US 20170257341A1

(19) United States

(12) Patent Application Publication

ARSENAULT et al.

(10) Pub. No.: US 2017/0257341 A1

(43) Pub. Date: Sep. 7, 2017

(54) DYNAMIC GENERATION OF UNIQUE IDENTIFIERS IN A SYSTEM OF CONNECTED THINGS

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)**, Stockholm (SE)

(72) Inventors: **Marc-Olivier ARSENAULT**, St-Constant (CA); **Steven Rochefort ROCHEFORT**, Pointe Claire (CA); **Lila MADOUR**, Kirkland (CA)

(73) Assignee: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)**, Stockholm (SE)

(21) Appl. No.: **15/513,032**

(22) PCT Filed: **Oct. 3, 2014**

(86) PCT No.: **PCT/IB2014/065050**

§ 371 (c)(1),
(2) Date: **Mar. 21, 2017**

Publication Classification

(51) **Int. Cl.**

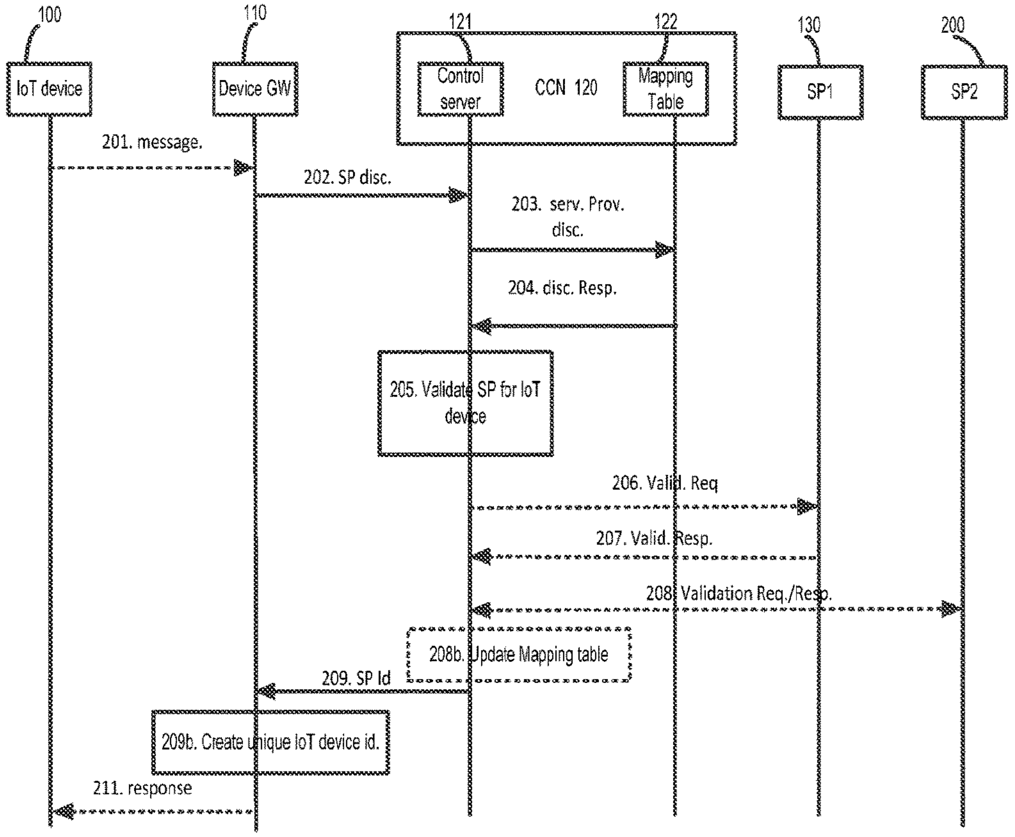
H04L 29/12	(2006.01)
G06F 21/73	(2006.01)
H04W 4/00	(2006.01)
H04L 29/08	(2006.01)

(52) **U.S. Cl.**

CPC ***H04L 61/20*** (2013.01); ***H04L 61/6004*** (2013.01); ***H04L 67/16*** (2013.01); ***G06F 21/73*** (2013.01); ***H04L 61/6022*** (2013.01); ***H04L 67/303*** (2013.01); ***H04W 4/005*** (2013.01); ***H04L 67/327*** (2013.01)

(57) ABSTRACT

Embodiments of the invention relates to methods, and apparatuses for dynamically creating and updating unique internet of Things (IoT) device identifiers in a common communication network, for the purpose of identifying different IoT devices from multiple access and transport technologies. The IoT devices are associated to various service provider networks, and this disclosure enables dynamic updates of the associations in the common communication network, allowing one or more of the IoT devices to be associated to different service provider networks at any given time.



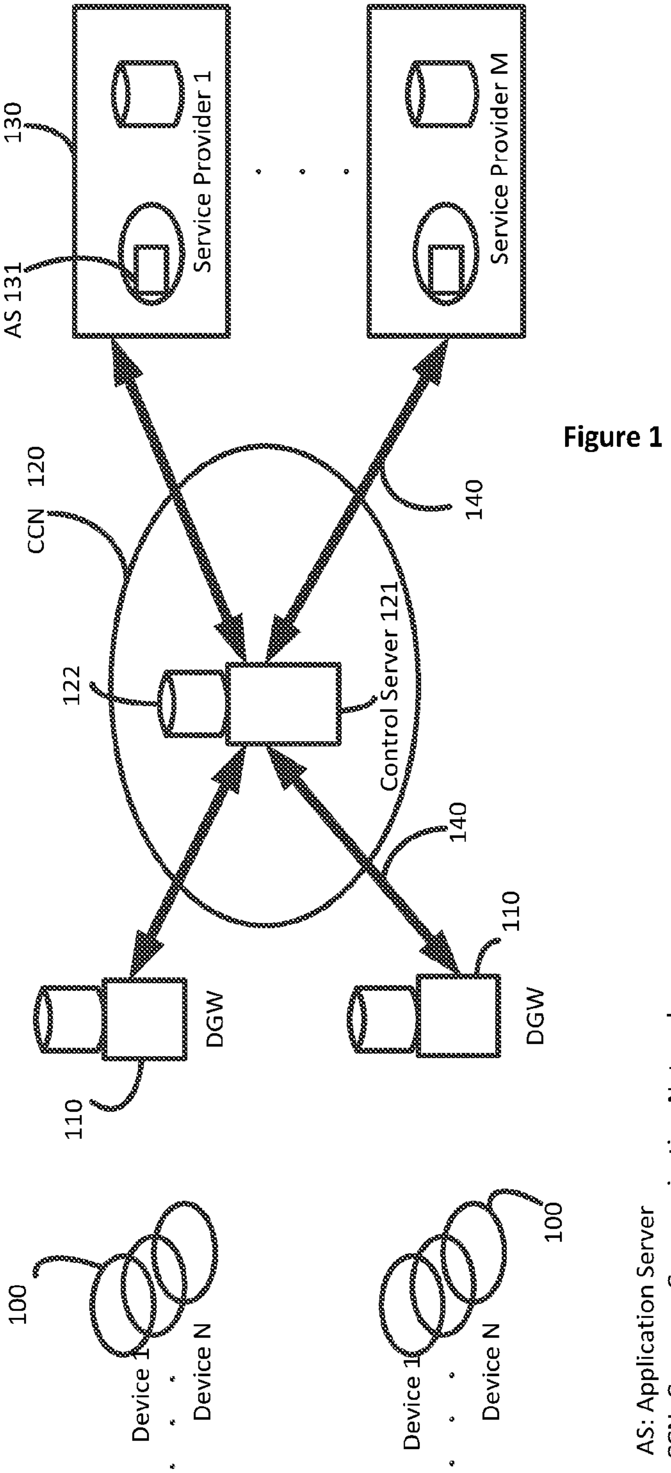


Figure 1

AS: Application Server
CCN: Common Communication Network

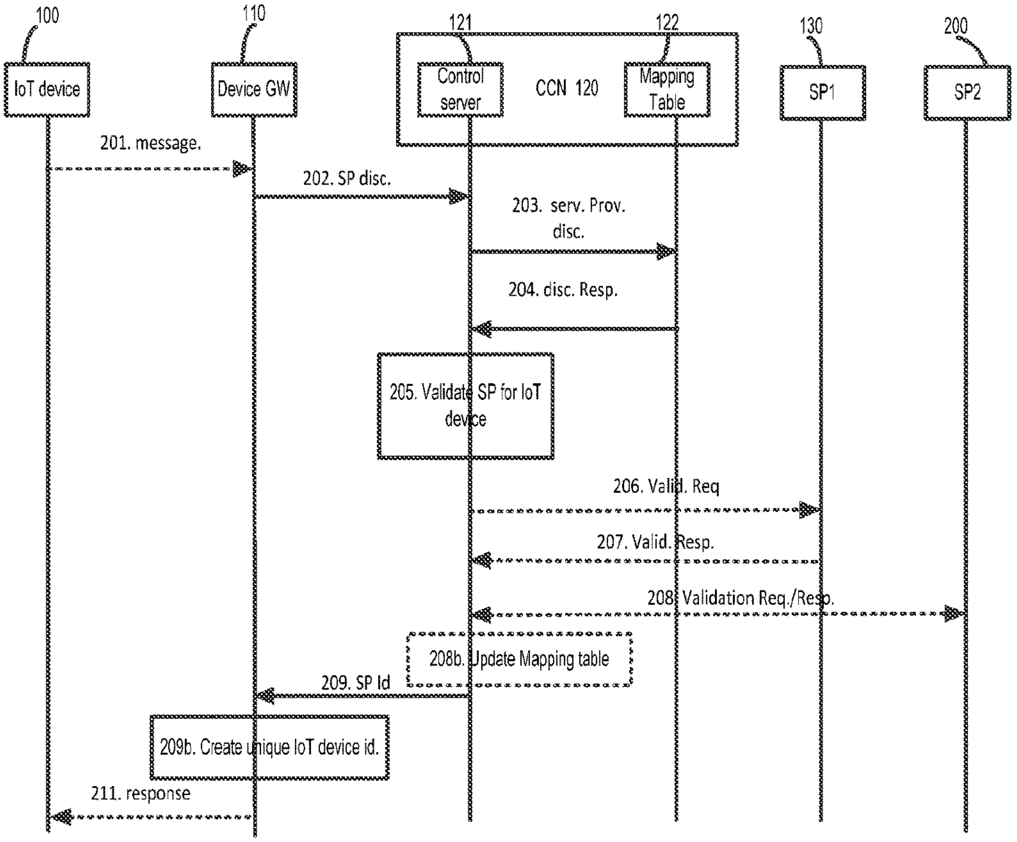

100
110
121
122
130
200
IoT device
Device GW
Control server
CCN 120
Mapping Table
SP1
SP2
201. message.
202. SP disc.
203. serv. Prov. disc.
204. disc. Resp.
205. Validate SP for IoT device
206. Valid. Req
207. Valid. Resp.
208. Validation Req./Resp.
208b. Update Mapping table
209. SP Id
209b. Create unique IoT device id.
211. response

Figure 2

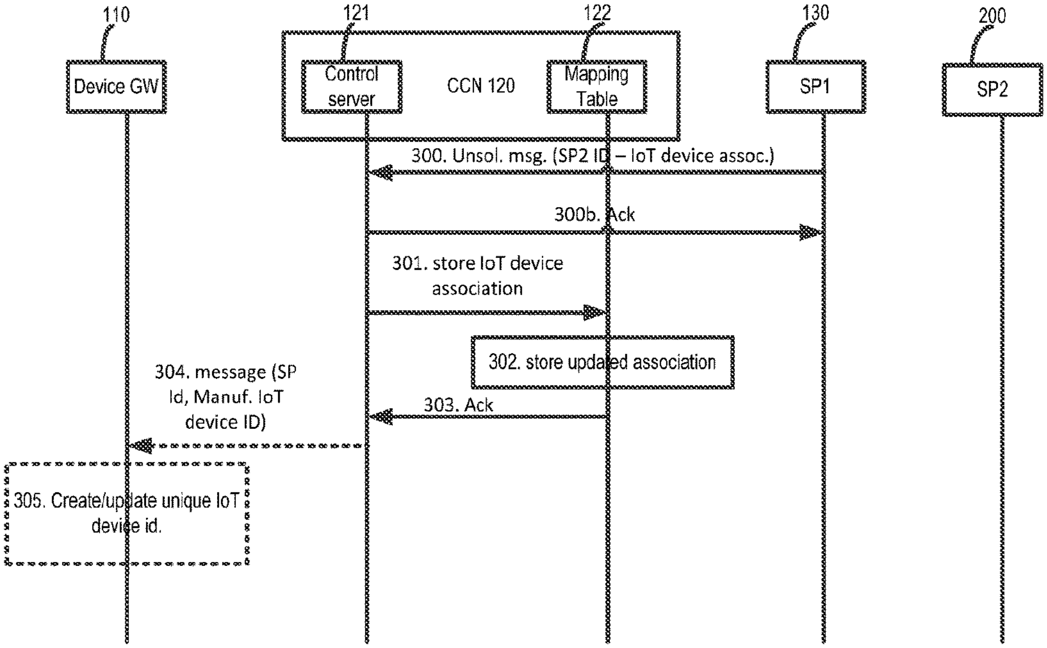

110
121
122
130
200
Device GW
Control server
CCN 120
Mapping Table
SP1
SP2
300. Unsol. msg. (SP2 ID – IoT device assoc.)
300b. Ack
301. store IoT device association
302. store updated association
303. Ack
304. message (SP Id, Manuf. IoT device ID)
305. Create/update unique IoT device id.

Figure 3

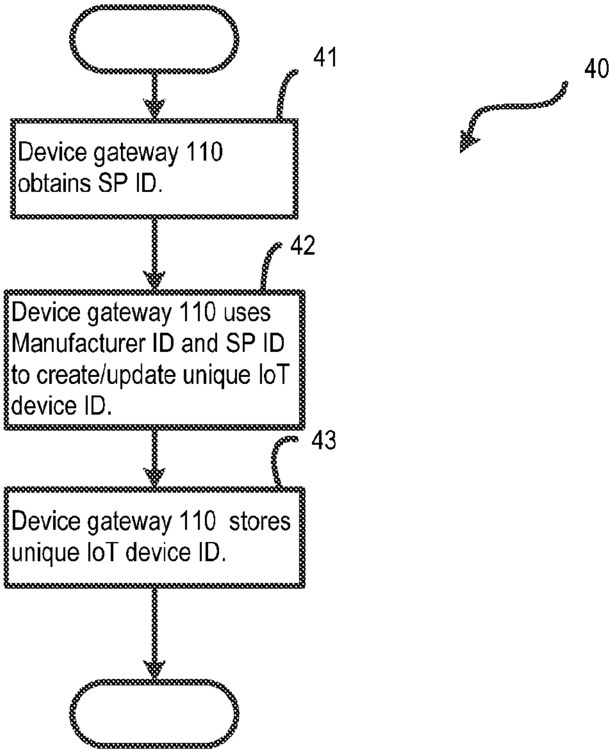

41
40
Device gateway 110 obtains SP ID.
42
Device gateway 110 uses Manufacturer ID and SP ID to create/update unique IoT device ID.
43
Device gateway 110 stores unique IoT device ID.

Figure 4a (Method in Device gateway)

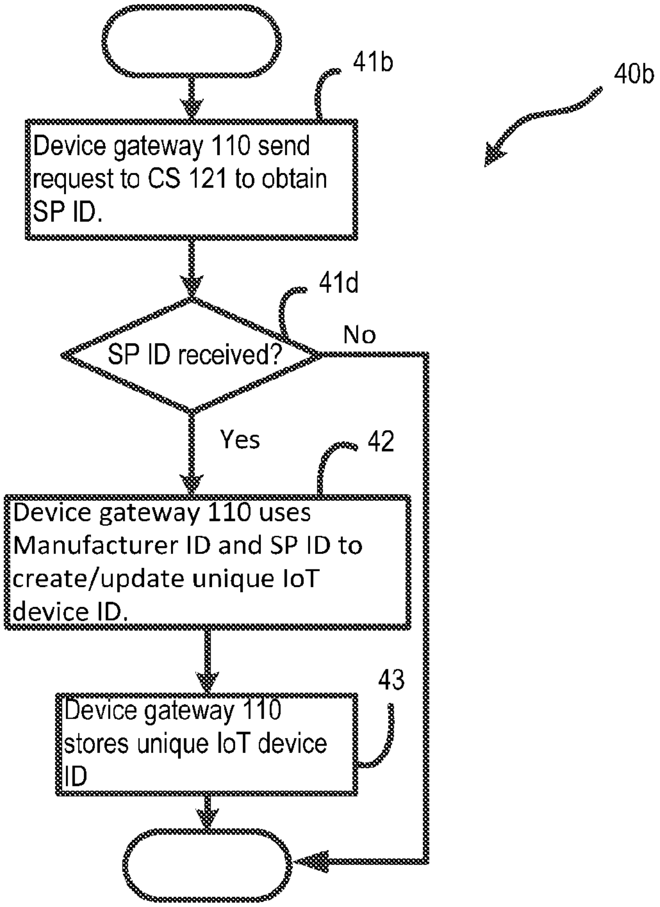

41b
40b
Device gateway 110 send request to CS 121 to obtain SP ID.
41d
SP ID received?
No
Yes
42
Device gateway 110 uses Manufacturer ID and SP ID to create/update unique IoT device ID.
43
Device gateway 110 stores unique IoT device ID

Figure 4b (Method in Device gateway)

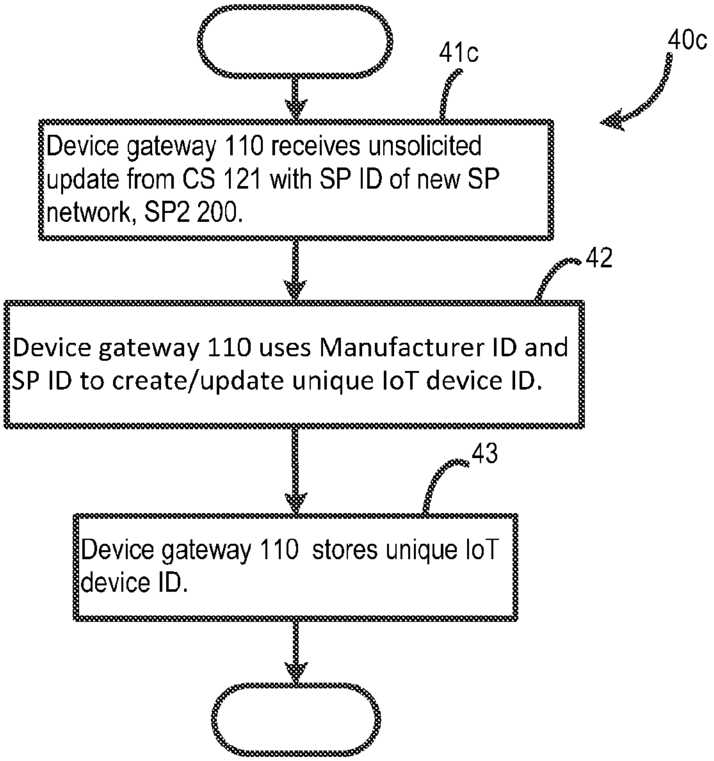

40c
41c
Device gateway 110 receives unsolicited update from CS 121 with SP ID of new SP network, SP2 200.
42
Device gateway 110 uses Manufacturer ID and SP ID to create/update unique IoT device ID.
43
Device gateway 110 stores unique IoT device ID.

Figure 4c (Method in Device gateway)

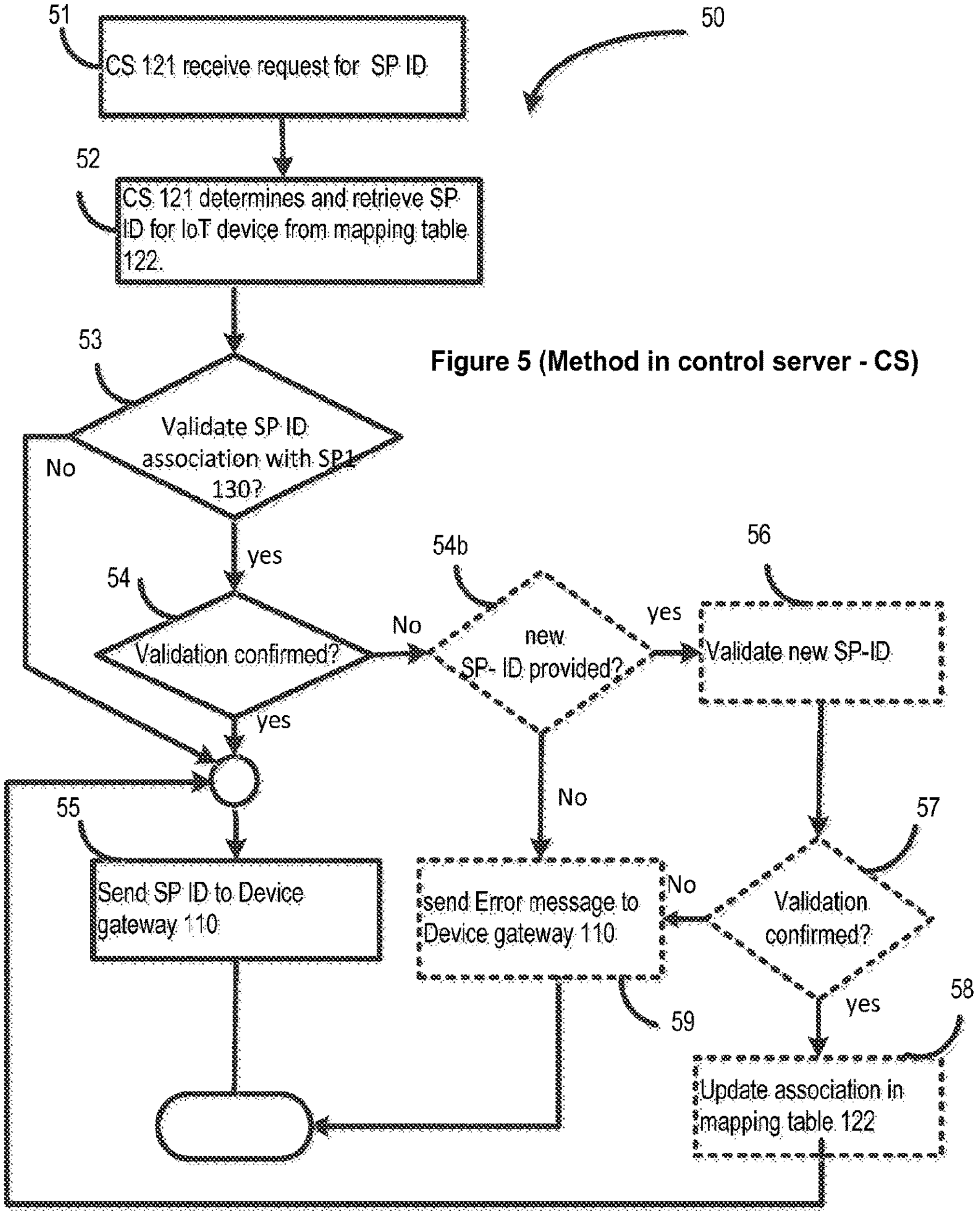

50
51
CS 121 receive request for SP ID
52
CS 121 determines and retrieve SP ID for IoT device from mapping table 122.
53
Validate SP ID association with SP1 130?
No
yes
54
Validation confirmed?
No
yes
54b
new SP- ID provided?
yes
No
56
Validate new SP-ID
57
Validation confirmed?
No
yes
55
Send SP ID to Device gateway 110
send Error message to Device gateway 110
59
58
Update association in mapping table 122

Figure 5 (Method in control server - CS)

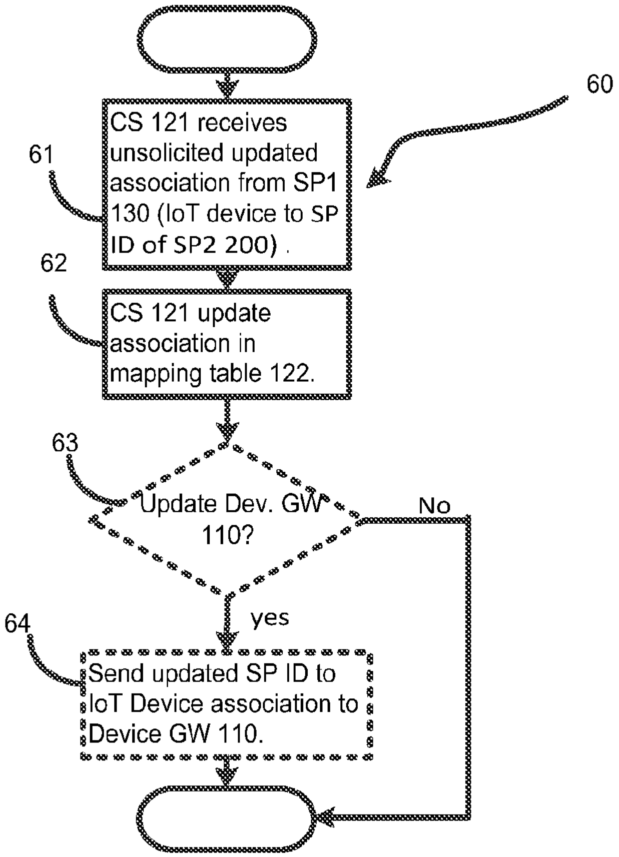

60
61
CS 121 receives unsolicited updated association from SP1 130 (IoT device to SP ID of SP2 200) .
62
CS 121 update association in mapping table 122.
63
Update Dev. GW 110?
No
yes
64
Send updated SP ID to IoT Device association to Device GW 110.

Figure 6 (Method in control server - CS)

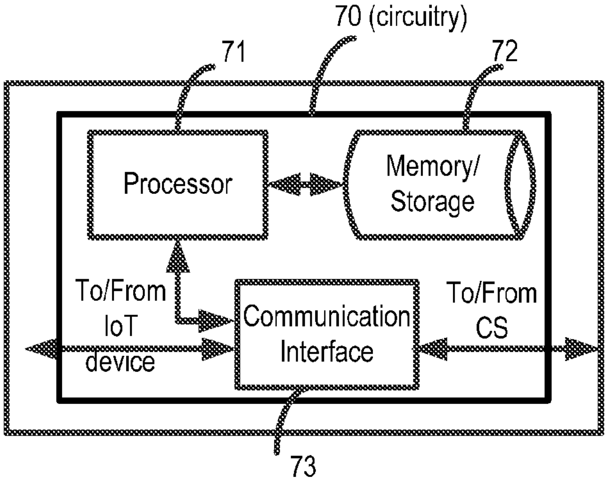


Figure 7 (Device Gateway)

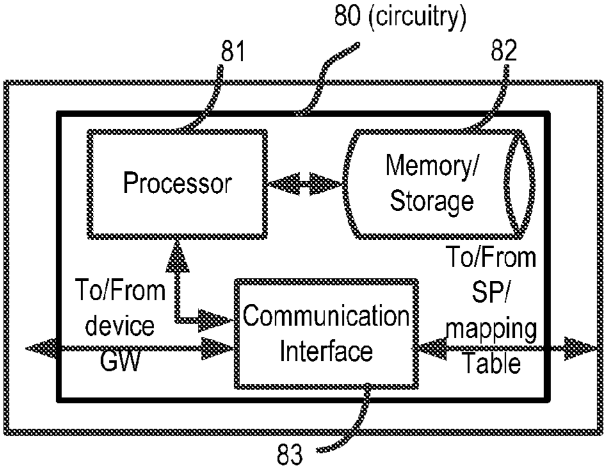


Figure 8 (Control Server - CS)

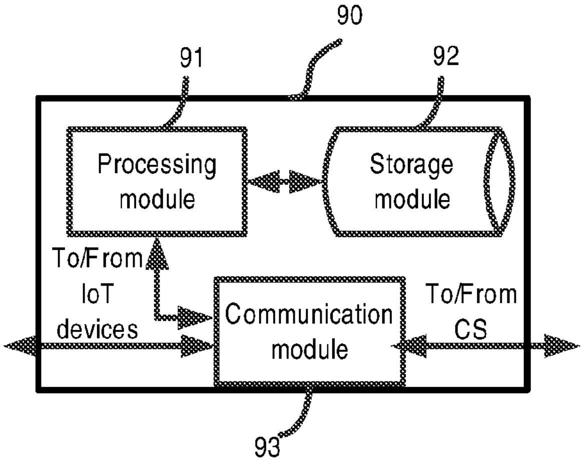


Figure 9 (Device Gateway)

DYNAMIC GENERATION OF UNIQUE IDENTIFIERS IN A SYSTEM OF CONNECTED THINGS

TECHNICAL FIELD

[0001] This disclosure relates generally to dynamically generating of unique identifiers for connecting Internet of Things (IoT) devices to the application servers over a communication network.

BACKGROUND

[0002] There is an increasing trend in integrating the internet with the physical world to create the Internet of Things (IoT), also referred to as Cloud of Things, Internet of Objects, Machine-to-Machine (M2M) communications, with a prediction that up to 50 billion devices will be connected to the internet by 2020. Connecting remote devices, machines, assets and other entities to create value-based systems, to optimize a variety of goods-delivery mechanisms and to improve people's lives represent the primary value proposition for the IoT. The term IoT is used henceforth in this disclosure to include not only the internet of things or objects, but also M2M communications.

[0003] Driving this trend is the emergence of various wireless technologies comprising low-cost wireless technologies such as Wi-Fi, ZIGBEE™, Z-WAVE™, etc. and other cellular technology such as 3G and Long Term Evolution (LTE), coupled with a growing proliferation of connected things or IoT devices such as connected consumer electronics, intelligent devices with integrated sensors, devices with actuation capabilities, smartphones, intelligent appliances, etc.

[0004] It is also desirable to use a common communication network for connecting IoT devices to their corresponding application servers in the various service provider networks. A typical deployment today consists of using separate or dedicated communication systems/networks to connect IoT devices from local/residential networks to the corresponding application servers offering different services.

[0005] An new trend is developing, and it consists of using a common communication network to support all the different IoT devices regardless of the communication interface they support, i.e., the IoT devices may be communicating over any type of access including but not limited to Wi-Fi, ZIGBEE™, Z-WAVE™, or 3G/4G/5G interfaces. According to this model, all the communications from the IoT devices converge to be transported through the common communication network to the various application servers in the corresponding service provider networks. One particularity of such system is that it should be able to cope efficiently with IoT devices changing their service provider network associations.

[0006] Indeed, it is common nowadays for a user of a given service to switch service providers when a competitive market exists. When users are confronted with that situation, the new selected service provider will have to re-install and commission its own new IoT devices at the user's premises, or the user will have to purchase a new IoT device. The user may need to pay additional fees, and sometimes deal with the extra burden of familiarizing himself with using the new IoT devices. The previously installed devices are usually decommissioned and returned to the service provider or discarded, which could lead to undesired environmental and economic impact.

[0007] Other likely scenario consists of a service provider selling one or more deployed services/applications to another service provider. To support this scenario, the new service provider may replace the IoT devices in the local/residential premises and may additionally update all the routing tables so the data from the new IoT devices is routed to the new service provider. The association between the IoT device and the service provider network is typically treated as a static business association and for many services, that association cannot be changed. The IoT devices used by a service provider network typically have manufacturer-defined IoT device identifiers.

[0008] Manufacturer-defined IoT device identifiers come in various formats. A well-known and used manufacturer-defined IoT device identifier is an Extended Unique Identifier (EUI) such as a 48-bit Extended Unique Identifier (EUI-48™) or a 64-bit Extended Unique Identifier (EUI-64™). EUI-48™ and EUI-64™, also referred to as Media Access Control (MAC) addresses that are bound to the hardware of the devices.

[0009] In a 48 bit MAC address, the leftmost 24 bits, called "prefix", is used to indicate an organizationally unique identifier (OUI) or a company ID (CID). An OUI is a 24-bit globally unique assigned number referenced by various standards and used to identify an organization/company where a globally unique identifier is needed. A CID, like the OUI, is a unique 24-bit identifier. However a CID cannot be used to generate universally unique MAC addresses. Therefore, the CID is especially applicable in applications where unique MAC addresses are not required. Each company/vendor and organization registers and obtains a CID or an OUI as assigned by the Institute of Electrical and Electronics Engineers (IEEE). One vendor or organization may own many CIDs or OUIs associated with their different products. The rightmost digits of a 48 bit MAC address indicate an identification number as assigned to the device by the vendor or the organization. Devices sharing the same OUI are assigned unique 24-bit identification numbers.

[0010] Some networks also use 64 bit MAC addresses, such as ZIGBEE™ networks or networks based on IEEE 802.15.4.

[0011] Typically, when a service provider deploys services at a user's residence or at a manufacturing plant, services such as a home automation services, surveillance or smart metering services, the service provider deploys the corresponding IoT devices that enable the services. The IoT devices may have MAC addresses comprising same or different OUI values. If the service provider is changed, its corresponding IoT devices are removed and replaced with other IoT devices provided by the new service provider. Sometimes the user is required to pay additional fees for installation of the new IoT devices. The new IoT devices have different MAC addresses comprising same or different OUI values. Although the OUI values are unique when assigned by the IEEE, the OUI cannot always be used to accurately identify the service provider that is currently providing the service and hence the ability to transport the data from the IoT device to the corresponding application server on the basis of the OUI alone is not sufficient.

[0012] When deploying a common communication network for the purpose of connecting all possible IoT devices, a number of challenges will have to be overcome. Some of those challenges include ease of service deployment, dynamic provisioning, dynamic unified identification, addressing and efficient transport of data from all the IoT devices to their associated service provider network.

[0013] PCT application PCT/IB2014/063785, entitled "data transfer in a System of connected Things" discloses one solution describing a common communication network connecting IoT devices over different wireless technologies to their corresponding application servers in different service provider networks without the IoT device or the common communication network knowing the corresponding application servers. The common communication network in PCT/IB2014/063785 supports different manufacturer IoT device identity format. Each IoT device has its own manufacturer IoT device identity, but the identity cannot be used as a unique IoT device identifier for communication within the common communication network. The common communication network efficiently transports data from an IoT device to the corresponding application server based on a unique IoT device identifier. PCT/IB2014/063785 does not disclose how it adapts to changing service provider network to IoT devices associations.

[0014] It would be desirable to provide a scalable system and method that obviate or mitigate the above described challenges.

SUMMARY

[0015] The following acronyms are used throughout this disclosure.

[0016] AS Application Server
[0017] CID Company IDentifier
[0018] CCN Common communication Network
[0019] CS Control Server
[0020] EUI Extended Unique Identifier
[0021] IoT Internet of things
[0022] MAC Media Access Control
[0023] OUI Organizational Unique Identifier
[0024] SP Service Provider

[0025] It is an object of the present invention to obviate or mitigate at least one disadvantage of the prior art and enable flexible and dynamic IoT device to service provider network association thereby dynamically creating and updating unique IoT device identifiers that would comprise the identity of the service provider network, and use the created unique IoT device identifier for IoT device communication over a common communication network such as the network described in PCT application PCT/IB2014/063785.

[0026] In accordance with the invention, there are provided methods and apparatuses according to the independent claims. Additional embodiments are set forth in the dependent claims.

[0027] According to one embodiment, a device gateway connected to one or more IoT devices obtains an identity of a service provider network associated to an IoT device. If a unique IoT device identifier is not already available at the device gateway then the device gateway creates a unique IoT device identifier by concatenating the identity of the service provider network associated to the IoT device with the manufacturer IoT device identity of the IoT device. If a unique IoT device identifier is already available at the device gateway then the device gateway updates the available unique IoT device identifier by concatenating the newly received identity of the service provider network with the existing manufacturer IoT device identity of the IoT device. Once the unique IoT device identifier is created or updated, the device gateway stores the identifier in its local memory.

[0028] According to another embodiment, the device gateway connected to one or more IoT devices determines that an IoT device, for which a manufacturer IoT device is known, has not been preconfigured with a unique IoT device identifier. The device gateway actively obtains the identity of the service provider network by sending a request message to a control server to request the identity of the service provider network associated with the IoT device, the request message comprises the manufacturer device identity. The control server is an entity of a common communication network. Once the device gateway acquires the service provider network identity associated with the IoT device, the device gateway dynamically creates a unique IoT device identifier comprising the acquired service provider network identity and the manufacturer device identity of the IoT device. In another embodiment, the device gateway may create a unique IoT device identifier by appending the service provider network identity, the manufacturer IoT device identity and the access technology type, as the manufacturer IoT device identity format may vary depending on the access technology type in use. The unique IoT device identifier could further be used to establish a path from the device gateway to the corresponding application server in the service provider network, over a common communication network, such as the one described in PCT application PCT/IB2014/063785, without the IoT device and the device gateway knowing the actual destination of the corresponding application server.

[0029] In one embodiment, the device gateway triggers the request message to request the service provider network identity associated with the IoT device, only if it receives a message from the IoT device that includes the manufacturer IoT device identity for which a unique IoT device identifier cannot be found.

[0030] One embodiment describes the request message as comprising a geographical location of the device gateway, as the device gateway may be a fixed residential gateway. Another embodiment further describes the message as comprising the subscription identity of the device gateway, as the device gateway may be a portable device with a subscription profile that may be maintained in the common telecommunication system or other network. In yet another embodiment, the request message may also comprise the service associated with the IoT device.

[0031] According to another embodiment, the device gateway connected to one or more IoT devices obtains an updated identity of the service provider network by receiving unsolicited update message from the control server in the common communication network. The unsolicited update message comprises one or more manufacturer IoT devices identifiers and the associated updated identity of the service provider network. This message will trigger the device gateway to update the corresponding unique IoT device identifiers by updating the identity of the service provider network associated with the one or more manufacturer IoT devices identities or create new unique IoT device identifiers if the one or more manufacturer IoT device identities included in the unsolicited update message are not found in the device gateway.

[0032] One other embodiment describes a control server in the common telecommunication network, receiving from a device gateway, a request message requesting an identity of a service provider network associated with an IoT device. The request message comprising the manufacturer IoT device identity. One embodiment describes the request message received at the control server as comprising a parameter describing the service as provided by the IoT device. In another embodiment, the request message may comprise the subscription identity of the device gateway and yet in another embodiment; the request message may comprise a geographical location of the device gateway.

[0033] The control server in the common communication network determines from a mapping table, a configured identity of the service provider network associated with the IoT device. The control server may validate the association and in an embodiment it may send a validation message to the service provider network requesting if the stored association is valid. In one embodiment, the validation response message from the service provider network indeed confirms the association with the IoT device, however, another embodiment describes a validation response message that may comprise another service provider network if the service is being provided or managed by another service provider network herein referred to as new service provider network or second service provider network. In the latter scenario, the server may validate the updated association by sending a new validation request to the new service provider network which responds by sending a validation response message that may comprise a confirmation of the updated association. The server may update the stored association in the mapping table when a new service provider network is associated to the IoT device. Assuming that either the service provider network or the new service provider network validates the association; the control server sends a message to the device gateway to signal the identity of the service provider network/new service provider network associated with the IoT device.

[0034] Furthermore, according to one embodiment described in this disclosure, the control server may receive an unsolicited message from an authorized service provider network, the unsolicited message comprising updated associations comprising an identity of a new service provider network to be associated with the one or more manufacturer IoT devices identities, in which case, the control server stores the updated associations in the mapping table and a timestamp indicating a date when the updated association is received, hence enabling up-to-date associations to be available at the mapping table. The control server may notify the one or more device gateways with the updated associations, to trigger the device gateway to create or update the corresponding one or more unique IoT device identifiers.

BRIEF DESCRIPTION OF THE DRAWINGS

[0035] Embodiments of the present invention will now be described, by way of example only, with reference to the attached Figures, wherein:

[0036] FIG. **1** is a schematic illustration of an overview of a system for connecting IoT devices through a common communication network to one or more service provider networks, according to an embodiment.

[0037] FIG. **2** illustrates a sequence diagram for acquiring a service provider network associated with a device gateway and creating a unique IoT device identifier, according to an embodiment.

[0038] FIG. **3** illustrates a sequence diagram for receiving unsolicited messages to update IoT device to service provider network association, according to an embodiment.

[0039] FIG. **4***a* illustrates a flowchart of a method executed at a device gateway, for creating and updating the unique IoT device identifier, according to an exemplary embodiment.

[0040] FIG. **4***b* illustrates a flowchart of a method executed at a device gateway, requesting an identity of the service provider network associated with an IoT device to create the unique IoT device identifier, according to an exemplary embodiment.

[0041] FIG. **4***c* illustrates a flowchart of a method executed at a device gateway unsolicitedly obtaining an identity of the service provider network associated with an IoT device to update or create the unique IoT device identifier, according to an exemplary embodiment.

[0042] FIG. **5** illustrates a flowchart of a method executed at a server in the common communication network, providing an identity of the service provider network associated with the IoT device, according to an exemplary embodiment.

[0043] FIG. **6** illustrates a flowchart of a method executed at a server in the common communication network, receiving unsolicited message comprising updated IoT device to service provider network association, according to an exemplary embodiment.

[0044] FIG. **7** is a schematic illustration of a device gateway, according to an embodiment.

[0045] FIG. **8** is a schematic illustration of the server in the common telecommunication network, according to an embodiment.

[0046] FIG. **9** is a schematic illustration of a device gateway, according to another embodiment.

DETAILED DESCRIPTION

[0047] The various features of the invention will now be described with reference to the figures. These various aspects are described hereafter in greater detail in connection with exemplary embodiments and examples to facilitate an understanding of the invention, but should not be construed as limited to these embodiments. Rather, these embodiments are provided so that the disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art.

[0048] Many aspects of the invention are described in terms of sequences of actions or functions to be performed by elements of a computer system or other hardware capable of executing programmed instructions. It will be recognized that the various actions could be performed by specialized circuits, by program instructions being executed by one or more processors, or by a combination of both. Moreover, the invention can additionally be considered to be embodied entirely within any form of computer readable carrier or carrier wave containing an appropriate set of computer instructions that would cause a processor to carry out the techniques described herein.

[0049] FIG. **1** is a schematic illustration of a system for connecting IoT devices **100** to application servers **131** in the respective service provider networks **130**; more specifically, the system comprises one or more IoT devices **100** connected to one or more device gateways **110**, a control server **121** of a common communication network **120**, and one or more service provider networks **130** hosting the corresponding application servers **131**. A device gateway **110** is connected to a control server **121**, over a communication interface **140**. The control server **121** of the common communication network **120** communicates with various service provider networks **130** over other communication interfaces **140**. The common communication network **120** enables transport of data from an IoT device **100** to an application server **131** in the service provider network**130** based on a unique IoT device identifier. An example of a common communication network **120** is disclosed in PCT application PCT/IB2014/063785. Although the unique IoT device identifier comprising the manufacturer device identity can be pre-configured in the device gateway, this disclosure describes methods and apparatuses for dynamically updating and creating the unique IoT device identifiers, enabling flexible and dynamic association of the IoT device to a service provider network **130**. The device gateway **110** preferably includes a storage that maintains the manufacturer IoT device identities and the created/updated unique IoT device identifiers for the IoT devices **100** connected to the device gateway **110** via various interfaces and access technology types such as Wi-Fi, ZIGBEE™, Z-WAVE™, 3G/4G/5G interfaces, etc. The device gateway **110** may be pre-configured with the manufacturer IoT device identifiers of the IoT devices it is connected to. Alternatively, the device gateway **110** may discover the IoT devices **100** and learn the corresponding manufacturer IoT device identities via any discovery mechanisms enabled by the access technology supported by the IoT devices. Once discovered, the device gateway **110** populates its storage with the manufacturer IoT device identities. Since the IoT devices **100** connected to a device gateway **110** are not necessarily of the same access technology type, the manufacturer IoT device identities may be of different types and formats. The so-created unique IoT device identifier for an IoT device **100** may comprise the manufacturer IoT device identity, the identity of the associated service provider network **130** and may further comprise the access technology type. The unique IoT device identifier is further used by the device gateway **110** to request a virtual data path as disclosed in PCT application PCT/IB2014/063785.

[0050] The device gateway **110** in FIG. **1** is configured to send a request message for an identity of a service provider network **130** associated to an IoT device **100** for the purpose of creating the unique IoT device identifier for the IoT device. The device gateway **110** is additionally configured to receive unsolicited update messages from the control server **121** in the common communication network **120**. The unsolicited update message comprises an updated association between an identity of a new service provider network **130** and an IoT device **100** for the purpose of updating or creating a unique IoT device identifier for the IoT device **100**.

[0051] A local or external storage in the common communication network **120** is used to hold a mapping table **122**. The mapping table **122** is used to maintain the associations between the manufacturer IoT device identities and the identities of the associated service provider networks **130**. Each association may also include a timestamp indicating the time when the association has been created or updated. The timestamp may be used by the control server **121** to determine if it needs to contact the service provider network **130** to validate a requested association. In other words, if the timestamp indicates that the association is recently updated/created, the control server **121** validates the association without further verification with the service provider network **130**; else the control server **121** requests the service provider network **130** obtained from the mapping table **122** to validate an association. This flexibility allows the common communication network **120** to control and optimize the signaling load to the service provider networks **130**.

[0052] The associations in the mapping table **122** are pre-configured, however, this disclosure presents embodiments where the associations are dynamically updated. The associations could be updated as a result of processing at the control server **121**, a request message from a device gateway **110**, requesting an identity of a service provider network **130** associated to the IoT device **100**. The control server **121** retrieves from the mapping table **122** the stored identity of the service provider network **130** associated to the IoT device. As the control server **121** validates the association with the service provider network, the latter identifies instead another service provider network that is associated with the IoT device. Following a subsequent validation with the other service provider network, the control server **121** may subsequently update the association in the mapping table **122**. Moreover, the associations could also be updated if the control server **121** receives unsolicited message comprising updated association between an identity of a service provider network and one or more manufacturer IoT device identity. The service provider network sending the unsolicited message may be either

[0053] a) the service provider network **130** from the current stored association in the mapping table **122**, which indicates an identity of a new service provider network for the corresponding IoT device(s), or

[0054] b) the new service provider network itself sending the unsolicited association update identifying its own identity and the associated IoT device(s). However, in order to receive and accept unsolicited association update from a new service provider that does not exist in the current mapping table, it may be necessary to execute authorization/authentication mechanisms between the common communication network **120** and the new service provider network.

[0055] Once the unsolicited message is received and accepted, the control server **121** updates the corresponding association in the mapping table **122** and stores the updated associations. In one embodiment, the control server **121** may send to the device gateway **110** the identity of the new service provider network associated with the one or more manufacturer IoT device identity of the IoT devices **100** connected to the device gateway **110**. Alternatively the control server **121** may create an updated unique IoT device identifier by concatenating the identity of the new service provider network and the manufacturer IoT device identity for the one or more IoT devices affected by the received updated associations and sends the identifiers to the device gateway **110**.

[0056] FIG. **2** illustrates a detailed sequence diagram based on the system illustrated in FIG. **1**, for creating a unique IoT device identifier at the device gateway **110** according to one embodiment. The system comprises an IoT device **100** connected to a device gateway **110**. The device gateway **110** communicates with a control server **121** in the common communication network **120**, which also comprises a mapping table **122** that maintains associations comprising identities of the service provider networks and the IoT devices. The system further illustrates a first service provider network **130**, and a second service provider network **200**. In step **202**, the device gateway **110** sends a request message to a control server **121** of the common communication network **120**, requesting an identity of a service provider network associated with an IoT device **100**, the request message comprises the manufacturer IoT device identity. The device gateway **110** initiates the request message on its own, after determining that a manufacturer IoT device identity in the local storage does not have a corresponding unique IoT device identifier. The device gateway **110** may alternatively trigger the request message for an identity of a service provider network upon receiving a message, step **201**, or data from an IoT device **100**. The message from the IoT device in step **201** may consist of a discovery message from an IoT device **100** over the access interfaces connecting the IoT device **100** to the device gateway **110**. The discovery message in step **201** may comprise the manufacturer IoT device identity. Alternatively, the message in step **201** may be an explicit request for an identity of a service provider network or for a unique IoT device identifier from the IoT device **100**, assuming the IoT device is capable of supporting the unique IoT device identifier in addition to the manufacturer IoT device identity. Following optional step **201**, the device gateway **110** may determine that a unique IoT device identifier is not found in the device gateway storage and triggers a request message for an identity of a service provider network.

[0057] In one embodiment, the request message in step **202** may comprise the subscription identity of the device gateway **110**. The subscription identity of the device gateway **110** may be used in for example situation where the device gateway **110** is a portable device (e.g., smartphone, tablet, etc.). The subscription profile may be stored in the mapping table **122** or in another external database (not shown in FIG. **2**). When a subscription identity of the device gateway **110** is included in the request message, the control server **121** and optionally the first service provider network **130** may use the device gateway subscription profile in the validation of the IoT device to service provider network association and may also be used to prevent any malicious requests from unauthorized device gateways.

[0058] Another embodiment describes the request message in step **202**, as comprising the geo-location of the device gateway, which is particularly useful in the case the device gateway **110** is a fixed residential gateway. The control server **121** and optionally the first and second service provider networks **130**, **200** may use the device gateway geo-location in the validation of the IoT device to service provider network association and may also be used to prevent any malicious requests from unauthorized device gateways. Another embodiment is included which describes the request message in step **202**, as comprising the service type provided or enabled by the IoT device for which an identity of the service provider network is requested.

[0059] In step **203**, the control server **121** sends a message to a mapping table **122** to request the available identity of a first service provider network **130** associated with the IoT device **100**. The message in step **203**, includes the manufacturer IoT device identity and may include the service type associated to the IoT device **200** and may additionally comprise the device gateway subscription profile and/or the device gateway geo-location. If an identity of a service provider network **130** is found, the mapping table **122**, in step **204**, returns the identity of the first service provider network **130** and may include a timestamp determining the time of creation or of last update of the association. The control server **121** validates the received identity of the service provider network **130**. If a timestamp is included in step **204**, and the time indicates a very recent creation or update of the available association, then based on the local network policies, the control server **121** determines that the available association is valid and sends a message in step **209** to the device gateway **110**, to signal the identity of the first service provider network **130** associated with the IoT device **100**. Alternatively, if in step **204**, the mapping table **122**, returns an identity of a first service provider network **130** but the control server **121** determines that the service provider should validate the association, then the control server **121** in step **206**, sends a validation request message to the first service provider network **130**. The validation request message comprises the manufacturer IoT device identity, and may include the service type, an optional device gateway subscription identity and an optional device gateway geo-location.

[0060] If the first service provider network **130** successfully validates the association in its internal database, it sends in step **207** a validation response message back to the control server **121** confirming the association. The control server **121** then sends in step **209**, the identity of the first service provider network **130** associated with the IoT device **100**. In an alternative embodiment, if the first service provider network **130** determines that the IoT device is in fact associated to a second service provider network **200** and the identity of the second service provider network **200** is available in the internal database at the first service provider network **130**, the first service provider network **130** sends a validation response message in step **207** to the control server **121** comprising the identity of the second service provider network **200**. The control server **121** may in step **208**, validate the new IoT device association with the second service provider network **200** by repeating step **206** with the second service provider network **200**. This may require executing an authentication procedure between the control server **121** and the second service provider network **200** prior to validating the new association. Although, the authentication process is not shown in FIG. **2**, a person skilled in the art understands that any existing authentication mechanism may be used between the control server **121** and the second service provider network **200**. If the second service provider network **200** validates successfully the new association, it returns a message confirming the new association.

[0061] Following optional step **208**, in FIG. **2**, if the second service provider network **200** validates the new IoT device association, the control server **121** sends in step **209**, the identity of the second service provider **200** to the device gateway **110**. In an alternative embodiment, the control server **121** may in step **208*b*** update the mapping table **122** with the identity of the second service provider network **200** associated with the IoT device **100**.

[0062] When the device gateway **110** in step **209**, receives an identity of a service provider network (either of a first or second service provider network) associated with the IoT device, the device gateway **110** in step **209***b*, creates and stores a unique IoT device identifier comprising the identity of the service provider network, the manufacturer IoT device identity and optionally the access technology type used by the IoT device.

[0063] Although the embodiment describes the device gateway **110** requesting an identity of a service provider network to create a unique IoT device identifier, other variations of FIG. **2** are possible, such as the device gateway **110** may instead request the unique IoT device identifier from the control server **121**, in which case the control server **121** creates and sends the unique IoT device identifier to the device gateway **110** later on at step **209***b*.

[0064] The device gateway **110** would then store the received unique IoT device identifier and the control server **121** may also store the unique IoT device identifier in the mapping table **122**.

[0065] If the request message in step **202** is triggered by a request from the IoT device **100** for a unique IoT device identifier or for an identity of a service provider network, the device gateway **110** sends in step **211** a response message back to the IoT device **100**, the response message in step **211** may then comprise the unique IoT device identifier created by the device gateway **110** or the received identity of the service provider network, in which case the IoT device creates and stores the unique IoT device identifier.

[0066] FIG. **3** illustrates a mechanism for updating the service provider network to IoT device associations stored in the mapping table **122** in the common communication network **120**, according to one embodiment. The mechanism is based on receiving at the common communication network **120**, an unsolicited message from a service provider network, the unsolicited message comprises updated associations between the identity of the service provider network and one or more manufacturer IoT devices identities. This is particularly useful when a user swaps a service provider for a specific service or if a deployed service is managed by a new service provider as a result of spin-off or out-sourcing. The unsolicited message comprising updated associations may be triggered from the first service provider network **130** known in the current association stored in the mapping table **122**, or may be triggered by a new service provider network **200** with which the IoT device **100** is now associated. The new service provider network **200** is also referred to as the second service provider network **200**. When triggered by the new service provider network **200**, a person skilled in the art understands that the common communication network **120** and the new service provider network **200** should communicate over a secure connection. FIG. **3** shows the option where the unsolicited message is triggered by the first service provider network **130** as per the current stored association in the mapping table **122**.

[0067] In step **300**, the first service provider network **130** sends to the control server **121** in the common communication network **120**, an unsolicited message for one or more IoT devices that are now being served by the second service provider network **200**. The unsolicited message in step **300** comprises one or more updated associations consisting of the identity of the second service provider network **200** and one or more manufacturer IoT devices identities for which the associations should be updated. The unsolicited message may also include the one or more device gateway identities to which the one or more IoT devices, identified by their manufacturer IoT devices identities, are connected. Moreover, the unsolicited message may also include the service type associated to the IoT devices. When the control server **121** receives the unsolicited message comprising one or more updated associations, it responds in step **300***b* with an acknowledgement back to the first service provider network **130** indicating that it accepts the message. The control server **121** sends, in step **301**, a message to the mapping table **122** to update the corresponding one or more associations. The message in step **301** comprises a timestamp indicating the time the updated associations are received, and the updated associations as received in the unsolicited message in step **300**, i.e., the identity of the service provider network and the one or more manufacturer IoT devices identities, etc. The mapping table **122** stores the updated associations and sends in step **303** an acknowledgement back to the control server **122**, the acknowledgement in step **303** may be sent immediately in response to the message received in step **301**. An alternative embodiment is described where the control server **122** further sends a message in step **304** to a device gateway **110**, the message comprising the identity of the second service provider network **200** and the associated one or more manufacturer IoT devices identities that are comprised in the received updated associations. If the concerned IoT devices are connected to different device gateways, the control server **121** may send a message to each of the corresponding device gateways **110**. The device gateway **110** in step **305**, updates or creates and stores the corresponding unique IoT devices identifiers. In an alternative embodiment for step **304**, the control server **121** may create unique IoT devices identifiers and include the identifiers in step **304**, which are then stored in the device gateway **110**. It is also understood that the unsolicited message received at step **300** may comprise one or more updated associations between one or more manufacturer IoT devices identities and one or more service provider networks identities.

[0068] FIG. **4***a* shows a flowchart of a method **40** executed at a device gateway **110** for creating unique IoT device identifiers, according to one embodiment. The device gateway **110** is the same device gateway illustrated in the previous figures. The method **40** comprises step **41** of obtaining or receiving at the device gateway **110**, an identity of a service provider network associated to an IoT device. The identity of the service provider network may be obtained from the control server **121** in the common communication network **120**. In step **42**, the device gateway **110** creates or updates the unique IoT device identifier for the IoT device, the identifier comprising a concatenation of the obtained/received identity of the service provider network, the manufacturer IoT device identity available at the device gateway **110** and may comprise the access technology type supported by the IoT device. The manufacturer IoT device identity corresponds to the hardware related identity of the IoT device connected to the device gateway **110**. The manufacturer IoT device identity is stored and known in the device gateway **110**, and is either pre-configured in the device gateway **110** or known through a discovery mechanism between the device gateway **110** and the IoT device. Once the device gateway **110** creates the unique IoT device identifier for an IoT device, the device gateway **11**, in step **43** stores the created/updated unique IoT device identifier in its local storage.

[0069] FIG. **4***b* shows a flowchart of a method **40***b* executed at a device gateway **110** for creating unique IoT device identifiers, according to one embodiment. The method **40***b* is a variation of method **40** and comprises step **41***b*, where the device gateway **110** obtains the identity of the service provider network by sending a request message to a control server **121** of the common communication network **120** requesting an identity of a service provider network associated to an IoT device. The request message comprises the manufacturer IoT device identity and may comprise the subscription identity of the device gateway and/or the geo-location of the device gateway. The device gateway initiates the request message on its own, after determining that a manufacturer IoT device identity in the local storage does not have a corresponding unique IoT device identifier. The device gateway may alternatively trigger the request message for an identity of a service provider network upon receiving a message or data from an IoT device. In step **41***d*, the device gateway receives a response to the request message sent in step **41***b*. If the response from the control server **121** does not include an identity of a service provider network, the device gateway ends the process, and if at step **41***d*, an identity of a service provider network is included in the response, the device gateway executes step **42** and step **43** in the same manner as method **40** above.

[0070] FIG. **4***c* shows a flowchart of a method **40***c* executed at a device gateway **110** for creating or updating unique IoT device identifiers, according to one embodiment. The method **40***c* is a variation of method **40** and comprises step **41***c*, where the device gateway **110** obtains the identity of a service provider network by receiving unsolicited update message from the control server **121** of the common communication network **120**, where the update message comprises an identity of new a service provider network **200** associated to an IoT device. The unsolicited update message comprises a manufacturer IoT device identity, an identity of a new service provider network **200**. If a unique IoT device identifier for the IoT device is already stored at the device gateway **110**, the device gateway **110**, in step **42** updates the unique IoT device identifier (consisting of a concatenation of identity of service provider network, manufacturer IoT device identity and optional access technology type used with the IoT device) by replacing the identity of the service provider network with the received identity of the new service provider network **200**. If a unique IoT device identifier for the IoT device is not available at the device gateway **110**, the device gateway **110**, upon receiving the unsolicited update message, in step **42** creates the unique IoT device identifier by concatenating the received identity of the new service provider network, manufacturer IoT device identity and optional access technology type used with the IoT device. The device gateway **110** executes step **43** and stores the updated or created unique IoT device identifier. In one embodiment, the unsolicited update message may trigger an update or creation of one or more unique IoT device identifiers at the device gateway **110**, in which case the message may comprise in addition to the identity of the service provider network a list of the affected IoT devices for which the unique IoT device identifiers should be updated or created. It should be noted that more than one identity of service provider network may be received. Each identity of service provider network is associated with one or more IoT devices.

[0071] In yet an alternative embodiment, the device gateway **110** may not recognize the manufacturer IoT device identity received in the unsolicited update message as it is not available in the device gateway local storage, in which case the device gateway **110** may create and store a new entry for a new IoT device. This scenario is useful for newly installed IoT devices **100** that the device gateway **110** is not yet aware of The device gateway **110** stores the manufacturer IoT device identifier and the created unique IoT device identifier.

[0072] FIG. **5** shows a flowchart of a method **50**, according to an embodiment, the method **50** executed at a control server **121** in a common communication network **120**. The method **50** comprises steps for providing in response to a request from a device gateway **110**, a valid identity of a service provider network associated to an IoT device. The method **50** comprises step **51** of receiving a request message from a device gateway **110** requesting an identity for a service provider network associated to an IoT device. The request message comprises the manufacturer IoT device identity, and may include the service type, an optional device gateway subscription identity and an optional device gateway geo-location. Method **50** further comprises step **52** where the control server **121** determines the requested identity of the service provider network by sending a request to a mapping table **122** to request the available identity of a service provider network associated to the IoT device. If an identity of a service provider network is found, herein referred to as first service provider network **130**, the mapping table **122** returns the identity of the first service provider network **130** and may include a timestamp determining the time of creation or of the last update executed for the association. The control server **121** in step **53** of method **50** validates the received identity of the first service provider network **130**. If a timestamp is included in step **52**, and the time indicates that the first service provider network **130** to IoT device association is recent (e.g., association is last updated/created 4 hours ago) then based on local network policies, the control server **121** may determine in step **53** that the association is valid and starts executing step **55** where the control server **121** sends a message to the device gateway **122**, where the message includes the identity of the first service provider network **130** associated with the IoT device as retrieved from the mapping table **122**. Back to step **53**, the control server **121** may determine that the retrieved identity of the first service provider network **130** from the mapping table **122** should be validated by the first service provider network **130**. Consequently, the control server **121** sends a validation request message to the first service provider network **130**, where it includes the manufacturer IoT device identity, an optional service type, an optional device gateway subscription identity and an optional device gateway geo-location. In step **54**, the first service provider network **130** sends a validation response to the control server **121**. If the validation response confirms the association of the IoT device with the first service provider network **130**, the control server **121** executes step **55**, where it sends a message to the device gateway **110** and includes the validated identity of the first service provider network **130** associated with the IoT device. Optional step **54***b* of method **50** indicates that the first service provider network **130** may fail in validating the association because the IoT device is no longer associated with the first service provider network **130**; however, the first service provider network **130** is aware of the identity of the new service provider network **200** that is now associated with the IoT device, herein referred to as second service provider network **200**. The first service provider network **130** sends a validation response message back to the control server **121** and includes the identity of the second service provider network **200** associated with the IoT device. The control server **121** may execute step **56**, where it proceeds to validate the IoT device association with the second service provider network **200**. This may require an authentication process between the control server **121** and the second service provider network **200** prior to validating the new association. If in step **57**, the second service provider network **200** validates successfully the new association, and sends a validation response message accordingly to the control server **121**, the control server **121** proceeds with executing step **55** and sends a message to the device gateway **110** where it includes the identity of the second service provider network **200** now associated with the IoT device. The control server **121** may furthermore execute optional step **58**, where upon receiving a validation response from the second service provider network **200** confirming the new association, the control server **121** may update the association in the mapping table **122** in the common communication network **120**. On the other hand, if in step **57** the second service provider network **200** fails in validating the new association, the control server **121** executes step **59** where it sends an error message to the device gateway **110** in response to the request message received during step **51** of the method.

[0073] FIG. **6** shows a flowchart of a method **60** executed at a control server **121**of a common communication network **120**, for updating and maintaining up-to-date associations stored in the mapping table **122** in the common communication network **120** according to an embodiment. In method **60**, the control server **121** manages updated associations received from a first service provider network **130**. The method **60** results in updating and maintaining up-to-date associations between the identities of the service provider networks and the one or more manufacturer IoT devices identities of the IoT devices as stored in the mapping table **122**. Method **60** is particularly useful when a service provider associated to one or more IoT devices is changed for a service, or device gateways, hence affecting the service provider network identity to manufacturer IoT devices identities associations of the one or more IoT devices maintained in the common communication network **121**. Step **61** shows the control server **121** receiving an unsolicited message comprising updated associations from a first service provider network **130**. The unsolicited message comprises the identity of a new service provider network **200**, herein referred to as second service provider network **200**, and the one or more affected manufacturer IoT devices identities. The unsolicited message may also include the one or more device gateway identities to which the one or more IoT devices identified by the one or more manufacturer IoT devices identities are connected and may further include the service type associated with the one or more IoT devices. In step **62**, the control server **121** sends a message to the mapping table **122** to update the corresponding one or more associations and store the updated associations. The message from the control server **121** to the mapping table **122** comprises the same information received in the unsolicited message from the first service provider network **130**. The optional step **63**, enables the control server **121** to determine if it should send the identity of the second service provider network **200** to the corresponding device gateway(s) **110**. The control server **121** may use local operator policies and/or network conditions to determine if the device gateway(s) **110** should also be updated. If the control server **121** determines that it should update the device gateway, it executes step **64**, where it sends a message to the device gateway **110** and includes the identity of the second service provider network **200** and the affected one or more manufacturer IoT devices identities. The device gateway **110** uses the information to create or update the one or more unique IoT devices identifiers as described in method **40**c above. If the affected IoT devices are connected to different device gateways, the control server **121** sends a message to each device gateway **110**.

[0074] An alternative embodiment, not shown in FIG. **6** consists of a capability where when receiving from the first service provider network **130** the updated associations between the identity of the service provider and the one or more manufacturer IoT devices identities, the control server **121** can create/update the one or more unique IoT devices identifiers and could send a message comprising the one or more created/updated IoT devices identifiers to each affected device gateways **110**. In this case, the device gateways **110** would only need to store the received one or more unique IoT devices identifiers.

[0075] In one embodiment illustrated in FIG. **7**, a device gateway comprises a circuitry **70** which executes the method steps according to the embodiments as described in FIG. **4***a*, FIG. **4***b* and FIG. **4***c*, along with steps **201**, **202**, **209**, **209***b* and **211** of FIG. **2** and steps **304** and **305** of FIG. **3** in addition to other embodiments described herein. In one embodiment, the circuitry **70** may comprise a processor **71** and a storage **72** (also referred to as memory) containing instructions, which when executed, cause the processor **70** to perform the steps in a method according to embodiments described herein. The circuitry **70** may further comprise a communication interface **73** to communicate with external entities such as IoT devices and the server in the network of interconnect end-points.

[0076] In another embodiment illustrated in FIG. **8**, a control server in the common communication network comprises a circuitry **80** which executes the method steps according to the embodiments as described in FIG. **5** and FIG. **6** along with steps **202-208**, **208***b* and **209** of FIG. **2** and steps **300**, **300***b*, **301-304** in FIG. **3**. In one embodiment, the circuitry **80** may comprise a processor **81** and a storage **82** (also referred to as memory) containing instructions, which when executed, cause the processor **81** to perform the steps in a method according to embodiments described herein. The circuitry **80** may further comprise a communication interface **83** to communicate with external entities which may comprise external service provider networks, device gateways and mapping table if not co-located with the server.

[0077] FIG. **9** illustrates an exemplary embodiment of a device gateway comprising a processing module **91** to obtain through a communication module **93**, the identity of the service provider network associated to a manufacturer IoT device identity of the IoT device. Once the identity of the service provider network is obtained, the processing module **91** determines if the unique IoT device identifier is available in the storage module **92**. If the unique IoT device identifier is not available, the processing module **91** creates the unique IoT device identifier comprising a concatenation of the identity of the service provider network and the manufacturer IoT device identity. If the unique IoT device identifier is available in the storage module **92**, the processing module **91** retrieves the unique IoT device identifier from the storage module **92** and updates the unique IoT device identifier comprising a concatenation of the identity of the service provider network and the manufacturer IoT device identity. The processing module **92** stores the unique IoT device identifier in the storage module **92**. The storage module **92** maintains IoT devices information comprising the manufacturer IoT device identity and the unique IoT device identifier provided by the processing module **91** for all the IoT devices connected to the device gateway.

[0078] A person skilled in the art would understand that the modules can be implemented as a computer program miming on a processor and that the modules are operative to execute the steps of the previously described method.

[0079] The invention has been described with reference to particular embodiments. However, it will be readily apparent to those skilled in the art that it is possible to embody the invention in specific forms other than those of the embodiments described above. The described embodiments are merely illustrative and should not be considered restrictive in any way. The scope of the invention is given by the appended claims, rather than the preceding description, and all variations and equivalents that fall within the range of the claims are intended to be embraced therein.

What is claimed is:

1. A method in a device gateway for dynamically creating and updating a unique Internet of Thing (IoT) device identifier, the method comprising:

obtaining an identity of a service provider network associated to a manufacturer IoT device identity of the IoT device;

if the unique IoT device identifier is not already available, creating the unique IoT device identifier comprising a concatenation of the identity of the service provider network and the manufacturer IoT device identity;

if the unique IoT device identifier is already available, updating the identity of the service provider network of the unique IoT device identifier; and

storing the unique IoT device identifier.

2. The method of claim **1**, wherein the step of obtaining further comprises

sending a request message to obtain the identity of the service provider network associated with the IoT device, the request message comprising the manufacturer IoT device identity; and

receiving a message comprising the identity of the service provider network associated with the manufacturer IoT device identity.

3. The method of claim **2**, wherein the step of sending the request message is executed thereupon receiving one of a message and data from the IoT device.

4. The method of claim **2**, wherein the request message comprises at least one of a geographical location of the device gateway, a subscription identity of the device gateway and a service associated with the IoT device.

5. (canceled)

6. (canceled)

7. The method of claim **1**, wherein the step of obtaining further comprises

receiving an unsolicited update message comprising the identity of the service provider network and the manufacturer IoT device identity to trigger the device gateway to update or create the unique IoT device identifier.

8. The method of claim **1**, wherein the unique IoT device identifier comprises the manufacturer IoT device identity, the identity of the service provider network and the access technology type used between the device gateway and the IoT device.

9. A method in a server of a network for providing to a device gateway an identity of a service provider network associated with an Internet of Thing (IoT) device connected to the device gateway for the purpose of creating a unique IoT device identifier, the method comprising:

receiving a request message from the device gateway for obtaining the identity of the service provider network associated with the IoT device, the request message comprising a manufacturer IoT device identity;

determining an association between the identity of the service provider network and the manufacturer IoT device identity; and

validating the association, and conditional to a successful validation sending a message to the device gateway for creating the unique IoT device identifier, the message comprising the identity of the service provider network and the manufacturer IoT device identity.

10. The method of claim **9**, wherein the request message comprises at least one of a subscription identity of the device gateway, a geographical location of the device gateway and a service associated with the IoT device.

11. (canceled)

12. (canceled)

13. The method of claim **9**, wherein the step of validating the association of the IoT device further comprises

sending a validation message to the service provider network, the validation message comprising the manufacturer IoT device identity of the IoT device; and

receiving a validation response.

14. The method of claim **13**, wherein the validation response validates the association comprising the manufacturer IoT device identity and the identity of the service provider network.

15. The method of claim **13**, wherein the validation response comprises an identity of a new service provider network associated to the manufacturer IoT device identity.

16. The method of claim **15**, wherein responsive to receiving the validation response, the method further comprises

sending a second validation request to the new service provider network; and

receiving a second validation response message confirming an updated association comprising the manufacturer IoT device identity and the identity of the new service provider network.

17. The method of claim **9**, wherein the method further comprises

receiving an unsolicited message comprising updated associations between one or more manufacturer IoT devices identities and the identity of a new service provider network associated therewith; and

storing the updated associations.

18. (canceled)

19. (canceled)

20. (canceled)

21. A device gateway configured to dynamically create or update a unique Internet of Thing (IoT) device identifier, the device gateway comprising a circuitry configured to:

obtain an identity of a service provider network associated to a manufacturer IoT device identity of the IoT device;

if the unique IoT device identifier is not already available, create the unique IoT device identifier comprising a concatenation of the identity of the service provider network and the manufacturer IoT device identity;

if the unique IoT device identifier is already available, update the identity of the service provider network of the unique IoT device identifier; and

store the unique IoT device identifier.

22. The device gateway of claim **21**, wherein the circuitry comprises a processor, a communication interface and a memory, the memory containing instructions executable by the processor.

23. A server in a network, configured to provide an identity of a service provider network associated with an Internet of Thing (IoT) device connected to a device gateway, the server comprising a circuitry configured to:

receive a request message from the device gateway for obtaining the identity of the service provider network associated with the IoT device, the request message comprising a manufacturer IoT device identity;

determine an association between the identity of the service provider network and the manufacturer IoT device identity; and

validate the association, and conditional to a successful validation sending a message to the device gateway for creating the unique IoT device identifier, the message comprising the identity of the service provider network and the manufacturer IoT device identity.

24. The server of claim **23**, wherein the circuitry comprises a processor, a communication interface and a memory, the memory containing instructions executable by the processor.

25. The server of claim **23**, wherein to validate the association of the IoT device, the circuitry is further configured to

send a validation message to the service provider network; and

receive a validation response.

26. The server of claim **25**, wherein the validation response confirms the association of the IoT device with the identity of the service provider network.

27. The server of claim **25**, wherein the validation response includes the identity of a new service provider network.

28. The server of claim **27**, wherein the circuitry is further configured to

send a second validation request to the new service provider network; and

receive a second validation response confirming an updated association comprising the manufacturer IoT device identity and the identity of the new service provider network.

29. The server of claim **23**, wherein the circuitry is further configured to

receive an unsolicited message comprising one or more updated associations between one or more manufacturer IoT devices identities and the identity of a new service provider network; and

store the updated associations.

30. (canceled)

* * * * *