SCP must obtain the NF profile from NRF **100**. The NF profile is a JSON data structure defined in 3GPP TS
25 29.510. Table 1 shown below illustrates attributes of the NF profile as defined in 3GPP TS 29.510.

Attribute name	Data type	P	Cardinality	Description
nfInstanceId	NfInstanceId	M	1	Unique identity of the NF Instance.
nfType	NFType	M	1	Type of Network Function
nfStatus	NFStatus	M	1	Status of the NF Instance (NOTE 5)
heartBeatTimer	integer	C	0..1	Time in seconds expected between 2 consecutive heart-beat messages from an NF Instance to the NRF. It may be included in the registration request. When present in the request it shall contain the heartbeat time proposed by the NF service consumer. It shall be included in responses from NRF to registration requests (PUT) or in NF profile updates (PUT or PATCH). If the proposed heartbeat time is acceptable by the NRF based on the local configuration, it shall use the same value as in the registration request; otherwise the NRF shall override the value using a preconfigured value.
plmnList	array(PlmnId)	C	1..N	PLMN(s) of the Network Function (NOTE 7). This IE shall be present if this information is available for the NF. If not provided, PLMN ID(s) of the PLMN of the NRF are assumed for the NF.
sNssais	array(Snssai)	O	1..N	S-NSSAIs of the Network Function. If not provided, the NF can serve any S-NSSAI. When present this IE represents the list of S-NSSAIs supported in all the PLMNs listed in the plmnList IE.

perPlmnSnssaiList	array(PlmnSnssai)	O	1..N	This IE may be included when the list of S-NSSAIs supported by the NF for each PLMN it is supporting is different. When present, this IE shall include the S-NSSAIs supported by the Network Function for each PLMN supported by the Network Function. When present, this IE shall override sNssais IE. (NOTE 9)
nsiList	array(string)	O	1..N	NSI identities of the Network Function. If not provided, the NF can serve any NSI.
Fqdn	Fqdn	C	0..1	FQDN of the Network Function (NOTE 1) (NOTE 2). For AMF, the FQDN registered with the NRF shall be that of the AMF Name (see 3GPP TS 23.003 [12] clause 28.3.2.5).
interPlmnFqdn	Fqdn	C	0..1	If the NF needs to be discoverable by other NFs in a different PLMN, then an FQDN that is used for inter-PLMN routing as specified in 3GPP TS 23.003 [12] shall be registered with the NRF (NOTE 8). A change of this attribute shall result in triggering a "NF_PROFILE_CHANGED" notification from NRF towards subscribing NFs located in a different PLMN, but the new value shall be notified as a change of the "fqdn" attribute.
ipv4Addresses	array(Ipv4Addr)	C	1..N	IPv4 address(es) of the Network Function (NOTE 1) (NOTE 2)
ipv6Addresses	array(Ipv6Addr)	C	1..N	IPv6 address(es) of the Network Function (NOTE 1) (NOTE 2)

allowedPlmns	array(PlmnId)	O	1..N	PLMNs allowed to access the NF instance. If not provided, any PLMN is allowed to access the NF. A change of this attribute shall not trigger a "NF_PROFILE_CHANGED" notification from NRF, and this attribute shall not be included in profile change notifications to subscribed NFs.
allowedNfTypes	array(NFType)	O	1..N	Type of the NFs allowed to access the NF instance. If not provided, any NF type is allowed to access the NF. A change of this attribute shall not trigger a "NF_PROFILE_CHANGED" notification from NRF, and this attribute shall not be included in profile change notifications to subscribed NFs.
allowedNfDomains	array(string)	O	1..N	Pattern (regular expression according to the ECMA-262 dialect [8]) representing the NF domain names allowed to access the NF instance. If not provided, any NF domain is allowed to access the NF. A change of this attribute shall not trigger a "NF_PROFILE_CHANGED" notification from NRF, and this attribute shall not be included in profile change notifications to subscribed NFs.

allowedNssais	array(Snssai)	O	1..N	S-NSSAI of the allowed slices to access the NF instance. If not provided, any slice is allowed to access the NF. A change of this attribute shall not trigger a "NF_PROFILE_CHANGED" notification from NRF, and this attribute shall not be included in profile change notifications to subscribed NFs.
Priority	integer	O	0..1	Priority (relative to other NFs of the same type) in the range of 0-65535, to be used for NF selection; lower values indicate a higher priority. If priority is also present in the nfServiceList parameters, those will have precedence over this value. (NOTE 4). The NRF may overwrite the received priority value when exposing an NFProfile with the Nnrf_NFDiscovery service.
Capacity	integer	O	0..1	Static capacity information in the range of 0-65535, expressed as a weight relative to other NF instances of the same type; if capacity is also present in the nfServiceList parameters, those will have precedence over this value. (NOTE 4).
Load	integer	O	0..1	Dynamic load information, ranged from 0 to 100, indicates the current load percentage of the NF.
Locality	string	O	0..1	Operator defined information about the location of the NF instance (e.g. geographic location, data center) (NOTE 3)

udrInfo	UdrInfo	O	0..1	Specific data for the UDR (ranges of SUPI, group ID ...)
udmInfo	UdmInfo	O	0..1	Specific data for the UDM (ranges of SUPI, group ID...)
ausfInfo	AusfInfo	O	0..1	Specific data for the AUSF (ranges of SUPI, group ID...)
amfInfo	AmfInfo	O	0..1	Specific data for the AMF (AMF Set ID, ...)
smfInfo	SmfInfo	O	0..1	Specific data for the SMF (DNN's, ...)
upfInfo	UpfInfo	O	0..1	Specific data for the UPF (S-NSSAI, DNN, SMF serving area, interface...)
pcfInfo	PcfInfo	O	0..1	Specific data for the PCF
bsfInfo	BsfInfo	O	0..1	Specific data for the BSF
chfInfo	ChfInfo	O	0..1	Specific data for the CHF
nrfInfo	NrfInfo	O	0..1	Specific data for the NRF
customInfo	object	O	0..1	Specific data for custom Network Functions
recoveryTime	DateTime	O	0..1	Timestamp when the NF was (re)started (NOTE 5) (NOTE 6)
nfServicePersistence	boolean	O	0..1	If present, and set to true, it indicates that the different service instances of a same NF Service in this NF instance, supporting a same API version, are capable to persist their resource state in shared storage and therefore these resources are available after a new NF service instance supporting the same API version is selected by a NF Service Consumer (see 3GPP TS 23.527 [27]). Otherwise, it indicates that the NF Service Instances of a same NF Service are not capable to share resource state inside the NF Instance.

nfServices	array(NFService)	O	1..N	List of NF Service Instances. It shall include the services produced by the NF that can be discovered by other NFs, if any.
nfProfileChanges SupportInd	boolean	O	0..1	NF Profile Changes Support Indicator. See Annex B. This IE may be present in the NFRegister or NFUpdate (NF Profile Complete Replacement) request and shall be absent in the response. true: the NF Service Consumer supports receiving NF Profile Changes in the response. false (default): the NF Service Consumer does not support receiving NF Profile Changes in the response. Write-Only: true
nfProfileChangesInd	boolean	O	0..1	NF Profile Changes Indicator. See Annex B. This IE shall be absent in the request to the NRF and may be included by the NRF in NFRegister or NFUpdate (NF Profile Complete Replacement) response. true: the NF Profile contains NF Profile changes. false (default): complete NF Profile. Read-Only: true

defaultNotificationSubscriptions	array(DefaultNotificationSubscription)	O	1..N	Notification endpoints for different notification types. (NOTE 10)
NOTE 1: At least one of the addressing parameters (fqdn, ipv4address or ipv6address) shall be included in the NF Profile. If the NF supports the NF services with "https" URI scheme (i.e use of TLS is mandatory), then the FQDN shall be provided in the NF Profile or the NF Service profile (see clause 6.1.6.2.3). See NOTE 1 of Table 6.1.6.2.3-1 for the use of these parameters. If multiple ipv4 addresses and/or ipv6 addresses are included in the NF Profile, the NF Service Consumer of the discovery service shall select one of these addresses randomly, unless operator defined local policy of IP address selection, in order to avoid overload for a specific ipv4 address and/or ipv6 address. NOTE 2: If the type of Network Function is UPF, the addressing information is for the UPF N4 interface. NOTE 3: A requester NF may use this information to select a NF instance (e.g. a NF instance preferably located in the same data center). NOTE 4: The capacity and priority parameters, if present, are used for NF selection and load balancing. The priority and capacity attributes shall be used for NF selection in the same way that priority and weight are used for server selection as defined in IETF RFC 2782 [23]. NOTE 5: The NRF shall notify NFs subscribed to receiving notifications of changes of the NF profile, if the NF recoveryTime or the nfStatus is changed. See clause 6.2 of 3GPP TS 23.527 [27]. NOTE 6: A requester NF may consider that all the resources created in the NF before the NF recovery time have been lost. This may be used to detect a restart of a NF and to trigger appropriate actions, e.g. release local resources. See clause 6.2 of 3GPP TS 23.527 [27]. NOTE 7: A NF may register multiple PLMN IDs in its profile within a PLMN comprising multiple PLMN IDs. If so, all the attributes of the NF Profile shall apply to each PLMN ID registered in the plmnList. As an exception, attributes including a PLMN ID, e.g. IMSI-based SUPI ranges, TAIs and GUAMIs, are specific to one PLMN ID and the NF may register in its profile multiple occurrences of such attributes for different PLMN IDs (e.g. the UDM may register in its profile SUPI ranges for different PLMN IDs). NOTE 8: Other NFs are in a different PLMN if they belong to none of the PLMN ID(s) configured for the PLMN of the NRF. NOTE 9: This is for the use case where an NF (e.g. AMF) supports multiple PLMNs and the slices				

supported in each PLMN are different. See clause 9.2.6.2 of 3GPP TS 38.413 [29].

NOTE 10: If notification endpoints are present both in the profile of the NF instance (NFProfile) and in some of its NF Services (NFService) for a same notification type, the notification endpoint(s) of the NF Services shall be used for this notification type.

Table 1: NF Profile Definition

As indicated in Table 1, the NF profile definition includes at least one of an FQDN, an IP version 4 address or an IP version 6 address. However, there is no requirement that the NF profile include individual IP addresses or IP endpoints associated with a producer NF service endpoint located on the producer NF service instance.

In Figure 1, any of the nodes (other than SCP **101** and NRF **101**) 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 and mobility 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 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 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
5 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.

Address information associated with service endpoints resident on any
10 of the NFs illustrated in Figure 1 that provide services can be tracked using the DNS discoverer micro-service described herein. In addition, non-5G service endpoints that provide services under given FQDN may be discovered and tracked by the DNS discover micro-service described herein. Thus, the term “producer NF service endpoint” as used herein is intended to refer to a
15 service endpoint present on any of the 5G or non-5G service provider nodes. Non-5G service provider nodes include 3G, 4G, or subsequent generation (post-5G) counterpart and non-3GPP service provider nodes.

As stated above, producer NFs register their NF profiles with the NRF. Consumer NFs can discover producer NFs that have registered to provide a
20 specific service by obtaining the NF profiles from the NRF. Consumer NFs can communicate directly with NF service producer NFs. Alternatively, consumer NFs can communicate indirectly with producer NFs via the SCP. In the direct communications mode, the consumer NF performs discovery of the target producer NF either by local configuration or via the NRF. The consumer
25 NF then communicates directly with the target service producer NF. In indirect communications mode, the consumer NF sends service request messages to the SCP, and the SCP may perform service discovery and selection of a producer NF on behalf of a consumer NF. In either the direct or indirect communications mode, the DNS discoverer micro-service described herein
30 may receive DNS resolution request from the consumer NF or from the SCP, query a DNS server on behalf of the consumer NF or SCP, communicate the address information associated with producer NF service endpoints to the

consumer NF or SCP, and continually monitor the FQDN received in the DNS resolution request for changes in address associated with the FQDN.

One problem that occurs in the architecture illustrated in Figure 1 is that the service communication proxy or consumer NF may have insufficient
5 information to load balance among service endpoints resident on producer NF service instances. Figure 2 illustrates this problem. Referring to Figure 2, service communications proxy **101** resides between 5G consumer NFs **200** and **202** and 5G producer NFs **204** and **206**. 5G producer NF **204** includes producer NF service endpoints **204A** and **204B**. 5G producer NF service
10 instance **206** includes producer NF service endpoints **206A** and **206B**.

In operation, consumer NFs **200** and **202** connect to service communications proxy **101**, and service communications proxy **101** load balances traffic among the producer NF service endpoints. Service communications proxy **101** determines producer NF service endpoints for load
15 balancing from the above-described NF profile and NF service contents that producer NFs **204** and **206** have registered with NRF **100**. However, as indicated above, because registering the address information associated with the individual service endpoints is not required, the load balancing performed by SCP **101** may not evenly balance a load among service endpoints.

20 As indicated above, in one scenario, a producer NF service instance may only register a fully qualified domain name at the NF service level. In another scenario, no IP endpoints and no fully qualified domain name may be registered at the NF service level and only the fully qualified domain name may be registered at the NF instance level. In either of these scenarios, the
25 service communications proxy lacks sufficient information for adequate load balancing.

The service communications proxy may determine the IP endpoints of service instances directly by the NF service or NF service instance through DNS-SRV records. In another example, the IP addresses may be exposed
30 by the NF service or NF service instance through DNS A/AAAA records and ports are taken as SCP configuration.

The addresses of producer NF service endpoints need to be known to the SCP when any NF registers or updates a registration. The addresses of

producer NF service endpoints also need to be known when the IP addresses or IP endpoints change without any NF profile or NF service updates. The SCP needs to track these changes for continued routing and load balancing purposes. The DNS discoverer micro-service described herein discovers
5 addresses of producer NF service endpoints and monitors FQDNs for changes in address associated with the FQDN.

As indicated above, the DNS discoverer (DNS-D) micro-service solves at least some of the problems associated with discovery and tracking of service endpoints. The DNS discoverer micro-service queries DNS servers
10 to obtain address information for producer NF service endpoints and provides that information to an SCP or consumer NF. Figure 3 is a network diagram illustrating a network architecture that includes the DNS discoverer micro-service. Referring to Figure 3, DNS discoverer micro-service **300** may be implemented on a computing platform separate from or the same as SCP
15 micro-services or consumer NF **302**. DNS discoverer micro-service **300** includes a DNS discoverer DNS client **304** that interfaces with external DNS servers **306**. DNS discoverer micro-service **300** also includes a database adapter **308** that maintains NF service endpoint information in a persistent database **310**. DNS discoverer micro-service **300** includes a DNS discoverer
20 server interface **312** that exposes the DNS discoverer micro-service to SCP micro-services or consumer NF **302** or non-5G service consumers. In the illustrated example, server interface **312** is a representational state transfer (REST) interface that interfaces with a REST client **314** provided by SCP micro-service **302**. DNS discoverer micro-service **300** further includes a DNS
25 discoverer REST client **316** that interfaces with a server interface **318** of SCP micro-services or consumer NF **302**.

DNS discoverer micro-service **300** can be used to resolve the challenge(s) identified above. In one example, DNS discoverer micro-service **300** may expose a REST/HTTP interface to listen for DNS resolution /
30 Monitoring requests from an SCP or any other service consumer(s). Consumer(s) send DNS requests as HTTP POST messages with callback uniform resource indicators (URIs) where DNS responses are expected. Being an asynchronous service, DNS discoverer micro-service **300** sends

back a 201 created message indicating a request is accepted. DNS discoverer micro-service **300** queries external DNS servers with the requested FQDN. After getting successful DNS resolution from these external DNS servers, DNS discoverer micro-service **300** sends a DNS response to the
5 callback URI received in a DNS resolution request as an HTTP PUT request. DNS discoverer micro-service **300** caches/stores the DNS query responses from external DNS server(s) and the times to live (TTLs) (received in the responses from the DNS servers) to enable DNS change monitoring (discussed below).

10 DNS discoverer micro-service **300** continually monitors (until stopped) all the requested FQDNs for the TTLs received in DNS query responses. DNS responses from external DNS servers are matched at every iteration with stored responses. Differences are indicated to the consumers in the callback URI as an HTTP PUT request. Consumer(s) may opt to stop monitoring by
15 sending an HTTP DELETE request message to DNS discover micro-service **300**.

Figure 4 is a call flow diagram illustrating DNS request servicing performed by DNS discoverer micro-service **300**. The DNS discoverer micro-service **300** includes the components illustrated in and described above with
20 regard to Figure 3. In addition to the components illustrated in Figure 3, DNS discoverer micro-service **300** includes a DNS records change discoverer **400** that monitors requested fully qualified domain names for the time to live values received in DNS query responses, re-queries DNS servers **306** when TTLs have expired, and communicates changes in resolved IP addresses or IP
25 endpoints to consumer NFs, SCPs, or non-5G service consumers.

Referring to the call flow in Figure 4, in line 1, a DNS consumer, such as SCP micro-services or consumer NF **302**, sends a DNS resolution request to server interface of DNS discoverer micro-service **300**. The DNS resolution request includes the FQDN to be resolved, the DNS query type, where the
30 query type indicates an IP address or an IP endpoint, a cookie identifier, and a callback URI for DNS responses and updates sent on DNS discoverer REST client **316** to the querying DNS consumer.

In line 2 of the call flow diagram, DNS discoverer server interface **312** sends a response indicating that the request has been received and accepted.

In line 3 of the call flow diagram, DNS client component **304** of DNS discoverer micro-service **300** sends a query to external DNS servers **306** to
5 resolve the fully qualified domain name in the DNS resolution request.

In line 4 of the call flow diagram, DNS servers **306** respond to DNS client **304** with a response to the DNS query. The response may include one or more IP addresses or IP endpoints that reside on a producer NF service instance corresponding to the FQDN in the DNS query.

10 In line 5 of the call flow diagram, DNS client component **304** communicates the IP address or IP endpoint information to DNS discoverer database adapter **308** and DNS discoverer database adapter **308** forwards the response to persistent database **310**. The response includes the fully qualified domain name from the DNS resolution request, the resolved IP
15 address (or IP addresses and ports depending on the type of response), and expiration time, which is the lowest TTL value of all of the TTL values of DNS resource records received in the query response.

In line 6, DNS discoverer database adapter **308** sends a message to DNS discoverer REST client **316** indicating that the database record has been
20 created, and DNS discoverer client **316** sends the DNS response to SCP micro-services or consumer NF **302**. The DNS response is sent on the callback URI received in the request. In line 7, SCP micro-services or consumer NF **302** sends a 200 OK response to DNS discoverer REST client **316**.

25 DNS records change discoverer **400** detects changes in resolved IP addresses or IP endpoints corresponding to a monitored FQDN. DNS records change discoverer **400** may periodically fetch all DNS records from storage and identify any records where the TTLs received in the DNS query responses have lapsed. For each record where the TTL has lapsed, DNS records
30 change discoverer **400** may re-query the external DNS servers to determine any changes. If any changes have occurred, no further action is required. If a change has occurred, DNS records change discoverer **400** may notify consumer NFs or SCPs that are subscribed to the given service through a

REST/HTTP PUT request on the call back URI received in the original DNS request. Figure 5 is a call flow diagram illustrating a DNS change monitoring call flow. Referring to Figure 5, in line 1, DNS records change discoverer **400** calculates the current timestamp. In line 2, DNS records change discoverer **400** queries persistent database **310** for all records that have a TTL or expiry time that has lapsed. In line 3 of the call flow diagram, persistent database **310** returns DNS records with lapsed call flows to DNS records change discoverer **400**.

In line 4 of the call flow diagram, DNS records change discoverer **400** notifies DNS discoverer client **304** of each FQDN for which the TTL has lapsed. In line 5, DNS discoverer client **304** queries external DNS servers **306** for each FQDN for which the TTL has lapsed. In line 6 of the call flow diagram, DNS discoverer DNS client **304** receives a DNS query response for each FQDN queried in line 5. In line 7, DNS discoverer DNS client **304** notifies DNS records change discoverer of the IP addresses or IP endpoints received in the responses in line 6. DNS records change discoverer **400** determines whether the IP addresses or IP endpoints received match the stored data for each FQDN. If the IP addresses or IP endpoints match, no further action is required on the part of DNS record change discoverer **400**. However, if the IP addresses or IP endpoints do not match, in line 8, DNS records change discoverer **400** communicates the changed IP addresses or IP endpoints to DNS discoverer REST client **316**. DNS discoverer REST client **316** informs SCP micro-services or consumer NF **302** of the change in IP addresses or IP endpoints using an HTTP put request on the call back URI received in the original request. In line 9 of the call flow diagram, DNS SCP micro-services or consumer NF **302** acknowledge receipt of the DNS responses in line 8.

Another operation performed by DNS discoverer micro-service **300** is to stop DNS monitoring, for example, when a consumer NF or SCP notifies DNS discoverer micro-service **300** that the consumer NF or SCP desires to stop monitoring a given FQDN. Figure 6 illustrates such a call flow. Referring to the call flow in Figure 6, in line 1, SCP micro-services or consumer NF **302** sends a DNS resolution request with the FQDN to be resolved but specifying the delete method to stop DNS monitoring for the FQDN. In line 2 of the call

flow diagram, DNS discoverer server interface **312** responds to the client indicating that the request has been accepted. In line 3 of the call flow diagram, DNS discoverer server interface **312** notifies DNS discoverer database adapter **308** that the consumer desires to cease monitoring the FQDN. DNS discoverer database adapter **308** sends a message to persistent database **310** to remove or update the record from persistent database **310** corresponding to the FQDN and notification URL specified in the original DNS resolution request. The message in line 3 will stop the DNS records change discoverer **400** from re-querying DNS servers **306** for the FQDN for this particular consumer.

Figure 7 is a block diagram illustrating an exemplary architecture for a computing platform including DNS discoverer micro-service **300**. Referring to Figure 7, computing platform **700** includes at least one processor **702** and a memory **704**. DNS discoverer micro-service **300** may be implemented by executable instructions embodied in memory **704**. In the illustrated example, DNS discoverer micro-service **300** includes DNS discoverer server interface **312**, DNS discoverer DNS client **304**, DNS discoverer REST client **316**, DNS discoverer database adapter **308**, and DNS records change discoverer **400**. Persistent database **310** may also reside in computing platform **700** for storing the IP addresses or IP endpoints for resolved FQDNs.

Figure 8 is a flow chart illustrating an exemplary process for actively discovering and tracking address information associated with 5G and non-5G service endpoints. Referring to Figure 8, in step **800**, a DNS resolution request is received from a requesting node. For example, DNS discoverer micro-service **300** may receive a DNS resolution request with an FQDN from a DNS discoverer consumer, such as an SCP a consumer NF, or a non-5G service consumer.

In step **802**, a DNS server is queried using the FQDN in the DNS resolution request. For example, DNS discoverer micro-service **300** may query external DNS servers **306** using an FQDN in a DNS request received from a DNS discoverer consumer.

In step **804**, a DNS response is received from the DNS server and, in step **806**, the addresses of producer NF service endpoints are stored in the

DNS discoverer database (i.e., in persistent database **310**). For example, DNS discoverer micro-service **300** may receive DNS responses from DNS servers **306** and store the IP addresses or IP endpoints associated with producer NF service endpoints in database **310**. In one example, the DNS resolution request from DNS discoverer micro-service **300** may be a DNS-A resolution request, and DNS servers **306** may return an IPv4 address or addresses corresponding to a service endpoint or endpoints associated with the FQDN. In another example, the DNS resolution request may be a DNS-AAAA request, and DNS servers **306** may return an IPv6 address or addresses corresponding to a service endpoint or endpoints associated with the FQDN. In yet another example, the DNS resolution request may be a DNS-SRV request, and DNS servers may return an IP address(es) and port number(s) corresponding to a service endpoint or endpoints associated with the FQDN.

In step **808**, a DNS response is sent to the requesting node. For example, DNS discoverer micro-service **300** may send a response to the requesting node including addresses associated with producer NF service endpoints received in the DNS response from DNS servers **306**.

In step **810**, FQDNs in the DNS discoverer database are monitored for changes in address. For example, DNS records change discoverer **400** may, for each FQDN whose TTL has expired in database **310**, query external DNS servers **306** to determine any IP address or IP endpoint changes.

In step **812**, the requesting node is notified of any changes in IP address or IP endpoint associated with the FQDN. For example, DNS records change discoverer **400** may notify SCP micro-services or consumer NF **302** of any detected changes in IP address(es) or IP endpoints associated with an FQDN for which SCP micro-services or consumer NF **302** has queried DNS discoverer micro-service **300**.

Thus, the subject matter described herein includes a DNS discoverer micro-service that discovers IP addresses or IP endpoints associated with producer NF service endpoints and monitors FQDNs for changes in such addresses. One advantage of such a service is the fact that consumer NFs and SCPs are not required to discover or actively monitor producer NFs for

changes in IP addresses or IP endpoints associated with a service. The consumer NF or SCP is only required to learn the FQDN of a service and communicate the FQDN to the DNS discoverer micro-service. In addition, because the DNS discoverer micro-service actively monitors FQDNs for

5 changes in IP address or IP endpoint, load balancing by nodes, such as SCPs and consumer NFs, will be more evenly distributed among producer NF service endpoints.

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

10 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 discovering and tracking addresses associated with producer network function (NF) service endpoints, the method comprising:
 - receiving a first domain name system (DNS) resolution request from a requesting node;
 - querying a DNS server using a fully qualified domain name (FQDN) extracted from the first DNS resolution request;
 - receiving a first response from the DNS server, the first response including an address associated with a producer NF service endpoint associated with the FQDN;
 - storing the address associated with the producer NF service endpoint in a database;
 - communicating the address associated with the producer NF service endpoint to the requesting node;
 - monitoring the FQDN for changes in address associated with the FQDN; and
 - notifying the requesting node of the changes in address associated with the FQDN.
2. The method of claim 1 wherein receiving the first DNS resolution request from a requesting node includes receiving the first DNS resolution request from a service communications proxy (SCP).
3. The method of claim 1 wherein receiving the first DNS resolution request from a requesting node includes receiving the first DNS resolution request from a consumer NF or a non-5G service consumer.
4. The method of any preceding claim wherein receiving the first DNS resolution request includes receiving the first DNS resolution request at a representational state transfer (REST) server interface provided by a DNS discoverer micro-service.
5. The method of any preceding claim wherein querying the DNS server includes querying the DNS server from a DNS discoverer micro-service separate from the requesting node and the DNS server.

6. The method of claim 4 wherein storing the address associated with the producer NF service comprises storing the address in a database local to the DNS discoverer micro-service.
7. The method of any preceding claims wherein monitoring the FQDN comprises:
 - 5 detecting expiration of a record storing the address or associated with the producer NF service endpoint in the database;
in response to detecting expiration of the record, querying the DNS server using the FQDN;
 - 10 receiving a second response from the DNS server;
comparing an address in the second response to the address associated with the FQDN stored in the record in the database; and
determining that a change address associated with the FQDN has occurred in response to the address in the second response being
15 different from the address associated with the FQDN stored in the record in the database.
8. The method of any preceding claim wherein the address associated with the producer NF service endpoint comprises an Internet protocol (IP) address or an IP endpoint.
- 20 9. The method of any preceding claim wherein monitoring the FQDN for changes in address includes continually monitoring the FQDN for changes in address until stopped in response to a message from the requesting node to cease monitoring the FQDN.
10. The method of claim 9 wherein the message from the requesting node to cease monitoring the FQDN comprises a second DNS resolution
25 request including a DELETE method type, and, in response, ceasing monitoring the FQDN.
11. A system for discovering and tracking addresses associated with producer network function (NF) service endpoints, the system
30 comprising:
 - a computing platform including at least one processor; and
 - a domain name system (DNS) discover micro-service located on the computing platform and implemented by the at least one processor

- for receiving a first domain name system (DNS) resolution request from a requesting node, querying a DNS server using a fully qualified domain name (FQDN) extracted from the first DNS resolution request, receiving a first response from the DNS server, the first response including an address associated with a producer NF service endpoint associated with the FQDN, storing the address associated with the producer NF service endpoint in a database, communicating the address associated with the producer NF service endpoint to the requesting node, monitoring the FQDN for changes in address associated with the FQDN, and notifying the requesting node of the changes in address associated with the FQDN.
12. The system of claim 11 wherein the DNS discoverer micro-service is configured to receive the first DNS resolution request from a service communications proxy (SCP).
13. The system of claim 11 wherein the DNS discoverer micro-service is configured to the first DNS resolution request from a consumer NF or a non-5G service consumer.
14. The system of any of claims 11 to 13 wherein the DNS discoverer micro-service includes a representational state transfer (REST) server interface for receiving the first DNS resolution request from the requesting node.
15. The system of any of claims 11 to 14 wherein the computing platform and the DNS discoverer micro-service are separate from the requesting node and the DNS server.
16. The system of claim 15 wherein the database is local to the DNS discoverer micro-service.
17. The system of any of claims 11 to 16 wherein the DNS discoverer micro-service includes a DNS records change discoverer for performing the monitoring of the FQDN by:
- detecting expiration of a record storing the address associated with the producer NF service endpoint in the database;
- in response to detecting expiration of the record, querying the DNS server using the FQDN;

- receiving a second response from the DNS server;
comparing an address in the second response to the address associated with the producer NF service endpoint stored in the record in the database; and
- 5 determining that a change in address associated with the FQDN has occurred in response to the address in the second response being different from the address associated with the producer NF service endpoint stored in the record in the database.
18. The system of any of claims 11 to 17 wherein the address associated
10 with the producer NF service endpoint comprises an Internet protocol (IP) address or an IP endpoint.
19. The system of claim 17 wherein the DNS record change discoverer is configured to continually monitor the FQDN for changes in address until stopped in response to a message from the requesting node to cease
15 monitoring the FQDN.
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:
- 20 receiving a first domain name system (DNS) resolution request from a requesting node;
- querying a DNS server using a fully qualified domain name (FQDN) extracted from the first DNS resolution request;
- receiving a first response from the DNS server, the response including an address associated with a producer network function (NF)
25 service endpoint associated with the FQDN;
- storing the address associated with the producer NF service endpoint in a database;
- communicating the address associated with the producer NF service endpoint to the requesting node;
- 30 monitoring the FQDN for changes in address associated with the FQDN; and
- notifying the requesting node of the changes in address associated with the FQDN.

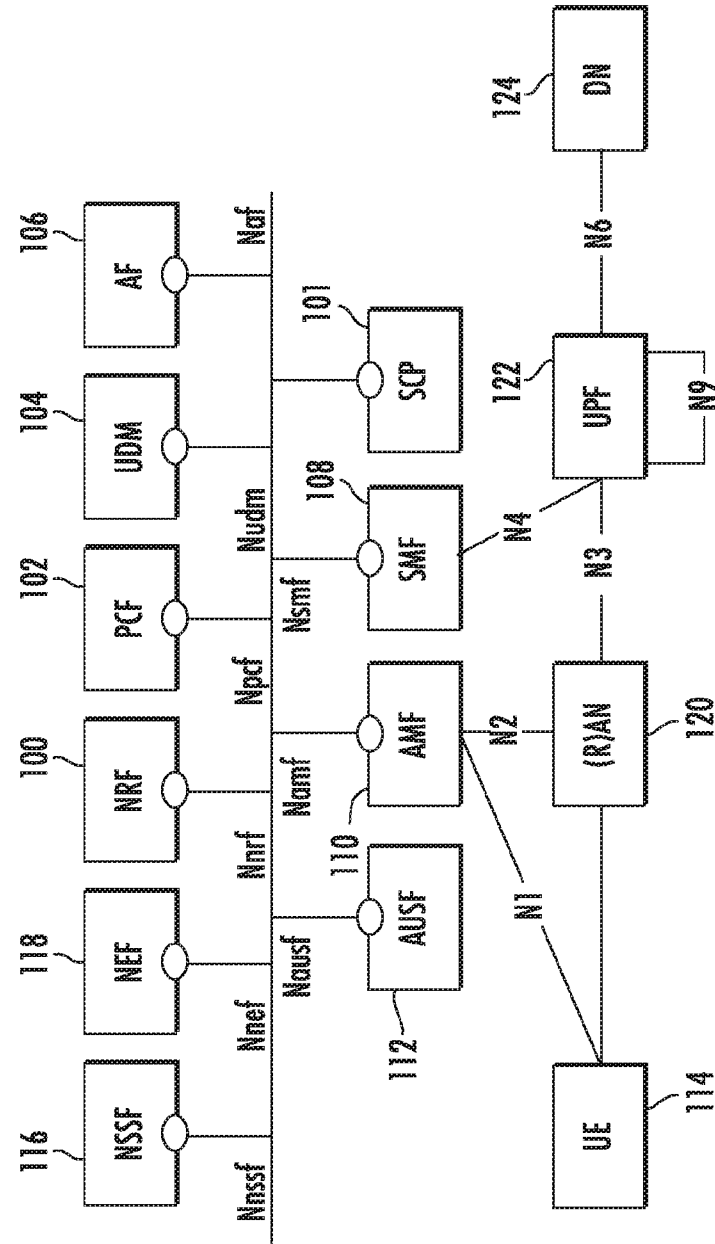


FIG. 1

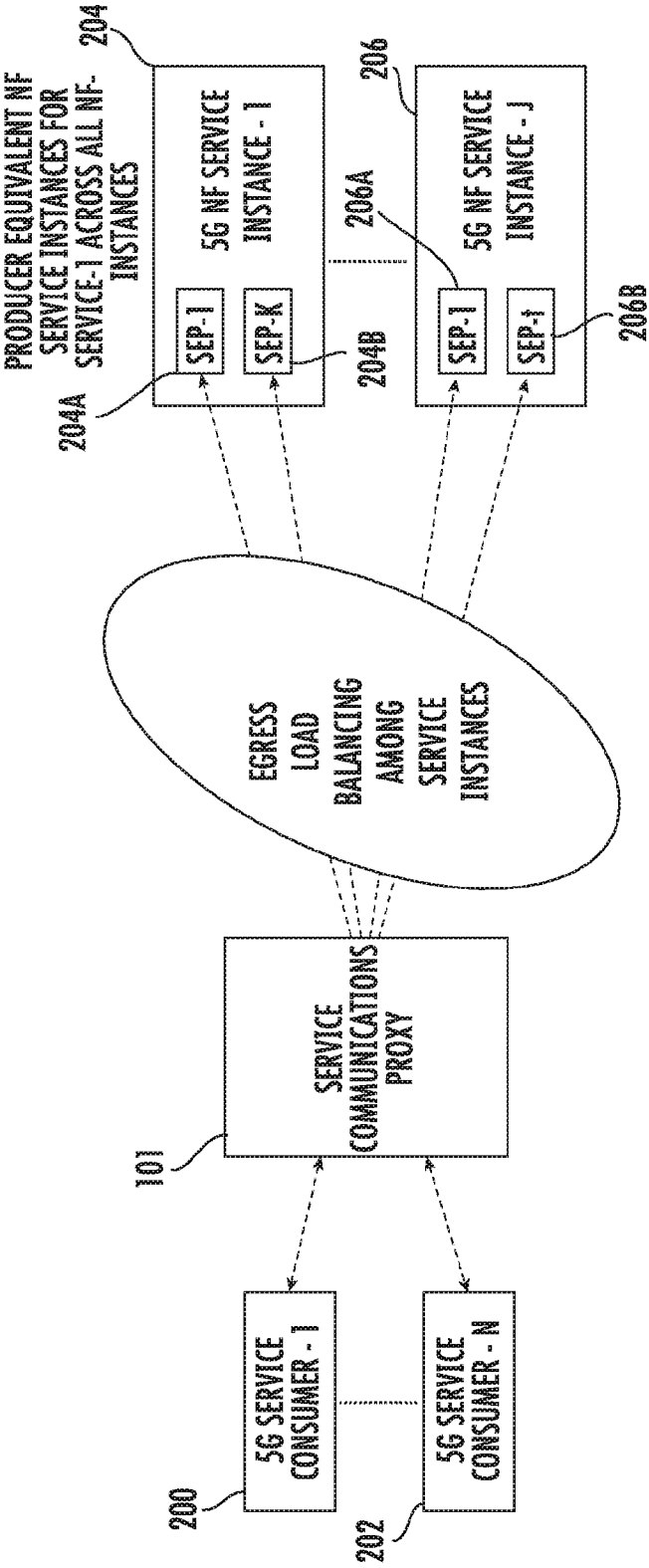
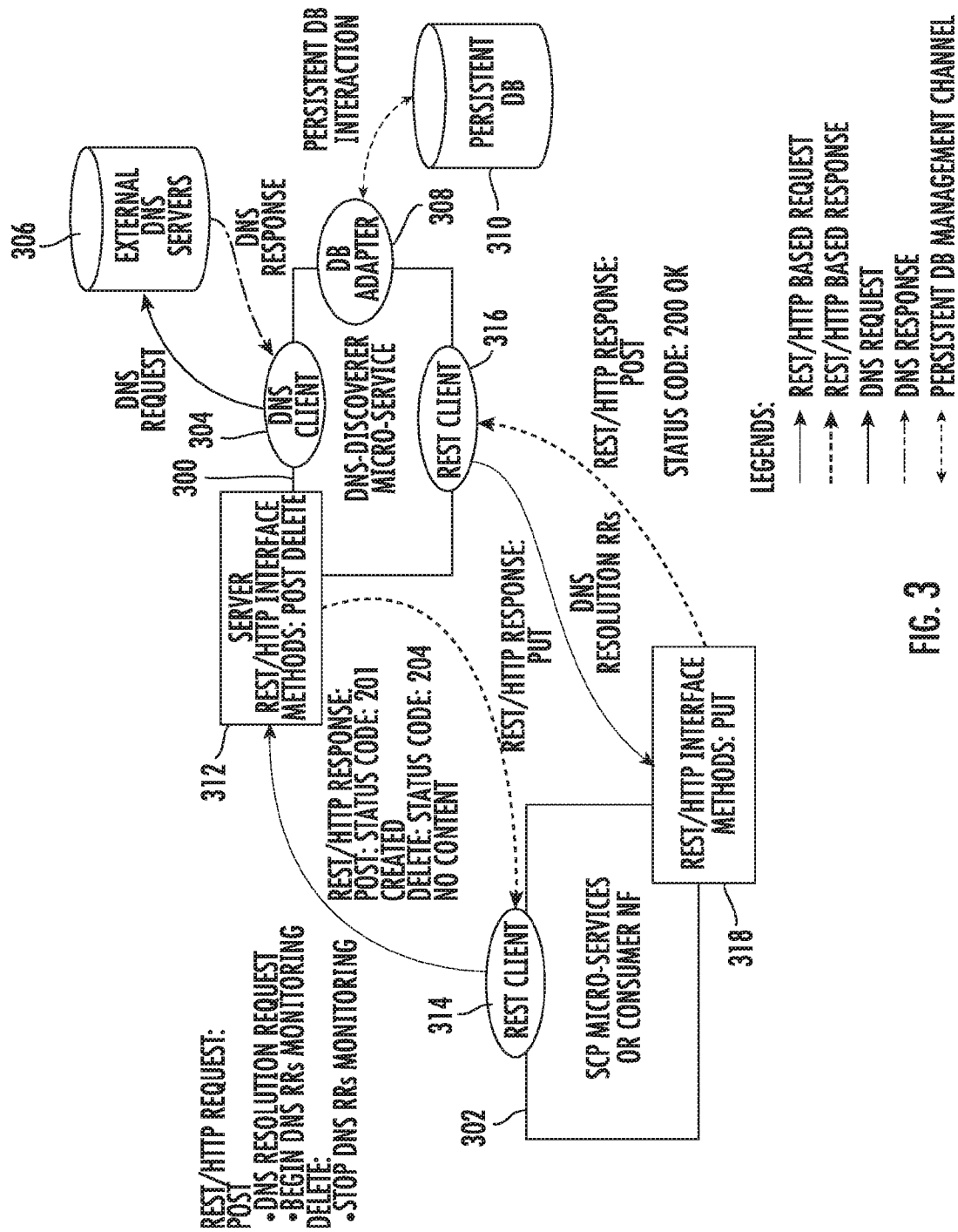


FIG. 2



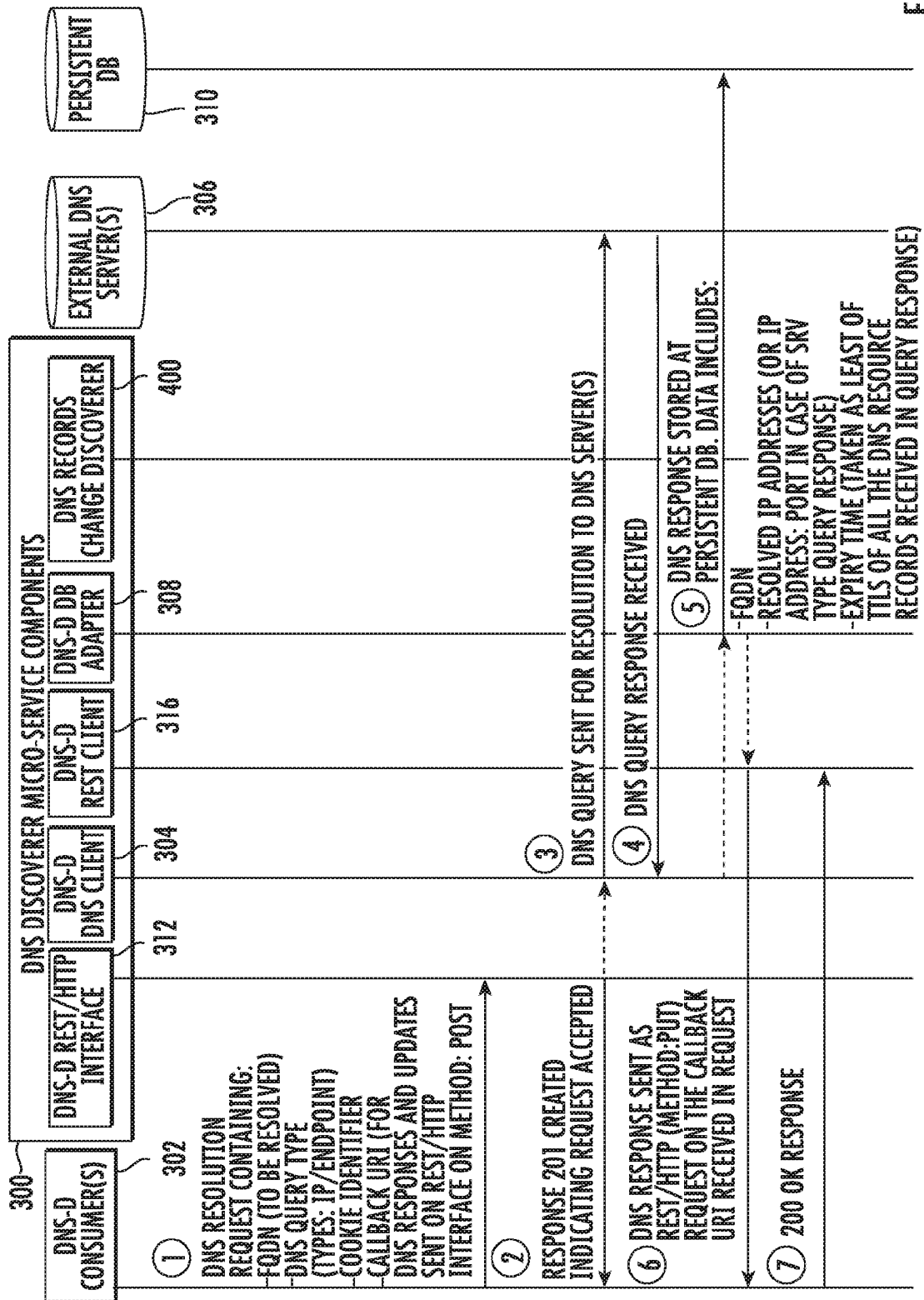


FIG. 4

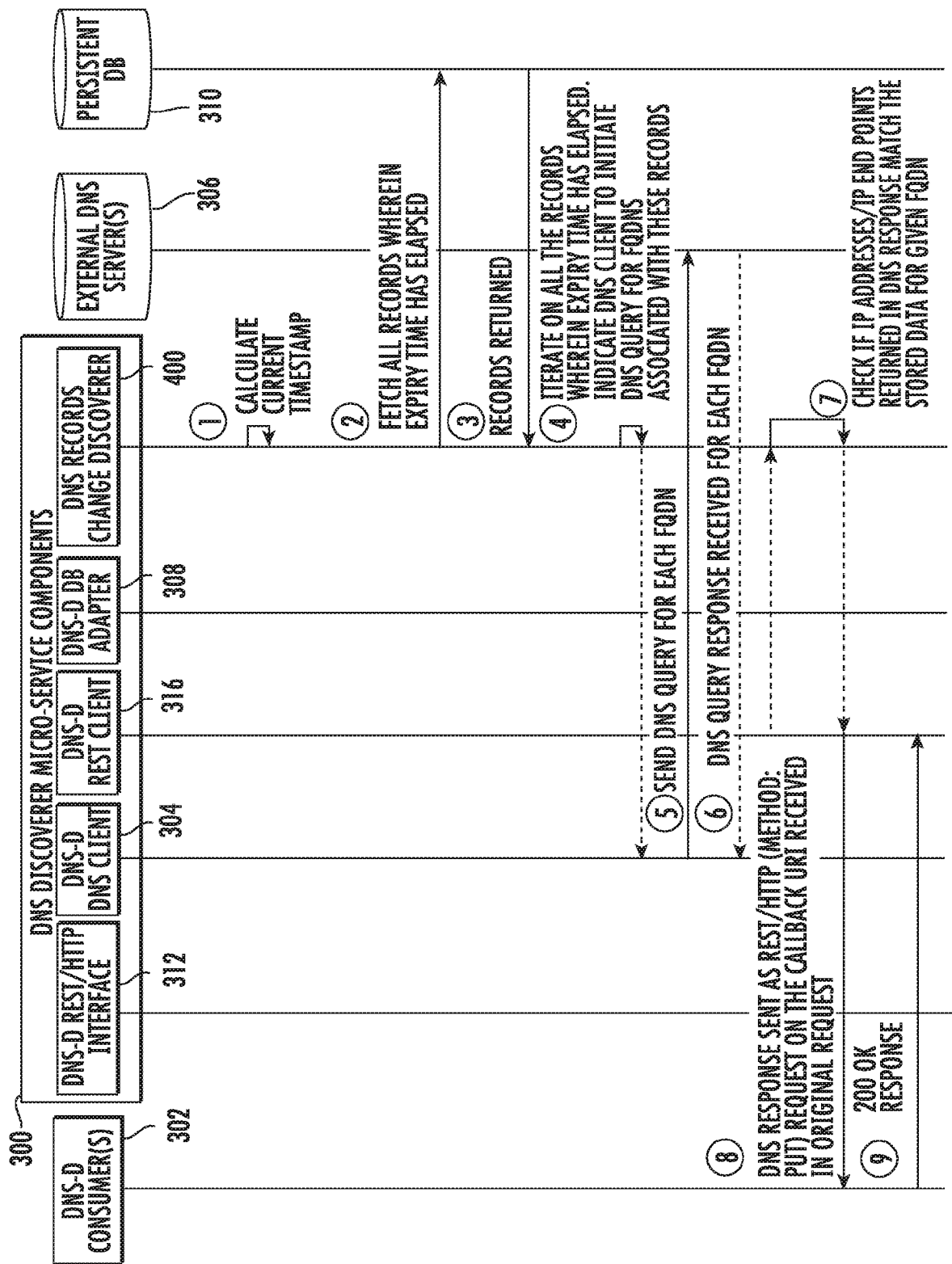


FIG. 5

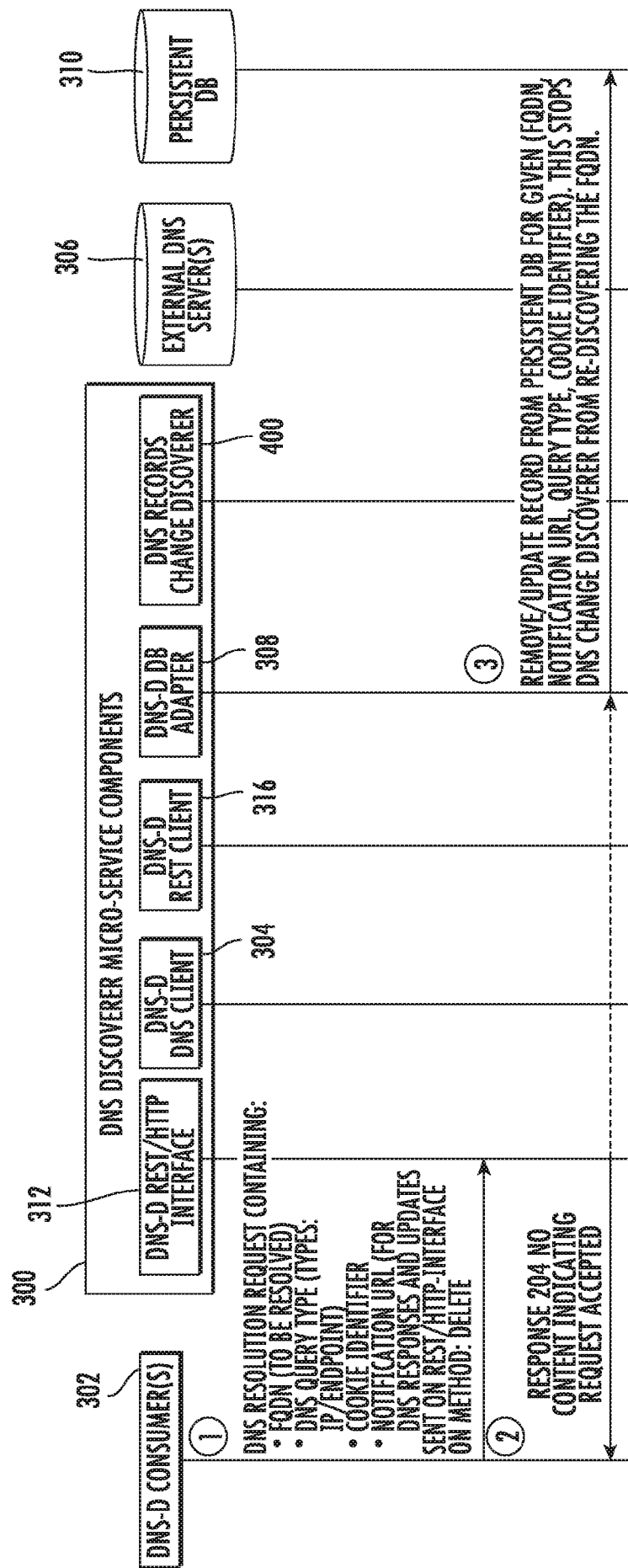


FIG. 6

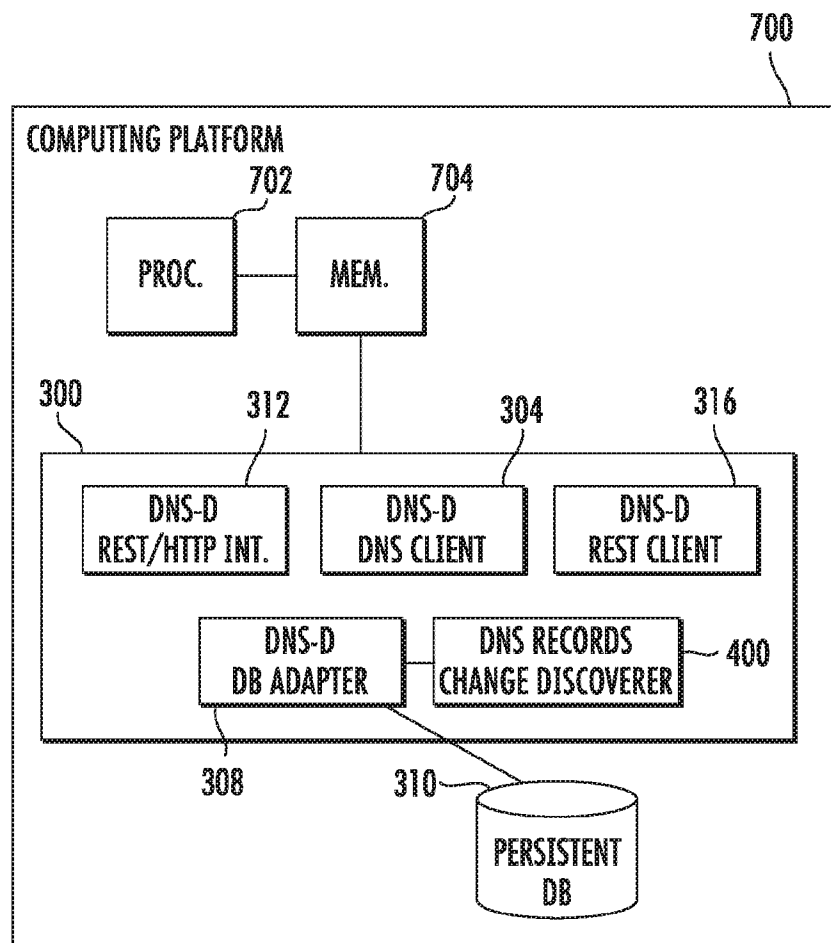


FIG. 7

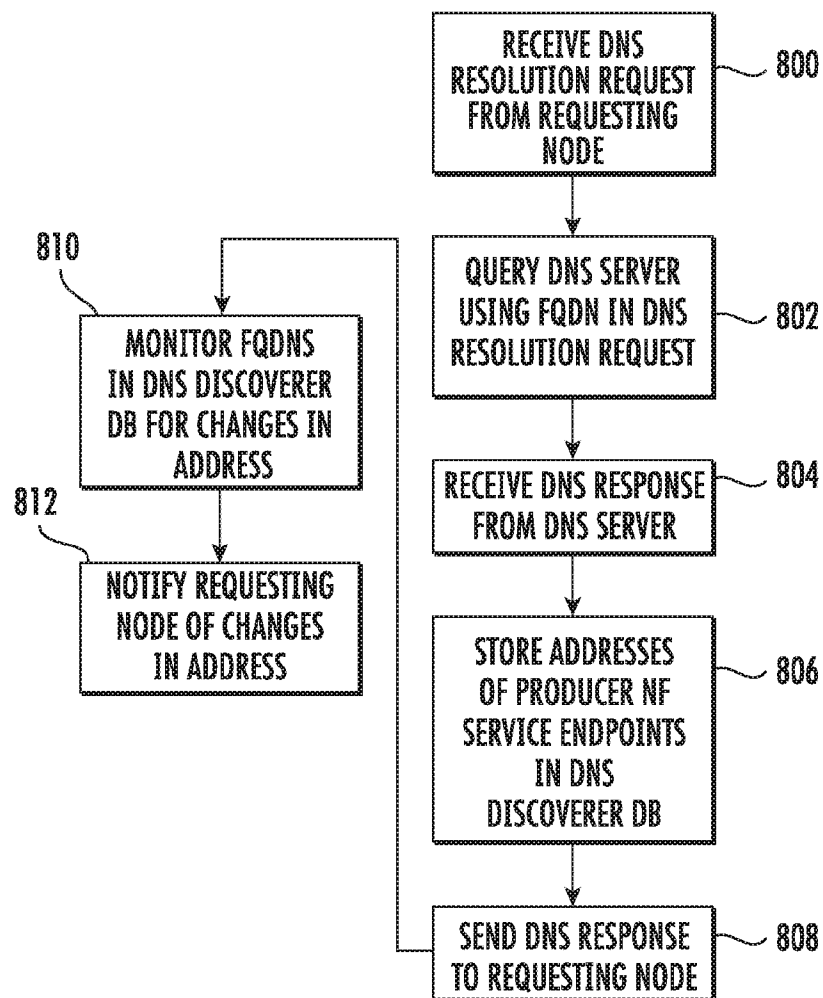


FIG. 8

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2020/035004

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/12
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)

EP0-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CHESHIRE M KROCHMAL APPLE INC S: "Apple's DNS Long-Lived Queries protocol ;draft-sekar-dns-llq-06.txt", APPLE'S DNS LONG-LIVED QUERIES PROTOCOL ;DRAFT-SEKAR-DNS-LLQ-06.TXT ;INTERNET-DRAFT: NETWORK WORKING GROUP, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE no. 6 23 August 2019 (2019-08-23), pages 1-26, XP015134842, Retrieved from the Internet: URL:https://tools.ietf.org/html/draft-sekar-dns-llq-06 [retrieved on 2019-08-23] abstract paragraphs [0001], [01.1], [0004], -/--	1-20



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

29 June 2020

Date of mailing of the international search report

07/07/2020

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Goller, Wolfgang

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2020/035004

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	[05.3], [0006] -----	
X	CN 109 788 078 A (HUAWEI TECH CO LTD) 21 May 2019 (2019-05-21) the whole document	1-20
X	US 2009/222584 A1 (JOSEFSBERG ARNE [US] ET AL) 3 September 2009 (2009-09-03) paragraphs [0053] - [0056], [0060] - [0065] -----	1-20
A	ABLEY ICANN W KUMARI GOOGLE J: "A Mechanism for Remote-Triggered DNS Cache Flushes (DNS FLUSH); draft-jabley-dnsop-dns-flush-00.txt", A MECHANISM FOR REMOTE-TRIGGERED DNS CACHE FLUSHES (DNS FLUSH); DRAFT-JABLEY-DNSOP-DNS-FLUSH-00.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, SWITZERLAND, 24 June 2013 (2013-06-24), pages 1-12, XP015090421, [retrieved on 2013-06-24] the whole document -----	1-20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2020/035004

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
CN 109788078	A	21-05-2019	NONE	

US 2009222584	A1	03-09-2009	NONE	
