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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 January 2014 (09.01.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/007604 A1

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

(21) International Application Number:
PCT/MY2013/000126

(22) International Filing Date:
4 July 2013 (04.07.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2012003072 5 July 2012 (05.07.2012) MY

(71) Applicant: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventor: **ETTIKAN, Kandasamy, A/L, Karu**; c/o MIMOS Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(74) Agent: **YAP, Kah Hong**; Pyprus Sdn Bhd, Suite 8.02, 8th Floor, Plaza First Nationwide 161, Jalan Tun H. S. Lee, 50000 Kuala Lumpur (MY).

(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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(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, 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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

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

(54) Title: SYSTEM AND METHOD FOR PRE-EMPTIVE ADDRESS CONFLICT RESOLUTION IN AUTOMATIC DEVICE ADDRESS ASSIGNMENTS

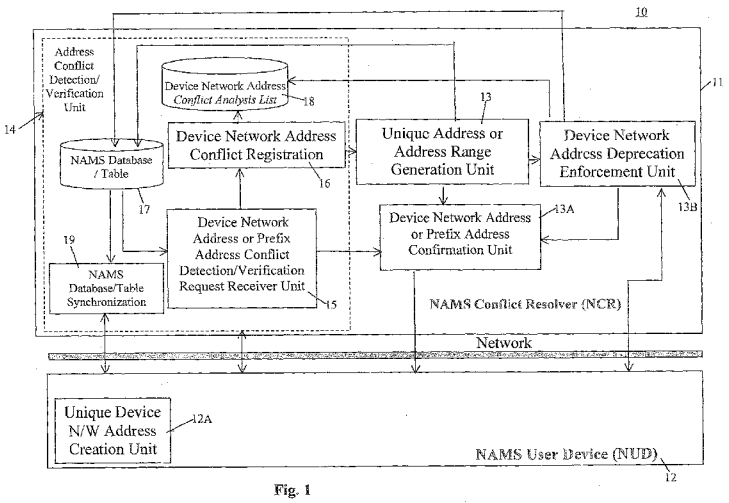

Fig. 1

(57) Abstract: The present invention provides a system for preemptive address conflict resolution in heterogeneous network environment, comprising a user device and a conflict resolver communicating with the user device. The conflict resolver comprises of a network address conflict verification and detection unit for detecting address conflicts between network, address of newly joined network device and existing addresses, wherein during verification, the network address of newly joined network device is verified against a network database storing all existing network addresses, including both active and non-active network address. The conflict resolver further comprises a conflict analysis list that stores all detected conflict information. The system is operationally adapted to preemptively resolve any potential conflict address. Method for preemptive address conflict resolution is also provided herewith.

WO 2014/007604 A1

System and Method for Pre-emptive Address Conflict Resolution in Automatic Device Address Assignments

Field of the Invention

[001] The present invention in general relates to device address assignments methodology in a network. In particular, the present invention relates to system and method for pre-emptive address conflict resolution for automatic device address assignments by maintaining the address uniqueness in a network.

Background

[002] With rapid development of Internet, different types of communication platforms are emerging in the market. International Telecommunication Union (ITU) has proposed IoT (Internet of Things) as next wave of new Internet. With IoT, it is expected that society composed by devices and people, with most communication done by devices themselves, are built ubiquitously.

[003] To achieve the above objectives, zero configuration addressing methodology performed by a device itself is very critical. One solution for such methodology has been proposed by IEEE 802.15.4 standard. In the proposed solution, each device scans their neighboring reachable network and discovers existing network address. Based on this scanned information, each device then configures themselves by assigning their network address, eliminating human intervention, and at the same time, achieving zero configuration state to maintain its uniqueness.

[004] Besides the above solutions, there are many other standard protocols available for connecting heterogeneous network to the Internet, either for Wireless Personal Area Network (WPAN), Home Network, or other device networks. The devices and networks may use different protocol standards such as IEEE802.15.4, Homeplug, IPv4, IPv6, LonWorks etc. However, regardless of unique addressability of these devices in the Internet or within a specific heterogeneous network domain, co-existence of multiple types of network devices in one network is unavoidable. For example, in home, office buildings or school, heterogeneous network environment, multi-protocol devices co-exist, and this may result in address conflicts. As such, unique addressability and address conflicts avoidance/resolution are very critical in both active and non-active network. Active network is the network which has constant communication with available devices in the network. The devices also respond constantly to the network probing or communication. On the other hand non-active network covers networks and/or devices which do not constantly communicate with each other. Their presences in the network are made known to others in periodic manner. For example, one device may go into 'sleep' state for long period, some devices are moved around from area to area, or due to battery outage, one device is disconnected from the network for a period ended until battery replacement is done.

[005] US 7,633,855 implements a system for effectively resolving conflicting network-device addresses in accordance with network priorities. The system includes an interface-monitoring module for providing a signal when an address conflict involving plural address occurs in a network. The system further includes a conflict-resolution module that selectively terminates one or more device

interfaces associated with the conflicting plural address in response to the signal and based on one or more precedence rules.

[006] Existing solutions of address conflicts resolution adopt corrective methods, whereby addresses are often assigned to devices being connected to a network first, and upon assignments, the network is accordingly scanned to detect any address conflicts. If address conflicts exist, new address will accordingly be allocated.

[007] While existing solutions adopt corrective method to resolve address conflicts, there is no unified approach for avoiding address conflicts, for either active or non-active networks or devices having different addressing method in heterogeneous network environment. In the event that the network scan is done when one of the networks is not active or device connected to that particular network is in hibernation mode, there will be no network address conflicts detected, and the network address coordinator may use that particular address. However, as the hibernating device awakes and the non-active network turns active, address conflict will happen. Accordingly, new address reassignment is required, yet cost of address reassignment is always much costlier after conflict being detected.

Summary

[008] In one aspect of the present invention, there is provided a method for preemptive network address conflict resolution for a newly joined network device to maintain address uniqueness in heterogeneous network. The method comprises the steps of requesting address conflict detection/verification for network address of the newly joined network device, performing conflict detection/verification for network address of the newly joined network device, and responding with address

detection/verification result. When network address conflict is detected, a different new unique network address is generated and assigned to the newly joined network device, and the conflicting address as well as the newly generated unique network address are deprecated.

[009] In a further embodiment of the present invention, the steps of performing detection/verification for the network address of the newly joined network device further comprises the steps of classifying type of the network address of the newly joined network device in heterogeneous network environment, extracting partial or full information of the network address of the newly joined network device for the specific network type, and performing a look-up of the information of the network address of the newly joined network device in a database storing all existing network addresses, including both active and non-active network addresses, received from neighboring network devices for identification of conflict. When network address conflict is detected, the address conflict is being recorded in a conflict list storing detected network address conflict information, and when no address conflict is detected, the conflict list is referred to further verify uniqueness of the network address of the newly joined network device.

[0010] In another further embodiment of the present invention, the steps of network address deprecation comprising the steps of receiving trigger of address conflict detection, referring to the database for identification of conflict address type, broadcasting address deprecation message to the newly joined network device informing that address conflict is detected, starting timer for deprecation completion, sending unicast message to the conflicting addresses informing status of the network

address deprecation, awaiting response from the conflicting addresses; and notifying completion of deprecation process.

[0011] In still another further embodiment of the present invention, the steps of broadcasting deprecation message further comprises the steps of receiving trigger of address deprecation instruction, removing current conflicting network address from the database, and requesting for new address assignment detection and verification.

[0012] In yet another further embodiment of the present invention, the method for preemptive network address conflict resolution for a newly joined network device further comprises the step of database synchronization. The database synchronization comprises the steps of receiving trigger to perform database synchronization, receiving new network address information to be added or deleted from the database, performing a look-up in the database and identifying changes in address entries, and updating the database. The database stores device address from same or heterogeneous networks.

[0013] In another embodiment of the present invention, the newly generated unique network address is generated through a method for generating a unique network address, wherein the method comprises the steps of receiving request for new full network address or partial network address generation, referring to the conflict list and extracting network address conflict field, allocating new full network address or partial network address, and performing a look-up for the new full network or partial network address.

[0014] Another aspect of the present invention provides a system for preemptive network address conflict resolution. The system comprises a user device assigned with a network address and a conflict resolver operationally communicating

with the user device. The conflict resolver comprises a network address conflict verification and detection unit for detecting address conflicts between the network address of the user device and existing addresses from neighboring network devices. The network address conflict verification and detection unit includes a network address conflict detection and verification request receiver unit for receiving request of conflict detection and verification for the network address of the user device, a network database storing all existing network addresses from neighboring network devices, the existing addresses including both active and non-active network addresses of heterogeneous network. Upon receipt of conflict detection and verification request, the network address is verified against the network database, thereby identifying any address conflict between the user device network address and the all existing network addresses. The network address conflict verification and detection unit further includes a network address conflict registration unit for registering address conflict information detected between the network address of the user device and the existing network addresses to a conflict list database. The conflict database stores the address conflict information detected.

[0015] In another embodiment of the present invention, the conflict resolver further comprises a unique address range generation unit operable for generating new unique network address range to be assigned to the user device when there is address conflict detected. The new unique network address is generated with reference to the network database to avoid any conflict between the new unique network address and the existing network addresses. This allows the device to use either one of the address or address range allocated to it.

[0016] In another embodiment of the present invention, the conflict resolver may further comprise a network address deprecation unit for deprecating the network address conflict detected and the newly generated unique network address.

[0017] In yet another further embodiment of the present invention, the network database further comprises information on devices protocol type, Layer 1 or Layer 2 address, and MAC address or EUI Type of each devices, and deprecated addresses.

Brief Description of the Drawings

[0018] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

[0019] Fig. 1 is a diagram illustrating a system for preemptive address conflict resolution, for both active and non-active network-device addresses in accordance with one embodiment of the present invention;

[0020] Fig. 2 illustrates a diagram of the preemptive address conflict resolution process performed by the system of Fig. 1, in accordance with one embodiment of the present invention;

[0021] Fig. 3 illustrates a diagram of device address or device address prefix/range conflict detection/verification process according to another embodiment of the present invention;

[0022] Fig. 4 is a flowchart illustrating a new address reassignment procedure according to one embodiment of the present invention;

[0023] Fig, 5 is a flowchart illustrating a new device address or device address prefix/range generation process according to one embodiment of the present invention;

[0024] Fig. 6 is a flowchart illustrating a NAMS Database/Table synchronization process occurring when there is device address or device address prefix/range conflict detected;

[0025] Fig. 7 illustrates a diagram of NAMS Table synchronization process as one embodiment of the present invention;

[0026] Fig. 8 illustrates a flowchart of address deprecation process according to one embodiment of the present invention;

[0027] Fig. 9 illustrates a diagram of address deprecation process according to a further embodiment of the present invention;

[0028] Fig. 10 illustrates an exemplary format of NAMS Database/Table in accordance with one embodiment of the present invention; and

[0029] Fig. 11 illustrates an exemplary format of Conflict Analysis List/Table in accordance with one embodiment of the present invention.

Detailed Description

[0030] The following descriptions of a number of specific and alternative embodiments are provided to understand the inventive features of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practiced without such specific details. Some of the details may not be described in length so as to not obscure the invention. For ease of reference, common reference

numerals will be used throughout the figures when referring to same or similar features common to the figures.

[0031] The present invention provides a system and method for preemptive address conflict resolution, for both active and non-active network and/or devices having different addressing method in heterogeneous network environment. The system and method utilize addresses that are not used by both active and non-active network and/or device to preemptively resolve address conflicts. This is the advantage of the present invention that even non-active networks or hibernating devices are being considered so as to preemptively resolve address conflicts. The present invention is also cost-advantageous for preemptively resolve address conflicts, since address conflict resolution or address reassignment is much costlier after conflict occurs and being detected.

[0032] Fig. 1 is a diagram illustrating a system 10 for preemptive address conflict resolution, for both active and non-active network-device addresses in accordance with one embodiment of the present invention. The system 10 can be implemented for both EUI48/64 and non-EUI48/64 group of devices for preemptive network addresses conflict resolution, covering heterogeneous network. The system 10 avoids address conflicts at Layer 2 and enables unique communication at Layer 2 or Layer 3 of a network architecture.

[0033] The system 10 utilizes Network Address Management Scheme (NAMS), which comprises two different entities, i.e. NAMS Conflict Resolver (NCR) 11 and NAMS User Device (NUD) 12. The NUD 12 communicates with the NCR 11.

[0034] The NUD 12 comprises a unique device address creation unit 12A. The unique device address creation unit 12A is responsible to generate a network address or range of network addresses assigned to a newly joined node/device. The NCR 11 is to detect and verify whether the network address generated by the unique device creation unit 12A is conflicting with any existing network address and to resolve the conflict detected, if any.

[0035] Still referring to Fig. 1, the NCR of the system 10 further comprises a unique address or address range generation unit 13 for generating new unique address or address range and a network address conflict detection/verification unit 14 for detecting address conflicts between new address and existing address.

[0036] The network address conflict verification and detection unit 14 further comprises a network address conflict detection and verification request receiver unit 15 for receiving request from the NUD 12 for a specific network address verification, a network address conflict registration unit 16 for communicating and registering any full or partial address conflict information to a network address Conflict Analysis List 18 which stores the information accordingly, and a NAMS Database/Table 17 which is a database storing all addresses assigned to neighboring network-devices. The NAMS Database/Table 17 is updated and synchronized by a NAMS Database/Table synchronization unit 19 upon receipt of synchronization request from the NUD 12. The NAMS Database/Table synchronization is performed between local NAMS Database/Table and neighboring NAMS Database/Table.

[0037] The unique address or address range generation unit 13 is configured to generate new unique address or address range with reference to the NAMS

Database/Table 17 of the address conflict detection/verification unit 14. A network address confirmation unit 13A further confirms that the newly generated address or address range is unique based on the verification result received from the address conflict verification/detection unit 14.

[0038] Still referring to Fig. 1, the NCR 11 further comprises a network address deprecation enforcement unit 13B. The network address deprecation enforcement unit 13B performs deprecation upon request from the NUD 12 when there is conflict detected. The network address deprecation enforcement unit 13B further updates the Network Address Conflict Analysis List 18 and ensure that all conflicts are well recorded in Conflict Analysis List 18.

[0039] The preemptive address conflict resolution process using the system 10 is described as follows. Fig. 2 illustrates a diagram of the preemptive address conflict resolution process 20 performed by the system 10 of Fig. 1, in accordance with one embodiment of the present invention.

[0040] Referring to Fig. 2, at step 21, the NUD sends requests for device address or device address prefix/range conflict detection/verification for a new device address or device address prefix/range assigned to a newly joined node. At step 22, the NCR receives requests for the device address or device address prefix/range conflict detection/verification. At step 23, the new device address or device address prefix/range is verified for any address conflict against local NAMS Table. At step 24, the NCR replies the NUD with the detection/verification results.

[0041] If no conflict is detected, the process 20 is terminated.

[0042] If the device address or device address prefix/range assigned to the newly joined node is in conflict with existing address, a new address reassignment procedure and an address deprecation procedure will be invoked.

[0043] Fig. 3 illustrates a diagram of device address or device address prefix/range conflict detection/verification process 30 according to another embodiment of the present invention. The device address conflict verification/detection method comprises the steps as follows. At step 31, the network-devices address conflict verification/detection unit of the NCR receives request for device address or device address prefix/range conflict detection/verification from NUD. Thereafter, at step 32, type of address to be analyzed is classified. Upon address classification, device address details are extracted at step 33 for detail analysis. The address details may include network prefix and device address. Subsequently at step 34, the address details are looked-up in the local NAMS Database/Table for conflict detection until end of the table entry is reached. If there is address conflict, then the details of the conflict will be stored in Conflict-Analysis list with conflict analysis information at step 35, and eventually a new address reassignment procedure and an address deprecation procedure will be invoked at step 36.

[0044] Still referring to Fig. 3, if there is no network-address conflict with all current entries in the local NAMS Table, then Conflict-Analysis list is referred for final verification of the device address or device address prefix/range at step 37. If there is no conflict occurring, no conflict (success) status will be returned at step 38 to NUD. If there is a conflict occurring, the conflicting portion of the device address or network address prefix/range is identified at step 39 and conflict (fail) status will be returned to NUD at step 40.

[0045] Fig. 4 is a flowchart illustrating a new address reassignment procedure 40 according to one embodiment of the present invention. As discussed above, the new address reassignment procedure 40 will be invoked when the device address or device address prefix/range assigned to the newly joined node is in conflict with existing address. At step 41, the NCR detects that the device address or device address prefix/range of the newly joined node is in conflict with existing address. At step 42, the NCR assigns another new device address or device address prefix/range to the newly joined node, and thereafter at step 43, the NCR updates the newly assigned device address or device address prefix/range to local NAMS Database/Table and invokes synchronization with neighboring NAMS Database/Table for only the updated part of NAMS Database/Table. The synchronization can be done in predetermined periodic manner.

[0046] When there is conflict of address between the address assigned to the newly joined node with the existing device address or device address prefix/range, the NCR is to generate another new address for the newly joined node. Fig. 5 is a flowchart illustrating a new device address or device address prefix/range generation process 50 according to one embodiment of the present invention. According to this embodiment, the new address generation method comprises the steps as follows. At step 51, trigger for new address or device address prefix/range generation is received. At step 52, a new address is generated. At step 53, Conflict Analysis List will be referred and device-network address of the newly generated address will be extracted for comparison. Since the Conflict Analysis List records all history of conflicting address, this step is ensures that the newly generated address does not conflict with any existing address. The conflict is also detected at partial address level, e.g network

prefix/s or node address/ID (some devices may use its node ID to generate an address). When the newly generated address conflicts with a device address or device address prefix/range belongs to an existing device, whether the existing device is active or hibernating, the newly generated address should not be allocated to the newly joined device. Accordingly, new full device address (i.e., both network address and device address) or new partial address (i.e., either network address or device address) will be allocated at step 54 or step 56 respectively. At step 55, local NAMS Database/Table will be referred to confirm that there is no address conflict with the newly generated full address, while at step 57, the local NAMS Database/Table will be referred to confirm that there is no address conflict in the newly generated partial address. Upon confirmation, new full or partial address is accordingly formed at step 58, after which the procedure terminates.

[0047] Fig. 6 is a flowchart illustrating a NAMS Database/Table synchronization process 60 occurring when there is device address or device address prefix/range conflict detected. At step 61, request for NAMS Database/Table synchronization with neighboring NAMS Database/Table is received from the NCR. At step 62, the NAMS Database/Table synchronization with the neighboring NAMS Database/Table is performed. At step 63, the local and the neighboring NAMS Database/Table is updated.

[0048] Fig. 7 illustrates a diagram of NAMS Database/Table synchronization process 70 as one embodiment of the present invention. According to this embodiment of the present invention, NAMS Database/Table synchronization process starts at step 70A, at which trigger for NAMS Database/Table synchronization is received. The trigger received can be either a timer trigger to perform synchronization received at

step 71, or a trigger to add/delete new address entries to the NAMS Database/Table received at step 72. At step 73, local NAMS Database/Table is referred and changes in address entries are identified. At step 74, partial NAMS Database/Table is sent to existing joined devices, while at step 75, entire NAMS Database/Table is sent to newly joined node,

[0049] Fig. 8 illustrates a flowchart of address deprecation process 80 according to one embodiment of the present invention. The address deprecation process 80 will be invoked when there is device address or device address prefix/range conflict detected by the NCR. The network-device address deprecation method 80 comprises the following steps. At step 81, trigger of address conflict detection is received. As the address conflict is detected, at step 82, local NAMS Database/Table is referred for identifying the type of the address conflict. At step 83, address deprecation message is broadcasted to newly joined node so that the newly joined node does not use the conflicted device address or device address prefix/range. At step 84, timer for network-device address deprecation process completion is started. The timer is required so as to notify the newly joined node and other nodes communicating with the newly joined node regarding the address deprecation process. At step 85, unicast message regarding the address conflict is sent to the existing node using the conflicting device addresses or device address prefixs/ranges and the newly joined node, respectively. Reply message from the existing node acknowledging that the existing nodes can keep using conflicting addresses is awaited. Simultaneously, reply message from the newly joined node acknowledging that the newly joined node is to use another new address is also awaited. If the reply message is not received, address deprecation message is broadcasted again. If the reply message is received, the deprecation process is

completed and notification of deprecation completion is delivered to the existing node and the newly joined node, respectively, at step 86.

[0050] Fig. 9 illustrates a diagram of address deprecation process 90 according to a further embodiment of the present invention. In this further embodiment, as the deprecation message is broadcasted to newly entered joined node, deprecation process is invoked. The deprecation process is initiated by receiving a trigger of address deprecation process instruction at step 91. Then at step 92, a look-up is performed for the specific conflicting address in the local NAMS Database/Table, and subsequently at step 93, the current conflicting address is removed from local NAMS Database/Table. At step 94, the Conflict Analysis List is updated with regards to the conflicting address to ensure that all conflicts are well recorded in Conflict Analysis List. The Conflict Analysis List keeps the information of all occurring conflicts. At step 95, it is confirmed that the conflicting address from the NAMS Database/Table is removed and the Conflict Analysis List is updated with regards to the conflicting address are confirmed. At step 96, new address reassignment and conflict detection/verification process are requested for to assign new address to the newly joined node and to ensure that the newly assigned address is unique and is not in conflict with existing addresses. The new address reassignment and conflict detection/verification process can be performed according to the procedures elaborated above.

[0051] Fig. 10 illustrates an exemplary format of NAMS Database/Table in accordance with one embodiment of the present invention. In this embodiment, the NAMS Database/Table includes information on devices protocol type, devices addresses of all neighboring devices, Layer 1 or Layer 2 address, and MAC address or

EUI Type of each device. The NAMS Database/Table further includes information on whether a particular address being a deprecated address.

[0052] Fig. 11 illustrates an exemplary format of Conflict Analysis List/Table in accordance with one embodiment of the present invention. The Conflict Analysis List/Table records all history of address conflict information. It is widely known to the person skilled in the art that a full format of a device address comprises at least one network prefix/address and device address, wherein the network prefix/address may change variably but device address remains the same. As such, it is preferable that when being recorded to the Conflict Analysis List/Table, all details of a device address, i.e. the network prefix/address and the device address, are being extracted and recorded separately. In this exemplary embodiment, the Conflict Analysis List/Table is used to record address conflict information, which format of the full address be xxx:yy:zzz. xxx is first network prefix/range, yy is second network prefix/range, and zzz is device address. The Conflict Analysis List/Table comprises five fields, wherein one field stores full address, two fields separately stores information of first and second network prefix/range, and one field stores information of device address. Such Conflict Analysis List/Table thus allows detailed look-up and analysis for address conflict detection/verification.

[0053] The system and method of the present invention can be deployed for, but not limited to, group of devices with protocol type of Ethernet, IEEE 802.15.4, group of devices of MAC/ EUI (64 bits/48 bits); group of devices of non- EUI, etc.

[0054] The system and method of the present invention provides solution for address conflicts by preemptively resolve address conflict, particularly at Layer 2 of a

network architecture as well as enabling unique communication at Layer 2 or Layer 3 of a network architecture. The present invention also allows multi-protocol type devices to be present in one network without conflicting each other.

[0055] The system and all processes or methodologies disclosed herein provide preemptive address conflicts resolution in various heterogeneous networks and network devices, such as WPAN, Home Network, and many other heterogeneous networks. The devices and networks may use different protocol standards such as IEEE802.15.4, Homeplug, IPv4, IPv6, LonWorks etc.

[0056] With the system of the present invention, each device can scan their neighboring reachable network and discover existing network address, and most importantly it is able to cover both active and non-active network and/or device address. Based on this information, the device is able to automatically configure their own unique address and connect themselves to the network while avoiding any address conflict. The system and method of the present invention thus eliminates any human intervention, provides devices zero configuration state, and increases efficiency on network devices communication.

[0057] The above description illustrates various embodiments of the present invention along with examples of how aspects of the present invention may be implemented. While specific embodiments have been described and illustrated it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the present invention. The above examples, embodiments, instructions semantics, and drawings should not be deemed to be the only embodiments, and are presented to

illustrate the flexibility and advantages of the present invention as defined by the following claims:

Claims

1. A method for preemptive network address conflict resolution for a newly joined network device, comprising the steps of:

requesting address conflict detection/verification for network address of the newly joined network device;

performing conflict detection/verification for network address of the newly joined network device; and

responding with address detection/verification result, wherein when network address conflict is detected, a new unique network address is generated and assigned to the newly joined network device and the conflicting address as well as the newly generated unique network address are deprecated.

2. The method according to claim 1, wherein the steps of performing detection/verification for the network address of the newly joined network device further comprises the steps of:

classifying type of the network address of the newly joined network device;

extracting partial or full information of the network address of the newly joined network device; and

performing a look-up of the information of the network address of the newly joined network device in a database storing all existing network addresses, including both active and non-active network addresses, received from neighboring network devices for identification of conflict, wherein when network address conflict is

detected, the address conflict is being recorded in a conflict list storing detected network address conflict information, and wherein when no address conflict is detected, the conflict list is referred to further verify uniqueness of the network address of the newly joined network device.

3. The method according to claim 1, wherein the steps of network address deprecation comprising the steps of:

receiving trigger of address conflict detection;

referring to the database for identification of conflict address type;

broadcasting address deprecation message to the newly joined network device informing that address conflict is detected;

starting timer for deprecation completion;

sending unicast message to the conflicting addresses informing status of the network address deprecation;

awaiting response from the conflicting addresses; and

notifying completion of deprecation process.

4. The method according to claim 3, wherein the steps of broadcasting deprecation message further comprises the steps of:

receiving trigger of address deprecation instruction;

removing current conflicting network address from the database; and

requesting for new address assignment detection and verification.

5. The method according to claim 1, further comprises the step of database synchronization, the step of database synchronization comprising the steps of:

receiving trigger to perform database synchronization;

receiving new network address information to be added or deleted from the database;

performing a look-up in the database and identifying changes in address entries; and

updating the database.

6. The method according to claim 1, wherein the newly generated unique network address is generated through a method for generating a unique network address comprising the steps of:

receiving request for new full network address or partial network address generation;

referring to the conflict list and extracting network address conflict field;

allocating new full network address or partial network address; and

performing a look-up for the new full network or partial network address.

7. A system for preemptive network address conflict resolution comprising:

a user device assigned with a network address;

a conflict resolver operationally communicating with the user device, the conflict resolver having:

a network address conflict verification and detection unit for detecting address conflicts between the network address of the user device and existing addresses from neighboring network devices; wherein the network address conflict verification and detection unit includes:

a network address conflict detection and verification request receiver unit for receiving request of conflict detection and verification for the network address of the user device;

a network database storing all existing network addresses from neighboring network devices, the existing addresses including both active and non-active network addresses, wherein upon receipt of conflict detection and verification request, the network address is verified against the network database, thereby identifying any address conflict between the user device network address and the all existing network addresses;

a network address conflict registration unit for registering address conflict information detected between the network address of the user device and the existing network addresses to a conflict list database, wherein the conflict database stores the address conflict information detected.

8. The system of claim 7, wherein the conflict resolver further comprises a unique address range generation unit operable for generating new unique network address range to be assigned to the user device when there is address conflict detected, wherein

the new unique network address is generated with reference to the network database to avoid any conflict between the new unique network address and the existing network addresses.

9. The system of claim 7, wherein the conflict resolver further comprises a network address deprecation unit for deprecating the network address conflict detected and the newly generated unique network address.

10. The system of claim 7, wherein the network database further comprises information on devices protocol type, Layer 1 or Layer 2 address, and MAC address or EUI Type of each devices, and deprecated addresses.

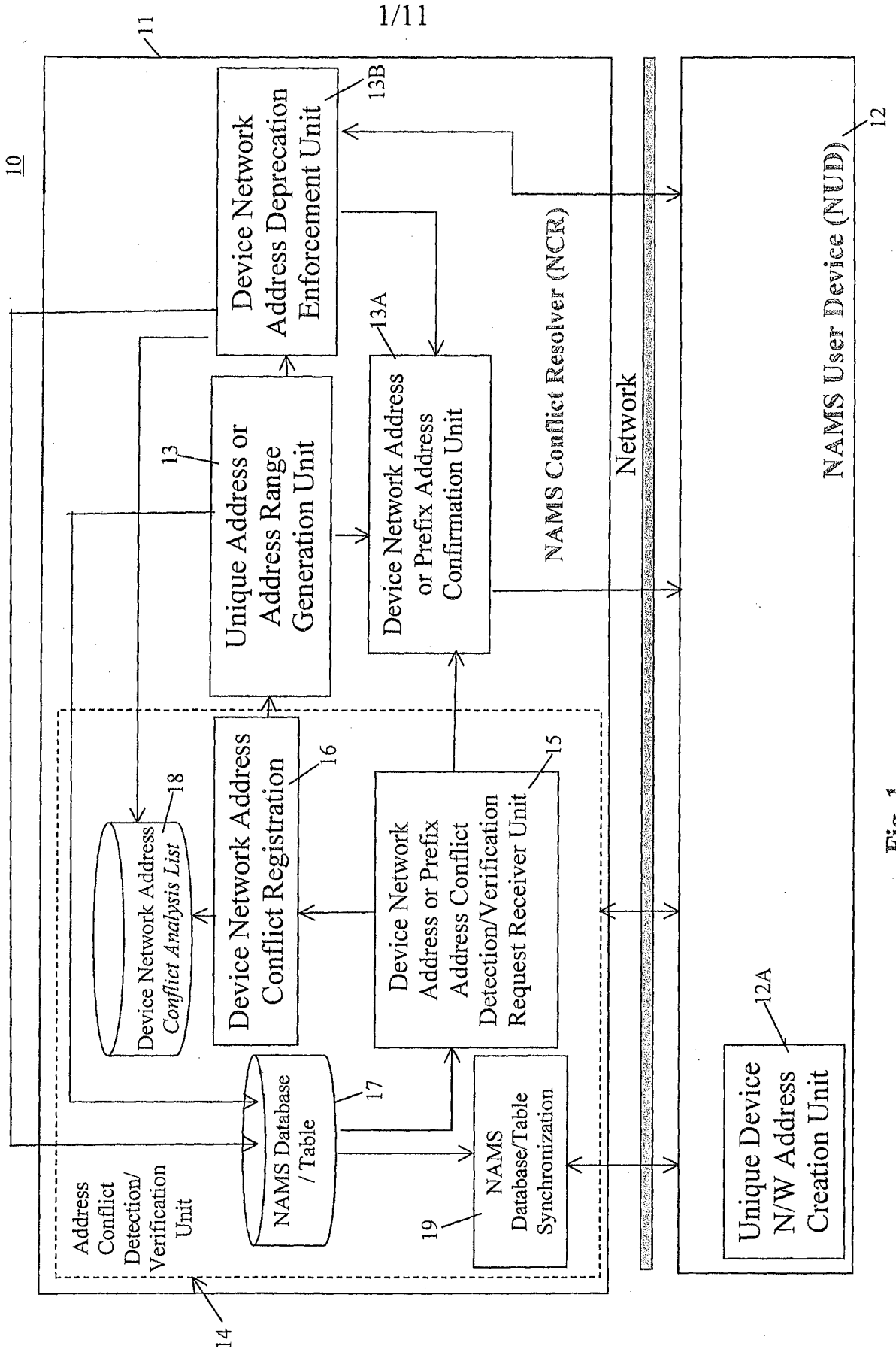
10
11
12
12A
13
13A
13B
14
15
16
17
18
19
Device Network Address Conflict Analysis List
Device Network Address Conflict Registration
Device Network Address or Prefix Address Conflict Detection/Verification Request Receiver Unit
NAMS Database / Table
NAMS Database/Table Synchronization
Address Conflict Detection/ Verification Unit
Unique Address or Address Range Generation Unit
Device Network Address or Prefix Address Confirmation Unit
Device Network Address Deprecation Enforcement Unit
NAMS Conflict Resolver (NCR)
Network
NAMS User Device (NUD)
Unique Device N/W Address Creation Unit

Fig. 1

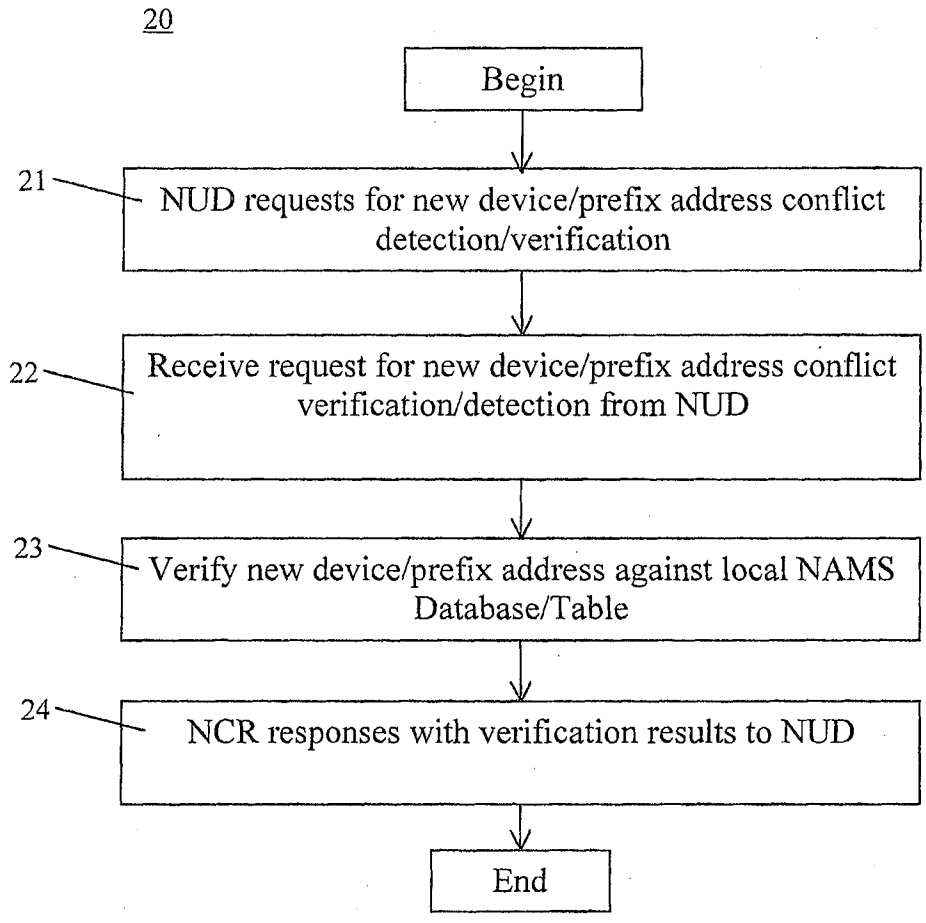
20
Begin
21
NUD requests for new device/prefix address conflict detection/verification
22
Receive request for new device/prefix address conflict verification/detection from NUD
23
Verify new device/prefix address against local NAMS Database/Table
24
NCR responses with verification results to NUD
End

Fig. 2

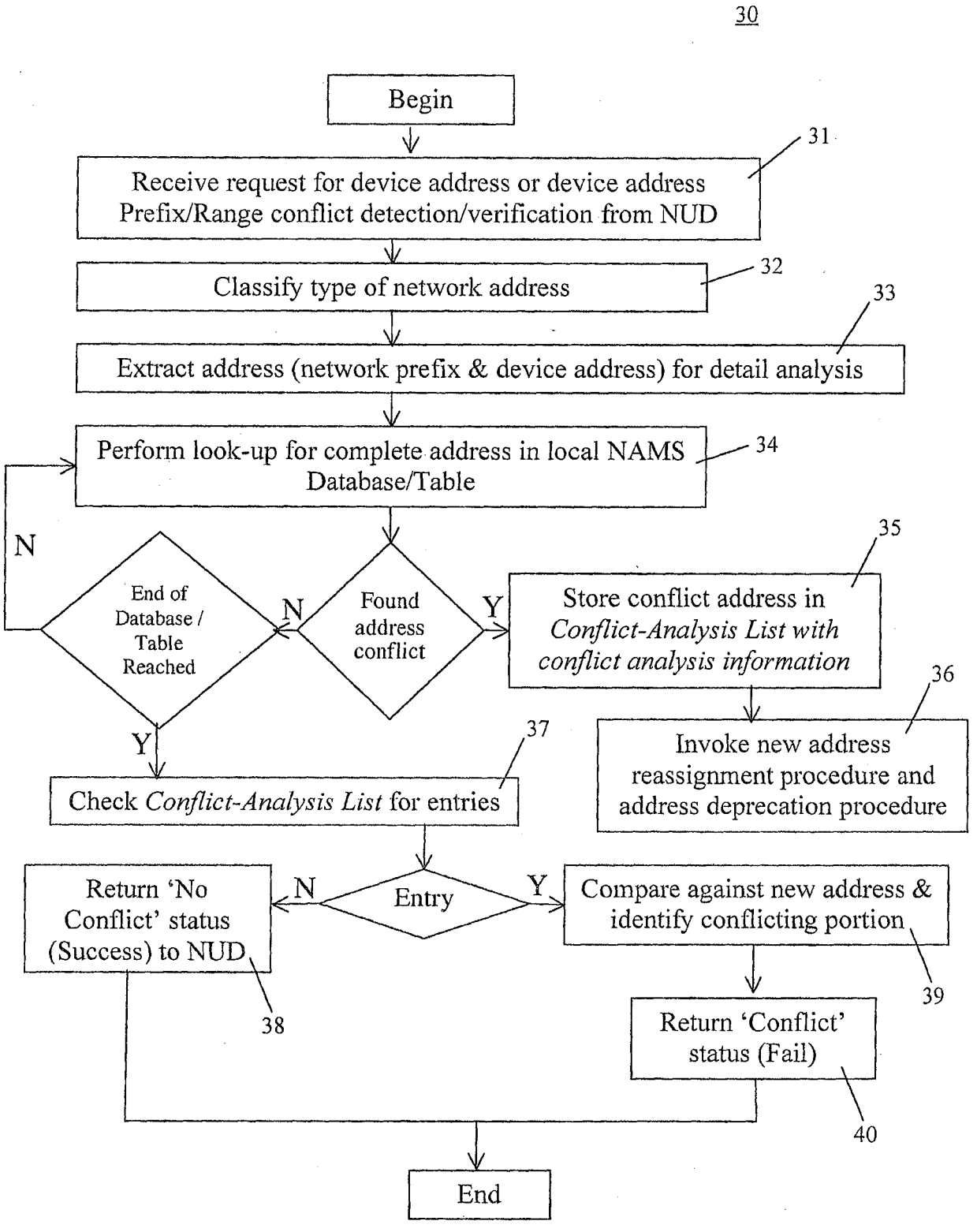
30
Begin
31
Receive request for device address or device address Prefix/Range conflict detection/verification from NUD
32
Classify type of network address
33
Extract address (network prefix & device address) for detail analysis
34
Perform look-up for complete address in local NAMS Database/Table
N
End of Database / Table Reached
N
Found address conflict
Y
35
Store conflict address in *Conflict-Analysis List with conflict analysis information*
36
Invoke new address reassignment procedure and address deprecation procedure
Y
37
Check *Conflict-Analysis List* for entries
Return 'No Conflict' status (Success) to NUD
N
Entry
Y
Compare against new address & identify conflicting portion
39
38
Return 'Conflict' status (Fail)
40
End

Fig. 3

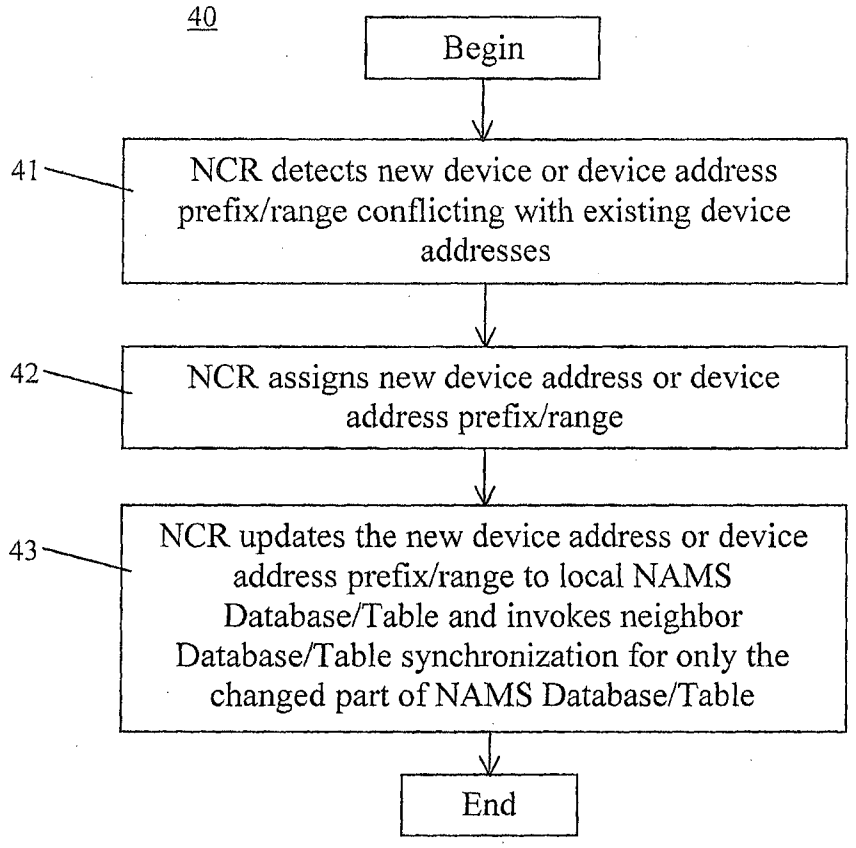
40
Begin
41
NCR detects new device or device address prefix/range conflicting with existing device addresses
42
NCR assigns new device address or device address prefix/range
43
NCR updates the new device address or device address prefix/range to local NAMS Database/Table and invokes neighbor Database/Table synchronization for only the changed part of NAMS Database/Table
End

Fig. 4

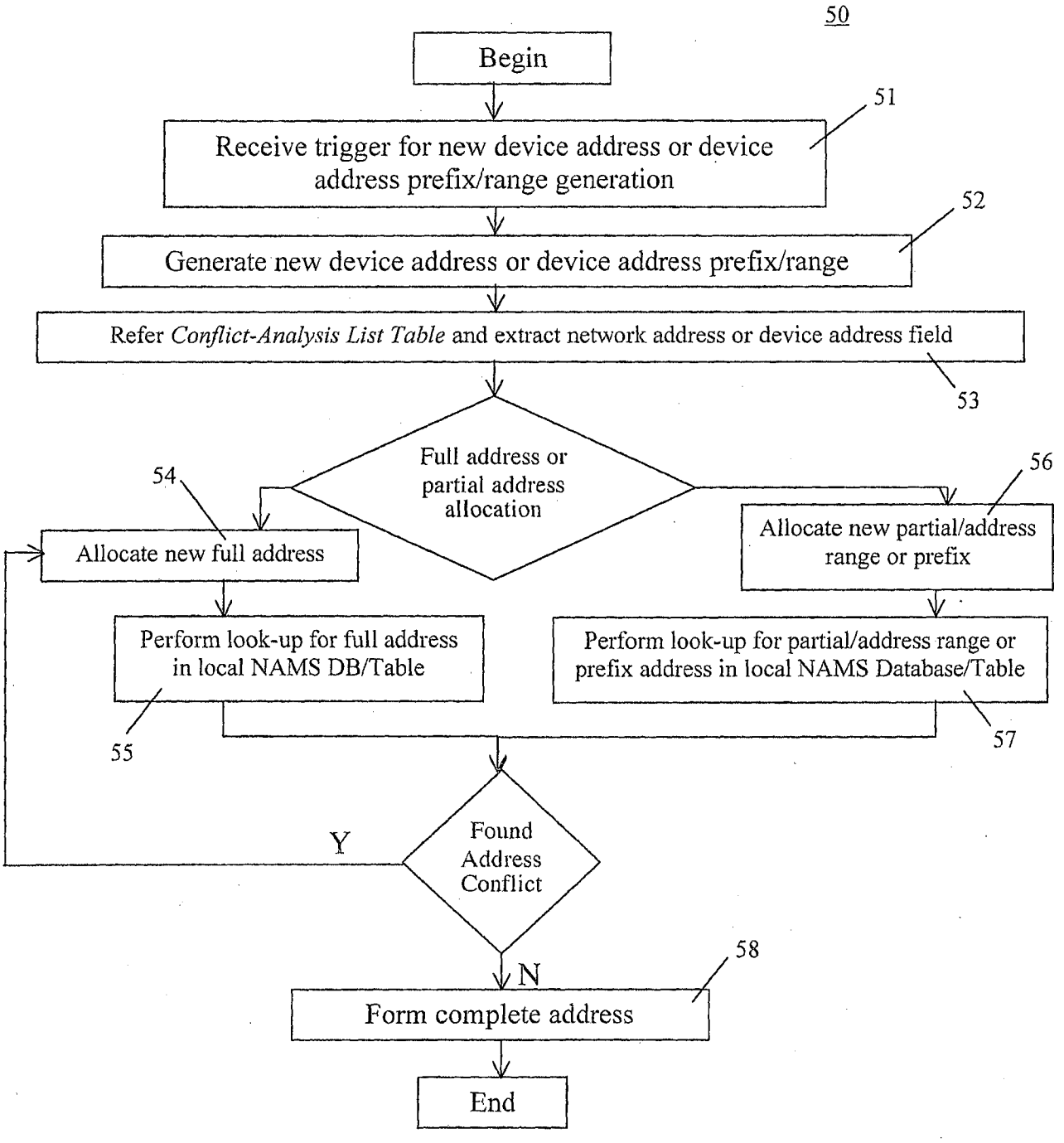
50
Begin
51
Receive trigger for new device address or device address prefix/range generation
52
Generate new device address or device address prefix/range
Refer *Conflict-Analysis List Table* and extract network address or device address field
53
Full address or partial address allocation
54
Allocate new full address
56
Allocate new partial/address range or prefix
Perform look-up for full address in local NAMS DB/Table
Perform look-up for partial/address range or prefix address in local NAMS Database/Table
55
57
Found Address Conflict
Y
N
58
Form complete address
End

Fig. 5

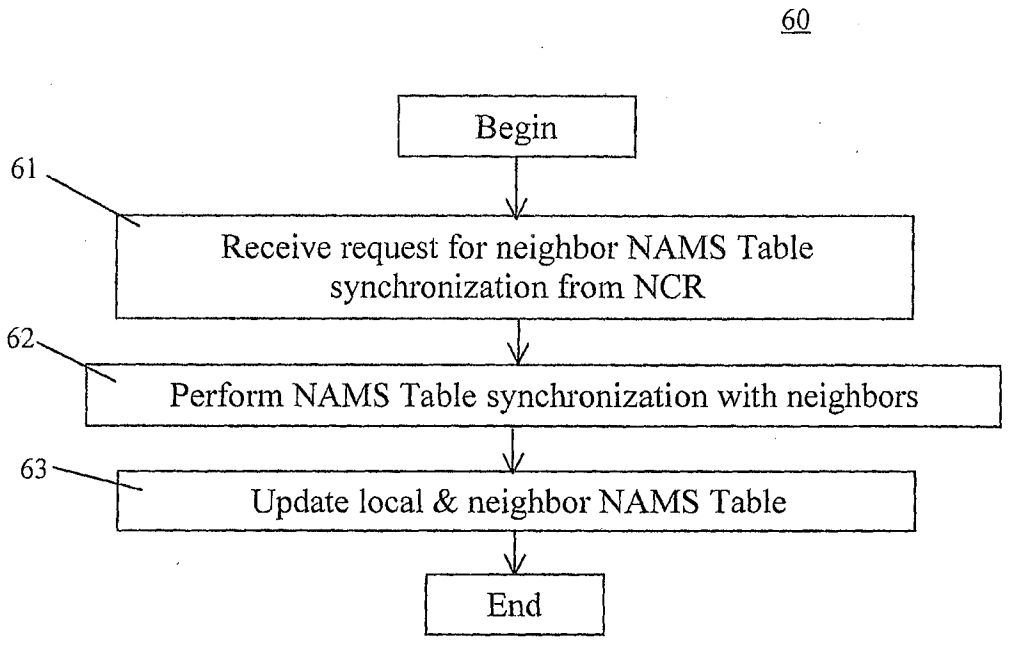
60
Begin
61
Receive request for neighbor NAMS Table synchronization from NCR
62
Perform NAMS Table synchronization with neighbors
63
Update local & neighbor NAMS Table
End

Fig. 6

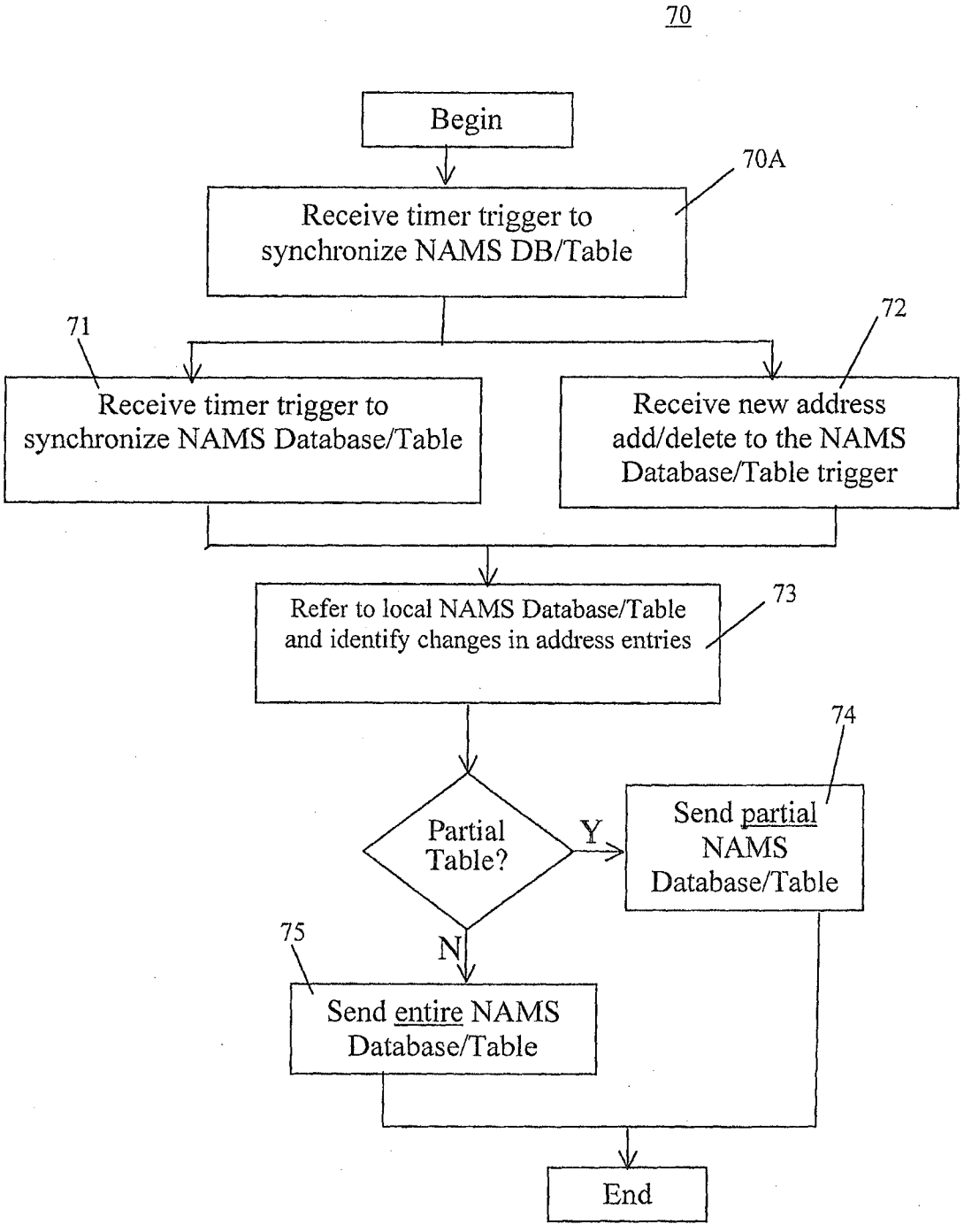
70
Begin
70A
Receive timer trigger to synchronize NAMS DB/Table
71
Receive timer trigger to synchronize NAMS Database/Table
72
Receive new address add/delete to the NAMS Database/Table trigger
Refer to local NAMS Database/Table and identify changes in address entries
73
74
Partial Table?
Y
Send partial NAMS Database/Table
N
75
Send entire NAMS Database/Table
End

Fig. 7

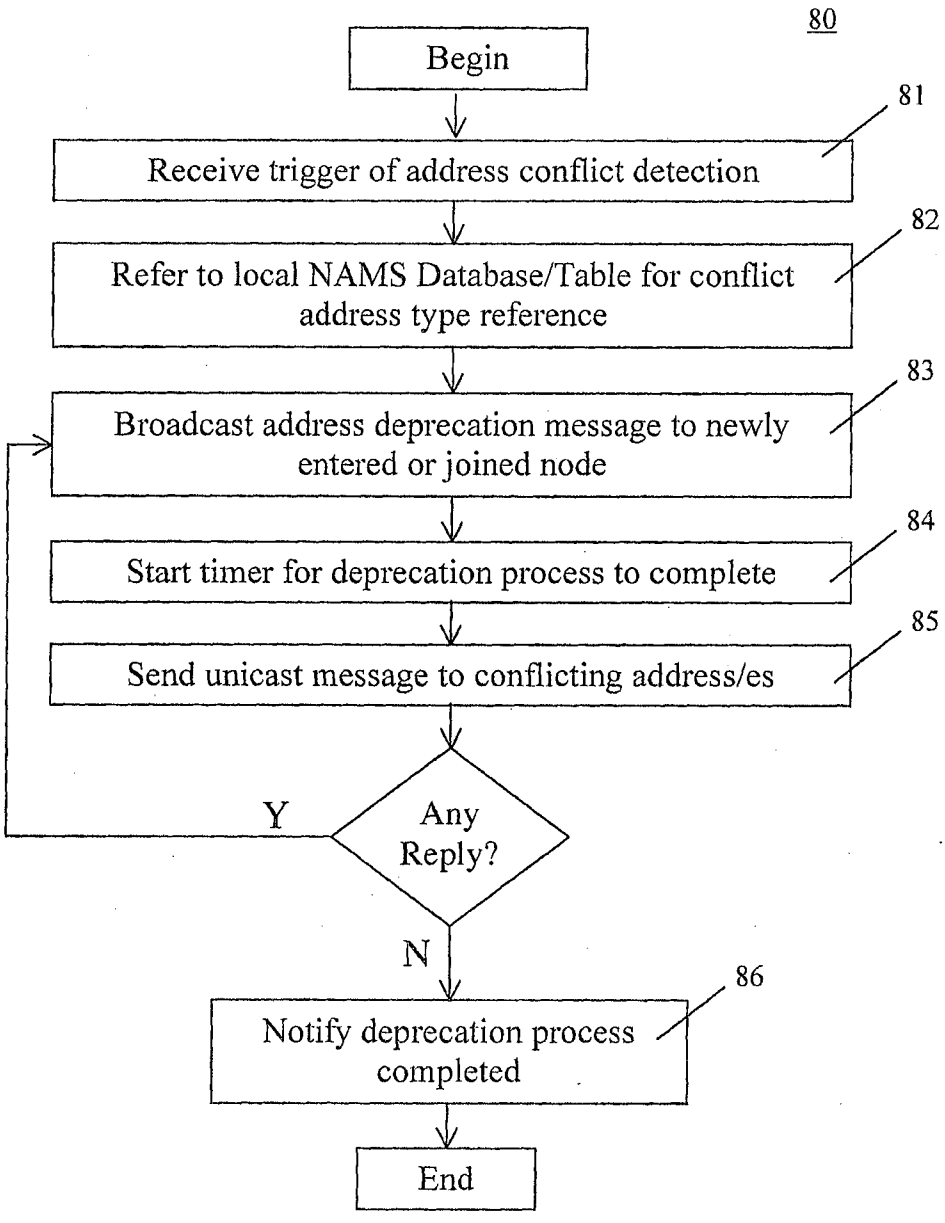
80
Begin
81
Receive trigger of address conflict detection
82
Refer to local NAMS Database/Table for conflict address type reference
83
Broadcast address deprecation message to newly entered or joined node
84
Start timer for deprecation process to complete
85
Send unicast message to conflicting address/es
Any Reply?
Y
N
86
Notify deprecation process completed
End

Fig. 8

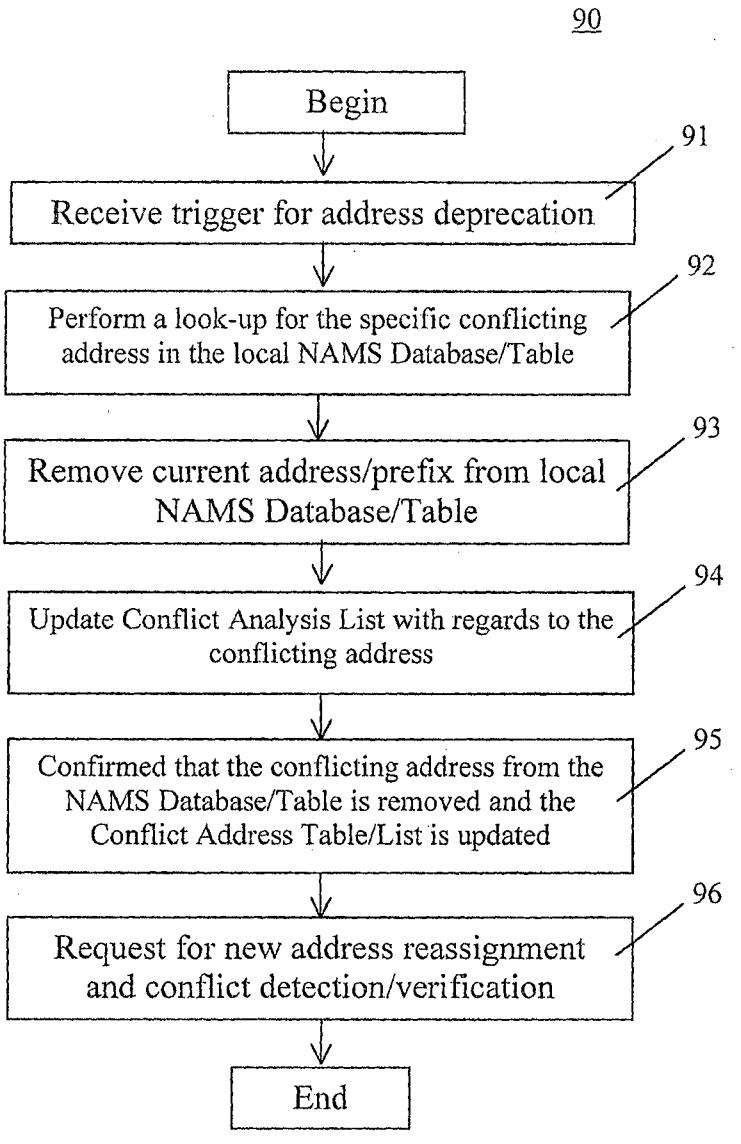
90
Begin
91
Receive trigger for address deprecation
92
Perform a look-up for the specific conflicting address in the local NAMS Database/Table
93
Remove current address/prefix from local NAMS Database/Table
94
Update Conflict Analysis List with regards to the conflicting address
95
Confirmed that the conflicting address from the NAMS Database/Table is removed and the Conflict Address Table/List is updated
96
Request for new address reassignment and conflict detection/verification
End

Fig. 9

NAMS Database/Table

Type Protocol	Layer 1 or 2 Address	MAC/ EUI Type		Non-EUI	Support IPv6 Address	Gateway ID	MAC Status	Protocol Translatable	New IPv6 Address Assigned (#)	Last Updated Time	Last Sync Time	Valid/ Deprecated Address	Address ID
		64	48										
Ethernet	√ (L2 Add)	x	√	x	√ (Address)	GW_001	Y	x	N	2011_03_11	2011_03_xx	Y	#1
802.15.4	√ (L2 Add)	√	x	x	√ (Address)	GW_001	Y	x	N	2011_03_11	2011_03_xx	Y	#2
M-Bus	x (L1 Add)	x	x	√	x	GW_002	N	√	Y (Add)	2011_03_09	2011_03_xx	Y	#3
RS-232	x (L1 Add)	x	x	√	x	GW_002	N	√	Y (Add)	2011_03_09	2011_03_xx	N	#4

Fig. 10

Conflict Analysis List

Address ID	Full Address	Network Prefix/ Range-1	Network Prefix/ Range-2	Device ID
#1	xxx:yy:zzz	xxx	yy	zz
#2				

Fig. 11

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2013/000126

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)

EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 655 928 A1 (HITACHI LTD [JP]) 10 May 2006 (2006-05-10) paragraph [0008] - paragraph [0067]; figure 4	1-10
A	THOMSON CISCO T NARTEN IBM T JINMEI TOSHIBA S: "IPv6 Stateless Address Autoconfiguration; rfc4862.txt", 20070901, 1 September 2007 (2007-09-01), XP015052408, ISSN: 0000-0003 Chapters 4 and 5.	1-10
A	US 2007/097992 A1 (SINGH PRADEEP [US] ET AL) 3 May 2007 (2007-05-03) paragraph [0007] - paragraph [0041]	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 November 2013	08/11/2013

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

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/MY2013/000126

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1655928 A1	10-05-2006	NONE	
US 2007097992 A1	03-05-2007	NONE	