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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 August 2013 (22.08.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/120513 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 12/26* (2006.01)
H04L 12/24 (2006.01)

(21) International Application Number:
PCT/EP2012/052516

(22) International Filing Date:
14 February 2012 (14.02.2012)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)** [SE/SE]; SE-164 83 Stockholm (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **OLROG, Christian** [SE/SE]; Eriksbergsgatan 38, S-114 30 Stockholm (SE).

(74) Agent: **BARRETT, Peter Andrew John**; Ericsson Limited, Patent Unit Optical Networks, Unit 4 Midleton Gate, Guildford Business Park, Guildford Surrey GU2 8SB (GB).

(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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

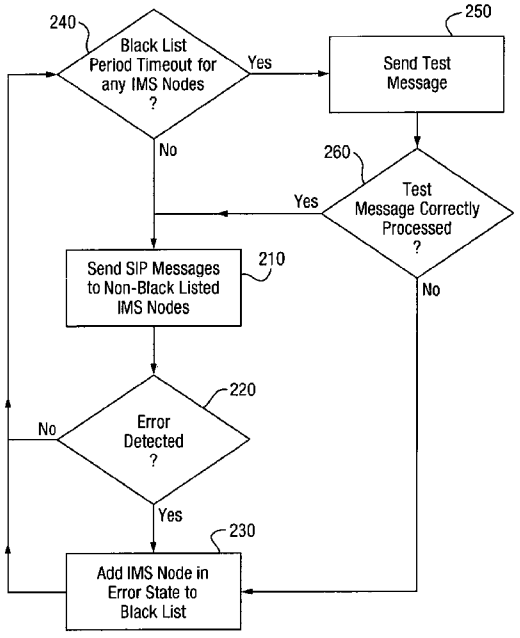
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR,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

Published:

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

(54) **Title**: METHOD AND APPARATUS FOR IMPROVED HANDLING OF IMS NODE BLACKLISTING

Fig. 2



(57) **Abstract**: Accordingly, there is provided an IMS node, comprising a transmission module and a processor. The transmission module is arranged to send SIP messages to a plurality of other IMS nodes. The processor arranged to detect an error in a particular other IMS node, the error indicating that the particular other IMS node is not available to receive traffic. In response to detection of such an error, the processor causes the particular other IMS node not to be used for a period of time. The transmission module is further arranged to send at least one test message to the particular other IMS node when the period of time expires. The processor is further arranged to determine if the at least one test message is successfully processed by the particular other IMS node, and in response to a positive determination then returning the particular other IMS node to use.

WO 2013/120513 A1

METHOD AND APPARATUS FOR IMPROVED HANDLING OF IMS NODE BLACKLISTING

Technical field

The present application relates to an IP Multimedia Subsystem (IMS) node, a method in an IMS node, and a computer-readable medium.

Background

In an IMS network, routing is used to find a user or a function in the network. The main mechanism used for routing in the IMS network is DNS. In operation a first IMS node may attempt to send a message to a second IMS node. If the second IMS node is, for some reason, not available to receive traffic it might be added to a blacklist maintained at the first IMS node. The second IMS node may indicate to the first IMS node that it is not available to receive traffic, or the first IMS node may detect the second IMS node is unavailable by the behaviour of the second IMS node.

Depending on the reason for blacklisting, an entire host or individual ports of a host (including its transport protocols) may have to be blacklisted. An IMS node is blacklisted for a predetermined period of time. The period of time may be determined according to the event that triggered the blacklisting.

As a faulting host is removed from a blacklist a large number of calls may fail. For example, consider a system whereby a first IMS node comprising a Call Session Control Function (CSCF) distributes Session Initiation Protocol (SIP) calls to two hosts which are a second and third IMS node. The CSCF has a call load of 100 Calls per second (Cps) and these are distributed over the two hosts round robin. If one of the hosts fails (e.g. the second IMS node enters an error state due to power failure), then 50% of calls will be directed towards the faulty host until the error state is detected and the failed host (the second IMS node) is blacklisted. Once the failed node is blacklisted then current implementations require that it is removed from the blacklist when the appropriate period of time has elapsed. Typically, after a few initial short trials

on the order of 30 seconds the CSCF will remove the failed host from the blacklist every 10 minutes on the assumption that by that time the failed host will have recovered.

If the failed host is in an error state for a prolonged period, then each time it is removed from the blacklist the error state will be detected again and the failed host will be blacklisted again.

Each time the failed host is removed from the blacklist it typically takes 32 seconds to detect that it has not yet recovered. (32 seconds is the SIP Transaction timeout default.) If we assume that anything above 10 seconds is considered a lost call, then 100Cps x ½ x 22 seconds = 1100 call setups lost before the failed host is again blacklisted. Accordingly, current arrangements require that a large number of call setups are lost every time a failed host is removed from blacklist before it has recovered from an error state. Lost call setups reduce the effectiveness of the network and also have a negative impact on the quality of service for the end users.

For at least the above reasons, there is a need for a method and apparatus for improved handling of IMS node blacklisting.

Summary

Accordingly, there is provided an IMS node, comprising a transmission module and a processor. The transmission module is arranged to send SIP messages to a plurality of other IMS nodes. The processor is arranged to detect an error in a particular other IMS node, the error indicating that the particular other IMS node is not available to receive traffic. In response to detection of such an error, the processor causes the particular other IMS node not to be used for a period of time. The transmission module is further arranged to send at least one test message to the particular other IMS node when the period of time expires. The processor is further arranged to determine if the at least one test message is successfully processed by the particular other IMS node, and in response to a positive determination then returning the particular other IMS node to use.

Prior art IMS nodes simply return the particular node to use upon expiry of the period of time for which the particular other IMS node is not used. If, at that time, the particular other IMS node is still in an error state then the prior art IMS node will detect further errors and the particular other IMS node is then not used for another period of time. A problem with the prior art arrangement is that there is a significant time delay in the detection of the error status in the particular other IMS node. A significant number of messages can be sent to the particular other IMS node during the time delay between it being returned to use and the error state being re-detected. All messages sent to the particular other IMS node during the period of the time delay are not properly processed and can result in network errors such as lost call setups.

The method and apparatus disclosed herein greatly reduces the number of network errors created by an IMS node experiencing an error state by testing an IMS node before returning it to use.

Causing the particular other IMS node not to be used for a period of time may comprise removing the particular other IMS node from use for a period of time. Causing the particular other IMS node not to be used may be achieved by blacklisting the particular other IMS node.

The transmission module may be further arranged to send SIP messages to other IMS nodes that are not blacklisted. The transmission module may be further arranged to send at least one test message to the particular other IMS node if incoming activity from the particular other IMS node is detected during the period of time for which the particular other IMS node is not being used.

If the processor determines that the at least one test message is not successfully processed by the particular other IMS node, then the processor may cause the particular other IMS node not to be used for a further predetermined period of time. The processor may determine that the at least one test message is successfully processed by the absence of an error being detected.

The test message may be at least one of: a SIP message received by the IMS node; a SIP message generated by the IMS node; a SIP OPTION message; a SIP INVITE message; an ICMP message; and a ping. The error may be detected by receipt of an error notification.

The IMS node may be at least one of: an IMS Application Server; a media gateway; a border gateway; a border controller and a CSCF.

There is further provided a method in an IMS node. The method comprises sending SIP messages to a plurality of other IMS nodes, and further comprises detecting an error in a particular other IMS node, the error indicating that the particular other IMS node is not available to receive traffic. The method also comprises not using the particular other IMS node for a period of time in response to the detection of the error, and sending at least one test message to the particular other IMS node when the period of time expires. The method further comprises determining whether the at least one test message is successfully processed by the particular node, and if it is, then returning the node to use.

Not using the particular other IMS node for a period of time in response to the detection of the error may comprise removing the particular other IMS node from use for a period of time in response to the detection of the error. Not using the particular other IMS node may be achieved by blacklisting the IMS node. SIP messages may be sent to other IMS nodes that are not blacklisted.

The method may further comprise sending at least one test message to the particular other IMS node if incoming activity from the particular other IMS node is detected during the period of time for which the particular other IMS node is not used.

If it is determined that the at least one test message is not successfully processed by the particular other IMS node, then the particular other IMS node may not be used for a further predetermined period of time.

The method may further comprise determining that the at least one test message is successfully processed in the absence of a further error being detected.

The at least one test message may comprise at least one of: a SIP message received by the IMS node; a SIP message generated by the IMS node; a SIP OPTION message; a SIP INVITE message; an ICMP message; and a ping.

The error may be detected by receipt of an error notification. The error notification may be received via a message from an external source, or the error notification may be internally generated.

The IMS node may be at least one of: an IMS application Server; a media gateway; a border gateway; and a CSCF.

There is further provided a computer-readable medium, carrying instructions, which, when executed by computer logic, causes said computer logic to carry out any of the methods defined herein.

Brief description of the drawings

A method and apparatus for improved handling of IMS node blacklisting will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 shows the components of an IMS network;

Figure 2 shows a method of black list handling in an IMS node; and

Figure 3 shows an IMS node for performing the method described herein.

Detailed description

Figure 1 shows a generic IP Multimedia Subsystem (IMS) network. The IMS network can broadly be defined as comprising 3 layers: an application layer 110, a control layer 120, and a connectivity layer 130. Each of the nodes in figure 1 may be considered to be an IMS network node as described herein.

The application layer 110 comprises application servers which provide services to users. The application layer 110 is shown as comprising a presence and group management server 112 and a business communication suite 114. The application layer 110 comprises SIP application servers to host, process and store data and provide various services to users. A third party service provider can host their service on an application server in the application layer 110 leaving network control to the other layers, which are typically maintained by service providers.

The control layer 120 can be considered as providing the intelligence in the network. The control layer 120 comprises: a home subscriber server 121, a call session control function (CSCF)/ breakout gateway control function 122, a domain name system / E.164 Number Mapping Server 124, a network session border controller 124, a media resource function controller 125, an access session border controller 126 and a media gateway controller 127. The control layer 120 manages the setup, call modification and call release. An important component of the control layer 120 is the CSCF server 122. The CSCF server 122 can be thought of as a SIP server, which manages call, session routing and file protocols. The control layer 120 also contains other servers to provide functions such as provisioning, charging and operation & management. Interfacing with other networks is provided by respective gateways. The home subscriber server 121 maintains a database to store the unique service profile for each end user.

The connectivity layer 130 comprises a network session border gateway 132, a media resource function processor 134, an access session border gateway 136, and a media gateway 138. The connectivity layer 130 comprises the network backbone as well as external access to the network. It provides an interface for the networks & devices that require access to the IMS network. The connectivity layer 130 functions as an entry and exit point to the network.

Access to another network 140, such as a VoIP network or other IMS network is provided by the network session border controller 124 and the network

session border gateway 136. Connection to an IP access network 150 is provided by the access session border controller 126 and the access session border gateway 136.

Figure 2 is a flow diagram illustrating the method disclosed herein. At 210 an IMS node sends SIP messages to a plurality of other IMS nodes that are not blacklisted. At 220, the IMS node determines if an error is detected in any of the IMS nodes to which it has sent a SIP message. If an error is detected at 220, then the IMS node for which the error is detected is blacklisted at 230. After blacklisting at 230, or if no error is detected at 220, then the process returns to 240 where a determination is made as to whether the blacklist time period has expired for any blacklisted IMS nodes. If no blacklist time periods have expired then the blacklist is unchanged and the process returns to 210 and the IMS node sends SIP messages to the non-blacklisted other IMS nodes.

If, at 240, a determination is made that the blacklist time period has expired for any blacklisted IMS nodes, then at 250 a test message is sent to the IMS nodes for which the blacklist time period has expired. At 260, a determination is made as to whether the test message is correctly processed by the IMS node to which it was sent. If the test message is not correctly processed, then the IMS node to which it was sent is determined to be in an error state and that IMS node is re-blacklisted at 230.

If the test message is correctly processed, then the IMS node to which it was sent is determined to no longer be in an error state and it is returned to normal use. The method then returns to 210 and the IMS node proceeds to send SIP messages to non-blacklisted other IMS nodes.

A previously blacklisted IMS node is removed from the blacklist upon expiry of the blacklist time period, but it is not returned to normal use until it is determined that it has successfully processed a test message sent to it. During the time between the blacklist time period expiring and the determination as to whether the test message is successfully processed, the

previously blacklisted IMS node can be considered to be in quarantine, whereby it is neither blacklisted nor in normal use. This means that an IMS node can classify the other IMS nodes in the network in one of three classes: blacklisted, in normal use, and in quarantine.

Regarding blacklisting, a connectivity problem may be related to firewall filtering on source addresses rather than other network or destination host failures. As such a destination may well be reachable from one source address but not from another. For these reasons, all blacklisting entries except those triggered by a SIP 503 response may include source transport address (IP address, port and transport protocol) in combination with destination transport address (IP address, port and transport protocol).

Figure 3 shows an IMS node 300 for performing the method described herein. The IMS node 300 comprises a reception module 310, a processor 320 and a transmission module 330. In operation, the reception module 310 receives a communication requiring the IMS node 300 to send a SIP message to another IMS node. The transmission module 330 of the IMS node 300 is arranged to send SIP messages to a plurality of other IMS nodes. The processor 320 is arranged to detect an error in a particular other IMS node, the error indicating that the particular other IMS node is not available to receive traffic. In response to such a detection, the processor 320 causes the particular other IMS node not to be used for a period of time, which comprises the blacklist time period.

The transmission module 330 is further arranged to send at least one test message to the particular other IMS node when the period of time expires. Further, the processor 320 is arranged to determine if the at least one test message is successfully processed by the particular other IMS node, and in response to a positive determination then returning the particular other IMS node to normal use.

It will be apparent to the skilled person that the exact order and content of the actions carried out in the method described herein may be altered according

to the requirements of a particular set of execution parameters. Accordingly, the order in which actions are described and/or claimed is not to be construed as a strict limitation on order in which actions are to be performed.

Further, while examples have been given in the context of particular communications standards, these examples are not intended to be the limit of the communications standards to which the disclosed method and apparatus may be applied. For example, while specific examples have been given in the context of IMS, the principles disclosed herein can also be applied to any network configuration which uses blacklisting to track errors at particular nodes.

Claims

1. An IMS node, comprising:

a transmission module arranged to send SIP messages to a plurality of other IMS nodes;

a processor arranged to detect an error in a particular other IMS node, the error indicating that the particular other IMS node is not available to receive traffic, and in response to such a detection, causing the particular other IMS node not to be used for a period of time;

wherein:

the transmission module is arranged to send at least one test message to the particular other IMS node when the period of time expires; and

the processor is arranged to determine if the at least one test message is successfully processed by the particular other IMS node, and in response to a positive determination then returning the particular other IMS node to use.

2. The IMS node of claim 1, wherein causing the particular other IMS node not to be used for a period of time comprises removing the particular other IMS node from use for a period of time.

3. The IMS node of claim 1 or 2, wherein causing the particular other IMS node not to be used is achieved by blacklisting the particular other IMS node.

4. The IMS node of claim 3, wherein the transmission module is arranged to send SIP messages to other IMS nodes that are not blacklisted.

5. The IMS node of any preceding claim, wherein the transmission module is further arranged to send at least one test message to the particular other IMS node if incoming activity from the particular other IMS node is detected during the period of time for which the particular other IMS node is not being used.

6. The IMS node of claim 5, wherein if the processor determines that the at least one test message is not successfully processed by the particular other

IMS node, then the processor causes the particular other IMS node not to be used for a further predetermined period of time.

7. The IMS node of claims 5 or 6, wherein the processor determines that the at least one test message is successfully processed by the absence of an error being detected.

8. The IMS node of claims 5, 6 or 7, wherein the at least one test message comprises at least one of: a SIP message received by the IMS node; a SIP message generated by the IMS node; a SIP OPTION message; a SIP INVITE message; an ICMP message; and a ping.

9. The IMS node of any preceding claim, wherein an error is detected by receipt of an error notification.

10. The IMS node of any preceding claim, wherein the IMS node is at least one of: an IMS Application Server; a media gateway; a border gateway; a border controller and a CSCF.

11. A method in an IMS node, the method comprising:

sending SIP messages to a plurality of other IMS nodes;

detecting an error in a particular other IMS node, the error indicating that the particular other IMS node is not available to receive traffic;

not using the particular other IMS node for a period of time in response to the detection of the error;

sending at least one test message to the particular other IMS node when the period of time expires; and

if it is determined that the at least one test message is successfully processed by the particular node, then returning the node to use.

12. The method of claim 11, wherein not using the particular other IMS node for a period of time in response to the detection of the error comprises removing the particular other IMS node from use for a period of time in response to the detection of the error.

13. The method of claims 11 or 12, wherein not using the particular other IMS node is achieved by blacklisting the IMS node.

14. The method of claim 13, wherein SIP messages are sent to other IMS nodes that are not blacklisted.

15. The method of any of claims 11 to 14, wherein the method further comprises sending at least one test message to the particular other IMS node if incoming activity from the particular other IMS node is detected during the period of time for which the particular other IMS node is not used.

16. The method of claim 15, wherein if it is determined that the at least one test message is not successfully processed by the particular other IMS node, then the particular other IMS node is not used for a further predetermined period of time.

17. The method of claims 15 or 16, further comprising determining that the at least one test message is successfully processed in the absence of a further error being detected.

18. The method of claims 15, 16 or 17, wherein the at least one test message comprises at least one of: a SIP message received by the IMS node; a SIP message generated by the IMS node; a SIP OPTION message; a SIP INVITE message; an ICMP message; and a ping.

19. The method of any of claims 11 to 18, wherein an error is detected by receipt of an error notification.

20. The method of any of claims 11 to 18, wherein the IMS node is at least one of: an IMS application Server; a media gateway; a border gateway; and a CSCF.

21. A computer-readable medium, carrying instructions, which, when executed by computer logic, causes said computer logic to carry out any of the methods defined by claims 11 to 20.

Fig. 1

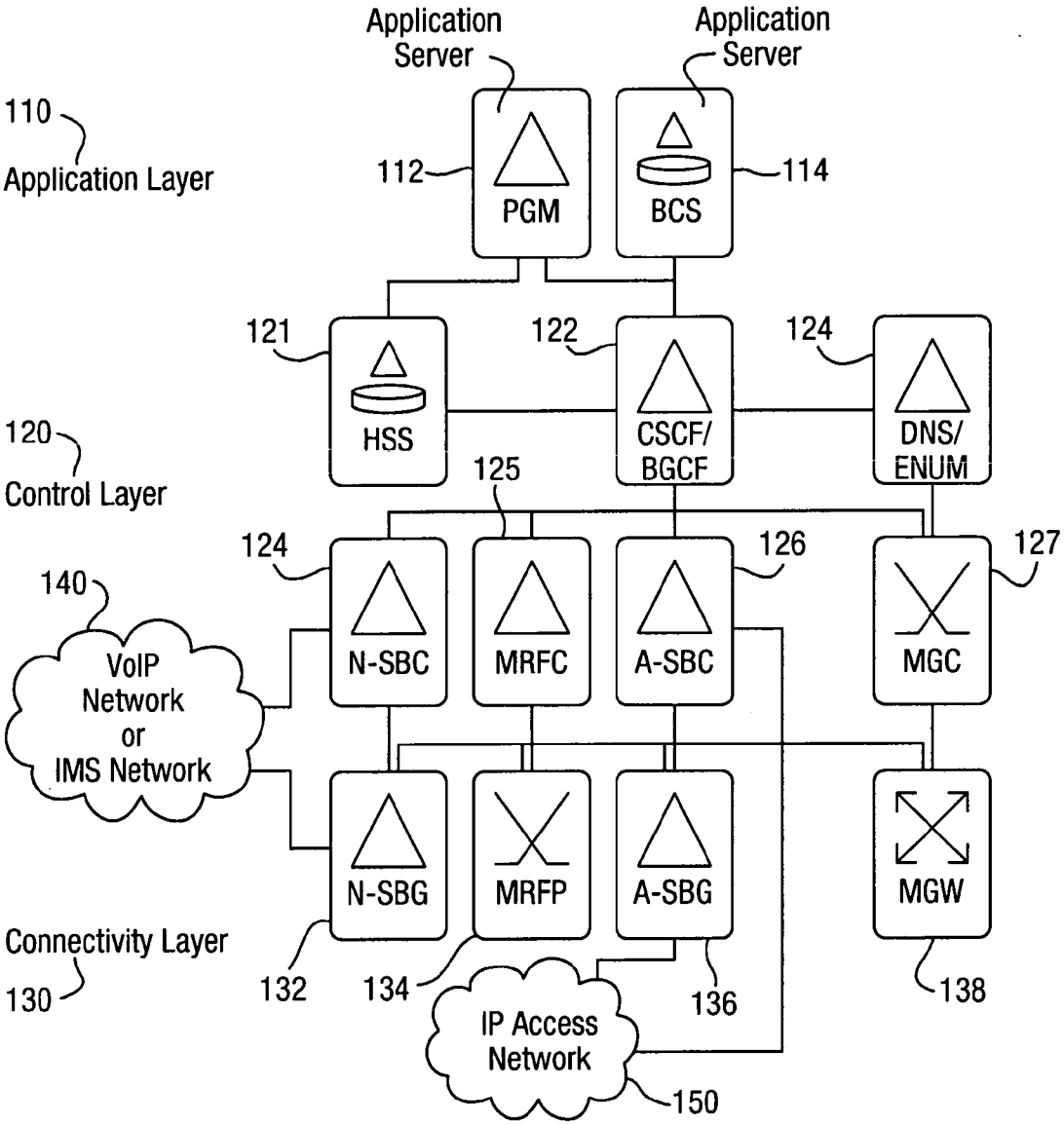

Application Server
Application Server
110
Application Layer
112
PGM
BCS
114
121
122
124
HSS
CSCF/ BGCF
DNS/ ENUM
120
Control Layer
125
124
126
127
140
VoIP Network or IMS Network
N-SBC
MRFC
A-SBC
MGC
N-SBG
MRFP
A-SBG
MGW
Connectivity Layer
130
132
134
136
138
IP Access Network
150

Fig. 2

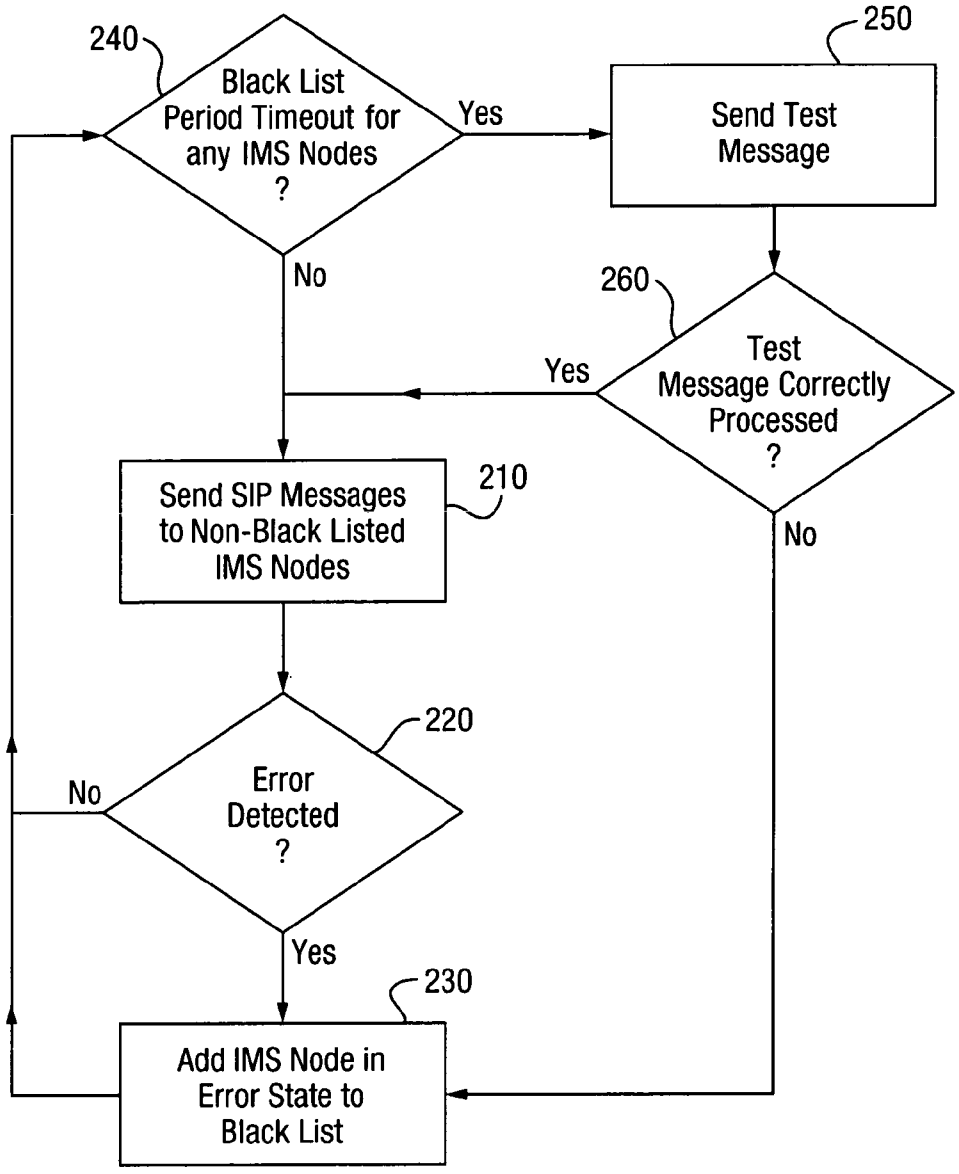
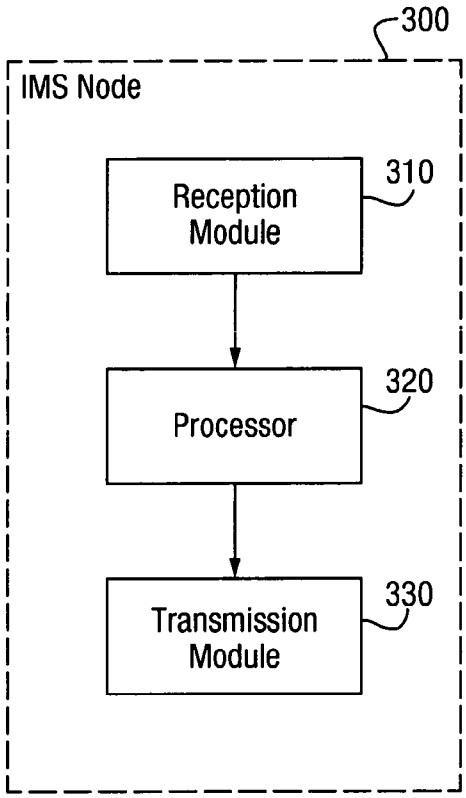

240
Black List Period Timeout for any IMS Nodes ?
Yes
No
250
Send Test Message
260
Test Message Correctly Processed ?
Yes
No
Send SIP Messages to Non-Black Listed IMS Nodes
210
220
Error Detected ?
No
Yes
230
Add IMS Node in Error State to Black List

Fig. 3


300
IMS Node
Reception Module
310
Processor
320
Transmission Module
330

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/052516

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L12/24 H04L12/26
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/008506 A1 (ASTIGARRAGA TARA [US] ET AL) 12 January 2012 (2012-01-12) paragraph [0045] - paragraph [0052] paragraph [0061] - paragraph [0070] paragraph [0080] - paragraph [0085] figure 7 -----	1-21
A	SHANKAI J S ET AL: "SNMP over SIP for network management", NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, 2004. NOMS 2004. IEEE/IFI P SEOUL, KOREA APRIL 19-23, 2004, PISCATAWAY, NJ, USA,IEEE, vol. 1, 19 April 2004 (2004-04-19), pages 881-882, XP010712728, ISBN: 978-0-7803-8230-5 the whole document -----	1-21

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

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 November 2012	08/11/2012

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

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2012/052516

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012008506 A1	12-01-2012	NONE	