

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
14 October 2004 (14.10.2004)

PCT

(10) International Publication Number
WO 2004/089005 A2

(51) International Patent Classification⁷: **H04Q 7/00**

(21) International Application Number:
PCT/GB2004/001321

(22) International Filing Date: 26 March 2004 (26.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0307373.1 29 March 2003 (29.03.2003) GB

(71) Applicant (for all designated States except US): **KING'S COLLEGE LONDON** [GB/GB]; The Strand, London WC2R 2LS (GB).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **ANTOINE, Stephane** [CI/GB]; Centre for Telecommunications Research, King's College London, The Strand, London WC2R 2LS (GB). **AGHVAMI, Abdol, Hamid** [GB/GB]; Centre for Telecommunications Research, King's College London, The Strand, London WC2R 2LS (GB).

(74) Agent: **CASBON, Paul, Richard**; Lucas & Co., 135 Westhall Road, Warlingham, Surrey CR6 9HJ (GB).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

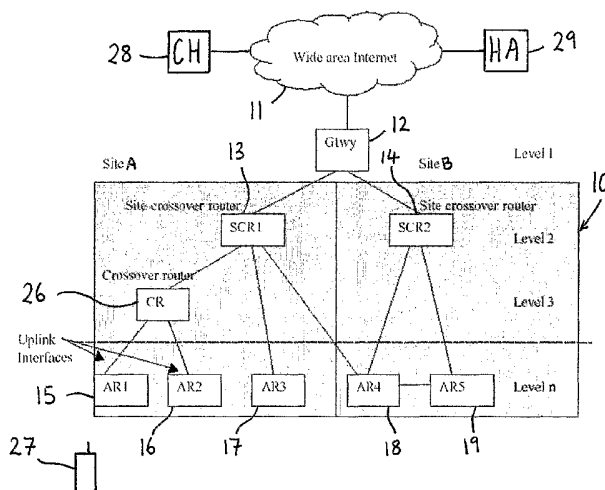
— of inventorship (Rule 4.17(iv)) for US only

Published:

— without international search report and to be republished upon receipt of that report

[Continued on next page]

(54) Title: METHOD, NETWORK NODE, MESSAGES AND COMPUTER PROGRAM FOR USE IN MOBILITY SUPPORT IN A PACKET-SWITCHED DATA COMMUNICATION NETWORK



(57) Abstract: In a packet-switched data communication network (10) comprising a plurality of network nodes and mobile nodes (27) between which data may be exchanged by means of a wireless link, mobile nodes (27) transmitting and receiving data to and from the communication network (10) via respective serving network nodes (15, 16, 17, 18, 19), a method of preparing a mobile node (27) for handover of service from one serving network node (15) to another, which method comprises the steps of: (1) obtaining an identity of one or more adjacent network node (16) adjacent the mobile node's serving network node (15); (2) using each identity to configure a candidate network address for the mobile node; such that (3) if and when the mobile node (27) is served by one of said one or more adjacent network nodes, the candidate network address configured from the identity of that adjacent network node can be assigned to the mobile node.



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

- 1 -

**METHOD, NETWORK NODE, MESSAGES AND COMPUTER PROGRAM
FOR USE IN MOBILITY SUPPORT IN A PACKET-SWITCHED DATA
COMMUNICATION NETWORK**

5

FIELD OF THE INVENTION

The present invention relates to a method of preparing a mobile node for handover of service from one network node to another, to a network node for use in such method, to a computer program for executing the method, to a product
10 comprising the computer program, and to messages and datagrams for use in the method. The present invention also relates to a method of administering a group of network nodes in a packet-switched data communication network, to a network node for use in the method, to a computer program for executing the method and to a product comprising the computer program. The present invention also relates to a
15 method of discovering off-link network node identities.

BACKGROUND OF THE INVENTION

The provision of mobility support in the packet-switched domain for mobile
20 nodes is the subject of ongoing research and development. Users of mobile nodes are demanding greater accessibility to Internet services whilst on the move. An increasing number of mobile nodes, for example portable computers, mobile telephones and personal digital assistants, offer access to packet-switched data networks (e.g. the Internet) via a wireless link and packet radio network. An example
25 of such a packet radio network is the Universal Mobile Telecommunications System (UMTS).

The network-layer protocol associated with the Internet is appropriately called the Internet Protocol (IP). In general, the IP connects the various networks and sub-
30 networks that make up the Internet by defining, among other things, the rules and procedures that govern the way IP data packets are routed from a source node to a destination node. To ensure that IP data packets are correctly routed, every node (or properly an interface of a node) is assigned an IP address, wherein the IP address defines a fixed network location associated with a correspondent node. While the IP
35 adequately handles the routing of data between fixed network nodes, it does not

- 2 -

adequately handle the routing of IP data packets to and/or from mobile nodes.

Mobile nodes may be assigned one or more IP addresses based on their "home" subnet. The home subnet might be that subnet where the mobile node is registered. Data sent by correspondent hosts from external packet data networks is routed via the home agent on the home subnet and is then sent over the wireless link to the mobile node. If the mobile node is moved out of the geographical area of coverage of its home subnet on the wireless link, datagrams will not reach the mobile node. The IP assumes that a host's point of attachment to the network is always the same and therefore cannot cope with a change.

The Mobile Internet Protocol (i.e. Mobile IP) was designed to specifically handle the routing of IP data packets to and/or from mobile nodes (i.e. mobile terminals which frequently change their point-of-attachment to the Internet). Moreover, Mobile IP was designed to handle the routing of IP data packets to and/or from mobile nodes without significantly interrupting on-going communications and without requiring mobile nodes to restart applications.

Mobile IP supports mobility, in part, by assigning two IP addresses to each mobile node. The first of these IP addresses is known as the "home" address. The home address is a permanent IP address, and it is associated with a mobile node's point-of-attachment in the mobile node's home network. The second IP address is called the "care-of" address. The care-of-address is assigned to a mobile node when the mobile node moves and attaches to a foreign network. Unlike the mobile node's home address, the care-of address is a temporary address. The care-of address is a temporary address because it changes whenever the mobile node undergoes a handover procedure from one point-of-attachment to another in a foreign network.

Presently, there are two versions of Mobile IP that have been proposed by the Internet Engineering Task Force (IETF): Mobile IP version 4 (MIPv4) and Mobile IP version 6 (MIPv6). Briefly, Mobile (IPv4) works as follows. Whenever a mobile node moves, and in so doing, attaches to the Internet through a foreign network, the mobile node informs a special node, herein referred to as the mobile node's home agent, as to its new care-of address.

- 3 -

This process involves sending the home agent both the current care-of-address and the home address. The process is also referred to as a registration or "binding update".

5 After the mobile node registers its new care-of address with the home agent, the home agent is able to serve as a proxy host for the mobile node. Accordingly, IP data packets addressed to the mobile node (i.e., the mobile node's home address) will be intercepted by the home agent. The home agent then encapsulates the IP data packet so that the destination address reflects the mobile node's care-of address. The
10 data packet is then sent from the home agent to the mobile node's care-of address. When the IP data packet arrives at the care-of address, the IP data packet is retransformed or de-capsulated by stripping away the care-of address so that the mobile node's home address once again appears as the destination address. The IP data packet can then be delivered to the mobile node, wherein the data contained
15 therein can be processed by the appropriate higher level protocols (e.g. TCP).

The general procedure for mobility support, and in particular handover, in Mobile IPv6 (MIPv6) is set out in the Internet Draft "Mobility Support in IPv6" by Johnson *et al* (presently available at [www.ietf.org/internet-drafts/draft-ietf-mobileip-
20 ipv6-19.txt](http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-19.txt)).

MIPv6 includes several features that were designed to overcome some of the deficiencies associated with MIPv4. One such feature, for example, is called route optimisation.

25 In accordance with the route optimisation feature, MIPv6 compatible nodes maintain a list that provides a mapping between a home address and a corresponding care-of-address for each of a number of mobile terminals. This list is maintained in what is referred to as a "binding cache". When a mobile node moves, it sends a
30 binding update message. Upon receiving the binding update message, each of the MIPv6 compatible nodes use the information contained in the binding update message to update their binding cache. The MIPv6 compatible nodes are then able to send IP data packets directly to the mobile node (i.e., to the mobile node's care-of-address) without first having to route the IP data packets through the mobile
35 terminal's home agent.

- 4 -

When a mobile node moves between sub-networks a new care-of address must be configured for the mobile node before it can begin communication again via the new sub-network and send the binding updates mentioned above. Configuration
5 of the new care-of address takes place during the handoff (or handover) procedure.

One problem with both MIPv4 and MIPv6 is that the configuration of a new care-of address takes time. The latency of the handover is the time between when the last datagrams can be sent and received through the old access router and the time
10 when datagrams can be sent and received through the new access router. This latency affects the quality of service and it is important to reduce this latency if possible.

A refinement of MIPv6 has been set out in the Internet Draft "Fast Handovers for Mobile IPv6" (FHMIPv6) by Dommety *et al* (presently available at
15 www.ieft.org/proceedings/02mar/I-D/draft-ietf-mobileip-fast-mipv6-03.txt). This refinement enables the mobile node to switch access routers and commence communication via the new access router without the need for any binding update to be sent immediately to the home agent. Essentially the mobile node informs the old access router of its new care-of address, so that datagrams addressed to the old care-
20 of address are tunnelled either to the new care-of address or to the new access router. The change of subnet does not need to be advertised to the home agent nor a binding update sent to any correspondent hosts before datagrams can be routed to the mobile node. The refinement is based upon configuring a new care-of address before the mobile node moves to the new access router. A further requirement is that the
25 selected care-of address should not already be in use at new access router.

However, the fast handover method relies upon the identity (e.g. IP address and MAC address) of the new access router being available prior to handover. It is assumed in the document that this information is available, but it is not specified
30 exactly how this information can be obtained or kept current.

US 2001/0036834 A1 discloses a method for fast intra-domain handoffs. A mobility agent defines groups of subnet agents, each of which comprises the subnet agent serving the mobile node and the subnet agents that neighbour the serving agent.
35 Each group forms a multicast group. When service to the mobile node is to be

- 5 -

switched from one subnet agent to another, the mobility agent tunnels packets destined for the mobile node to each member of the multicast group. The members of the group buffer the packets for a limited time. When the mobile node requests a new care-of address on a neighbouring subnet, that subnet forwards the packets it has buffered to the mobile node. Clearly this method is not efficient in terms of network bandwidth. Furthermore, no information about neighbouring subnet agents is made available to the mobile node prior to handoff.

Accordingly it is apparent that there is a need for an improved method and apparatus for managing handoffs of mobile nodes at the network layer of a packet-switched communication network.

SUMMARY OF THE PRESENT INVENTION

Preferred embodiments of the present invention are based on the insight that the identity of neighbouring access routers can be obtained and used to configure candidate care-of addresses for a mobile node before any handover steps are initiated. Thus when handover needs to be performed, a mobile node simply selects the appropriate candidate care-of address that is associated with the identity of the new access router, thereby reducing latency.

According to one aspect of the present invention there is provided in a packet-switched data communication network comprising a plurality of network nodes and mobile nodes between which data may be exchanged by means of a wireless link, mobile nodes transmitting and receiving data to and from the communication network via respective serving network nodes, a method of preparing a mobile node for handover of service from one serving network node to another, which method comprises the steps of:

- (1) obtaining an identity of one or more adjacent network node adjacent the mobile node's serving network node;
- (2) using each identity to configure a candidate network address for the mobile node; such that
- (3) if and when the mobile node is served by one of said one or more adjacent network nodes, the candidate network address configured from the identity of that adjacent network node can be assigned to the mobile node. By "candidate"

- 6 -

care-of address it is meant a potential care-of address that might be required by the mobile node next. One advantage of this is that configuration of candidate care-of addresses can be configured in advance of any handover so that this part of the fast handover process does not need to be performed during an actual handoff, thereby
5 reducing latency. A serving network node is preferably the last router between the network and the mobile node. The serving network node may be an access router with a wireless interface that behaves like a base station for example. The group of network nodes (e.g. access routers) may be such that the serving network node is surrounded or substantially surrounded by adjacent network nodes. In one
10 embodiment the serving network node and at least one adjacent network node are off-link with respect to one another. The network address is preferably a layer 3 address.

Preferably, each network node is associated with a geographical area of signal coverage on the wireless link and the or each adjacent network node for which said
15 identity is obtained is such that, if said mobile node moves from the geographical area of its serving network node, the next serving access router will be one of said adjacent network nodes. The geographical area may include more than one base station i.e. more than one individual cell. Thus the candidate care-of addresses are configured for access routers that are one signal boundary crossing away. However,
20 candidate care-of addresses may be configured for access routers that are more than one boundary crossing away from the network node presently serving the mobile node. This may be useful for serving mobile nodes that are moving with speed across the network.

Advantageously, steps (1) and (2) are initiated in response to completion of a
25 handover of the mobile node from one network node to another, or in response to the initiation of packet flow through a serving network node to or from the mobile node, such that at least one candidate network address is available prior to any subsequent handover. In this way, candidate care-of addresses are configured well before a
30 further handoff. Furthermore, the reliability of the candidate care-of addresses is increased.

Preferably, said serving network node and the or each adjacent network node
35 comprise a multicast group having a multicast address, the method further comprising the step of said serving network node communicating by means of said multicast

- 7 -

address with the or each adjacent network node to obtain said identity. It is possible for members of the group to communicate by unicast messages. However, a multicast configuration reduces overhead on the network. Furthermore, this enables the serving network node to discover the identity of adjacent access routers that are off-link. In one embodiment the multicast address is of organization local scope to prevent the multicast messages leaving the organization. In another embodiment the multicast address is of site local scope. The multicast address may be assigned to the uplink interface of adjacent network nodes. In one embodiment the multicast address may specify a group identity that serves to identify the group of network nodes. In combination with the scope this helps to inhibit multicast messages leaving the scope of an organization or site.

Advantageously, step (1) of the method comprises said serving network node sending a network address (CoA) solicitation message to said multicast address to solicit a response from each adjacent network node containing the respective identity or candidate network address.

Preferably, each network node can be both a serving network node and an adjacent network node simultaneously, said method further comprising the step of each network node sending said network address (CoA) solicitation message to the multicast group of which it is a centre serving access node. By only sending the network address (CoA) solicitation message to the multicast address of which a node is centre, replies are sent by only those nodes that are adjacent the centre. If a node sends a solicitation message to a multicast address of which it is not the centre, it will receive replies from members of the group that are not adjacent to it.

Advantageously, the method further comprises the steps of providing the data link-layer identity of the mobile node and/or present network layer identity of the mobile node in said network address (CoA) solicitation message to help the adjacent network node to identify the mobile node after a handover. This helps to further reduce latency. This also helps the adjacent network node to identify the mobile node if it moves into its signal area. The data-link layer identity may be the ID of the mobile node used for configuring a care-of address for example.

Preferably, said method further comprises the steps of providing said network

- 8 -

address (CoA) solicitation message with a first flag for instructing each adjacent access router to configure said candidate network address either in a stateful way or in a stateless way. The preferred method uses stateless address autoconfiguration (see RFC 2462).

5

Advantageously, said method further comprises the steps of providing said network address (CoA) solicitation message with a second flag for instructing each adjacent network node whether or not to buffer packets received for said mobile node before completion of a handover.

10

Preferably, said network address (CoA) solicitation message is an Internet Control Message Protocol (ICMP) message carried in an IP packet. In this way, the network address (CoA) solicitation message is only processed by members of the group and not by intermediate routers.

15

Advantageously, the method further comprises on receiving said network address (CoA) solicitation message the step of each adjacent network node of said group responding to said serving network node with a network address (CoA) advertisement message in which the identity of the adjacent network node or candidate network address for the mobile node is advertised to the serving network node. It is possible for a candidate network address to either be configured by an adjacent network node or by the serving network node for example.

20

Preferably, said method further comprises the step of providing said network address (CoA) advertisement message with a site identifier and/or domain identifier to identify the site and/or domain in which the adjacent network node is located.

25

Advantageously, said method further comprises the step of providing said network address (CoA) advertisement message with the identity of the adjacent network node sending the message. This may be sent where the serving network node is to configure the candidate care-of address for the mobile node.

30

Preferably, said method further comprises the step of providing said network address (CoA) advertisement message with the network address and/or network prefix and/or link-layer address of a wireless interface of the adjacent network node

35

- 9 -

sending the message. The network address may be an IPv6 address, the network prefix may be the subnet prefix of the adjacent access router and the link-layer address may be derived from the MAC address. This information may be sent to the mobile node to help it recognize the adjacent access router.

5

Advantageously, said method further comprises the step of providing said network address (CoA) advertisement with a lifetime value useable by the serving network node to determine the time for which the information in the network address (CoA) advertisement message is valid. This inhibits the chances of the serving network node sending out of date information to the mobile node.

10

Preferably, said method further comprises the steps of sending said network address (CoA) advertisement as an option to an IPv6 datagram and addressing said IPv6 datagram to the network node serving the mobile node, such that the network address (CoA) advertisement is only processed by said serving network node.

15

Advantageously, said method further comprises the step of periodically sending said network address (CoA) advertisement from a network node, said network address (CoA) advertisement being addressed to the multicast group of which the network node is centre. Preferably this is performed by all of the network nodes of the network. In this way a serving network node will have continually updated care-of addresses for its adjacent network nodes. As soon as that network node serves a mobile node it can send the mobile node's candidate care-of addresses without having to solicit an update from the adjacent network nodes.

20

Preferably, said serving network node further performs the step of forwarding said candidate network address(es) toward the mobile node, and said mobile node performing the step of caching the candidate network address(es) in memory for use in a subsequent handover to an adjacent network node. In this way the mobile node can quickly ascertain the correct care-of address when it detects a new network node.

25

In one embodiment the step of forwarding comprises the step of inserting a candidate network address into an options field of a Proxy Router Advertisement message. The Proxy Router Advertisement message may be similar to that specified in the draft "Fast Handovers for Mobile IPv6" mentioned above.

30

35

- 10 -

In one embodiment, the method further comprises the step of providing said Proxy Router Advertisement message with a field for indicating to a mobile node whether or not it contains a candidate network (CoA) address.

5

Advantageously, in response to a need for handover of service from one network node to another, the method further comprises the steps of advertising to the mobile node the identity of the adjacent network node that will assume responsibility for serving the mobile node, and the mobile node uses said identity to search its
10 cached list of candidate network addresses for one suitable for use after handover.

Preferably, the method further comprises the step of performing duplicate address detection on said candidate network addresses, thereby inhibiting the need to perform duplicate address detection during a subsequent handover of the mobile node
15 from one network node to another. Preferably, in response to receipt of a network address solicitation message, the or each adjacent network node configures a candidate care-of address, performs duplicate address detection thereon, and sends back to the serving network node a respective valid candidate care-of address. Alternatively, duplicate address detection may be performed by the serving network
20 node for example.

Advantageously, service of said mobile node having been handed over from a first serving network node to a second network node, the method further comprises the steps of:

25 (1) informing said first serving network node of said handover with a fast binding update;

(2) forwarding datagrams from said first serving network node to the new network address of the mobile node or to the second serving network node;

(3) said first serving network node acknowledging said fast binding
30 update with a fast binding acknowledgement;

such that said mobile node can use its new network address as a source address in datagrams sent to the communication network. These steps may be performed so as to comply with the Fast Handover for Mobile IPv6 draft.

35 In one embodiment said identity is a network prefix of each adjacent network

- 11 -

node.

Preferably, said candidate network address is a care-of address (CoA) obtainable by appending the interface ID (e.g. MAC address) of the mobile node to a network prefix.

According to another aspect of the present invention there is provided a network node for use in a packet-switched data communication network, which network node comprises means for storing and executing computer executable instructions for performing either:

- (1) any of the serving network node method steps set out above; or
- (2) any of the adjacent network node method steps set out above; or
- (3) any of the mobile node method steps set out above.

According to another aspect of the present invention there is provided a computer program comprising computer executable instructions for causing a network node to perform the method steps set out. The computer program or any part thereof may be downloaded from one network node to another.

Preferably the computer program is embodied on a record medium, stored in a computer memory, embodied on a read-only memory or carried on an electrical carrier signal.

According to another aspect of the present invention there is provided for use in a method as set out above, a network address (CoA) solicitation message comprising fields for carrying information as set out in any of claims 7 to 9 appended hereto.

According to another aspect of the present invention there is provided for use in a method as set out above, an IPv6 datagram comprising a network address (CoA) solicitation message as set out above.

According to another aspect of the present invention there is provided for use in a method as set out above, a network address (CoA) advertisement message comprising fields for carrying information as set out in any of claims 11 to 15

- 12 -

appended hereto.

According to another aspect of the present invention there is provided for use in a method as set out above, an IPv6 datagram comprising a network address (CoA)
5 solicitation message as set out above.

According to another aspect of the present invention there is provided a method of administering a group of network nodes of a packet-switched communication network, which method comprises the steps of:

10 (1) maintaining an electronic database of an association between a group identity, a serving network node and one or more adjacent network node adjacent the serving network node;

(2) updating the database with exchange of one or more electronic messages between a node storing the database and each network node identified in
15 the database such that datagrams addressed to the group of network nodes may be routed thereto by means of the association. The association may be between a group identity, and one or more network nodes through which data is routed to reach the serving network node and adjacent network node.

20 Advantageously, each network node is associated with a geographical area of signal coverage on the wireless link and the or each adjacent network node is such that, if a mobile node moves from the geographical area of its serving network node, the next serving access router will be one of said adjacent network nodes.

25 Preferably, each network node can communicate directly or indirectly with a crossover node and/or a site crossover node, the crossover node having a link to one or more network nodes and the site crossover node having a link to one or more crossover nodes and/or network nodes, the method further comprising the step of storing a database at each crossover node and site crossover node, such that
30 datagrams addressed to the group of network nodes and received at a crossover router and/or site crossover router may be routed to said group. In this way a hierarchical structure of network nodes is provided. Datagrams addressed to the group are routed via crossover routers and site crossover routers that each maintains a database of members of the group. In some situations the database at a crossover node will not
35 contain all members of a group. This may occur where a member is off link from that

- 13 -

node. The database at the site crossover router may store details of all groups and all members thereof. In this way datagrams can always be routed to the members of the group. A crossover node may be a router that has interfaces with at least two links to different routers or access routers.

5

Advantageously, each database further comprises an indicator of the maximum number of members of said group, the method further comprising the step of, upon receipt of a datagram for said group at a crossover node, comparing said indicator against the number of network nodes in said database, and if said number is less than said indicator, forwarding said datagram to a site crossover node in addition to forwarding said datagram to each network node of the group identified by the database. In this way the reachability of all members of the group is maintained.

10

Preferably, the method further comprises the step of providing the electronic database with an interface identifier for each network node of the group, the interface identifier identifying the interface through which each member of the group may be reached. This interface may not necessarily be the uplink interface of the network node that is the member of the group. The interface may be the uplink interface of an intermediate node (e.g. crossover network node) from which a datagram was received.

15

20

Advantageously, the method further comprises the step of sending a membership query message to determined whether or not each network node is affiliated with said group. The message may be sent to the interface in the database through which the member may be reached.

25

Preferably, the method further comprises the step of periodically sending said membership query message. In this way the database is automatically updated.

30

35

Advantageously, the method further comprises the step of starting a timer when said membership query is sent, said timer having a limit within which the network node sending the membership query expects a reply. The timer may be set to meet the needs of the network administrator. In one embodiment the timer is approximately 60 seconds. By setting the timer for a longer duration, e.g. greater than 60 seconds, overhead on the network is reduced.

- 14 -

Preferably, the method further comprises the step of sending a further membership query message within a predetermined time after expiry of said timer. In one embodiment this predetermined time is substantially zero seconds.

5

In one embodiment, the method further comprises the step of deleting the entry for the or each network node from said database if a reply is not received within the period of said timer. In this way the database is kept current.

10

Advantageously, the method further comprises the step of a network node that is a member of a group of network nodes sending a membership report message to a network node in which its membership is recorded, the membership report message containing the group identifier of the group of which it is a member. The function of this message is to keep the or each database updated.

15

In one embodiment said membership report is sent periodically.

Preferably, the method further comprises the step of resetting a lifetime associated with said network node in said database upon receipt of said membership report message. In this way the database maintains information that is current within the length of the lifetime.

20

Advantageously, the method further comprises the step of sending a membership query message as set out above upon expiry of said lifetime.

25

Preferably, the method further comprises the steps of (1) a network node sending a join message to a network node storing a database in order to join a group of network nodes, the join message comprising the group identifier of the group that the network node wishes to join and the identity of the joining network node, and (2) the network node adding the joining network node to the database.

30

Advantageously, the method further comprises the steps of the serving network node sending an update message to a network node that maintains the database, the update message comprising the group identifier and the identity of the serving network node, and the network node maintaining the database refreshing the

35

- 15 -

group identity and entry for the serving network node. The update message may be sent by the "centre" network node only.

5 Preferably, said messages comprise an ICMP message. In this way only the network node to which the message is addressed processes it. The message is transparent to intermediate network nodes.

Advantageously, said ICMP message comprises a field that specifies whether the message is a query, report, join or update message.

10

Preferably said group of network nodes is a multicast group and said group identifier is the multicast address of the multicast group.

According to another aspect of the present invention there is provided a network node for use in a packet-switched data communication network, which network node comprises means for storing and executing computer executable instructions for performing any of the method steps set out above.

15

According to another aspect of the present invention there is provided a computer program comprising computer executable instructions for causing a network node to perform the method steps as set out above. The computer program or any part thereof may be downloaded from one network node to another.

20

Advantageously, the computer program is embodied on a record medium, stored in a computer memory, embodied on a read-only memory or carried on an electrical carrier signal.

25

According to another aspect of the present invention there is provided in a packet switched data network comprising a plurality of network nodes, a method of discovering the identity of off-link network nodes, which method comprises the steps of:

30

- (1) forming one or more off-link network nodes into a group; and
 - (2) using a multicast protocol to assist distribution the identity of each network node amongst one or more members of the group. The multicast protocol may be used to solicit responses from members of the group in which an identity is
- 35

- 16 -

unicast back to the network node that multicast the solicitation. Alternatively each member of the group may multicast a response. This aspect of the invention may be combined with any of the steps set out above.

5

BRIEF DESCRIPTION OF THE DRAWINGS

In order to provide a more detailed explanation of how the invention may be carried out in practice, a preferred embodiment relating to use on part of an IPv6 network will now be made, by way of example only, to the accompanying drawings, in which:

10

Fig. 1 is a schematic representation of the signalling procedure over time (y-axis) between a mobile node, old access router and new access router as proposed in the network-determined handover of the draft FHMIPv6;

15

Fig. 2 is a schematic representation of a hierarchical topology of a part of a communication network in accordance with the present invention;

Fig. 3 is a schematic representation of the geographical coverage of the access routers of the computer network of Fig. 2;

20

Fig. 4 is a schematic representation of the access routers of Fig. 2 arranged into groups;

Fig. 5 is a table representing a database containing details of multicast groups, each multicast group containing a centre and one or more adjacent access routers;

Fig. 6 is a schematic representation of the address part of an IPv6 header of a multicast packet;

25

Figs. 7 and 7' are a flow diagram of a signalling exchange procedure in accordance with the present invention for fast handover of a mobile node on the computer network of Fig. 2;

Fig. 8 is a block diagram of a site crossover router in accordance with the present invention;

30

Fig. 9 is a flow diagram of the steps performed by the site crossover router of Fig. 8 as part of the method of Figs. 7 and 7';

Fig. 10 is a table representing a database created and stored by the site crossover router of Fig. 8;

Fig. 11 is a flow diagram of the steps performed by the serving access router as part of the method of Figs. 7 and 7';

35

Fig. 12 is a table representing a database created and stored by the serving

- 17 -

access router, which contains prefix details of the access routers adjacent to the serving access router serving the mobile node;

Fig. 13 is a table representing a database created and stored by the serving access router, which contains the candidate care-of address for each adjacent access router together with an indication of the validity or invalidity of each candidate care-of address;

Fig. 14 is a schematic representation of a mobile node in accordance with the present invention;

Fig. 15 is a flow diagram of the steps performed by the mobile node of Fig. 14 as part of the method of Figs. 7 and 7';

Fig. 16 is a schematic representation of an ICMP multicast control message for use in a method according to the present invention;

Fig. 17 is a schematic representation of a care-of address solicitation message for use in a method according to the present invention;

Fig. 18 is a schematic representation of the adjacent access router advertisement carried in the destination options field of an IPv6 header; and

Fig. 19 is a schematic representation of an ICMP Proxy Router Advertisement used in a method in accordance with the present invention; and

Fig. 20 is a schematic view of the options part of the Proxy Router Advertisement of Fig. 19.

DESCRIPTION OF THE PREFERRED EMBODIMENT

Fig. 1 shows the signalling procedure for network-determined handover as proposed in the draft "Fast Handovers for Mobile IPv6" July 2001 (at present available at www.ietf.org/proceedings/02mar/I-D/draft-ietf-mobileip-fast-mipv6-03.txt). In this scenario the serving access router (OldAR) receives an indication that the mobile node needs to handover, such as a layer 2 (link layer) trigger based on the signal-to-noise ratio. The serving access router then configures a new care-of address for the mobile node (MN). The candidate care-of address is then sent to the mobile node (MN) in a Proxy Router Advertisement (PrRtAdv) message 1. At the same time a Handover Initiate (HI) message 2 is sent to the new access router (NewAR) indicating the mobile node's old care-of address as well as the new care-of address. The new access router (NewAR) performs duplicate address detection (DAD) on the new care-of address to determine whether or not it is valid. The new access router

- 18 -

responds with a Handover Acknowledgement (Hack) 3 that indicates whether or not the care-of address is valid. If the care-of address is valid the old access router will prepare to forward packets to the new care-of address. However, if the care-of address is not valid the old access router will prepare to forward packets to the new access router. The mobile node (MN) sends a Fast Binding Update (BU) 4 to the old access router (OldAR) that replies with a Fast Binding Acknowledgement (BACK) 5 via the old access router (OldAR) and new access router (NewAR). The old access router can then begin forwarding packets 6 addressed to the old care-of address to the new access router. From here packets can be delivered 7 to the mobile node.

10

Referring to Fig. 2 part of a communication network is generally identified by reference numeral 10 comprises a number of network nodes, all of which are IPv6 enabled and run "Neighbour Discovery for IPv6" (see RFC 2461). The network nodes have one wireless interface each and one or more wired interfaces. The network nodes may transmit and receive packet data over a packet switched network, in this case the Internet 11 that may not be completely IPv6 enabled. A gateway router 12 serves a local area network (LAN) or a wireless local area network (WLAN) that may cover a town, city or university for example. The gateway router 12 receives all packets from the Internet 11 destined to the network nodes and transmits all packets to the Internet from the network nodes for onward routing. The gateway router 12 distributes data to a relatively large geographical area as mentioned above, which is further divided by a network administrator into a number of sites or sub-domains in this case, site A and site B covering separate geographical areas. Each site is controlled by the gateway router 12 (it would be possible to run the network with more than one gateway router 12). Respective site crossover router controllers 13 and 14 route data traffic to and from each site. Below each site crossover router controller 13 and 14 (in hierarchical terms) there are a number of access routers 15, 16, 17 and 18, 19 respectively, although there may be more or less than two in each site of course. Access routers 15, 16, 17 and 18, 19 are members of only one site respectively. In UMTS (Universal Mobile Telecommunication System) terminology the access routers are base stations. Each access router may comprise one apparatus, for example a base station in an IEEE802.11b (or IEEE802.11a or IEEE802.11g) network. The access routers are the first/last IPv6 addressable routers seen by traffic from or destined to the mobile node 27. A crossover router 26 may be located between the site crossover routers 13, 14 and the access routers.

- 19 -

5 A mobile node 27, such as a mobile telephone, personal digital assistant (PDA), or notebook computer for example, communicates with a correspondent host 28 (another mobile telephone, personal digital assistant (PDA), notebook computer or server for example) over the Internet 11. Data is transmitted and received by the mobile node 27 over a wireless link to base station 20. In transmission, the data is routed from the access router 15 to crossover router 26, to the site crossover router 13, to the gateway 12 onto the Internet 11 and ultimately to the correspondent host 28.

10

The mobile node 27 has a home agent 29 that is a router in the mobile node's home network. The home agent 29 performs mobility management functions for the mobile node 27. In Fig. 2 the mobile node 27 is away from its home network and is visiting a foreign network. The access router 15 enables the mobile node 27 to communicate with the correspondent host 28 over the Internet 11 by performing some mobility management functions whilst the mobile node 27 is resident in the foreign network.

20 Each access router 15, 16, 17 and 18, 19 is responsible for the transmission and reception of data to and from the mobile station 27 using electromagnetic waves, usually radio waves. Referring to Fig. 3 each access router 15, 16, 17, 18, 19 covers (in terms of transmission and reception) a respective geographical area 20, 21, 22 and 23, 24 the exact size and shape of which depends on a wide variety of parameters. As shown in Fig. 3 each geographical area 20, 21, 22 and 23, 24 has been approximated to a hexagon when viewed from above. When a network administrator plans coverage of a town or city for example with base stations it is usual to approximate the coverage area of each base station with the same shape. Thus, for example, the area may be covered by a grid of squares, hexagons or triangles, or any other shape that permits substantially all of the ground area to be covered. An area covered by one base station is usually known as a "cell" (or "basic service set" under the 802.11 standard). Fig. 3 also shows the number of cells in the sites A and B.

35 Referring to Fig. 4 the access routers 15, 16, 17, 18, 19 are shown in All Adjacent Access Router Multicast Groups ("AAARMG") 32, 33 and 34. When setting up or maintaining part of the network, the network administrator examines the

- 20 -

geographical layout and coverage as shown in Fig. 3. For each access router the network administrator creates group of adjacent access routers that are one access router boundary crossing away and in the same site. For example, access routers 15 and 16 are adjacent to each other. It will be apparent that access routers will not necessarily be on the same link or logically adjacent. The network administrator enters this information into a database shown schematically by a table 35 in Fig. 5 so as to associate a multicast group entry 36 with a centre access router entry 37 and a number of adjacent access routers entry 38. In order to distribute this information amongst the access routers 15, 16, 17, 18, 19 details may be extracted from the table 35 and sent to each access router. For example the table 35 may be used to configure access router 16 (AR2) that it is a member of AAARMG2 and AAARMG3, and that it is the centre of AAARMG2. This may be done statically by the network administrator i.e. by manual configuration of each access router. Alternatively, the configuration may be performed dynamically by designing a suitable protocol. Access router 16 then sends a join message to its nearest serving router, in this case crossover router 26 that then unicasts site crossover router 13 to set up the multicast path in the conventional way.

It will be apparent that the shape chosen to approximate the coverage of each base station will determine the maximum number of access routers in any one AAARMG and that each access router is the centre of only one AAARMG. In the example above, use of a hexagonal topology results in a maximum of seven members of any one AAARMG (six adjacent plus one centre). Use of a shape with fewer sides will result in creation and maintenance of fewer AAARMGs. Furthermore access routers at the edge of a site will have fewer members in their AAARMGs.

Each AAARMG has an All Adjacent Access Router Multicast Address ("AAARMA") identified by reference numeral 40 in Fig. 6 that comprises the first 8 bits 41 as all 1s, a 4-bit flags field 42, a 4-bit scope field 43 and a 112-bit group ID field 44. The scope field 43 of the AAARMAs is set to 8 i.e. organization local scope. The group ID field 44 is chosen by the site crossover router 13, 14 that also maintains a list of allocated group IDs to ensure that they are not assigned twice in the same site. The format of the AAARMA in hexadecimal is ff08::group ID. For example if one AAARMG has a group ID of AB17 in hexadecimal, the AAARMA for that AAARMG will be ff08::AB17. The combination of the scope field 43 and the group

- 21 -

ID field 44 ensure that multicast packets are not routed outside the scope of the organization. By appropriate configuration of boundary routers, the organization may be defined to cover site A or site B in Fig. 2 for example, or a subset thereof.

5 Since the user of the mobile node 27 is free to move, there will come a point at which a handover of service between access routers is necessary. For example in Fig. 2 the user of the mobile node 27 moves in the direction of the arrow 30. Eventually service will need to be handed over from access router 15 to access router 16. Furthermore, when the user then moves in direction of arrow 31 in Fig. 3 there
10 will come a point at which handover between access router 15 and access router 16 is necessary. Both of these handovers will require configuration of a respective new care-of address for the mobile node 27.

Referring to Fig. 7 the overall method of handover from one access router to
15 another is generally indicated by reference numeral 50. The method 50 is initiated at step S1 when the access router 15 serving the mobile node 27 detects a flow of packets from or to the mobile node 27 (alternatively the method may be initiated after a mobile node enters the area served by an access router). At step S2 the access router 15 sends a "Care-of Address Solicitation" message addressed to the AAARMA for
20 which the access router 15 is the centre router of the AAARMG. The function of this message is to cause all of the access routers that are adjacent to the access router 15 to configure a respective "candidate" care-of address for the mobile node 27 at step S3. This is done in a stateless way, in which the candidate CoA is formed by appending the interface identifier (ID) of the mobile node 27 to the prefix advertised
25 by an adjacent access router. For example if the prefix of access router 16 is 3ffe:28ac:4525:3::/64 and the MAC address of the mobile node 27 is 5C-66-AB-90-75-B1, the candidate CoA for the mobile node 27 in the area covered by access router 16 is 3ffe:28ac:4525:3:5C:66:AB:90:75:B1:: Further details of stateless CoA configuration can be found in RFC 2462.

30

At step S4 each adjacent access router performs duplicate address detection (DAD) on the candidate care-of address to determine whether or not it is unique on its link(s). For each candidate CoA, the DAD test involves sending neighbour solicitation messages with the target address as the candidate CoA to access routers
35 on-link. The on-link access routers receiving the neighbour solicitation message

- 22 -

check whether or not the candidate CoA is in use on the same link and respond accordingly in a neighbour advertisement message (further details of the DAD test can be found in RFC 2462 for example). At step S5 each adjacent access router notes whether or not the candidate care-of address is valid. If it is valid, the adjacent access router sends the candidate care-of address to the serving access router in a “CoA Advertisement” message at step S6. Each CoA Advertisement contains the IP address, prefix, the valid candidate care-of address for the mobile node 27, and MAC address of the wireless interface of the adjacent access router i.e. the downlink interface.

10

If at step S5 the candidate care-of address does not pass the DAD test, the adjacent access router does not send a CoA Advertisement at step S7. The adjacent access router may configure an alternative candidate care-of address for the mobile node or, if not possible, send a message to the serving access router 15 that the determination of a valid care-of address failed. In this case, if the mobile node 27 moves to this access router, handover may be accomplished in accordance with the ordinary procedure specified in MIPv6, details of which can be found in “Mobility Support in IPv6” by Johnson *et al* (mentioned above), for example.

15

20

At step S8 the access router 15 then sends each candidate CoA that it has received to the mobile node 27 in the options field of a Proxy Router Advertisement (PrRtAdv) message that will be described in greater detail below. The mobile node 27 stores the candidate CoAs in a cache at step S9.

25

It will be noted that all of the above steps have been performed before any fast handover steps have been initiated. Indeed the user of the mobile node 27 may be stationary in the area covered by access router 15 whilst the above steps are performed. The aim of these steps is to provide the mobile node with a list of candidate CoAs for all of the possible (or as many as possible) access routers that might serve the mobile node 27 next. Thus, whichever direction the user chooses to move subsequently with the mobile node 27, the mobile node 27 should have the new CoA that it needs to be served by the new access router when the need for fast handover arises. In this manner the latency of the handover can be reduced, improving the service provided to the user.

30

35

- 23 -

At step S10, the mobile node 27 awaits reception of a PrRtAdv from a new access router that serves to trigger fast handover. When such a PrRtAdv is received the mobile node determines at step S11 which CoA of its cached candidate CoAs is correct for the new access router. This is done by performing a longest prefix match
5 algorithm on the candidate CoAs using the prefix advertised by the new access router. If one prefix of the candidate CoAs matches the advertised prefix, the mobile node 27 sends a fast binding update at step S12 to the old access router 15. The old access router responds with a fast binding acknowledgement at step S13. Alternatively if there is no match between the advertised prefix and any of the
10 candidate CoAs, the method diverts to standard handover for MIPv6, details of which can be found in "Mobility Support in IPv6" by Johnson *et al* (mentioned above), for example.

Greater detail of the structure, function and advantages of the methods,
15 network nodes and messages used in the above method will be described below.

Referring to Fig. 8 the site crossover router 13 comprises a case 51 having network interface ports 52 and 53 to which respective cables 54 and 55 provide a physical link to respective IP sub-networks. Two network interface cards 56 and 57
20 are connected to their respective network interface ports 52 and 53. A hardware packet switch 58 connects the network interface cards 56 and a central processing unit (CPU) 59 can communicate with a routing table 60 and router management tables 61.

Each network interface card 56, 57 comprises a link layer protocol controller
25 62 that has access to an interface management table 63 and a hardware address table 64 (e.g. Address Resolution Protocol cache). In communication with the link protocol controller 62 is a network protocol-forwarding engine 65 having access to a forwarding table 66 (route cache), and an interface queue manager 67. Both the
30 network protocol forwarding engine 65 and interface queue manager 67 have an interface to and from the packet switch 58 respectively.

In use, frames are received by the link layer protocol controller 52 that handles the link layer protocol (e.g. HDLC, Ethernet) used over the physical link.
35 Frame integrity is checked and valid frames are converted into packets by removing

- 24 -

the link layer header and, if necessary, the packets are queued in a queue 68. Storage capacity is often in the form of a ring of memory buffers. One packet at a time is removed from the queue 68 by the network protocol-forwarding engine 65 and the forwarding table 56 determines whether or not the packet requires detailed examination by the CPU 59. Via the CPU 59 the next router (i.e. crossover or access) to which the packet should be sent is looked up in the routing table 61. Once the destination IP address is found the CPU (IPv6 module) searches the ARP IPv6 neighbouring cache for a Media Access Control (MAC) address for the destination. The CPU 59 now knows where to send the packet and the new link layer header to use. The link layer address is added and the packet is linked into the list of frames to be sent on from the appropriate network interface card. The packet is then forwarded to the packet switch 58 and onto the network interface card where the packet joins a queue 69 to be processed by the interface queue manager 67. From here the packet joins one of a number of link output queues 70 until the link layer protocol controller 62 can process it. The link layer protocol controller 62 encapsulates the packet in a link layer header that includes the Media Access Control (MAC) address of the next router to which the packet is to be sent. The MAC address is obtained from the hardware address table 54. The packet is then placed on the physical channel by the link layer protocol controller 32 and sent to the next router.

20

Various types of router are available and the present invention is not limited to that described above. Further examples are available from Cisco Systems, Inc. (www.cisco.com) for example.

25

In addition the CPU 59 of the site crossover router 13 has access to a memory 71. The memory 71 stores the computer executable instructions that must be performed and the database that must be created and maintained by the site crossover router 13 in performing the handover method described above. The access routers 15, 16, 17, 18 and 19 are all similar in structure to that described above.

30

Referring to Fig. 9 the computer executable instructions stored by the memory 71 are shown in the form of a flowchart generally identified by reference numeral 80. The site crossover router 13 assumes the function of maintaining a database of the various AAARMGs in its site. The database is shown in Fig. 10 and is generally identified by reference numeral 81. The database (or routing table) 81 comprises a

35

- 25 -

“Destination Address” column 82 that lists each multicast address for the AAARMGs presently used in the site. Associated with each destination address 82 is a “Group Centre” column 83 that contains the unicast address of the access router that is the centre of that AAARMG_i. The centre access router is a member of the AAARMG for which it is centre. A “Multicast Member” column 84 contains the unicast address of the uplink interface of each member of the AAARMG_i (i.e. the IP address of the interface on the “fixed” part of the network), associated with which is a respective lifetime 85, flags 86 and interface 87. The interface 87 is the interface of the router from which the Membership Report was received for that Multicast Member. This interface may or may not be the IP address of the access router from which the message originated (i.e. the Multicast Member), depending on the topology of the network.

Referring again to Fig. 9 the computer executable instructions 80 perform the following steps when run on the site crossover router 13, 14. At step S1 the site crossover router 13 awaits receipt of a “Multicast Entries Update” message from a centre access router of each AAARMG that will be described in greater detail below. The Multicast Entries Update message contains the multicast address of the AAARMG of which the sending access router is centre. This multicast address is used at step S2 to search for an entry in the destination address column 82 of the database 81. If no entry is found the site crossover router creates an entry at step S3 and then proceeds to step S7. If an entry is found the routine proceeds straight to step S7 where the lifetime of that entry is reset, and countdown commences. The lifetime is 30 minutes, although it can be set to any value by the network administrator.

Simultaneously with step S1, the routine awaits receipt at step S4 of a “Multicast Group Join” message from adjacent access routers in each AAARMG. The function of this message is to cause the site crossover router 13, 14 to create an entry in the database 81 for the adjacent access router in the appropriate AAARMG. One multicast group join message is required for each AAARMG that the adjacent access router wishes to join. At step S5 the site crossover router extracts the AAARMA from the multicast group join header as will be explained in greater detail below. The site crossover router adds the details of the access router from which the multicast group join message was received to the database 81 at step S6. The routine then proceeds to step S7 and the lifetime of the new entry is reset.

- 26 -

At step S8 the routine examines the lifetime field for each of the entry in the database 81 to determine whether or not it is within a predetermined time of expiry. The predetermined time is between 0 and 30 seconds. If the lifetime is within the predetermined time or has expired, the site crossover router 13, 14 sends at step S9 a
5 "Query" message to each member of the AAARMG. The function of the query message is to trigger a "Membership Report" message to be sent by each access router that is a member of the AAARMG. At step S10 the routine returns to step S7 if all access routers in the AAARMG reply to the query message. If any particular
10 access router does not respond to the query message details of that access router are deleted from the database 81 and the routine returns to the start at which receipt of a multicast entries update or group join message is awaited.

It will be noted that the site crossover router 13, 14 performs this routine for
15 each AAARMG in the database 81. Thus, once an AAARMG has been set up steps S7 to S10 run in loop until either a lifetime of a member expires or if a multicast update message is received by the site crossover router. Steps S4 to S6 run in the background to permit new AAARMGs to be created as soon as a multicast join message is received.

20

Referring to Fig. 11 a flowchart representation of a set of computer executable instructions stored and executed by access routers 15, 16, 17, 18 and 19 is generally identified by reference numeral 90. As mentioned above the access routers 15, 16, 17, 18, and 19 are each similar in structure to the site crossover router 13, 14
25 shown in Fig. 8 and the accompanying description to which reference is made. The routine 90 is initiated at step S1 by the mobile node commencing communication via the access router 15 for example (or after entering the area served by a new access router). This may be either by data being sent either from or to the mobile node 27. At step S2 the access router 15 prepares and transmits the CoA Solicitation message.
30 The CoA solicitation message is addressed to the AAARMG for which the access router presently serving the mobile node 27 is centre. It will be appreciated that addressing this message to any other multicast groups of which the access router 15 is a member will result in CoA advertisement replies being received from access routers that are not all adjacent to the serving access router 15. Thus it is important that the
35 CoA solicitation message is sent only to the AAARMA for which it is the centre

- 27 -

access router.

As explained above the function of the CoA solicitation message is to cause the access routers that are adjacent the access router 15 (and therefore in the same AAARMG) to reply with a respective CoA advertisement message containing a valid candidate CoA at each adjacent access router that the mobile node 27 could use if it moves to one of those adjacent access routers. At step S3 the access router 15 starts a timer of 60s duration in which it expects to receive CoA advertisement messages from all of the adjacent access routers. The routine waits at step S4 for these replies (received via the site crossover router). Part of the routine includes information of the topology used by the network administrator to design network coverage. From this information, the access router 15 can determine how many CoA advertisement messages it expects to receive. For example, if the coverage has been calculated using a square cell network topology then the access router knows that it must receive four CoA advertisement messages. Alternatively, if the network topology is hexagonal, the access router 15 must receive six CoA advertisement messages.

Once all of the CoA advertisement messages have been received from the adjacent access routers, the access router (the centre one) 15 compiles a table of candidate CoAs at step S5 that is stored in memory. Alternatively this may be done after expiry of a timer or if a certain number of failed attempts have been made to solicit a CoA advertisement message from one or more of the adjacent access routers. This table is generally identified by reference numeral 100 in Fig. 12 and comprises a column of adjacent access router 101 against a captured prefix column 102 and adjacent access router's ID column 103.

A table of candidate CoAs generally identified by reference numeral 110 is shown in Fig. 13 that comprises a column 111 containing the identity of the serving access router and the mobile node ID (MAC address); a column 112 containing details of each access router that is adjacent to the serving access router; and a column 113 of the candidate CoAs that have been configured by the serving access router as described above. As DAD has been performed by each adjacent access router, the serving access router 15 knows that each candidate CoA is valid on the link(s) of its corresponding adjacent access router. At step S6 the access router 15 sends the candidate CoAs in a Proxy Router Advertisement (PrRtAdv) at step S8.

- 28 -

Following this procedure it is possible that the candidate CoAs for all of the adjacent access routers will not necessarily be made available to the mobile node 27. If the mobile node 27 moves to an adjacent access router for which the mobile node does not have a care-of address, handover may be performed according to standard Mobile IPv6 procedures. However, if the mobile node 27 moves to an adjacent access router for which it has a care-of address the mobile node 27 can begin using it immediately.

The method described above permits the serving access router 15 to configure candidate CoAs for the mobile node 27 before any steps for handover have been initiated. Indeed, whether the mobile node 27 is moving or not is irrelevant and it may well be stationary in the area covered by access router 15 whilst this procedure is performed. The aim of the procedure is to provide the mobile node 27 with a list of all possible CoAs that it may need next, depending on the area to which it moves. In this way, latency of the handover process can be reduced, enhancing the quality of service for the user. Furthermore, this provides a solution to the proposed method of fast handover for IPv6 in which no mechanism for ascertaining the new CoA for the mobile node was described. Also the need for the proposed HI (Handover Initiate) and HAck (Handover Acknowledgement) messages is mitigated.

Referring to Fig. 14 part of the mobile node 27 is shown in greater detail. It comprises a memory 120, a microprocessor 121, amplifiers 122, a display 123 (and an input means not shown e.g. keyboard, touch-sensitive screen), digital-signal processing (DSP) 124, radio control 125 and an antenna 126. The aforementioned parts are in electronic communication with one another. In use, data may be sent to and received from the "fixed" part of the network (access routers 15, 16, 17, 18 and 19) by means of the antenna 126. Data to be sent from the an application running on the mobile node 27 is segmented and placed in IPv6 packets under control of the DSP 124 and microprocessor 121, framed and sent over the wireless link with a MAC protocol (e.g. IEEE 802.11b, Hiperlan 2, Bluetooth) by the radio control 125. Similarly data received from the fixed part of the network over the wireless link is passed to radio control 125 where it de-framed, the IPv6 headers removed and the data ordered and passed up to the application level where it may be stored in the memory 120 and/or viewed on the display 123.

- 29 -

In addition to the functionality described above the memory 120 stores and executes computer executable instructions shown in flowchart form in Fig. 15 and generally identified by reference numeral 130. At step S1 the mobile node 27 commences communication via access router 15 i.e. data is sent to or received from the access router 15. After a short period of time the mobile node receives at step S2 a Proxy Router Advertisement (PrRtAdv) message from the serving access router that is presently serving it i.e. access router 15. In many networks the period between Proxy Router Advertisements is 1 second. Accordingly the mobile node 27 can expect to receive some or all of the new candidate care-of addresses within 1 second of commencing communication at best. The PrRtAdv contains candidate CoAs for the mobile node 27 and the link-layer addresses of the adjacent access routers on which the candidate CoAs are valid. The PrRtAdv will be described in greater detail below. At step S3 the mobile node 27 checks whether or not it already has a cache of candidate CoAs in memory 120. If not, a cache is created at step S4 and the routine proceeds to step S5 (this cache is separate from the cache of CoAs that are presently in use by the mobile node – this mitigates the chance of mis-management and error). Otherwise the routine proceeds straight to step S5 where the candidate CoAs and link-layer addresses are added to the cache. Instead of only one PrRtAdv containing all available candidate CoAs being sent to the mobile node 27, PrRtAdvs could be created and sent as and when one or more CoA advertisements are received from the adjacent access routers. In this case, steps S2 to S5 are repeated as and when these PrRtAdvs are received.

At step S6 the mobile node 27 awaits receipt of a PrRtAdv from another access router i.e. one that is not presently serving the mobile node. Such a PrRtAdv is likely to be received when the mobile node 27 is moved further away from the base station 20 where signal strength and therefore quality of service is likely to be lower. In order to increase the quality of service to the user, handover is necessary between the serving access router and the new access router. The receipt of the new PrRtAdv serves to trigger step S7 of the routine where the mobile node 27 extracts the new access router IP address i.e. the IP address of the wireless (downlink) interface. From this it is possible for the mobile node 27 to extract the network prefix of the new access router. The mobile node 27 then performs a longest prefix match algorithm on the cache of candidate CoAs.

- 30 -

Although the source IP address of the PrRtAdv from the new access router will contain the IP address of the downlink i.e. wireless network interface, the network prefix of each IP address will be the same. Thus it is possible for the mobile
5 node to use the source IP address of the new PrRtAdv to perform a longest prefix match on its list of candidate CoAs.

Whichever of the candidate CoAs most closely matches the source IP address of the PrRtAdv is selected by the mobile node 27 as its new CoA at step S8 and the
10 network proceeds at step S9 with the remaining signalling procedure for fast handover as set out in the draft. In particular, the mobile node 27 sends a fast binding update (F-BU) to the old access router 15 that replies with a fast binding acknowledgement (F-Back). The old access router then commences forwarding packets for the mobile node 27 to the new access router. At step S11 the mobile node
15 27 deletes the stored candidate CoAs from the cache. As the mobile node is now served by a new access router the routine 130 will be repeated at the new access router to prepare the mobile node for another handover should it be necessary.

If no match is found by the longest prefix match at step S8, the routine diverts
20 to normal handover for MIPv6 at step S10.

Having described the operations performed by each of the network nodes a more detailed description of the messages used in the signalling procedure is provided below.

25

Referring to Fig. 16 a new ICMPv6 (Internet Control Message Protocol) message is generally identified by reference numeral 140. The ICMP message 140 is used to transmit the following messages mentioned above:

- 30
- (1) Multicast Membership Query message;
 - (2) Multicast Membership Report message;
 - (3) Multicast Group Join message; and
 - (4) Multicast Entries Update message.

35 The ICMP message 140 comprises a Type field 141, a Code field 142, a

- 31 -

Checksum field 143, a Max Response field 144, a Lifetime field 145 and an AAARMA field 146 of 128 bits. In use the ICMP message 140 is encapsulated in an IPv6 packet with a source IP address of the interface from which the message originated. The destination IP address of the packet is, in the case of messages (2), (3) and (4) above, the site crossover router 13, 14; in the case of message (1) above the destination address can be the AAARMA or a unicast address of a particular access router.

The various fields of the ICMP message are used as follows:

10

Type: This is to be assigned by IANA (Internet Assigned Numbers Authority) see www.iana.org

15

Code: This field defines whether the ICMP message 140 is a Query, Report, Update or Join message; this code may also be assigned by IANA.

20

Max Response Time: This field is used in the Query messages to set a maximum response time in seconds within which the access router must respond to the Query by the site crossover router. This time may be set arbitrarily and may be of the order of approximately 3 seconds. As opposed to RFC 2236 (Internet Group Management Protocol, Version 2) in which it is suggested that this time should be expressed in units of $1/10^{\text{th}}$ second in order to solicit a quick response, it is not necessary in this case as the access routers are fixed in position. By making the maximum response time longer, traffic associated with administration of the multicast groups is reduced.

25

Lifetime: This field is used in the Report, Join and Update messages to inform the site crossover router of the duration of an access router's association with a multicast group. Typically, the lifetime is of the order of 1800 seconds (30 minutes).

30

Checksum: The checksum is the 16 bit one's complement of the one's complement sum of the whole ICMP message 140 as in RFC 2236. For calculating the checksum, the checksum field is set to zero. When transmitting the ICMP message the computed checksum is inserted into the checksum field. When receiving an ICMP message the checksum must be verified before the packet is processed.

35

- 32 -

Multicast Address: In the Report message this field holds the IP multicast address of the group being reported. For example, an access router may be a member of seven multicast groups in a hexagonal topology (six as an adjacent access router and one as a centre access router). Accordingly it will need to send a Membership Report message for each of the seven multicast groups of which it is a member. In a Query message sent from the site crossover router, this field is set to zero if the message is directed at only one access router and set to the AAARMA if the query is for the whole AAARMG. A group Query solicits a response from an entire AAARMG.

The other two messages that require description are:

- (5) CoA solicitation message; and
- (6) CoA advertisement message.

Referring to Fig. 17 an ICMPv6 CoA solicitation message generally identified by reference numeral 150 comprises a Type field 151, a Code field 152, a Checksum field 153, an identifier field 154, a stateful address configuration flag field 155, a buffer flag field 156, a flag field 157 identifying whether or not the mobile node link-layer address is present in the Options field, a flag field 158 identifying whether or not the mobile node CoA is present in the Options field, a reserved field 159 for possible future extensions of the protocol, and an Options field 160 that contains the mobile node's IPv6 address (that includes the mobile node's ID and current CoA of the mobile node that is communicating via the access router sending the CoA solicitation message). This enables the adjacent access router to record the MAC ID of the mobile node that will help the adjacent access router to identify the mobile node after handover.

In use the CoA solicitation message 150 is placed in an IPv6 packet and sent to the AAARMG of which the serving access router is the centre, as explained above. The hop limit field of the IPv6 header is set to 255 (by convention the hop limit is set to this value; however, it might be set to a lower value depending on the number of access routers in the site, which would further reduce the chance of the CoA solicitation message leaving the site) If no reply is received within a predetermined time (for example 3 seconds, 9 seconds etc.) the CoA solicitation message should be re-sent up to four times using a short re-transmission timer (for example of duration 3

- 33 -

seconds, 9 seconds etc.).

Type: This is to be assigned by IANA (Internet Assigned Numbers Authority) see www.iana.org

5

Code: This may be set to zero, as there is only one type of CoA solicitation message.

Identifier: This field is set by the sender so that it can match replies.

10 S: This field is the stateful address configuration flag; when set, this flag requests the recipient adjacent access router to configure a candidate CoA for the mobile node in a stateful way. The flag is not sent in the procedure described above, as stateless address autoconfiguration is used.

15 U: This field contains a buffer flag; when set, this flag instructs the recipient adjacent access router to buffer any packets intended for the mobile node identified by the link-layer address and CoA in the Options field. This helps to reduce packet loss during and shortly after handover.

20 ML: When this flag is set, the link-layer address of the mobile node is present in the Options field of the message.

MC: When this flag is set, the CoA that the mobile node is presently using is present in the Options field of the message.

25

Reserved: This field is set to zero and is ignored by the recipient adjacent access router.

30 Options: As explained above this field contains the IPv6 address of the mobile node and the ID of the mobile node. This enables the access router receiving the solicitation to configure a new candidate CoA by appending the ID to the prefix of its subnet. Thereafter it can perform DAD in the candidate CoA.

35 CoA Solicitation messages 150 are sent out from the centre (or serving) access router and will propagate to the nearest crossover router (via none or more

- 34 -

intermediate routers). The crossover router checks its database (similar to the database 81) for an entry for the group based on the multicast address of the IP packet containing the CoA Solicitation message 150. If the entry for that group is complete, the IP packet containing the CoA Solicitation message is duplicated and unicast to
5 each member of the group based on the unicast address (or interface from which a multicast update was received) of each member stored in the database. If there is no entry at the crossover router the IP packet is forwarded to the site crossover router, where a similar procedure is performed.

10 Referring to Fig. 18 a CoA Advertisement message generally identified by reference numeral 170 comprises a Next Header field 171; a Header Extension Length field 172; a Type field 173; an Options Data Length field 174; a Site ID field 175; a Domain ID field 176; a Prefix flag field 177; a Link-Layer flag field 178; a Lifetime field 179; a IP address field 180; a Prefix field 181; a Link-Layer address
15 field 182; and a Candidate CoA field 183. The entire CoA Advertisement message is carried as a Destination Options field (see RFC 2460) in addition to the standard IPv6 header. Although IPv6 headers do not contain an explicit Options field, it is possible to point to this Option header from within the "next header" field of the IPv6 datagram. Thus when decapsulating the IPv6 packet, the serving access router will be
20 informed by the next header field that there is an Options header (containing the CoA Advertisement message) after the IPv6 header.

The IPv6 datagram containing the CoA Advertisement message has a source address of the uplink interface of the access router sending the CoA Advertisement.
25 The destination IP address of the packet is the AAARMA of the AAARMG that the sending access router is the centre of (of course, it would be possible to send unicast messages to the group; however, this would generate additional overhead). The CoA Advertisement message will only be processed when the IPv6 packet reaches the router or routers that are the intended recipients of the Advertisement. The CoA
30 Advertisement is transparent to intermediate routers.

CoA Advertisement messages can be both solicited and unsolicited i.e. they are sent in response to a CoA solicitation message 150 as described above and they are sent periodically in any event to ensure that details of the IP addresses, network
35 prefixes and MAC addresses of adjacent access routers at the serving access router

- 35 -

are current. This is important if any of the access routers crash or need to be re-numbered for example. A suggested time interval for sending CoA solicitation messages is 10 minutes, although it may be desirable to increase this in congested networks or decrease it when network traffic is lighter.

5

Details of the fields of the CoA Advertisement are as follows:

Next Header: This field identifies the type of header immediately following the destination option header, and uses the same value as the IPv4 protocol in this field.
10 The values are specified in RFC 2460 (Internet Protocol Version 6 Specification).

Hdr Ext Len: This field is an 8 bit unsigned integer that specifies the length of the Options header in 8 octet units as specified in RFC 2460.

15 Type: This field specifies that the Destination Option header is a CoA Advertisement message. If the access router does not recognise the value of the field the message will be discarded. Accordingly routers must be updated to ensure that they are aware of the new message type.

20 Opt Data Len: This field specifies the length of the Destination Options header in octets (see RFC 2460 for further details).

Site ID: This field contains an 8 bit unassigned integer that indicates the ID of the site in which the access router that originated the CoA Advertisement is located
25 (see below).

Domain ID: This field contains a domain ID of the access router that sent the CoA Advertisement. Routers and access routers may be attributed to a site and a domain, each with an identity (Site ID and Domain ID). A domain covers one or more sites.
30 By specifying the Domain ID in the CoA Advertisement the receiver can determine whether or not the sender of the option is in the same Domain. If the Domain ID of the sender and receiver are different the receiving access router knows that the sender is outside the Domain and will discard the advertisement. Thus, CoA Advertisements can be confined to one Domain only. This also inhibits bogus advertisements from
35 hackers outside the domain from being passed to higher layers of access routers in

- 36 -

another Domain.

P Flag: When this flag is set, the serving access router knows that the prefix of the adjacent access router wireless (i.e. downlink) interface is present in the Destination Option header.

L Flag: When this flag is set, the serving access router knows that the link-layer address (MAC) is present in the Destination Option header.

Lifetime: This value specifies the time in seconds for which the details in the CoA Advertisement are valid at the serving access router. This value is arbitrary, but should be at least approximately the period between consecutive CoA advertisements. This may be useful if the serving access router does not solicit an advertisement from the adjacent access router when compiling candidate CoAs for a mobile node. In this case the serving access router can simply use the prefix advertised to it by an adjacent access router to compile a candidate CoA for the mobile node, providing the details are still current based on the value of the lifetime. This disadvantage of this is that DAD will have to be deferred until after handover. However, given the very low probability of the candidate CoA failing DAD, this is a viable alternative.

IP address of the Wireless Interface: This field contains the IP address of the wireless interface (i.e. downlink) of the adjacent access router that sends the CoA Advertisement.

Prefix of Wireless Interface: This may be used by the serving access router to configure a candidate CoA for the mobile node, if necessary.

Link-Layer Address of Wireless Interface: This field contains the MAC address of the wireless (i.e. downlink) interface of the adjacent access router sending the Advertisement. This field is necessary to avoid performing neighbour discovery on the new wireless link before attaching the mobile node to the new access router.

Candidate CoA: As explained above, this field contains a valid care-of address that may be used by the mobile node if it moves to the particular access router

- 37 -

sending the CoA Advertisement.

Referring to Fig. 19 a modified ICMP Proxy Router Advertisement generally identified by reference numeral 190 comprises a Type field 201, a Code field 202, a
5 Checksum field 203, an Identifier field 204, a Reserved field 205 and an Options field 206.

The IP datagram in which the PrRtAdv is sent has as its source address the mobility interface (i.e. physical wireless interface) of the serving access router
10 instead of the link-local address (i.e. FE80::/64 where /64 is the interface identifier derived from the MAC address of uplink interface of the serving access router) as in the draft. The advantage of this is that, in the selection of a candidate care-of address by the mobile node when it is served by a new access router, the mobile node only
15 needs to lookup the source address of the IP datagram containing the PrRtAdv, reducing processing time. This is then used in the longest prefix match process as described above. The destination IP address is the care-of address that the mobile node is presently using on the link.

Details of the PrRtAdv fields are as follows:

20

Type: This will be specified by IANA.

Code: This field is set to 0 when the PrRtAdv carries a CoA Advertisement for the mobile node. Thus the mobile node knows that the PrRtAdv contains candidate CoA
25 information that it must store. If there is no CoA Advertisement present the code is set to 1 and the mobile node knows that the PrRtAdv is not of importance in this regard.

Checksum: This checksum is computed as in RFC 2463.

30

Identifier: This field is set to 0 as the PrRtAdv is unsolicited.

Reserved: This field is set to 0 by the access router and is ignored by the mobile
node.

35

- 38 -

Options: A candidate CoA and link-layer address that have been configured by the access router are carried in this field.

Referring to Fig. 20 the Options field of the PrRtAdv generally identified by reference numeral 200 comprises a Type field 201, a Length field 202, a reserved field 203, a Valid Lifetime field 204, a field 205 for the candidate CoA and a field 206 for the link-layer address of the adjacent access router mobility interface. Details of these fields are as follows:

10 Type: To be defined by IANA.

Length: This field is an 8 bit unsigned integer that indicates the length of the Options field in units of 8 octets.

15 Reserved: This 16 bit field is reserved for future extension of the CoA option.

Valid Lifetime: This field indicates to the mobile node how long the advertised candidate CoA is valid for. Typically the candidate CoA should be valid for approximately 1800 seconds (30 minutes). This value is effectively arbitrary, but should be at minimum a few multiples of the period between consecutive router advertisements.

Candidate CoA: This 128-bit field contains the candidate CoA for an adjacent access router.

25 Link-layer address: This field contains the link-layer address of the adjacent access router mobility interface

One PrRtAdv is sent to the mobile node 27 that contains the candidate CoAs for all (or all those that have been determined) of the access routers adjacent to the access router serving the mobile node 27. The PrRtAdv 190 contains a number of Options fields 206, one for each candidate CoA.

35 The database shown in Fig. 10 may be stored solely at the site crossover router in each site, with all messages being routed and sorted thereby. However, this

- 39 -

places a large processing requirement on the site crossover router. An alternative would be for each crossover router and site crossover router to store similar databases of those network nodes that are members of a group. Crossover routers will only be able to store details of members that are reachable through one of its downlinks.

5 Accordingly, these routers may perform a check when receiving a multicast membership report message that the maximum possible number of members is stored in light of the topology used to cover the wireless links. For example, if a hexagonal approximation is used, a crossover router knows that it should have seven members in one group (provided that it is not on the edge of a site for an example). If it has any

10 less than this it should forward the multicast membership report to a crossover router at a higher level or to the site crossover router that will be able to update its database. Thus, handling of the database records is primarily performed by network nodes lower in the hierarchy.

15 Instead of serving access routers sending CoA Solicitation messages when it is desired to compile a list of candidate CoAs for a mobile node, the method may rely upon the periodic and frequent sending CoA Advertisement messages by all access routers in the network. In this case, the serving access router would have the responsibility of configuring the candidate CoAs based on the prefixes advertised by

20 adjacent access routers. The disadvantage with this is that DAD can only be performed with access routers on-link with the serving access router. Accordingly, some DAD checks may have to be performed after handover in this scenario resulting in greater overhead. However, as explained above, given the low probability of DAD failing for a given candidate CoA, this method may present an alternative.

25 If a mobile node remains resident in a particular cell served by an access router for a given amount of time, e.g. 30 minutes, 60 minutes etc., the method may be performed periodically to ensure that the candidate CoAs held by the mobile node remain current.

30 Whilst the discovery protocol described above has been described in connection with FHMIPv6 network determined handover, it can be used in any other IP based network determined handover.

35 The terms "handover" and "handoff" are used interchangeably throughout this

- 40 -

document.

Although the embodiments of the invention described with reference to the drawings comprise computer apparatus and methods performed in computer apparatus, the invention also extends to computer programs, particularly computer programs on or in a carrier, adapted for putting the invention into practice. The program may be in the form of source code, object code, a code intermediate source and object code such as in partially compiled form, or in any other form suitable for use in the implementation of the methods according to the invention. The carrier may be any entity or device capable of carrying the program.

For example, the carrier may comprise a storage medium, such as a ROM, for example a CD ROM or a semiconductor ROM, or a magnetic recording medium, for example a floppy disc or hard disk. Further, the carrier may be a transmissible carrier such as an electrical or optical signal that may be conveyed via electrical or optical cable or by radio or other means.

When the program is embodied in a signal that may be conveyed directly by a cable or other device or means, the carrier may be constituted by such cable or other device or means.

Alternatively, the carrier may be an integrated circuit in which the program is embedded, the integrated circuit being adapted for performing, or for use in the performance of, the relevant methods.

25

- 41 -

CLAIMS

1. In a packet-switched data communication network comprising a plurality of network nodes and mobile nodes between which data may be exchanged by means of a wireless link, mobile nodes transmitting and receiving data to and from the communication network via respective serving network nodes, a method of preparing a mobile node for handover of service from one serving network node to another, which method comprises the steps of:
- (1) obtaining an identity of one or more adjacent network node adjacent the mobile node's serving network node;
- (2) using each identity to configure a candidate network address for the mobile node; such that
- (3) if and when the mobile node is served by one of said one or more adjacent network nodes, the candidate network address configured from the identity of that adjacent network node can be assigned to the mobile node.
2. A method as claimed in claim 1, wherein each network node is associated with a geographical area of signal coverage on the wireless link and the or each adjacent network node for which said identity is obtained is such that, if said mobile node moves from the geographical area of its serving network node, the next serving access router will be one of said adjacent network nodes.
3. A method as claimed in claim 1 or 2, wherein steps (1) and (2) are initiated in response to completion of a handover of the mobile node from one network node to another, or in response to the initiation of packet flow through a serving network node to or from the mobile node, such that at least one candidate network address is available prior to any subsequent handover.
4. A method as claimed in claim 1, 2 or 3, wherein said serving network node and the or each adjacent network node comprise a multicast group having a multicast address, the method further comprising the step of said serving network node communicating by means of said multicast address with the or each adjacent network node to obtain said identity.
5. A method as claimed in claim 4, wherein step (1) of the method comprises

- 42 -

said serving network node sending a network address (CoA) solicitation message to said multicast address to solicit a response from each adjacent network node containing the respective identity or candidate network address.

- 5 6. A method as claimed in claim 5, wherein each network node can be both a serving network node and an adjacent network node simultaneously, said method further comprising the step of each network node sending said network address solicitation message to the multicast group of which it is a centre serving access node.

10

7. A method as claimed in claim 5 or 6, further comprising the steps of providing the data link-layer identity of the mobile node and/or present network layer identity of the mobile node in said network address (CoA) solicitation message to help the adjacent network node to identify the mobile node after a handover.

15

8. A method as claimed in claim 5, 6 or 7, further comprising the steps of providing said network address (CoA) solicitation message with a first flag for instructing each adjacent access router to configure said candidate network address either in a stateful way or in a stateless way.

20

9. A method as claimed in any of claims 5 to 8, further comprising the steps of providing said network address (CoA) solicitation message with a second flag for instructing each adjacent network node whether or not to buffer packets received for said mobile node before completion of a handover.

25

10. A method as claimed in any of claims 5 to 9, wherein said network address (CoA) solicitation message is an Internet Control Message Protocol (ICMP) message carried in an IP packet.

30

11. A method as claimed in any of claims 5 to 10, further comprising on receiving said network address (CoA) solicitation message the step of each adjacent network node of said group responding to said serving network node with a network address (CoA) advertisement message in which the identity of the adjacent network node or candidate network address for the mobile node is advertised to the serving network node.

35

- 43 -

12. A method as claimed in claim 11, further comprising the step of providing said network address (CoA) advertisement message with a site identifier and/or domain identifier to identify the site and/or domain in which the adjacent network node is located.
13. A method as claimed in claim 11 or 12, further comprising the step of providing said network address (CoA) advertisement message with the identity of the adjacent network node sending the message.
14. A method as claimed in claim 11, 12 or 13, further comprising the step of providing said network address (CoA) advertisement message with the network address and/or network prefix and/or link-layer address of a wireless interface of the adjacent network node sending the message.
15. A method as claimed in any of claims 11 to 14, further comprising the step of providing said network address (CoA) advertisement with a lifetime value useable by the serving network node to determine the time for which the information in the network address (CoA) advertisement message is valid.
16. A method as claimed in any of claims 11 to 15, further comprising the steps of sending said network address (CoA) advertisement as an option to an IPv6 datagram and addressing said IPv6 datagram to the network node serving the mobile node, such that the network address (CoA) advertisement is only processed by said serving network node.
17. A method as claimed in any of claims 11 to 16, further comprising the step of periodically sending said network address (CoA) advertisement from a network node, said network address (CoA) advertisement being addressed to the multicast group of which the network node is centre.
18. A method as claimed in any preceding claim, said serving network node further performing the step of forwarding said candidate network address(es) toward the mobile node, and said mobile node performing the step of caching the candidate network address(es) in memory for use in a subsequent handover to an adjacent

- 44 -

network node.

19. A method as claimed in claim 18, wherein said step of forwarding comprises the step of inserting a candidate network address into an options field of a Proxy Router Advertisement message.

20. A method as claimed claim 19, further comprising the step of providing said Proxy Router Advertisement message with a field for indicating to a mobile node whether or not it contains a candidate network (CoA) address.

10

21. A method as claimed in any of claims 18 to 20, wherein in response to a need for handover of service from one network node to another, the method further comprises the steps of advertising to the mobile node the identity of the adjacent network node that will assume responsibility for serving the mobile node, and the mobile node uses said identity to search its cached list of candidate network addresses for one suitable for use after handover.

15

22. A method as claimed in any preceding claim, further comprising the step of performing duplicate address detection on said candidate network addresses, thereby inhibiting the need to perform duplicate address detection during a subsequent handover of the mobile node from one network node to another.

20

23. A method as claimed in any preceding claim, service of said mobile node having been handed over from a first serving network node to a second network node, the method further comprising the steps of:

25

(1) informing said first serving network node of said handover with a fast binding update;

(2) forwarding datagrams from said first serving network node to the new network address of the mobile node or to the second serving network node;

30

(3) said first serving network node acknowledging said fast binding update with a fast binding acknowledgement;

such that said mobile node can use its new network address as a source address in datagrams sent to the communication network.

24. A method as claimed in any preceding claim, wherein said identity is a

35

- 45 -

network prefix of each adjacent network node.

25. A method as claimed in any preceding claim, wherein said candidate network address is a care-of address (CoA).

5

26. A network node for use in a packet-switched data communication network, which network node comprises means for storing and executing computer executable instructions for performing either:

- 10 (1) any of the serving network node method steps of any of claims 1 to 10 and 18 to 22; or
- (2) any of the adjacent network node method steps of any of claims 1 to 4, 11 to 17, and 22; or
- (3) any of the mobile node method steps of any of claims 18 to 21.

15 27. A computer program comprising computer executable instructions for causing a network node to perform the method steps of any of claims 1 to 25; any of claims 1 to 10, and 18 to 22; any of claims 1 to 4, 11 to 17, and 22; or any of claims 18 to 21.

20 28. A computer program as claimed in claim 27, embodied on a record medium, stored in a computer memory, embodied on a read-only memory or carried on an electrical carrier signal.

25 29. For use in a method as claimed in any of claims 1 to 25, a network address (CoA) solicitation message comprising fields for carrying information as set out in any of claims 7 to 9.

30 30. For use in a method as claimed in any of claims 1 to 25, an IPv6 datagram comprising a network address (CoA) solicitation message as claimed in claim 29.

31. For use in a method as claimed in any of claims 1 to 25, a network address (CoA) advertisement message comprising fields for carrying information as set out in any of claims 11 to 15.

35 32. For use in a method as claimed in any of claims 1 to 25, an IPv6 datagram comprising a network address (CoA) solicitation message as claimed in claim 31.

- 46 -

33. For use with a method as claimed in any of claims 1 to 26, a method of administering a group of network nodes of a packet-switched communication network, which method comprises the steps of:

5 (1) maintaining an electronic database of an association between a group identity, a serving network node and one or more adjacent network node adjacent the serving network node;

(2) updating the database with exchange of one or more electronic messages between a node storing the database and each network node identified in the database such that datagrams addressed to the group of network nodes may be
10 routed thereto by means of the association.

34. A method as claimed in claim 33, wherein each network node is associated with a geographical area of signal coverage on the wireless link and the or each
15 adjacent network node is such that, if a mobile node moves from the geographical area of its serving network node, the next serving access router will be one of said adjacent network nodes.

35. A method as claimed in claim 33 or 34, wherein each network node can
20 communicate directly or indirectly with a crossover node and/or a site crossover node, the crossover node having a link to one or more network nodes and the site crossover node having a link to one or more crossover nodes and/or network nodes, the method further comprising the step of storing a database at each crossover node and/or site crossover node, such that datagrams addressed to the group of network
25 nodes and received at a crossover router or site crossover router may be routed to said group.

36. A method as claimed in claim 35, each database further comprising an indicator of the maximum number of members of said group, the method further
30 comprising the step of, upon receipt of a datagram for said group at a crossover node, comparing said indicator against the number of network nodes in said database, and if said number is less than said indicator, forwarding said datagram to a site crossover node in addition to forwarding said datagram to each network node of the group identified by the database.

35

- 47 -

37. A method as claimed in claim 35 or 36, further comprising the step of providing the electronic database with an interface identifier for each network node of the group, the interface identifier identifying the interface through which each member of the group may be reached.
- 5
38. A method as claimed in claim 33, 34, 35, 36 or 37, further comprising the step of sending a membership query message to each network node in said group to determine whether or not each network node is affiliated with said group.
- 10
39. A method as claimed in claim 38, further comprising the step of periodically sending said membership query message.
- 15
40. A method as claimed in claim 38 or 39, further comprising the step of starting a timer when said membership query is sent, said timer having a limit within which the network node sending the membership query expects a reply.
- 20
41. A method as claimed in claim 40, further comprising the step of sending a further membership query message within a predetermined time after expiry of said timer.
- 25
42. A method as claimed in claim 39 or 40, further comprising the step of deleting the entry for the or each network node from said database if a reply is not received within the period of said timer.
- 30
43. A method as claimed in any of claims 33 to 42, further comprising the step of a network node that is a member of a group of network nodes sending a membership report message to a network node in which its membership is recorded, the membership report message containing the group identifier of the group of which it is a member.
- 35
44. A method as claimed in claim 43, further comprising the step of sending said membership report periodically.
45. A method as claimed in claim 43 or 44, further comprising the step of resetting a lifetime associated with said network node in said database upon receipt of

- 48 -

said membership report message.

46. A method as claimed in claim 45, further comprising the step of sending a membership query message as set out in any of claims 38 to 42 upon expiry of said
5 lifetime.

47. A method as claimed in any of claims 33 to 46, further comprising the steps of (1) a network node sending a join message to a network node storing a database in order to join a group of network nodes, the join message comprising the group
10 identifier of the group that the network node wishes to join and the identity of the joining network node, and (2) the network node adding the joining network node to the database.

48. A method as claimed in any of claims 33 to 47, further comprising the steps
15 of the serving network node sending an update message to a network node that maintains the database, the update message comprising the group identifier and the identity of the serving network node, and the network node maintaining the database refreshing the group identity and entry for the serving network node.

49. A method as claimed in any of claims 38 to 48, wherein said messages
20 comprise an ICMP message.

50. A method as claimed in claim 49, wherein said ICMP message comprises a
25 field that specifies whether the message is a query, report, join or update message.

51. A method as claimed in any of claims 33 to 50, wherein said group of
network nodes is a multicast group and said group identifier is the multicast address of the multicast group.

52. A network node for use in a packet-switched data communication network,
30 which network node comprises means for storing and executing computer executable instructions for performing either:

- (1) any of the steps of claims 33 to 42, 45 or 46; or
- (2) any of the steps of claims 43, 44, 47 or 48.

35

- 49 -

53. A computer program comprising computer executable instructions for causing a network node to perform the method steps of any of claims 33 to 51; any of claims 33 to 42, 45 or 46; and/or any of claims 43, 44, 47 or 48.
- 5 54. A computer program as claimed in claim 53, embodied on a record medium, stored in a computer memory, embodied on a read-only memory or carried on an electrical carrier signal.
55. In a packet switched data network comprising a plurality of network nodes, a
10 method of discovering the identity of off-link network nodes, which method comprises the steps of:
- (1) forming one or more off-link network nodes into groups; and
 - (2) using a multicast protocol to distribute the identity of each network
node amongst one or more members of the group.

15

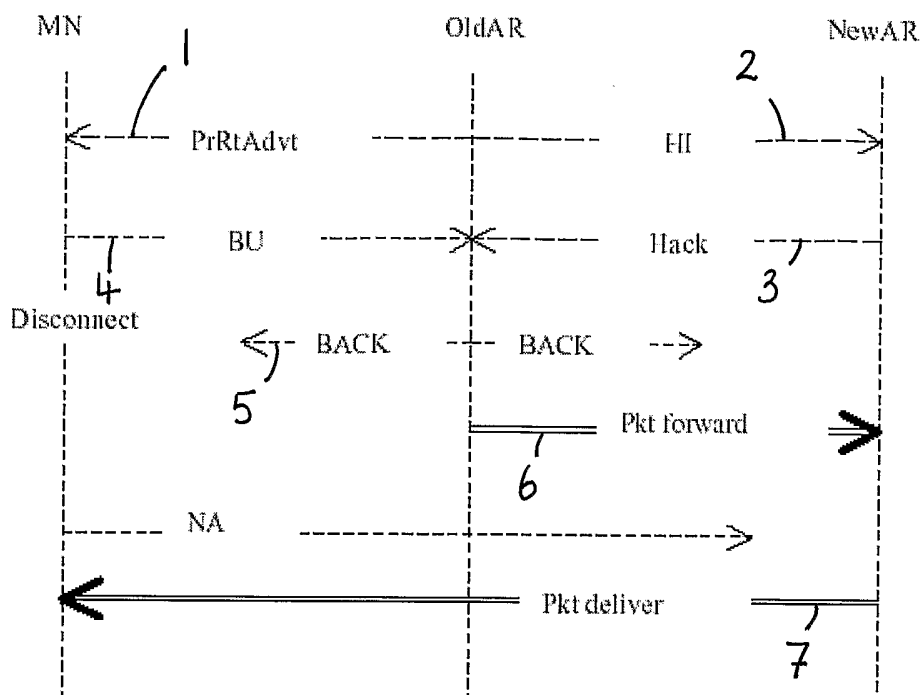


FIG. 1

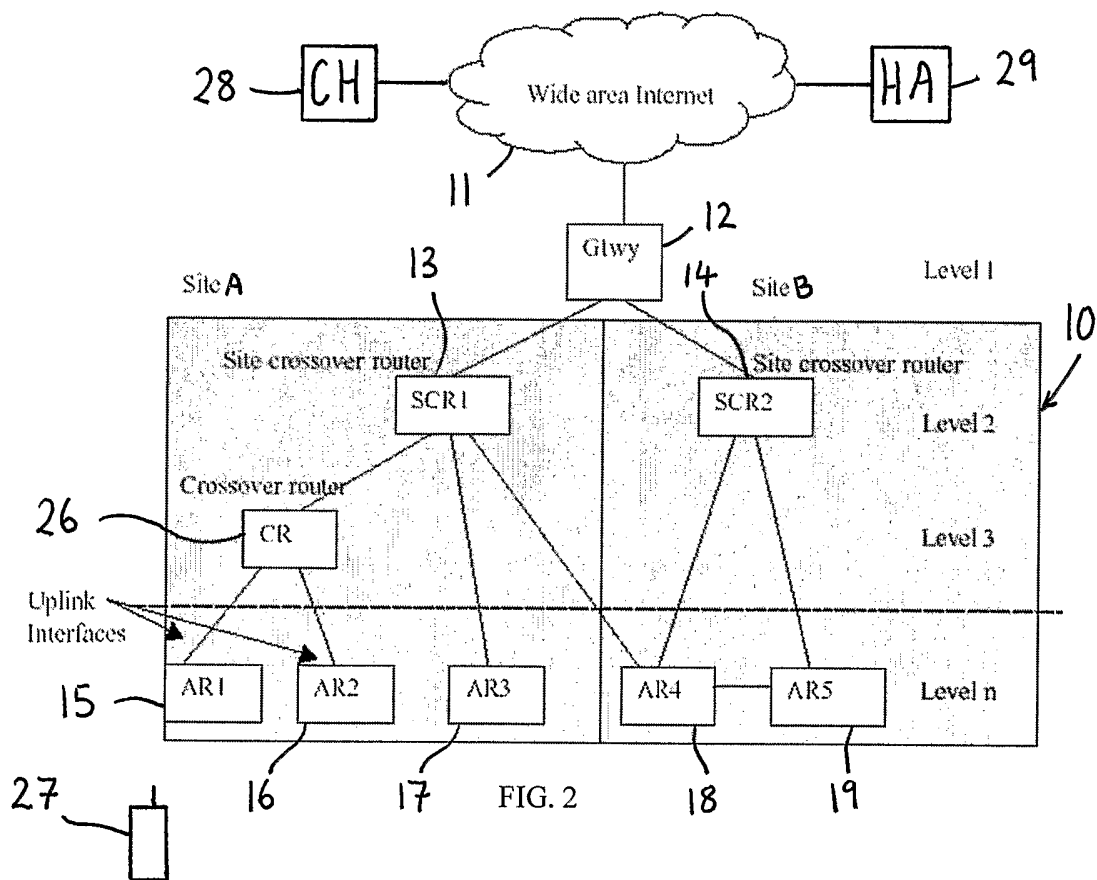


FIG. 2

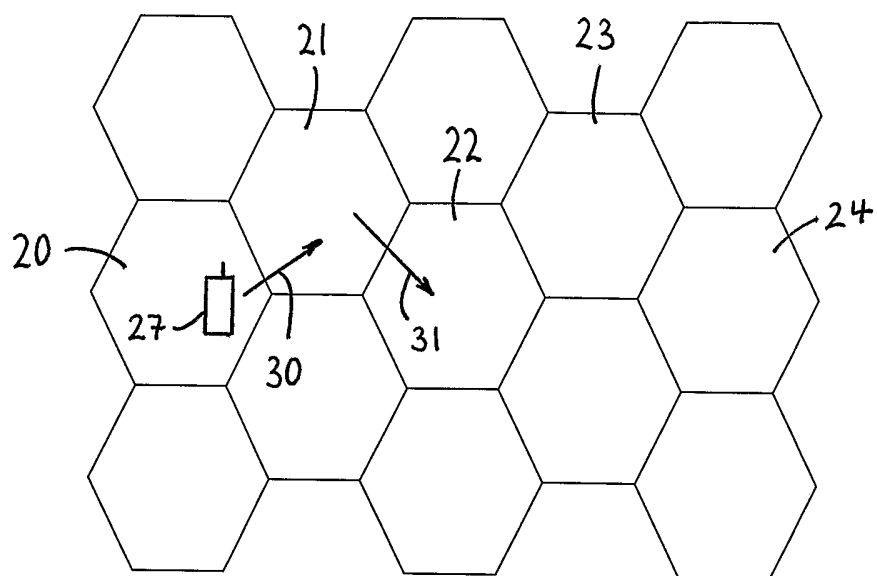


FIG. 3

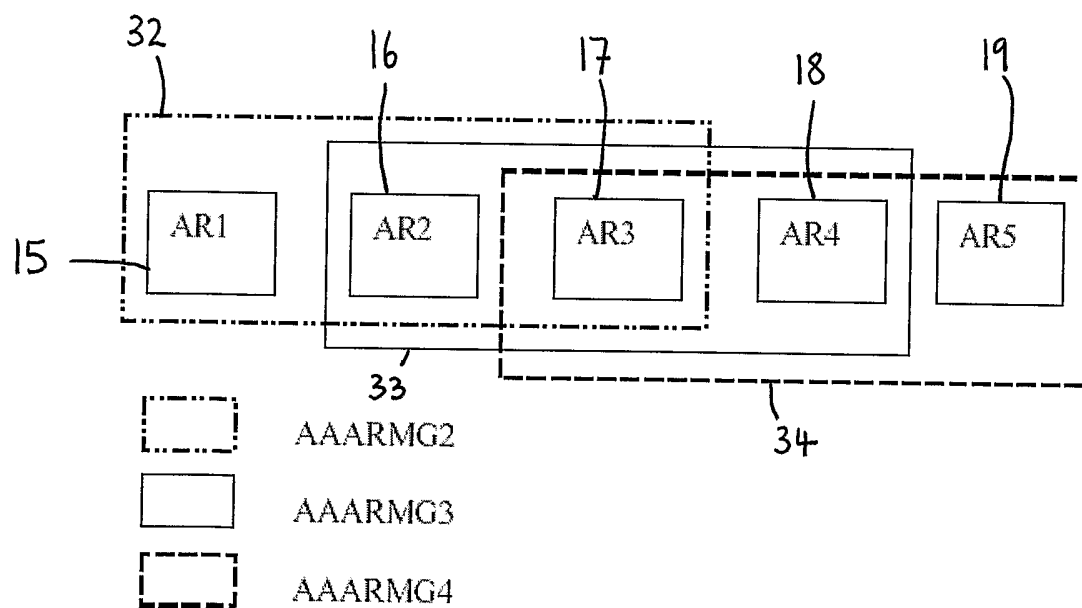


FIG. 4

36

35

<u>MULTICAST GROUP</u>	<u>CENTRE ACCESS ROUTER</u>	<u>ADJACENT ARs</u>	
AAARMG2	AR2	AR1	AR3
AAARMG3	AR3	AR2	AR4
AAARMG4	AR4	AR3	AR5

37

38

FIG. 5

40

8 bits	4 bits	4 bits	112 bits
11111111	FLAGS	SCOPE	Group ID

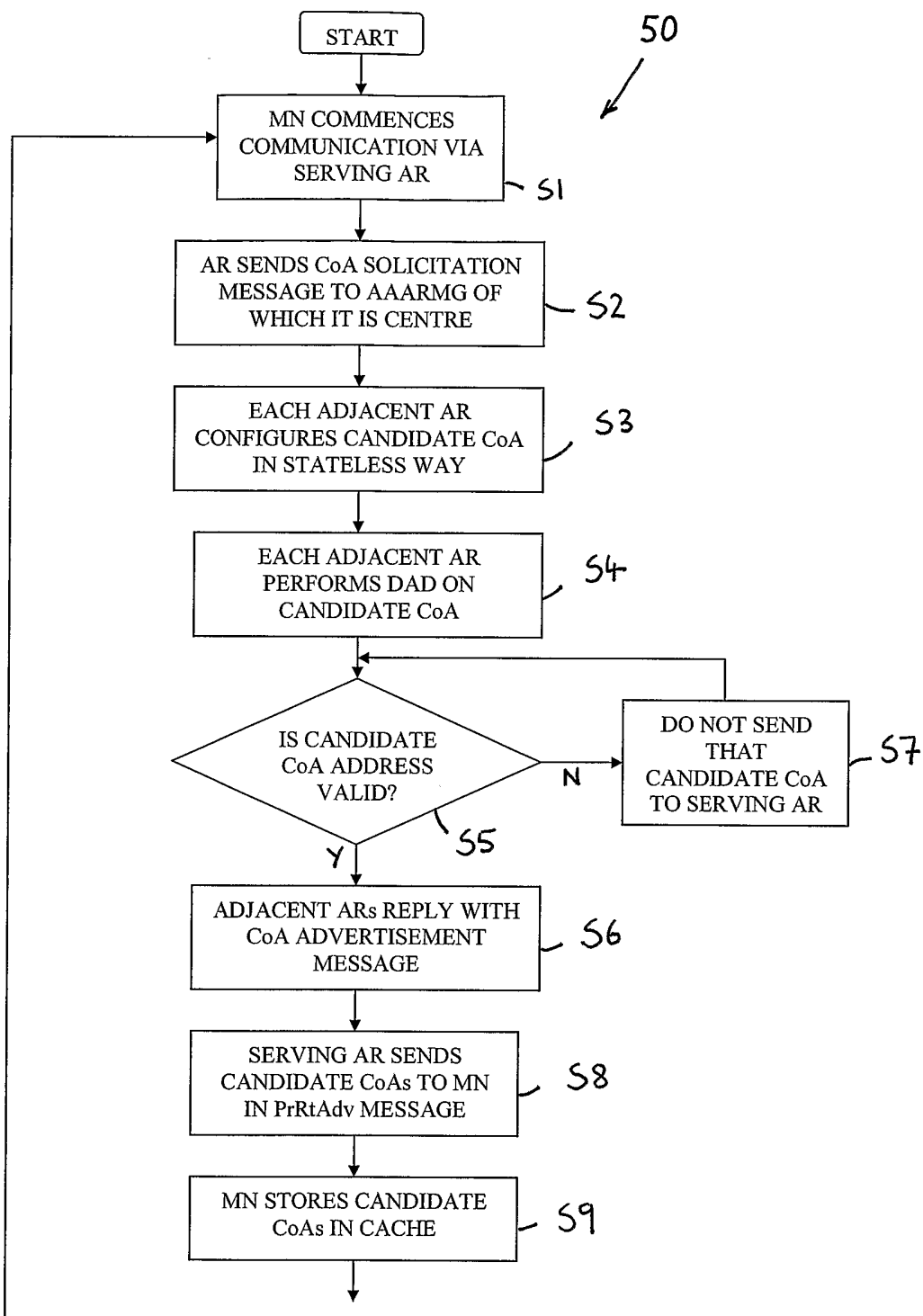
41

42

43

44

FIG. 6



Cont. Fig. 7'

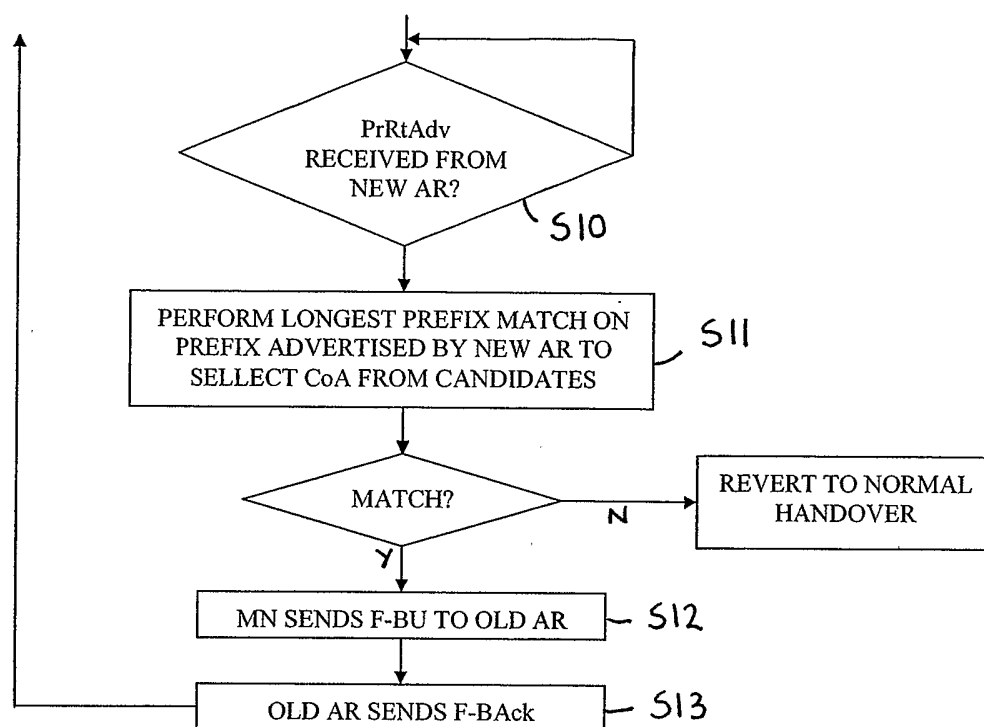


FIG. 7'

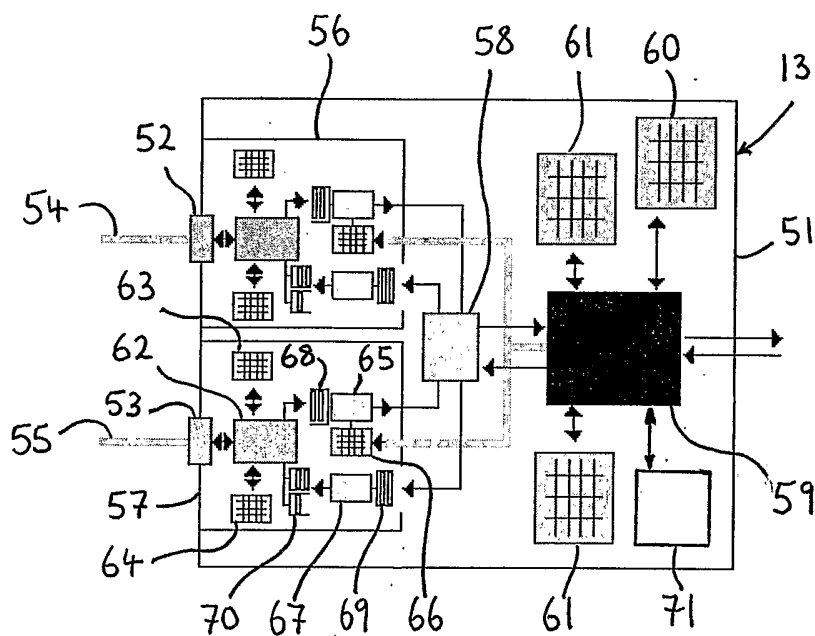
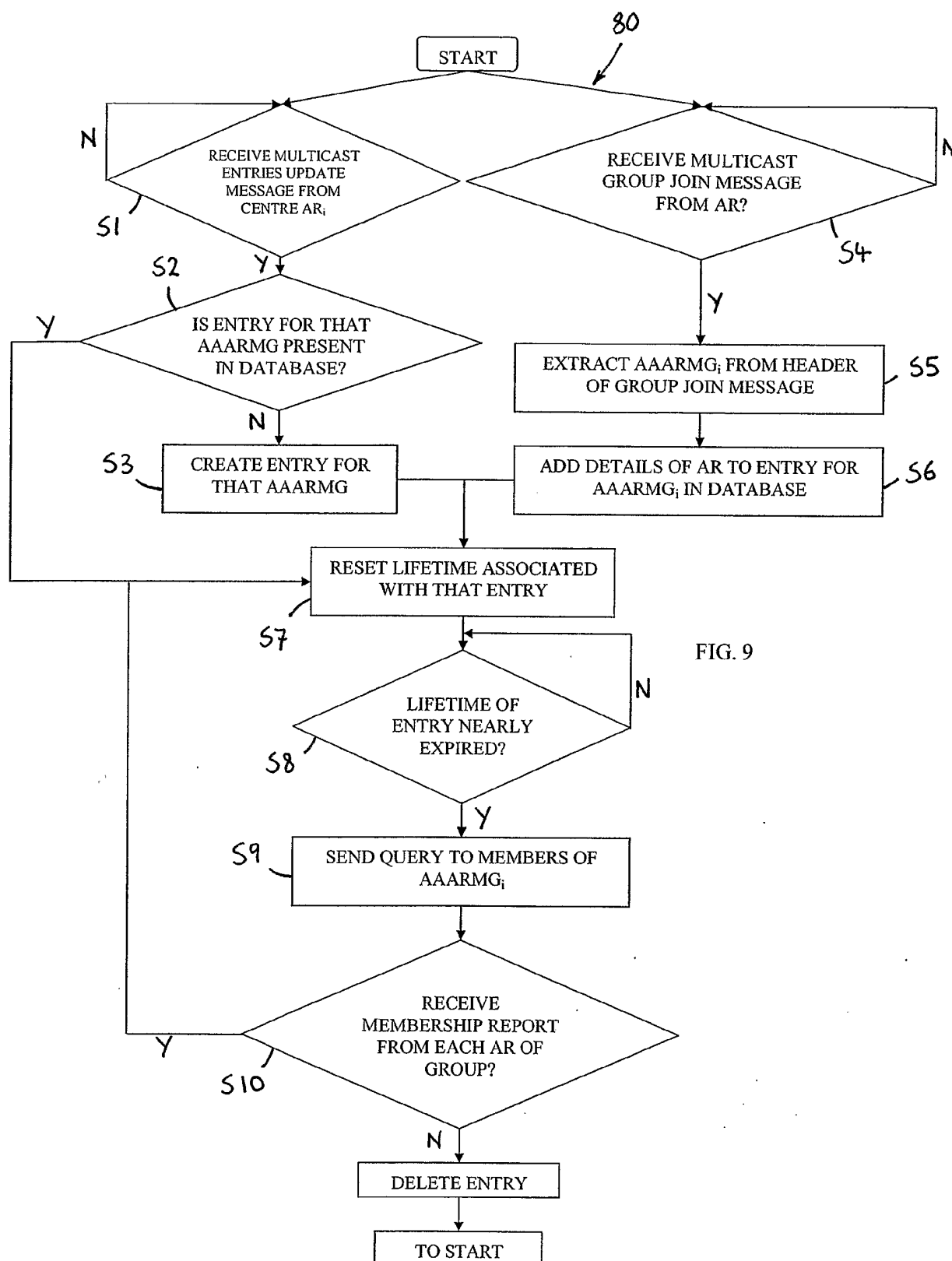


FIG. 8



84

81

Destination address	Group Center	Multicast Member	Lifetime	Flags	Interface
AAARMG _i	AR _i n>i>1	Unicast address of the AR ₁	Lf ₁	F ₁	Interface 1
		Unicast address of AR ₂	Lf ₂	F ₂	Interface 2
		...	...	...	...
		Unicast address AR _n	Lf _n	F _n	Interface n

82 83 85 86 87

FIG. 10

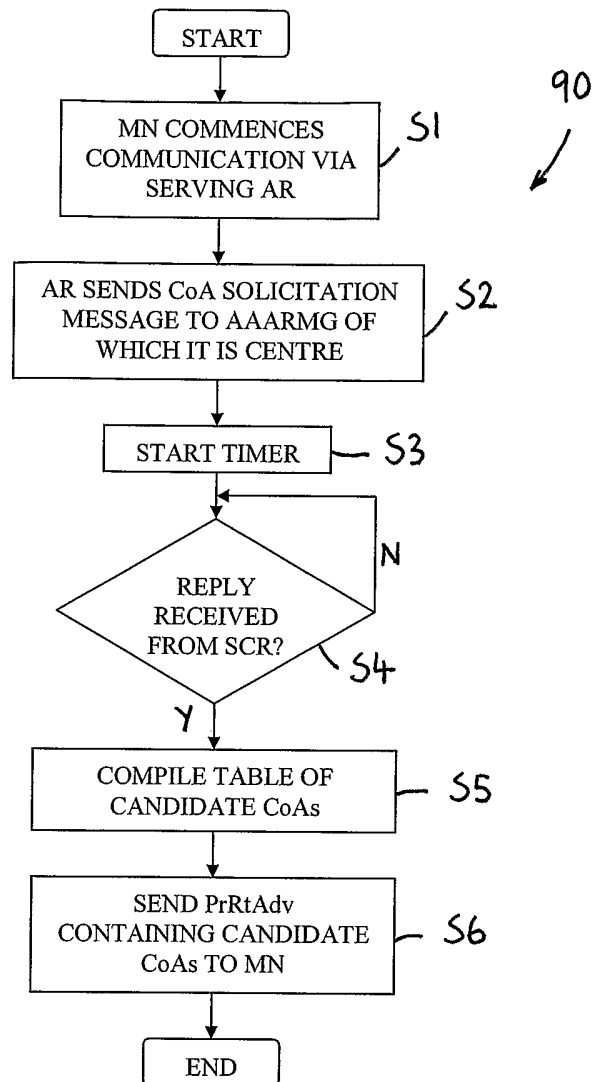


FIG. 11

100

Adjacent Access Router to AR ₀	Prefixes captured	Access Routers ID
AR1	3ffe:327e:2:2:: /64	cac8:d5ff:47d1:2faa
AR2	3ffe:28ac:4525:3:: /64	adc8:d5ff:33d5:2fba
AR3	...	...
...		
AR _n	3ffe:47be:92d2:n:: /64	Cac7:cc45:48d5:6fca

101
102
103

FIG. 12

110

Serving AR: AR ₀	Adjacent Access Router	Configured candidates Care of Address for the MN.
MN ID	AR1	3ffe:327e:2:2: MN ID
	AR2	3ffe:28ac:4525:3: MN ID
	...	
	AR _n	3ffe:47be:92d2:n: MN ID

111
112
113

FIG. 13

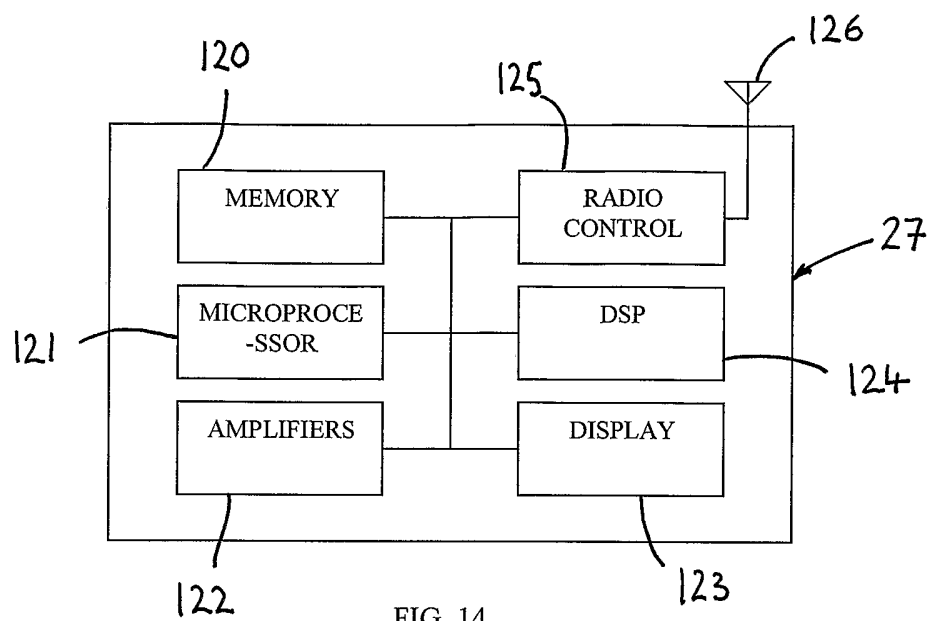


FIG. 14

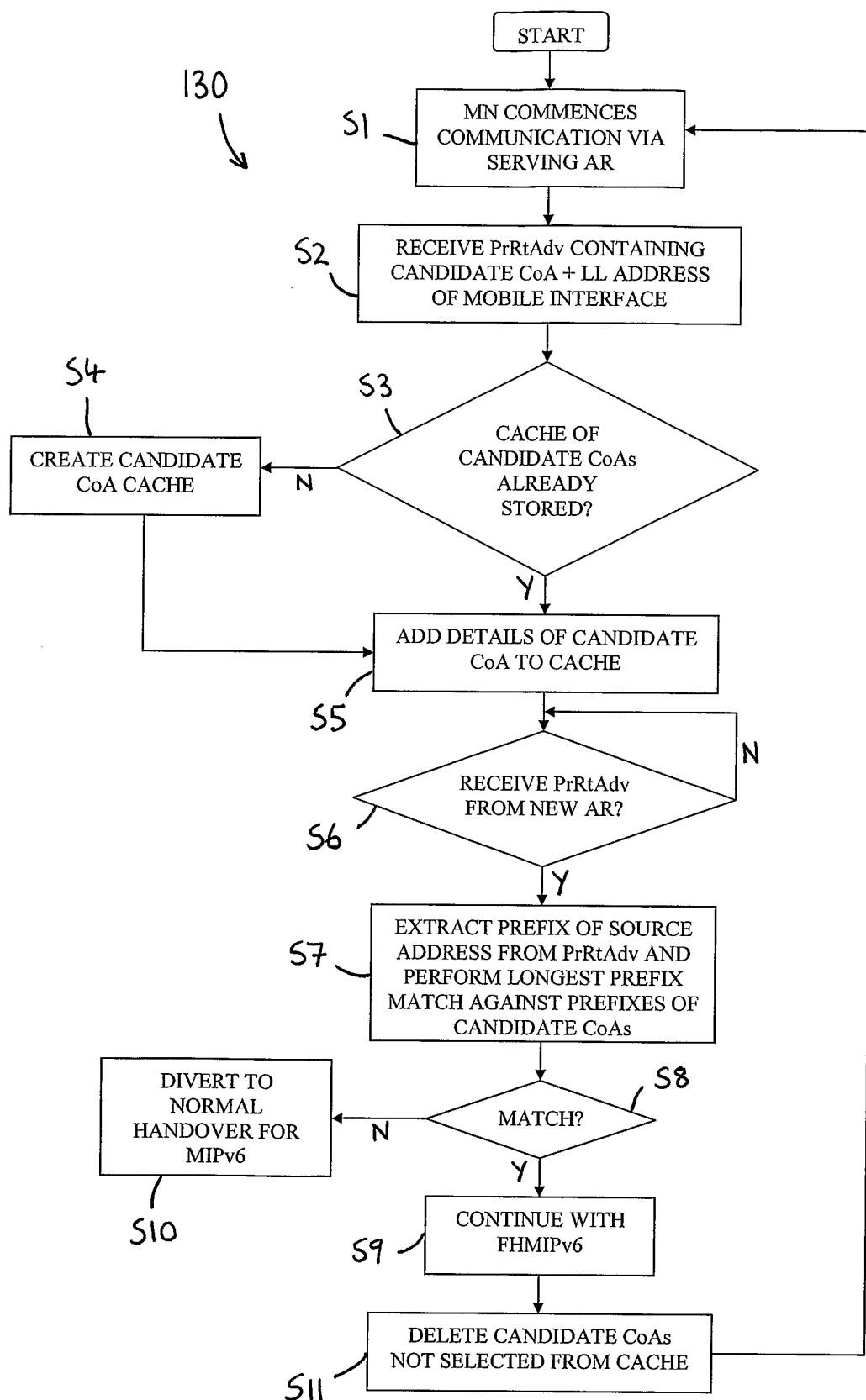


FIG. 15

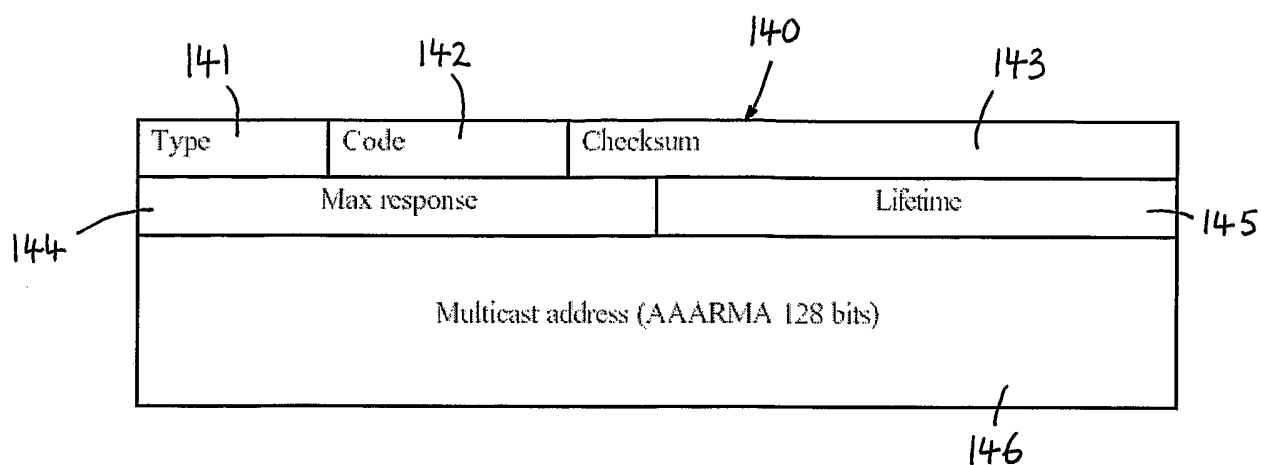


FIG. 16

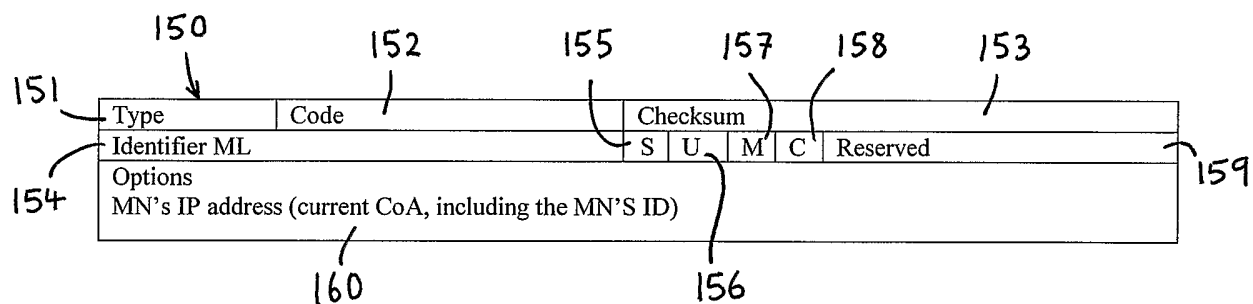


FIG. 17

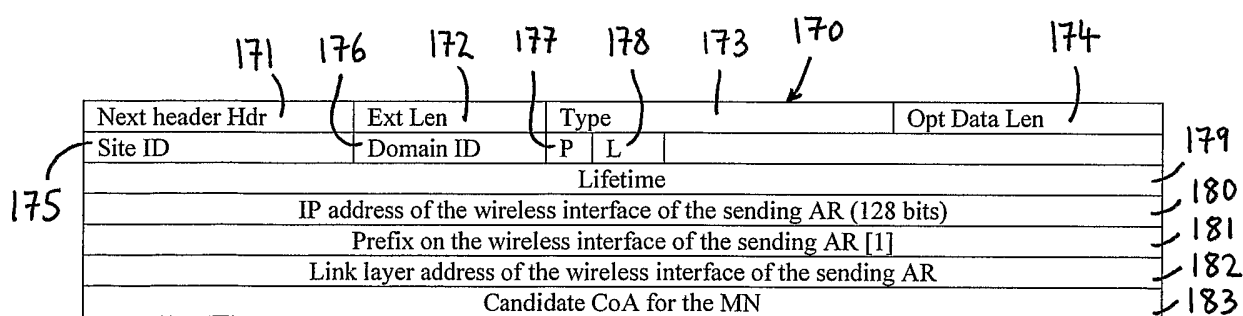


FIG. 18

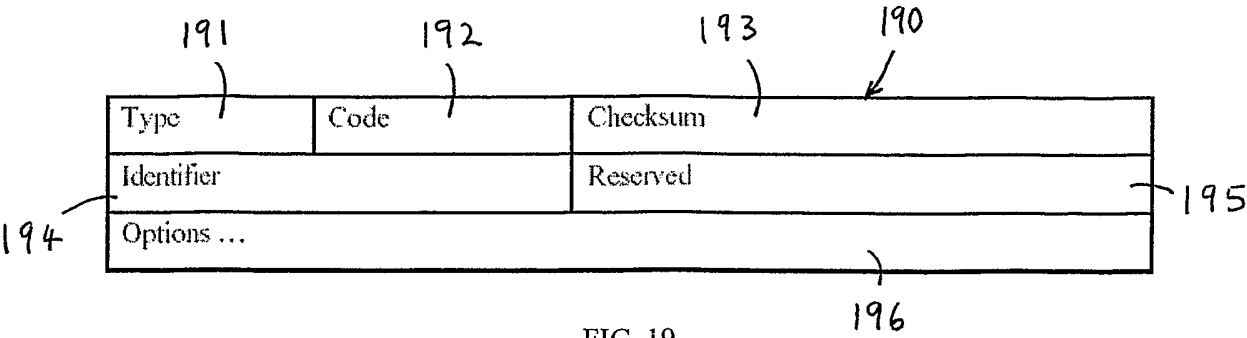


FIG. 19

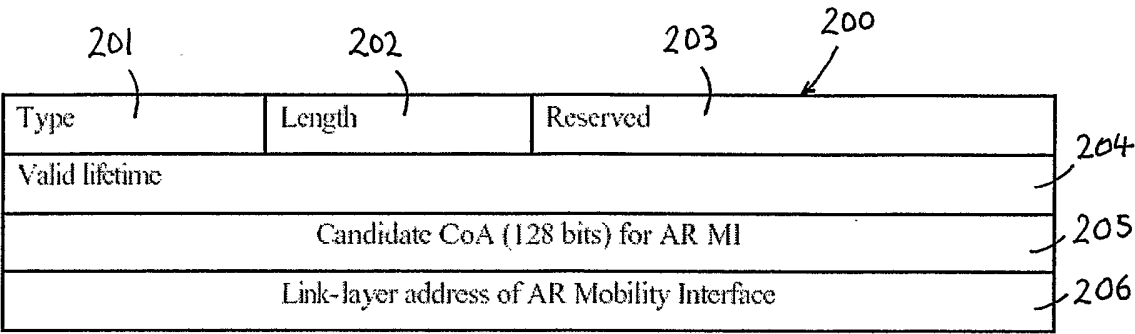


FIG. 20