



(43) International Publication Date
4 September 2014 (04.09.2014)

- (51) International Patent Classification:
H04L 12/24 (2006.01) *H04L 29/06* (2006.01)
- (21) International Application Number:
PCT/US2014/018797
- (22) International Filing Date:
26 February 2014 (26.02.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
13/783,184 1 March 2013 (01.03.2013) US
- (71) Applicant: **T-MOBILE USA, INC.** [US/US]; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US).
- (72) Inventors: **MUFTI, Shujaur, Rehman**; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US). **HOOKER, William, Michael**; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US).
- (74) Agents: **BHANDARI, Susmita** et al.; Perkins Coie LLP, P.O. Box 1247, Seattle, WA 98111-1247 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CL, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) Title: SYSTEMS AND METHODS FOR EMERGENCY CALL ROUTE FAILOVER

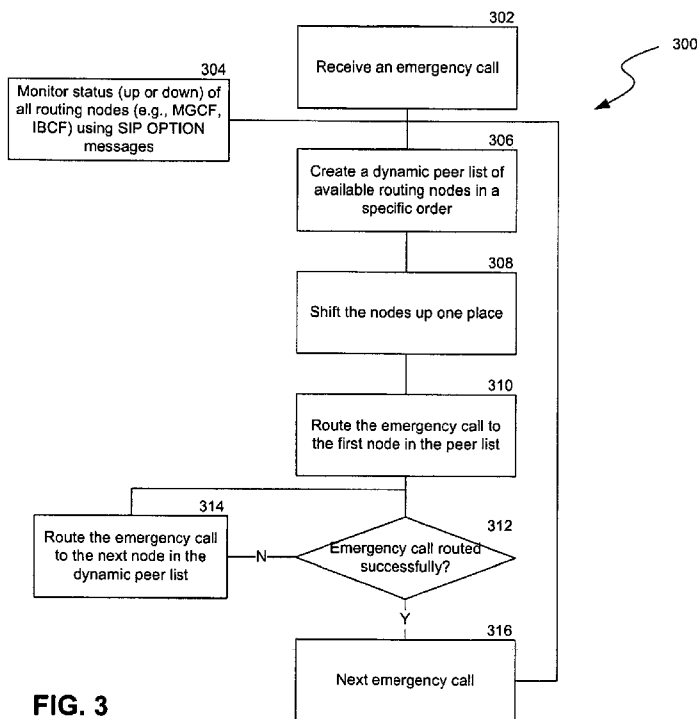


FIG. 3

(57) Abstract: A system and method for performing an emergency call route failover between an Emergency Call Session Control Function (E-CSCF) and multi-homed remote end-point functions such as Border Gateway Control Function(BGCF)/Media Gateway Control Function (MGCF) or Interconnection Border Control Function (IBCF) in an Internet Protocol Multimedia Subsystem (IMS) uses Session Initiation Protocol (SIP) and/or Domain Name System (DNS) methods. The E-CSCF and/or a DNS server monitors the availability of the remote end-points to create a peer list of route options. The E-CSCF or the DNS server selects a route option from the peer list to route an emergency call to an appropriate Public Safety Answering Point (PSAP). In the event that the route option fails, the E-CSCF fails over to the next available route option to route the emergency call.

WO 2014/134220 A1

SYSTEMS AND METHODS FOR EMERGENCY CALL ROUTE FAILOVER

BACKGROUND

[0001] The Internet Protocol Multimedia Subsystem (“IMS”), developed by the standards organization known as the 3rd Generation Partnership Project (“3GPP”), is an architectural framework for delivering Internet Protocol (“IP”) multimedia to mobile users, such as users of various mobile devices. An IMS core network (“IMS core”) allows wireless and wireline devices to access multimedia, messaging, and voice applications and services. To ease the integration of an IMS core with Internet resources, 3GPP specifications use Internet Engineering Task Force (“IETF”) protocols, such as the Session Initiation Protocol (“SIP”) and Diameter, within the IMS core.

[0002] The IMS core, as defined in the 3GPP TS 23.167 specification, supports emergency services by routing emergency calls (e.g., “911” calls) to the nearest Public Safety Answering Point (PSAP), which is a physical location that receives emergency calls from the public.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] Figure 1 shows a representative Internet Protocol Multimedia Subsystem (“IMS”) environment having redundancy mechanism in place for routing emergency calls to Public Safety Answering Points (“PSAPs”).

[0004] Figure 2A is a call flow diagram illustrating periodic monitoring of remote nodes in the IMS environment.

[0005] Figure 2B is a call flow diagram illustrating emergency call set up in the IMS environment.

[0006] Figure 2C is a call flow diagram illustrating an emergency call route failover based on Session Initiation Proxy (“SIP”) OPTIONS method in the IMS environment.

[0007] Figure 2D is a call flow diagram illustrating an emergency call route failover based on Domain Name System (“DNS”) supervision in the IMS environment.

[0008] Figure 3 is a logic flow diagram illustrating an emergency call route failover based on a dynamically created peer list in the IMS environment.

[0009] Figure 4 is a logic flow diagram illustrating peer list selection in the IMS environment based on PSAP capability.

[0010] Figure 5 is a diagrammatic representation of a machine in the example form of a computer system within which a set of instructions, for causing the machine to perform any one or more of the methodologies discussed herein may be executed.

DETAILED DESCRIPTION

[0011] The Internet Protocol Multimedia Subsystem (“IMS”) core network (“IMS core”) supports emergency services (e.g., “911” calls) via an IMS functional element known as an Emergency Call Session Control Function (“E-CSCF”). The E-CSCF routes emergency call requests to the nearest Public Safety Answering Point (“PSAP”) via remote end-point functional elements or gateway nodes such as a Border Gateway Control Function (“BGCF”), a Media Gateway Control Function (“MGCF”) or an Interconnection Border Control Function (“IBCF”). Multimedia sessions between these and other IMS functional elements are created and controlled using a client-server signaling protocol known as the Session Initiation Protocol (“SIP”).

[0012] In implementations described in detail below, systems and methods for emergency call route failover are disclosed. The failover routing mechanisms are used to manage redundancy in signaling gateway nodes such as the BGCF/MGCF and the IBCF by the E-CSCF to select appropriate failover nodes in the event of some form of failure.

[0013] When an emergency call request arrives, the E-CSCF identifies an appropriate PSAP, and routes the request to the PSAP via a BGCF (which determines the MGCF), an MGCF or an IBCF (each hereinafter “remote node” or “node”). When a remote node selected by the E-CSCF for routing the emergency call request is down, or otherwise unavailable, there is no redundancy mechanism available or outlined in the existing E-CSCF specifications and standards to complete the connection to the PSAP. The systems and methods disclosed allow the E-CSCF to monitor remote nodes to determine their status (e.g., up or down) and select a routing option towards a remote node that is available, based on different unique criteria, such as a SIP OPTIONS

method and a Domain Name Service (“DNS”) method, as described in detail below. The implementation of one or more failover routing mechanisms provide redundancy in emergency call routing and provide the advantage of faster and/or efficient routing of emergency calls to appropriate PSAPs.

[0014] Various embodiments of the disclosed systems and methods will now be described. The following description provides specific details for a thorough understanding and an enabling description of these embodiments. One skilled in the art will understand, however, that the invention may be practiced without many of these details. Additionally, some well-known structures or functions may not be shown or described in detail, so as to avoid unnecessarily obscuring the relevant description of the various embodiments. The terminology used in the description presented below is intended to be interpreted in its broadest reasonable manner, even though it is being used in conjunction with a detailed description of certain specific embodiments of the invention.

[0015] Figure 1 is a diagram of a representative IMS environment 100 having a redundancy mechanism in place for routing emergency calls to PSAPs. Environment 100 includes a user equipment (“UE”) 102 for initiating an emergency call. The UE 102 connects to an Internet Protocol (“IP”) Connectivity Access Network (“IP-CAN”) 104. IP-CAN 104 is a collection of network entities and interfaces that provide the underlying IP transport connectivity between the UE 102 and the IMS entities. The IMS core is not dependent on any specific type of access network. Thus the IP-CAN 104 can include, for example, General Packet Radio Service (“GPRS”), Universal Mobile Telecommunications System (“UMTS”), Long Term Evolution (“LTE”), CDMA2000, fixed wireline (e.g., DSL, Ethernet, cable, etc.), WiMax, fixed broadband access, Wireless Local Access Network (“WLAN”), or other wired or wireless communications connection. The UE 102 may include any devices that can connect to the IP-CAN 104. Some of the devices can be IMS-capable (i.e., can handle signaling and/or media transport protocols of the IMS core), while others can be non-IMS-capable. For example, the UE 102 may include, but is not limited to: mobile phones, Voice over Internet Protocol (“VoIP”) devices, personal digital assistants, radio frequency devices, infra-red devices, hand-held computers, laptop computers, desktop computers, netbooks, wearable computers, tablet devices, pagers, voice over IP (VoIP) phones, media players, gaming device, set-top boxes, and the like.

[0016] A call request from the UE 102, which can be an emergency call request (e.g. "911 call") or a normal call request, is received by a Proxy Call Session Control Function ("P-CSCF") 110. The P-CSCF 110 examines the received call request to determine whether the call request is an emergency call request or a normal or non-emergency call request. If the call request is a normal or non-emergency call request, the P-CSCF 110 communicates with the Serving Call Session Control Function ("S-CSCF") 106 and the Interrogating Call Session Control Function ("I-CSCF") 108 to route the call request to a terminating UE in the Public Switched Telephone Network ("PSTN") 118 or the IP network 128. For example, in one implementation, the call may be routed via a Media Gateway Control Function ("MGCF") 114 selected by a Border Gateway Control Function ("BGCF") to the PSTN 118. In another implementation, the call may be routed via an Interconnection Border Control Function ("IBCF") 116 to the IP network 128. In order to perform the routing, the P-CSCF 110 and/or other IMS entities may use information from the tElephone NUmber Mapping server ("ENUM") 122 and/or Home Subscriber Server ("HSS") 124.

[0017] When the call request is an emergency call request, the P-CSCF 110 classifies or flags the call request as an emergency call request and selects an E-CSCF 112 in the same network to handle the emergency call request. The E-CSCF 112 communicates with a Location Retrieval Function ("LRF") 126, which retrieves location information for the UE 102, and obtains routing information (e.g., address of the PSAP) for the emergency call from one or more entities supporting location services as the Gateway Mobile Location Center ("GMLC") (not shown).

[0018] As described above, the MGCF 114 supports the IMS-PSTN interworking. The IBCF 116 supports interworking with other networks that are more likely to be IP networks 128 than Time Division Multiplexing ("TDM") networks such as PSTN 118. The IBCF 116 sits on a Session Border Controller ("SBC", not shown) at the edge of the IMS core. Depending on the details associated with the emergency call request, the emergency call may be routed to a BGCF/MGCF 114 or to an IBCF 116. If the E-CSCF 112 selects an MGCF 114 as the routing node, the MGCF 114 routes the emergency call to a PSAP 120 sitting in the PSTN network 118. Similarly, if the E-CSCF 112 selects an IBCF 116 as the routing node, the IBCF 116 routes the emergency call to a PSAP 130 in the IP network 128. The S-CSCF 106, the I-CSCF 108, the P-CSCF 110,

the E-CSCF 112, the BGCF/MGCF 114, IBCF 116, ENUM 122, HSS 124 and LRF 126 may be considered as IMS entities that are a part of the IMS core 132.

[0019] Figure 2A is a flow diagram illustrating periodic monitoring of remote nodes 202 in the IMS environment by the E-CSCF 112. The E-CSCF 112 uses a SIP-based method to monitor the availability of each of the nodes 202, which may include the BGCF/MGCF nodes 114 and/or the IBCF nodes 116. In one implementation, the E-CSCF 112 initiates or sends a SIP "OPTIONS" message 204 towards each of the nodes 202 at a configurable frequency (e.g., every 5 seconds). At any given time, some of the nodes 202 may be available, while others may be unavailable or down. If a node is up and running, the node responds with a "200 OK" message 206.

[0020] Alternately, if a node is unavailable, an error code 208 may be returned. In one implementation, the error code 208 may be a "503" (Service Unavailable) error response. In other implementations, other server failure 5xx error codes may be returned by the nodes to indicate an error condition, such as a particular error condition. 5xx error codes may include, for example, "500" (Server Internal Failure), "502" (Bad Gateway), "504" (i.e., Server Timeout), "505" (Version Not Supported) and "513" (Message too Large). The errors are described in detail in RFC 3261 "SIP: Session Initiation Protocol" which is incorporated by reference herein.

[0021] At block 210, when any server failure error code 5xx is received as a response to the OPTIONS message from a node, or no response is received, the E-CSCF112 initiates an internal failover to take the node out of route choices for routing emergency call traffic. In one implementation, the E-CSCF 112 may maintain a first peer list for BGCF/MGCF nodes and a second peer list for IBCF nodes. Of course, other peer lists are possible, such as an all-inclusive list of BGCF/MGCF or IBCF nodes. The nodes may be identified based on an identifier or IP address. Based on the responses, the E-CSCF 112 may mark or flag the nodes responding with a 5xx error code as being unavailable in the corresponding peer list (or if no response is received). Alternately, the unavailable nodes may be removed from the corresponding peer list. In either implementation, the unavailable nodes are detected, and are not used as a peer for routing emergency call traffic, at least for a time duration. In this way, the E-CSCF maintains an active, current list of remote nodes to use when it receives an emergency call.

[0022] In one implementation, the E-CSCF 112 may not send any heartbeat signal (e.g., OPTIONS message, polling signal, etc.) towards a node if the link between the E-CSCF 112 and the node is active. When the link between the two is idle, the E-CSCF 112 may start sending heartbeats at a configurable frequency (e.g., few milliseconds to a few seconds). The sending of the heartbeat signals may be automated using retransmit timers that back off exponentially. When a previously unavailable node becomes available, the node may be added to the corresponding peer list by the E-CSCF 112.

[0023] Figure 2B is a flow diagram illustrating an emergency call set up in the IMS environment. For clarity, the UE 102 is illustrated as an IMS-capable device (e.g., a SIP phone) using SIP signaling for communication with various IMS core entities such as the LRF 126, P-CSCF 110 and the E-CSCF 112. However, it should be noted that UE 102 may be any other device that is not IMS-capable (e.g., a GSM phone) that can connect to one of many IP-CAN 104 supported by the IMS core.

[0024] At block 212, the UE 102 initiates an emergency call request. The emergency call request is for establishing an emergency call with an appropriate PSAP, and for delivery of location information associated with the subscriber's UE 102 to the PSAP. The location information may be acquired via one or more procedures. For example, in one implementation, the UE 102 may determine its own location or location identifier with or without the assistance of the IP-CAN 104 at block 214. Various location determining methods are of course possible.

[0025] The UE 102 next sends a SIP INVITE request message 216 with an emergency indication to the P-CSCF 110. For non-IMS-capable UEs, the gateways (e.g., a media gateway) can send a SIP INVITE message with an emergency indication to the P-CSCF 110 on behalf of the UE. In some implementations, the INVITE message 216 may include location information, such as the location information acquired at block 214.

[0026] The P-CSCF 110 detects the INVITE request message 216 as an emergency call request at block 218. The P-CSCF 110 then selects an E-CSCF 112 in the same network to handle the emergency call request. The P-CSCF 110 forwards the INVITE request message 220 to the E-CSCF 112. In one implementation, the INVITE request message 220 may include insufficient or no location information for the E-

CSCF 112 to determine the geographical location of the UE 102 and/or the address of the PSAP where the emergency call should be routed to. The E-CSCF 112 may thus send a request 222 to the LRF 126 to retrieve location and/or routing information based on which E-CSCF 112 can redirect the emergency call to the next hop (i.e., BGCF/MGCF or IBCF). The location request 222 may include information identifying the IP-CAN 104, the UE 102, means to access the UE (e.g. UE's IP address or other electronic address/identifier), or the like.

[0027] The LRF 126 may obtain and/or verify the location of the UE 102 at block 224. The LRF 126 may use procedures defined in 3GPP TS 23.271 for control plane location or procedures defined by the Open Mobile Alliance (“OMA”) for Secure User Plane Location (“SUPL”) to determine the location of the UE 102. The LRF 126 may also determine an address for a PSAP selected for the emergency call via the GMLC or by invoking a Routing Determination Function (“RDF”) to convert the location of the UE 102 into a PSAP address. In one implementation, the LRF 126 stores some or all the information obtained, received and/or associated with the UE 102 and the emergency call request in a record. The LRF 126 may send the location information (UE location) and/or the routing information (PSAP address) 226 to the E-CSCF 112. In addition to the location and/or routing information, the LRF 126 may also send correlation information to the E-CSCF 112. The correlation information identifies the record for the emergency call stored in the LRF 126, and can be used by the PSAP as a key to later request the UE's location information from the LRF 126. The correlation information may include an Emergency Services Routing Key (“ESRK”) or the Emergency Services Query Key (“ESQK”). An ESRK is a 10-digit (or may be more or less digits) routable, but not necessarily dialable, number that may be used to identify the UE 102 and the LRF 126 for the emergency call. For example, each LRF may allocate ESRK numbers from a different unique range of numbers, which allows the PSAP to determine the LRF based on the number range for a particular ESRK. The details of the acquiring of location information and/or routing information are described in detail in the 3GPP TS 123.167 technical specification, which is incorporated by reference herein.

[0028] Figure 2C is a flow diagram illustrating an emergency call route failover based on a SIP OPTIONS method in the IMS environment. When the E-CSCF 112 has the location and/or routing information, the E-CSCF 112 may route the emergency call to a PSAP 252. The PSAP 252 may be a PSAP 120 sitting behind a PSTN network 118

or an IP-capable PSAP 130 sitting behind an IP network 128. At block 228, the E-CSCF 112, depending on the details of the INVITE request and/or the PSAP address, dynamically creates a peer list (“dynamic peer list” or “hunt list”) of available BGCF/MGCF nodes or available IBCF nodes arranged in a specific order. The dynamic peer list may also be generated before receiving an emergency call (e.g. before for each emergency call request received by the E-CSCF 112).

[0029] At block 230, the E-CSCF 112 selects a target node from the dynamic peer list, and modifies or adjusts the INVITE request message received from the P-CSCF 110 for delivery to the selected node 254a. For example, if the selected node 254a is an MGCF, the INVITE request message may include the address of the PSAP 252 as destination, the host/domain name or IP address of the MGCF as the next hop, UE location information, the ESRK, and the like. Similarly, if the selected node is an IBCF, the INVITE message may include the PSAP address as the Request Uniform Resource Identifier (“R-URI”), the host/domain name or the IP address of the IBCF as the next hop, UE location information, the ESRK, and the like. The E-CSCF 112 sends the modified or adjusted INVITE request message 232 to the selected node 254a. If the INVITE request message 232 is successfully received by the selected node 254a, a “200 OK” message 234 is sent by the selected node 254a to the E-CSCF 112 to acknowledge the receipt.

[0030] The selected node 254a, depending on the TDM or IP connectivity of the PSAP 252, may send a SIP INVITE message 238 or an Initial Address Message (“IAM”) 240 to the PSAP 252. For example, an MGCF may convert the SIP INVITE request message 232 to an Integrated Services Digital Network User Part (“ISUP”) IAM 240, which is a part of the Signaling System No. 7 (“SS7”) used for setting up telephone calls in the PSTN. An IBCF, on the other hand, may adjust and forward the SIP INVITE request message 238 to an IP capable PSAP.

[0031] Alternately, in one implementation, the selected node 254a may not be able to process the INVITE request message 232 due to various reasons such as temporary overloading or maintenance, etc. The selected node 254a may respond with a 5xx error code (e.g., “503” or Service Unavailable error). Alternately, the selected node 254a may provide no response at all, in which case, the E-CSCF 112 may self-generate an error code such as “408” (Request Time out) error. In case of the “503”, “408” or other error

codes that indicate failed response to the INVITE request message, the E-CSCF 112 selects the next node in the sequence of available nodes in the dynamic peer list as an option for routing the emergency call request. The E-CSCF 112 sends a SIP INVITE request message 244 to the selected node 254b. The E-CSCF 112 may continue to hunt for an available or responsive node by moving down the nodes in the dynamic peer list until one of the nodes responds with a "200 OK" message. As before, the selected node 254b forwards the SIP INVITE request message 245 to a SIP/IP capable PSAP or sends an ISUP IAM 248 to a PSAP with TDM connectivity. Following delivery of the SIP INVITE request message or ISUP IAM message to the PSAP 252, the emergency call establishment is completed at block 250.

[0032] Figure 2D is a flow diagram illustrating an emergency call route failover based on Domain Name System ("DNS") supervision in the IMS environment. In one embodiment, the IMS core 132 may implement a DNS server 256 to monitor the health of the nodes 202. Alternatively or additionally, the DNS server 256 may implement a load balancing strategy to distribute the routing of emergency calls to different nodes. The DNS server 256 resolves a Fully Qualified Domain Name ("FQDN") to different IP addresses corresponding to different nodes based on round-robin or other strategy to load balance.

[0033] In one implementation, the E-CSCF 112 sends a DNS query 258 to the DNS server 256 to resolve the FQDN of an MGCF node (e.g., mgcf1@t-mobile.com) or an IBCF node (e.g., ibcf1@t-mobile.com), for example. The DNS server 256 monitors the health of the nodes 202 by performing periodic checks using one or more diagnostic methods such as ping polling, Simple Network Management Protocol ("SNMP") polling, and the like. In one implementation, the nodes 202 may include an interface such as the SNMP interface to provide node-specific information to the DNS server 256. For example, the DNS server 256 periodically sends a GET/SET request 260 towards the nodes 202. SNMP agents running on the nodes 202 respond with a response 262. In one implementation, the response 262 may be variables, data or other node-specific information collected by the SNMP agents and acknowledgement to the GET/SET requests. Alternatively, the response 262 may be an error response.

[0034] In one embodiment, the DNS server 256 is responsible for dynamically creating a peer list of nodes that are diagnosed as being healthy, and selecting a node

from the dynamic peer list to which an emergency call request is routed. In one implementation, static peer lists for BGCF/MGCF and IBCF nodes may be maintained by the DNS server 256. At block 264, the DNS server 256 updates a peer list of BGCF/MGCF nodes and/or a peer list of IBCF nodes by marking those nodes that respond with an error as being down or unavailable, fail to respond, or are otherwise unusable by the system. Alternately, the nodes that respond with acknowledgement and/or other data may be marked as being up or available. At block 266, the DNS server 256 uses the updated peer list to select an available target node IP address from the peer list. In one implementation, the DNS server 256 may use a round-robin scheduling, geographical scheduling, selection based on area code/Automatic Number Identification (“ANI”), or any other methods to select an available target node IP address to implement load sharing among the available nodes.

[0035] The DNS server 256 provides a response 268 that includes an IP address of the selected node to the DNS query from the E-CSCF 112. The E-CSCF 112 then sends an INVITE request message 274 towards the selected node 270. The selected node 270 acknowledges receiving the INVITE request message 274 by returning a “200 OK” message 276 to the E-CSCF 112. Depending on the node type, the selected node then forwards the SIP INVITE request message 278 to a PSAP with IP connectivity or an ISUP IAM 280 towards a PSAP with TDM connectivity. At block 282, the emergency call establishment is completed.

[0036] In one implementation, the DNS query 258 to the DNS server 256 may time out. When the DNS server 256 times out, without providing an IP address of the next hop for routing the emergency call request, the E-CSCF 112 may use a backup peer list to select a node and route the emergency call request via the selected node. If the selected node is down, the E-CSCF 112 may hunt down the peer list to select a different node for routing the emergency call until the SIP INVITE request message to a node is successfully acknowledged by the node. In one implementation, the E-CSCF 112 may take on the role of selecting a node for routing emergency calls until the DNS server comes back up.

[0037] Figure 3 is a logic flow diagram illustrating a method 300 for an emergency call route failover based on a dynamically created peer list in the IMS environment. In one implementation, at block 304, an E-CSCF 112 monitors the status of all remote

nodes (i.e., BGCFs/MGCFs and/or the IBCFs) using, e.g., the SIP OPTIONS method as described in detail with respect to Figure 2A. At block 302, the E-CSCF 112 receives a SIP INVITE request message for an emergency call. At block 306, the E-CSCF 112 dynamically creates a peer list for the emergency call request based on status information on the nodes, or uses a previously created peer list. The dynamic peer list may list only the available nodes in a specific order. Alternately, the dynamic peer list may list all the nodes in a specific order, but mark each node as being up (available) or down (unavailable). In another implementation, instead of dynamically creating a new peer list when an INVITE request arrives, a persistent or static peer list may be created and maintained by the E-CSCF 112. The static peer list may be periodically or continually updated as the E-CSCF 112 detects any change on the up or down status of the nodes.

[0038] At block 308, in one implementation, the E-CSCF 112 shifts the nodes up one place in the peer list for load balancing. By shifting the nodes up one place, the E-CSCF 112 avoids selecting the previously selected node for routing the emergency call. In an alternate implementation, the dynamic and/or static peer list may include a pointer, a bit increment or other indicator means for identifying the next node in the queue for selection. The shifting or tracking ensures that nodes selected for routing are constantly cycled and routing load is distributed among the available nodes. In one implementation, block 308 may be performed when the peer list is dynamically generated. The block 308 may be optional in some implementations. Other load balancing methods are of course possible.

[0039] At block 310, the E-CSCF 112 selects a node from the dynamic peer list to route the emergency call. The E-CSCF 112 may include additional information such as location of the caller, R-URI or other identifier of the PSAP, and the like before forwarding the INVITE request message to the IP address of the selected node. In response to the INVITE request message, the E-CSCF 112 may receive a response or no response at all. In one implementation, at decision block 312, if the emergency call is routed successfully to the selected node, as evidenced by receipt of an acknowledgement message (e.g., "200 OK") from the selected node, the E-CSCF 112 concludes the emergency call routing process and moves on to handle another emergency call at block 316. Alternately, if the emergency call routing is not successful, as evidenced by lack of a response from the selected node (e.g., 408 error code for

Request Timeout) or an error response (e.g., 503 error code for Service Unavailable), the E-CSCF 112 selects the next available node from the dynamic (or static) peer list and routes the emergency call to the selected node at block 314. The process of selecting the next available node from the dynamic or static peer list and attempting to route the emergency call may continue until a node responds with a success message. When another emergency call is received at block 316, the process moves to block 306, where a new peer list is dynamically created for the emergency call or a static peer list is accessed to select an available node for routing.

[0040] As described above, two peer lists may be created and/or maintained by or at the E-CSCF 112. One of the peer lists includes a list of BGCF/MGCF nodes that are available and the other includes a list of IBCF nodes that are available for emergency call routing. A BGCF/MGCF node helps route the emergency call to a PSAP in the PSTN by translating the SIP signaling to ISUP IAM. Similarly, an IBCF node accepts SIP signaling and helps route the emergency call to a PSAP in an IP network. In one embodiment, to implement an emergency call route failover in both situations, the E-CSCF 112 may implement a method 400 illustrated in Figure 4 to select a peer list based on the border node (e.g., IBCF on SBC) in the IMS environment.

[0041] In one implementation, at block 402, the E-CSCF 112 receives an emergency call request (i.e., a SIP INVITE) from the P-CSCF 110. At block 404, the E-CSCF 112 obtains a steering key for steering digits (e.g., ESRK or an E-164 number) associated with the emergency call. As previously described, each LRF 126 (or another location server) may allocate ESRK numbers from a different unique range of numbers to an emergency call. At decision block 406, the E-CSCF 112 determines if the ESRK from the LRF matches the ESRK ranges in a flat file (or any other type of file or record) that the E-CSCF 112 has access to. If there is no match, the emergency call is identified as a phase 0 call. A phase 0 call is routed to an appropriate PSAP without location information. A phase 0 PSAP may handle only phase 0 emergency calls and may not have the facilities to request additional information about the emergency call from the LRF. For example, a state highway patrol PSAP or a small town PSAP may only accept phase 0 emergency calls. At block 424, the phase 0 call is classified as an emergency call and routed to the appropriate PSAP with caller ID information at block 426.

[0042] Alternately, at decision block 406, the E-CSCF 112 may determine that the ESRK from the LRF matches the ESRK ranges in the file. At block 408, the E-CSCF allocates an ESRK from a range of ESRK numbers associated with the PSAP. For example, a range of ESRK numbers may be associated with a New York Police Department (“NYPD”) PSAP. Emergency calls going to the NYPD PSAP are assigned an ESRK number from the range in sequence to allow each emergency call to be uniquely identified. The PSAP uses the ESRK number in the emergency call request to obtain location and other information (e.g., Global Positioning System coordinates) from the E-CSCF 112 or the LRF, for example.

[0043] At decision block 410, the E-CSCF 112 determines whether an IBCF ID or an SBC ID is present. An IBCF ID may be an identifier, an FQDN, an IP address, or the like that indicates that the emergency call is to be routed via an IBCF to a PSAP in another IP network. In one implementation, the IBCF ID may be included in the routing header of the SIP INVITE request message as a hop in the path of the emergency call. In another implementation, the IBCF ID may be provided by the LRF 126, for example. If the IBCF ID is present, the E-CSCF 112 selects an IBCF node from a static peer list of IBCF nodes. In one implementation, a dynamic peer list including IBCF nodes that are available may be created or generated. At block 420, the E-CSCF modifies the emergency call request message (e.g., INVITE) to include or change some information in the emergency call request message. For example, the emergency call request message may be adjusted to include the assigned ESRK as the R-URI, the IP address of the selected IBCF node in the routing header, or the like. At block 422, the E-CSCF 112 forwards the emergency call request message to the selected IBCF node for routing towards a PSAP associated with the ESRK.

[0044] In another implementation, if the IBCF ID is not present, the E-CSCF 112 selects a BGCF/MGCF node from a static peer list of BGCF/MGCF nodes. In one implementation, a dynamic peer list including available BGCF/MGCF nodes may be created. At block 414, the E-CSCF 112 modifies the emergency call request message to include the ESRK, the IP address of the selected BGCF/MGCF node, or the like. The E-CSCF 112 forwards the emergency call request message to the selected MGCF node for routing to an appropriate PSAP associated with the ESRK at block 416.

[0045] Similar methodology may be implemented by a DNS server when the DNS server is responsible for monitoring availability of remote nodes, and selecting a route option from the available remote nodes.

[0046] Figure 5 is a diagrammatic representation of a machine in the example form of a computer system or machine 500 within which a set of instructions, when executed, may cause the machine to perform any one or more of the methods (e.g., methods 300 and 400) described above.

[0047] In some embodiments, the machine 500 operates as a standalone device, while in other embodiments, the machine 500 may be connected (e.g., networked) to other machines. In a networked deployment, the machine may operate in the capacity of a server or a client user machine (e.g., UE102) in a client-server network environment, or as a peer machine in a peer-to-peer (or distributed) network environment.

[0048] The machine may comprise a server computer, a client computer, a personal computer (PC), a tablet PC, a laptop computer, a set-top box ("STB"), a personal digital assistant ("PDA"), a cellular telephone, a smart phone, a telephone, a web appliance, a network router, switch or bridge, a console, a hand-held console, a (hand-held) gaming device, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine. In general the machine 500 includes any electronic devices that provide voice, video and data communication. In one embodiment, the machine 500 may include the SIP servers or proxies (e.g., S-CSCF 106, I-CSCF 108, P-CSCF 110, E-CSCF 112, BGCF/MGCF 114, IBCF 116, and the like). While a single machine is illustrated, the machine 500 may include any collection of machines that individually or jointly execute instructions to perform any of the methods described above.

[0049] The machine 500 may include a processor 502, a main memory 506 and a bus 524. The bus 524 is a subsystem for transferring data between the components of the machine 500, including transferring data between the main memory 506 and the processor 502. The bus 524 may represent one or more separate physical buses, point to point connections, or both, connected by appropriate bridges, adapters, or controllers. The machine 500 may also include a display device 514 (e.g., Liquid Crystal Display ("LCD"), Cathode Ray Tube ("CRT"). etc.), one or more input devices

516 (e.g., a keyboard, a touch screen, etc.), a cursor control device 518 (e.g., a mouse), a drive unit 520, a signal generation device or output device 522 (e.g., a speaker, a remote control, etc.) and a network interface device 510, among others.

[0050] The processor(s) 502 (e.g., a Central Processing Unit (“CPU”), a Graphics Processing Unit (“GPU”), or both) controls the overall operation of the machine 500. The processor(s) 502 executes computer programs or firmware stored in memory (e.g., 506, 520). The processor(s) 502 may include, one or more programmable general-purpose or special-purpose microprocessors, digital signal processors (“DSPs”), programmable controllers, application specific integrated circuits (“ASICs”), programmable logic devices (“PLDs”), trusted platform modules (“TPMs”), or the like, or a combination thereof.

[0051] The main memory 506 represents any form of random access memory (“RAM”), read-only memory (“ROM”), flash memory, or the like, or a combination of such devices connected to the bus 524. The drive unit 520 may include a machine-readable medium or machine-readable storage medium that stores, encodes or carries one or more sets of instructions for execution by the machine 500 to perform any or all of the methods described above. It should be noted that the term “machine-readable medium” and “machine-readable storage medium” may include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions embodying any or all of the methods described above. Examples of machine-readable media or machine-readable storage media include, but are not limited to: recordable type media such as volatile (e.g., RAM, non-volatile memory devices (e.g., ROM), the main memory 506, solid state memories, floppy and other removable disks, hard disks, optical disks (e.g., Compact Disk Read-Only Memory (“CD ROMS”), Digital Versatile Disks, (“DVDs”), etc.), or the like.

[0052] In general, the routines executed to implement the embodiments of the disclosure, may be implemented as part of an operating system or a specific application, component, program, object, module or sequence of instructions referred to as “computer programs.” The computer programs typically comprise one or more instructions set at various times in various memory and storage devices in a computer, and that, when read and executed by one or more processing units or processors in a

computer, cause the computer to perform operations to execute elements involving the various aspects of the disclosure.

[0053] The network interface device 510 allows the machine 500 to mediate data in various networks with one or more entities that are external to the machine, through any known and/or convenient communications standards and protocols supported by the machine 500 and the external entities. Example protocols supported by the machine 500 includes, but is not limited to: IP protocols for the application layer (e.g., SIP, Session Description Protocol (“SDP”), Real Time Transport Protocol (“RTP”), Hypertext Transfer Protocol (“HTTP”), SNMP, etc.), transport layer protocols (e.g., Transmission Control Protocol (“TCP”), User Datagram Protocol (“UDP”), etc.), Internet layer protocols (e.g., IPv4, IPv6, etc.), link layer protocols (e.g., Digital Subscriber Line (“DSL”), Ethernet, etc.), or the like. The network interface device 510 can include one or more of a network adaptor card, a wireless network interface card, a router, an access point, a wireless router, a switch, a multilayer switch, a protocol converter, a gateway, a bridge, bridge router, a hub, a digital media receiver, a repeater, or other interfaces for supporting the various protocols. Although the present disclosure describes the components and functions implemented in the embodiments with reference to particular standards and protocols that represent examples of the state of the art, the disclosure is not limited to such standards and protocols, and includes functional equivalents that may supersede the current state of the art.

[0054] The above detailed description of embodiments of the disclosure is not intended to be exhaustive or to limit the teachings to the precise form disclosed above. While specific embodiments of, and examples for, the disclosure are described above for illustrative purposes, various equivalent modifications are possible within the scope of the disclosure, as those skilled in the relevant art will recognize. For example, while processes or blocks are presented in a given order, alternative embodiments may perform routines having steps, or employ systems having blocks, in a different order, and some processes or blocks may be deleted, moved, added, subdivided, combined, and/or modified to provide alternative or subcombinations. Each of these processes or blocks may be implemented in a variety of different ways. Also, while processes or blocks are at times shown as being performed in series, these processes or blocks may instead be performed in parallel, or may be performed at different times.

[0055] The teachings of the invention provided herein can be applied to other systems, not necessarily the system described above. The elements and acts of the various examples described above can be combined to provide further implementations of the invention. Some alternative implementations of the invention may include not only additional elements to those implementations noted above, but also may include fewer elements. Any patents and applications and other references noted above, including any that may be listed in accompanying filing papers, are incorporated herein by reference. Aspects of the invention can be modified, if necessary, to employ the systems, functions, and concepts of the various references described above to provide yet further implementations of the invention.

[0056] To reduce the number of claims, certain aspects of the invention are presented below in certain claim forms, but the applicant contemplates the various aspects of the invention in any number of claim forms. For example, while only one aspect of the invention is recited as a means-plus-function claim under 35 U.S.C. sec. 112, sixth paragraph, other aspects may likewise be embodied as a means-plus-function claim, or in other forms, such as being embodied in a computer-readable medium. (Any claims intended to be treated under 35 U.S.C. §112, ¶6 will begin with the words “means for”, but use of the term “for” in any other context is not intended to invoke treatment under 35 U.S.C. §112, ¶6.) Accordingly, the applicant reserves the right to pursue additional claims after filing this application to pursue such additional claim forms, in either this application or in a continuing application.

CLAIMS

We claim:

1. A computer-implemented method of performing an emergency call route failover within a telecommunications network, the method comprising:
 - receiving a Session Initiation Protocol (SIP) request associated with an emergency call;
 - initiating a SIP OPTION message towards each of multiple gateway nodes;
 - determining a status of each of the multiple gateway nodes based on the initiated SIP OPTION message; and
 - based on the determined status, removing one or more gateway nodes from a list of the multiple gateway nodes,
 - wherein the list provides one or more routing options for the received SIP request associated with the emergency call.

2. The method of claim 1, further comprising:
 - selecting a gateway node from the list of one or more routing options; and
 - forwarding a SIP request associated with the emergency call to the selected gateway node to provide the emergency call to an emergency network or emergency network node,wherein the multiple gateway nodes are Media Gateway Control Function (MGCF) nodes when the emergency network has Time Division Multiplex (TDM) connectivity, and
wherein the multiple gateway nodes are Interconnection Border Control Function (IBCF) nodes when the emergency network has Internet Protocol (IP) connectivity.

3. The method of claim 1, further comprising:
 - selecting a gateway node from the list of one or more routing options; and
 - forwarding a SIP request associated with the emergency call to the selected gateway node to provide the emergency call to an emergency network or emergency network node.

4. The method of claim 1, wherein the determining includes determining a failed status as detected when a gateway node from the multiple gateway nodes provides a response indicating server failure in response to the SIP OPTION message.

5. The method of claim 1, wherein the determining includes:
determining a failed status as detected when a gateway node from the multiple gateway nodes fails to provide a response to the SIP OPTION message within a predefined amount of time; and,
generating a request timeout error when no response is received from the selected gateway node.

6. The method of claim 1, wherein the determining includes:
determining a failed status as detected when a gateway node from the multiple gateway nodes fails to provide a response to the SIP OPTION message within a predefined amount of time.

7. The method of claim 6, further comprising:
failing over to a new gateway node selected from the one or more routing options by sending a SIP request associated with the emergency call to the new gateway node.

8. The method of claim 6, further comprising:
failing over to a new gateway node selected from the one or more routing options by sending a SIP request associated with the emergency call to the new gateway node,
wherein the one or more routing options are arranged in a specific order, and the new gateway node is selected to load balance distribution of emergency calls among the one or more routing options.

9. The method of claim 1, wherein the SIP OPTION message is initiated towards each of the multiple gateway nodes at a preconfigured frequency to monitor the status of each of the multiple gateway nodes, and

wherein the method further comprises adding one or more gateway nodes having a success status and that are not among the one or more routing options to the list based on the monitoring.

10. A system for implementing redundancy in routing emergency calls via gateway nodes in an Internet Protocol Multimedia Subsystem (IMS) network, comprising:

at least one processor;

an Emergency Call Session Control Function (E-CSCF) executed by the processor and configured to:

receive a Session Initiation Protocol (SIP) INVITE request associated with an emergency call;

dynamically create a peer list including gateway nodes that successfully respond to a SIP OPTIONS request;

select a gateway node from the peer list; and

initiate a SIP INVITE request associated with the emergency call towards the selected gateway node to deliver the emergency call to a public safety answering point (PSAP).

11. The system of claim 10, wherein the E-CSCF is further configured to: determine, based on presence or absence of information relating to Interconnection Border Control Function (IBCF) or Session Border Controller (SBC), whether to dynamically create the peer list including IBCF servers as gateway nodes or Border Gateway Control Function (BGCF) servers or Media Gateway Control Function (MGCF) servers as gateway nodes.

12. The system of claim 10, wherein the E-CSCF is further configured to: detect a failover condition when the selected gateway node fails to respond to the SIP INVITE request within a time period; and in response to the failover condition, continue to select a new gateway node from the peer list and initiate a SIP INVITE request associated with the

emergency call towards the new gateway node until a successful response to the SIP INVITE request is received by the E-CSCF.

13. The system of claim 10, wherein the E-CSCF is further configured to: obtain, from a location server, routing information for the PSAP, wherein the routing information for the PSAP includes routing information for a Public Switched Telephone Network (PSTN) PSAP or an Internet Protocol (IP) PSAP, and

wherein the routing information for the PSTN PSAP or the IP PSAP includes an Emergency Service Routing Key (ESRK) that is used by the PSTN PSAP or the IP PSAP to request location information associated with the emergency call.

14. At least one tangible machine-readable medium storing instruction, which when executed by at least one computer, analyzes nodes for use with emergency call routing in an Internet Protocol Multimedia Subsystem ("IMS") network, comprising:

receiving a Session Initiation Protocol (SIP) request associated with an emergency call;

determining a status of each of multiple gateway nodes; and,

based on the determined status, adjusting a status of one or more gateway nodes in a list of gateway nodes,

wherein the list provides one or more routing options for the received SIP request associated with the emergency call.

15. The least one tangible machine-readable medium of claim 14, further comprising:

initiating, by an Emergency Call Session Control Function (E-CSCF), a Domain Name System (DNS) request to determine a routing option for routing the emergency call;

detecting a DNS request time out event; and

in response to the detected DNS request time out event,

selecting a routing option from the list of routing options; and

initiating a Session Initiation Protocol (SIP) INVITE request for the emergency call towards the selected routing option.

16. The least one tangible machine-readable medium of claim 14, wherein the determining includes:

initiating a SIP OPTION message towards each of the multiple gateway nodes;
determining a status of each of the multiple gateway nodes based on the initiated SIP OPTION message, and

wherein the list of routing options includes Media Gateway Control Function (MGCF) servers, or Border Gateway Control Function (BGCF) servers which select MGCF servers, or Interconnection Border Control Function (IBCF) servers.

17. The least one tangible machine-readable medium of claim 14, further comprising:

selecting a routing option from the list of routing options; and
detecting a failover condition when the selected routing option provides an error response or the selected routing option fails to provide a response within a time duration.

18. The least one tangible machine-readable medium of claim 14, further comprising:

selecting next routing option from the list of routing options; and
initiating a Session Initiation Protocol (SIP) INVITE request for the emergency call towards the selected routing option.

19. A system for performing an emergency call route failover, comprising:
at least one processor;
means for initiating a request towards each of multiple gateway nodes;
means for identifying one or more gateway nodes from the multiple gateway nodes,

wherein the means for identifying identifies nodes as being available to receive an emergency call, as being unavailable to receive an emergency call, or both;

means for receiving a Domain Name System (DNS) request from an Emergency Call Control Session Function (E-CSCF);

means for selecting a gateway node to receive an emergency call; and

means for providing the selected gateway node as a response to the DNS request.

20. The system of claim 19, further comprising:

means for determining that the emergency call is associated with a gateway node of a specific type; and

means for selecting the available gateway nodes of the specific type to dynamically create a list of available nodes

wherein the specific type is one of: a Border Gateway Control Function (BGCF), Media Gateway Control Function (MGCF) or an Interconnection Border Control Function (IBCF).

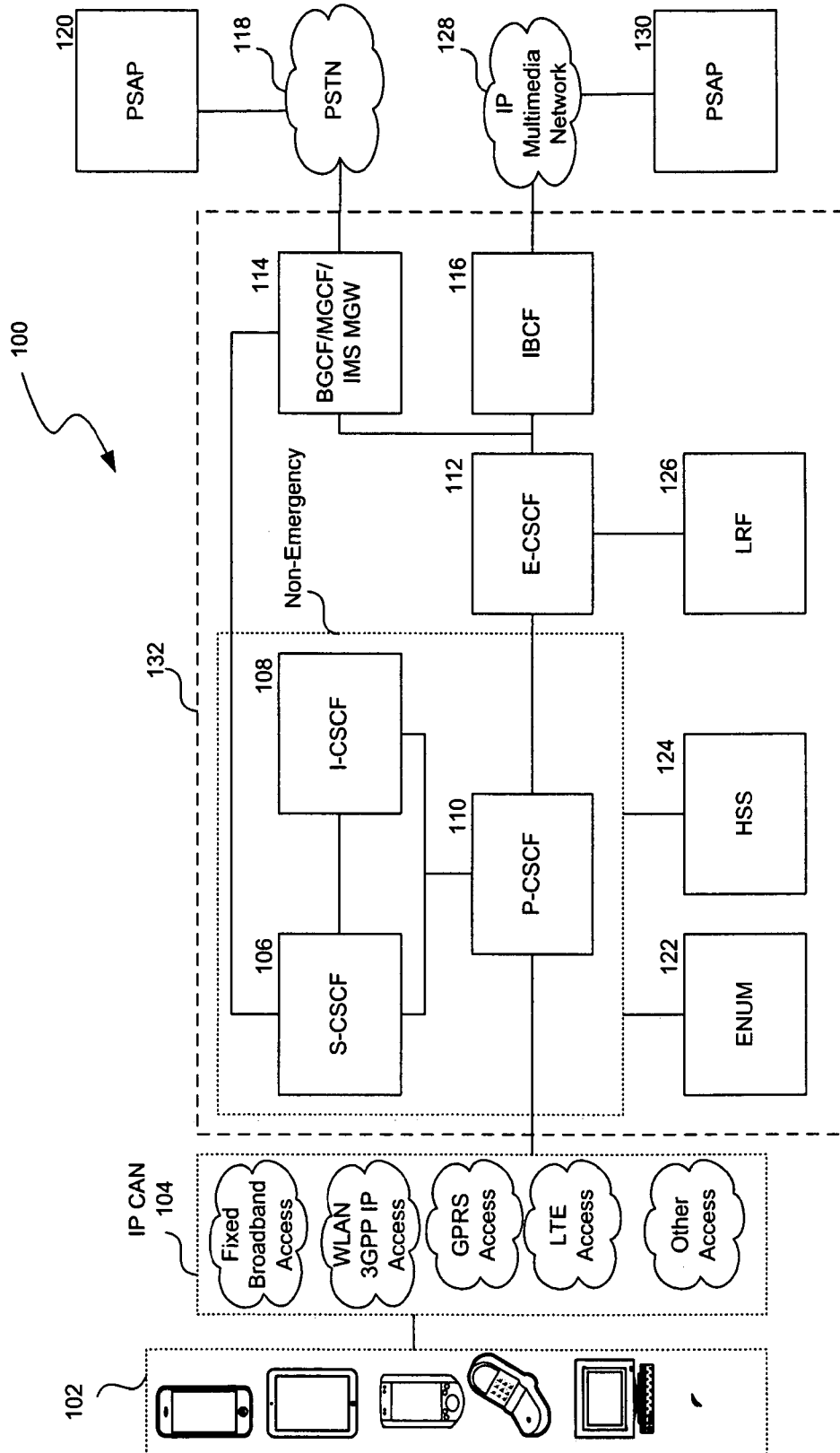


FIG. 1

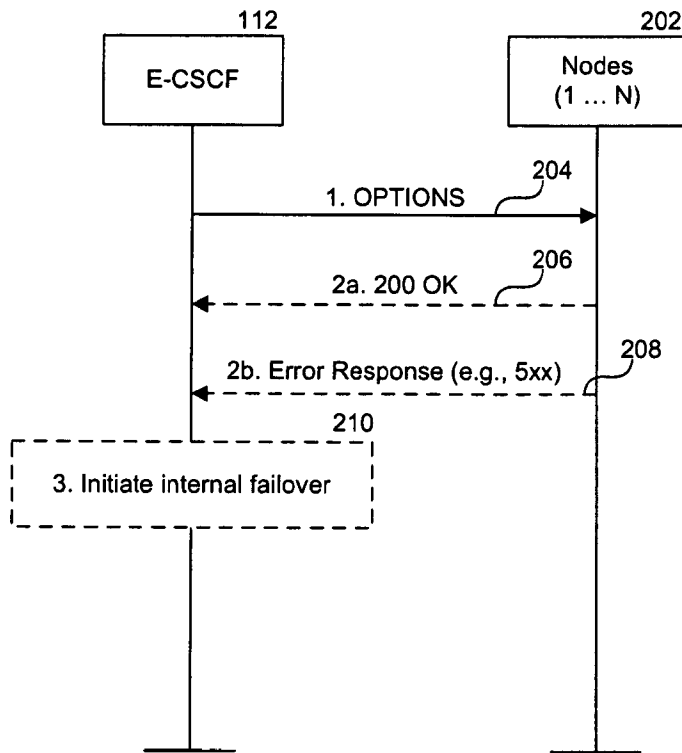


FIG. 2A

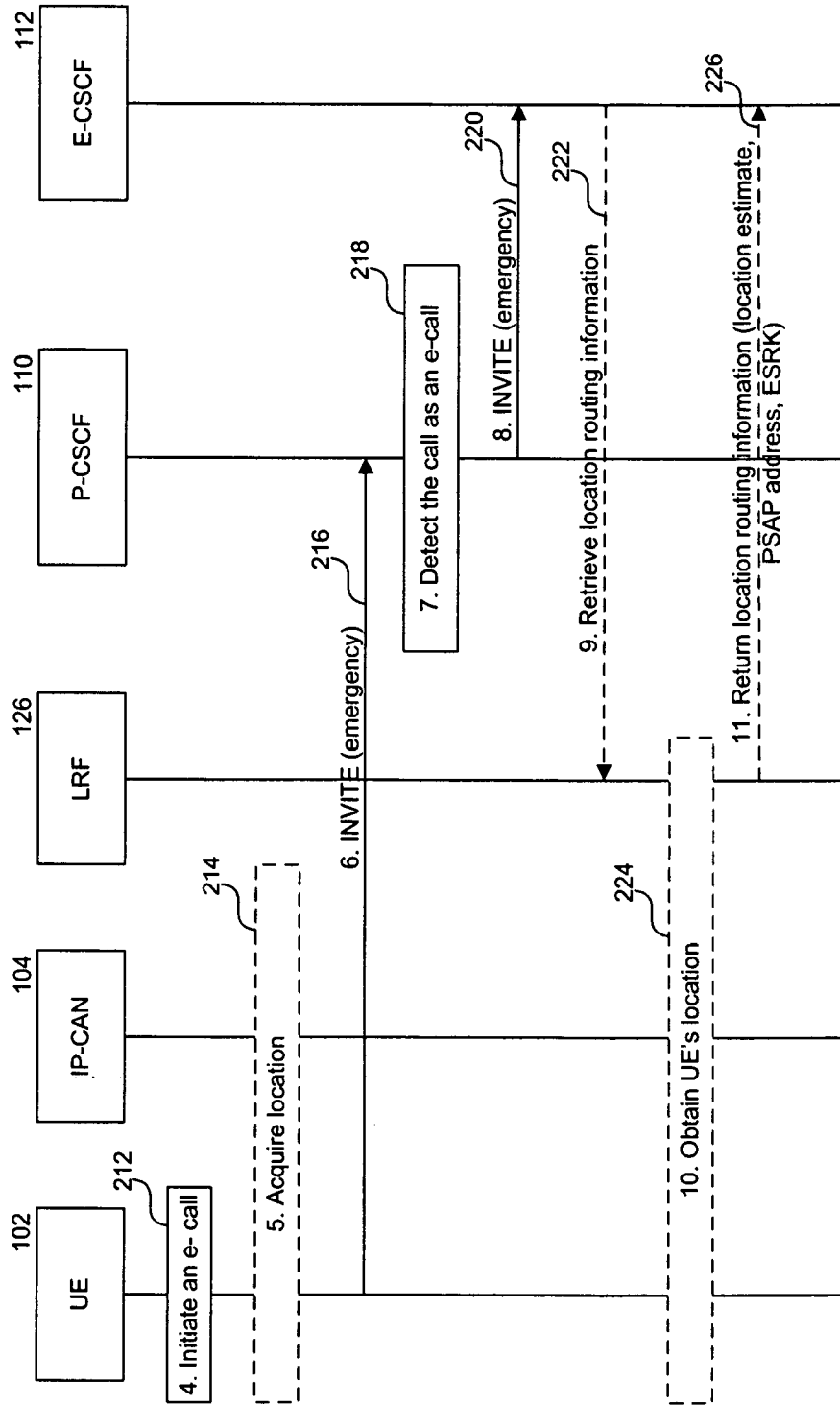


FIG. 2B

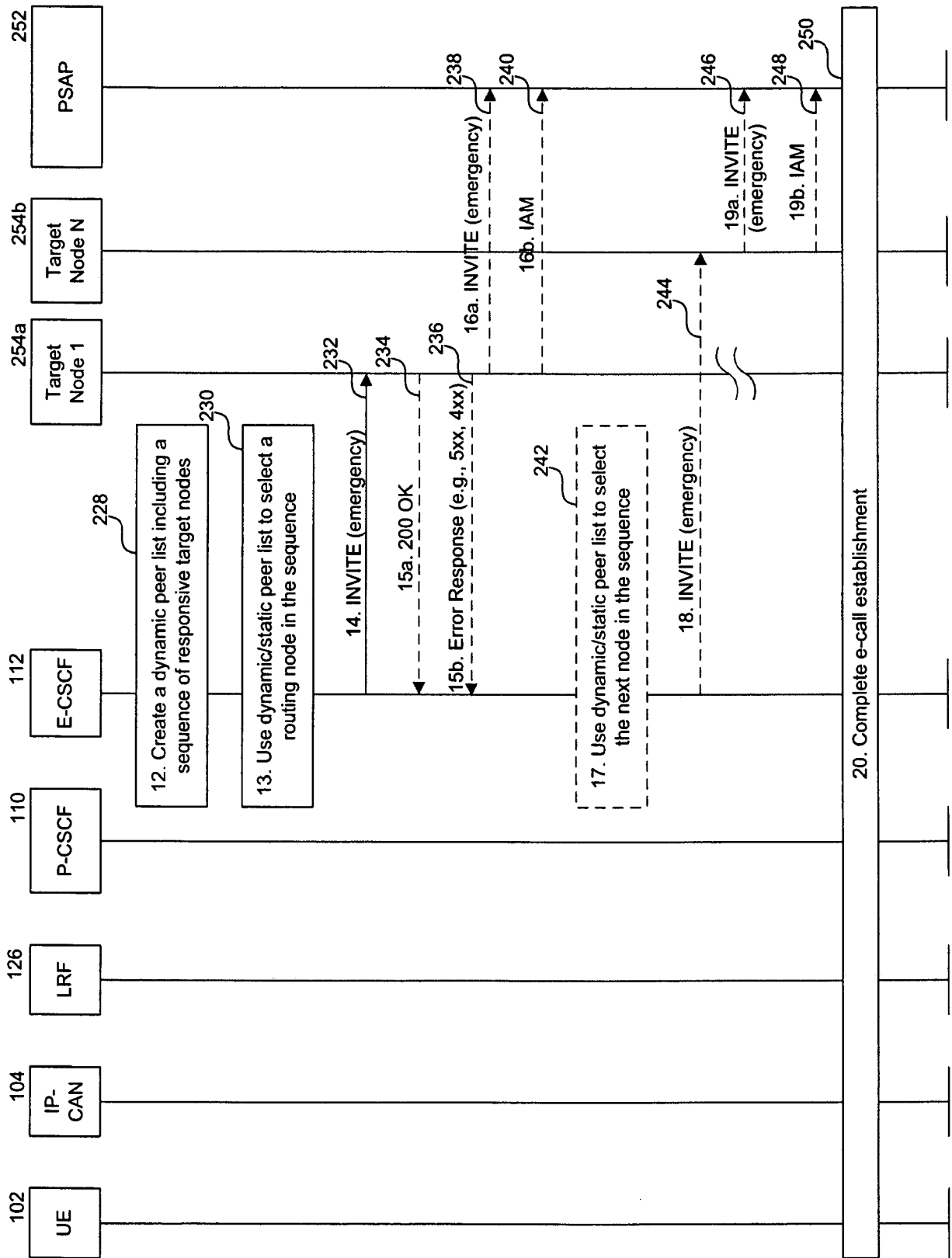


FIG. 2C

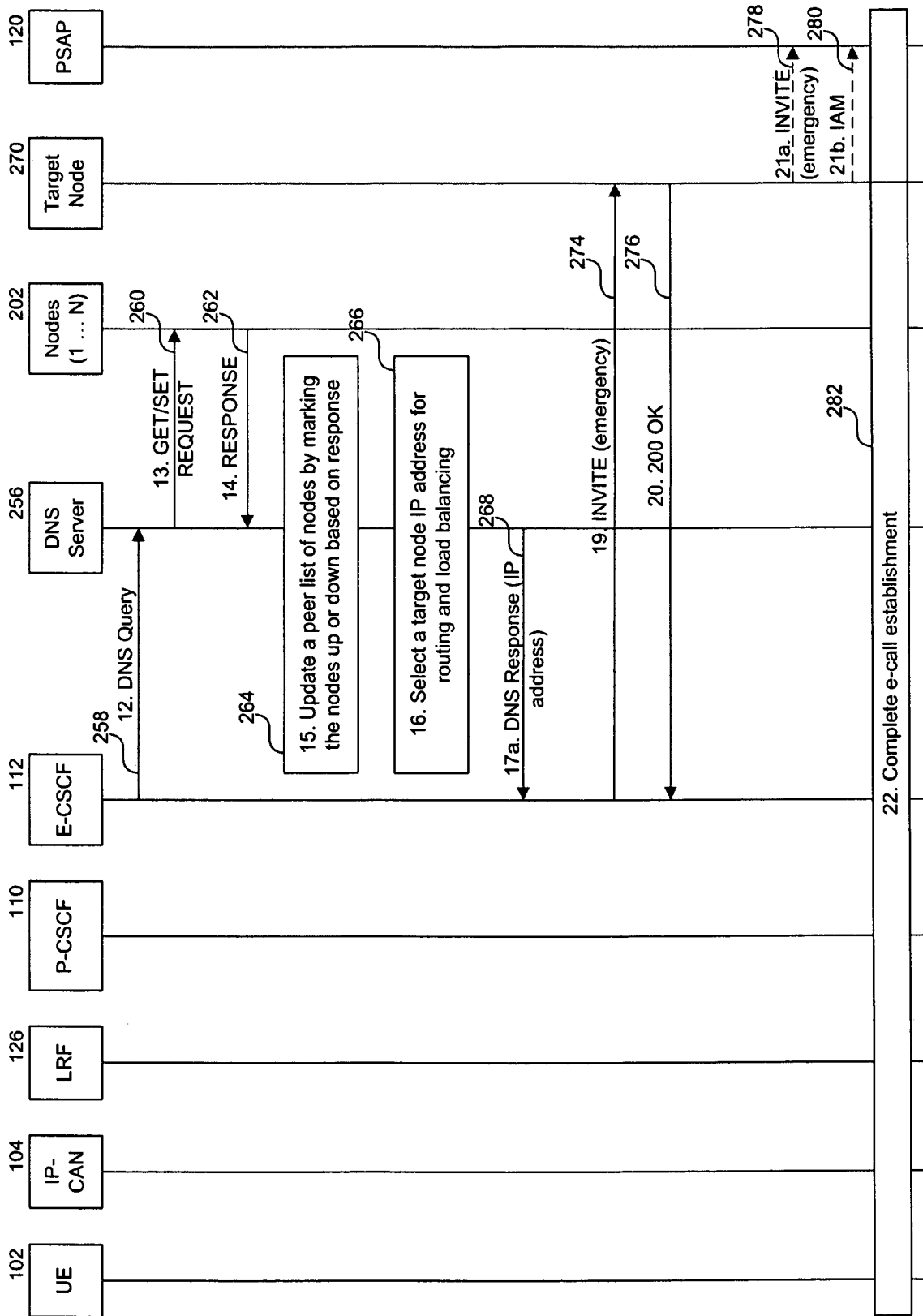


FIG. 2D

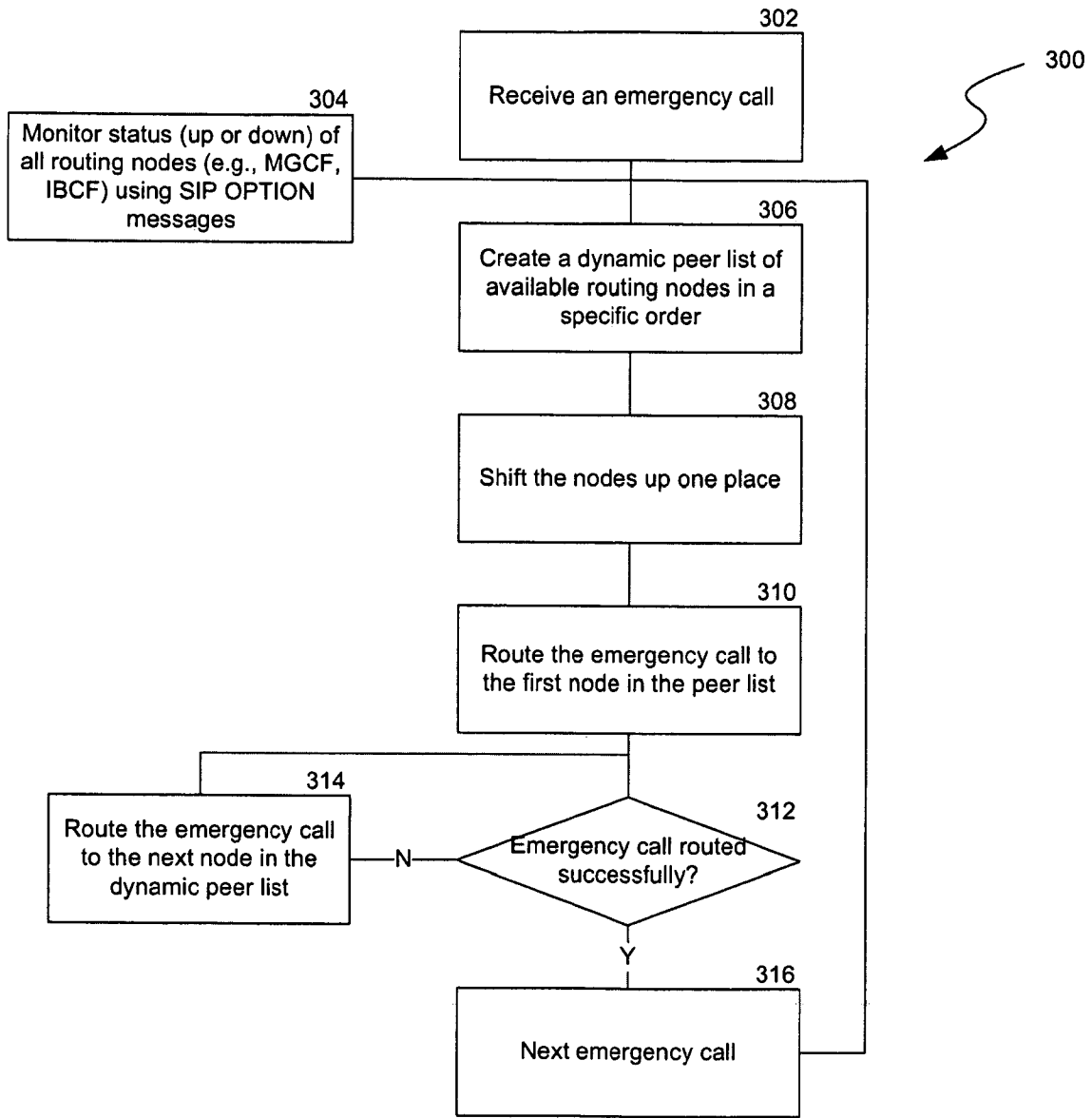


FIG. 3

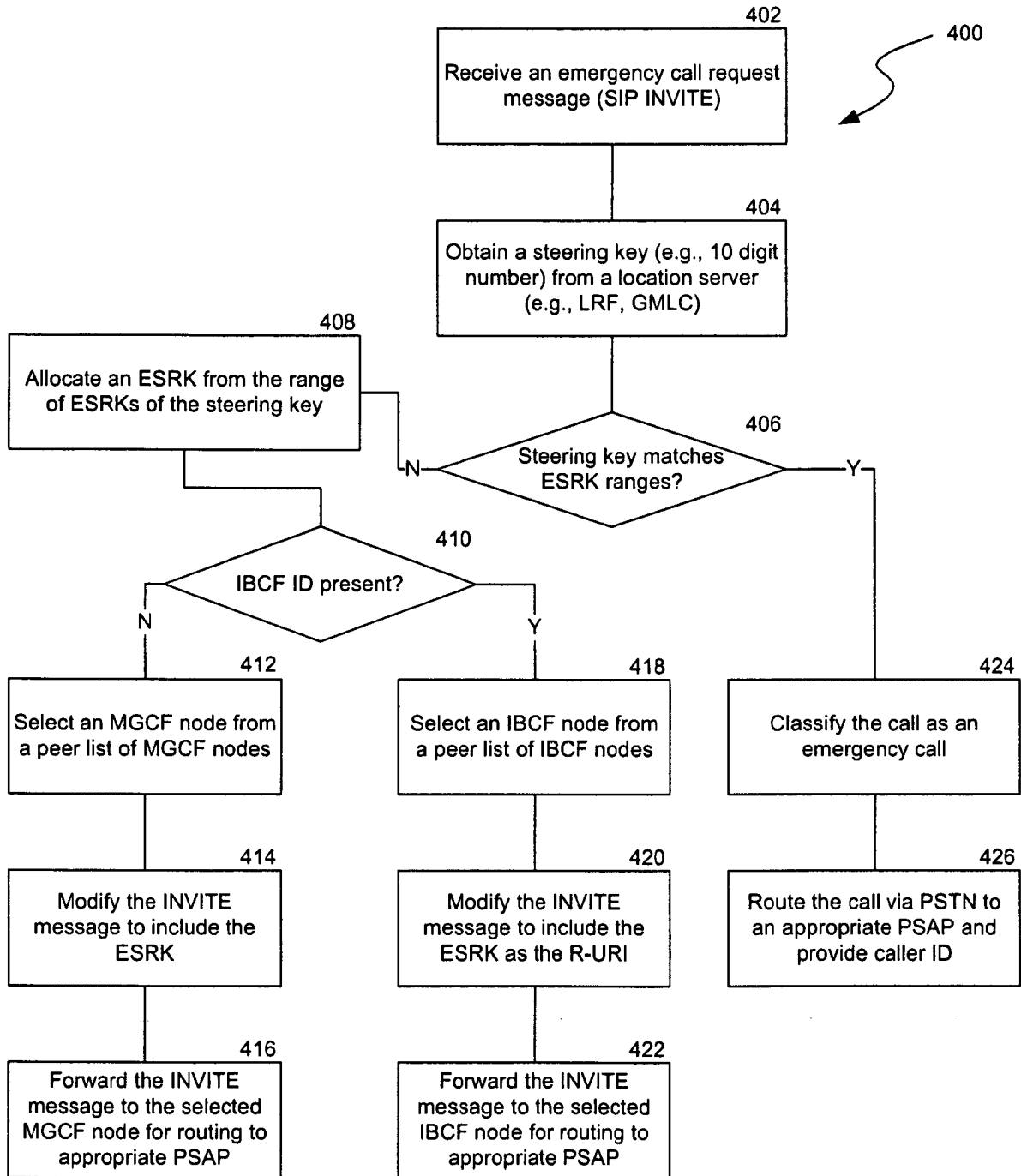


FIG. 4

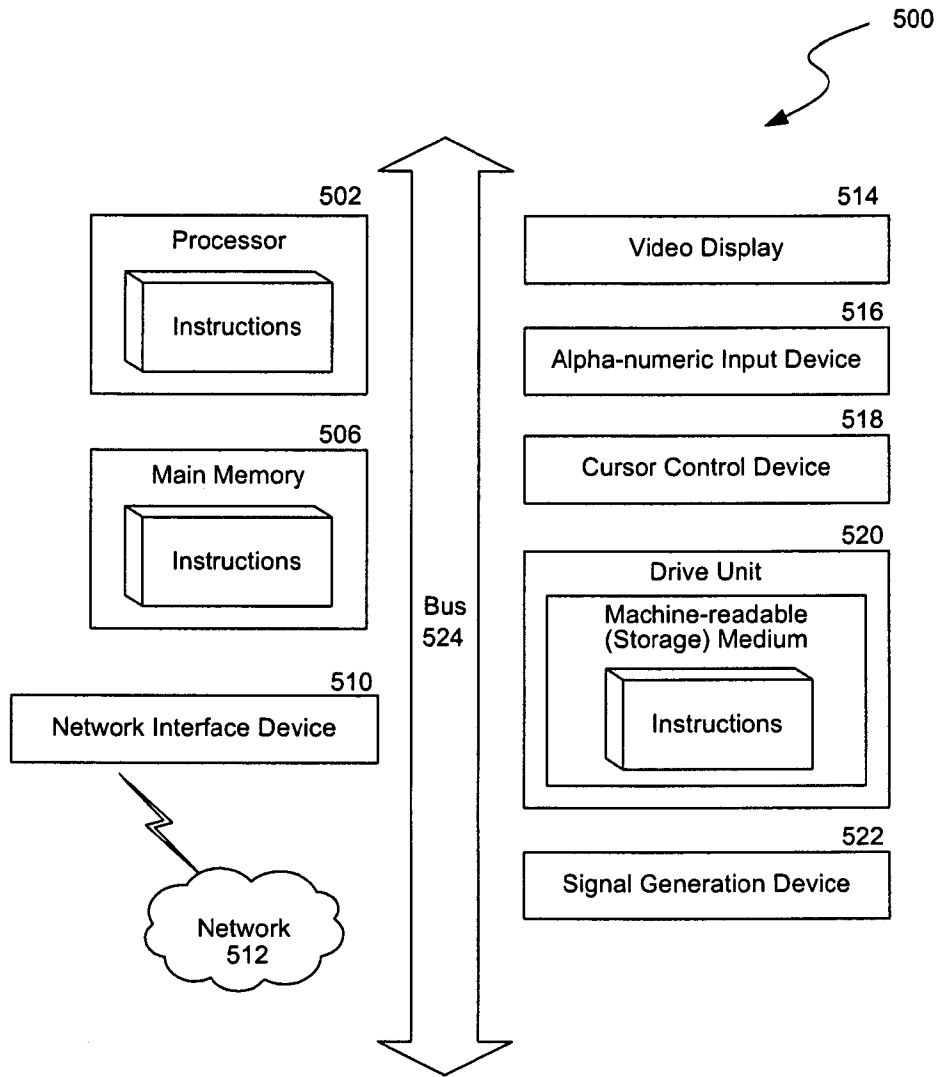


FIG. 5

A. CLASSIFICATION OF SUBJECT MATTER**H04L 12/24(2006.01)i, H04L 29/06(2006.01)i**

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 12/24; H04W 4/22; G06F 15/16; H04Q 7/00; H04M 11/04; H04L 12/66; H04W 80/10; H04L 29/06

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & keywords: emergency, session, route, list

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2013-0029634 A1 (MINGXING LI) 31 January 2013 See paragraphs [0012]-[0015], [0031], [0053], [0059]-[0060], claims 1-2 and figures 1, 5.	1-20
Y	US 2009-0245183 A1 (AL BAKER et al.) 01 October 2009 See paragraphs [0047], [0072], [0085]-[0098], [0104] and figures 1, 3.	1-20
A	JP 2012-169872 A (NTT DOCOMO INC.) 06 September 2012 See abstract, claims 1-8 and figure 4.	1-20
A	US 2012-0269188 A1 (JAY MERANCHIK) 25 October 2012 See abstract, paragraphs [0018]-[0027] and figures 1-2.	1-20
A	US 2012-0179829 A1 (RICHARD JOHN GEORGE) 12 July 2012 See abstract, paragraphs [0049]-[0050], claim 1 and figures 10-11.	1-20

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

18 June 2014 (18.06.2014)

Date of mailing of the international search report

23 June 2014 (23.06.2014)

Name and mailing address of the ISA/KR

International Application Division
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

KIM, Seong Woo

Telephone No. +82-42-481-3348



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/018797

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013-0029634 A1	31/01/2013	None	
US 2009-0245183 A1	01/10/2009	BR PI0903066 A2 CN 101557393 A CN 101557393 B EP 2111015 A1 EP 2111015 B1 JP 05008647 B2 JP 2009-239892 A KR 10-1387287 B1 KR 10-2009-0102621 A MX 2008015826 A US 8107361 B2	13/07/2010 14/10/2009 12/03/2014 21/10/2009 20/06/2012 22/08/2012 15/10/2009 28/04/2014 30/09/2009 25/09/2009 31/01/2012
JP 2012-169872 A	06/09/2012	CN 103339970 A EP 2677782 A1 JP 05456708 B2 US 2013-0309993 A1 WO 2012-111473 A1	02/10/2013 25/12/2013 02/04/2014 21/11/2013 23/08/2012
US 2012-0269188 A1	25/10/2012	US 2010-260170 A1 US 8228901 B2	14/10/2010 24/07/2012
US 2012-0179829 A1	12/07/2012	CA 2823653 A1 EP 2475145 A1 WO 2012-092670 A1	12/07/2012 11/07/2012 12/07/2012