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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2013 (31.01.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/015669 A1

(51) International Patent Classification:
H04L 29/08 (2006.01)

(21) International Application Number:
PCT/MY2012/000129

(22) International Filing Date:
20 June 2012 (20.06.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI2011003452 25 July 2011 (25.07.2011) MY

(71) Applicant *(for all designated States except US)*: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ABDELGADIR, Tageldin** [SD/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **SHARIQ, Haseeb** [IN/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **MOHAMMAD, Moshee Uddin** [BD/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **MUHAMMAD, Faheem Mohd Ezani** [MY/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **MOHD ARIFF, Abdulllah** [MY/MY]; c/o Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(74) Agent: **MIRANDAH, Patrick**; Patrick Mirandah Co. (malaysia) Sdn. Bhd., Suite 3B-19-3, Plaza Sentral, Jalan Stesen Sentral 5, 50470 Kuala Lumpur (MY).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, 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).

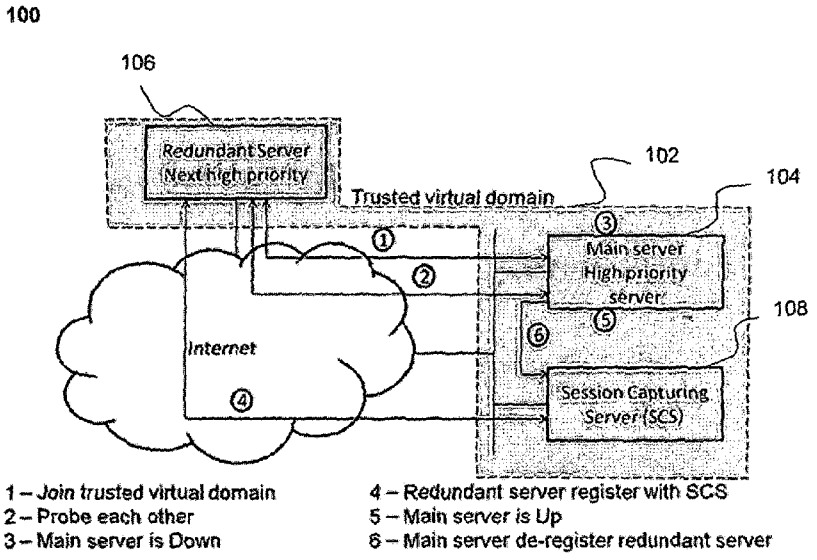
Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *of inventorship (Rule 4.17(iv))*

[Continued on next page]

(54) **Title**: GLOBAL SERVICES REDUNDANCY USING IP ADDRESS MOBILITY



(57) **Abstract**: Global services redundancy is provided using IP address mobility wherein the main server obtains an address which is the same address registered in the DNS server which allows clients access services offered by the server through the assigned IP in the DNS. Redundant server is required to be in the same LAN as the main server and if the link to both the servers fails, then the service is disrupted. The present invention introduces a Session Capturing Server (SCS) the Session Capturing Server (SCS) to maintain mapping table of redundant servers IP address with main servers IP address. Session Capturing Server (SCS) captures ongoing sessions of the main server that has failed and forward the captured sessions to a backup server for continuing services.

WO 2013/015669 A1

Published:

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

GLOBAL SERVICES REDUNDANCY USING IP ADDRESS MOBILITY

FIELD OF INVENTION

The present invention relates to a system and method for providing redundancy within communication network using IP address mobility.

BACKGROUND ART

Server reliability provides for retrievable backups of user session in a scalable way on a network during server failure at web-hosting sites. Regardless of the reliability of servers, servers are prone to failure. Server redundancy is desirable within communication networks such as providing a backup server within the said communication network.

At present, the availability of server redundancy in Local Area Network (LAN) solves the problem of server failure. Redundant server is required to be in the same LAN as the main server to ensure continuous service is maintained. However, service is disrupted if the linkage between the main server and the redundant server fails.

The approach of the present invention provides a system and a method for solving server failure by introducing redundancy of servers in a LAN. The present invention requires redundant server to be in the same LAN as the main server. The service would be disrupted if the link to both the servers fails. Therefore, the present invention provides for the Session Capturing Server (SCS) to maintain mapping table of redundant servers IP address with main servers IP address. Further, the Session Capturing Server (SCS) of the present invention is captured to ongoing sessions of the main server that has failed and the captured sessions is forwarded to a backup server for continuing services.

The subject matter claimed herein is not limited to embodiments that solve any disadvantages or that operate only in environments such as those described above. Rather, this background is only provided to illustrate one exemplary technology area where some embodiments described herein may be practice.

SUMMARY OF INVENTION

The present invention provides a system for providing redundancy within communication network using IP address mobility. The system comprising at least one trusted virtual domain. The trusted virtual domain comprising at least one main server, at least one redundant server and at least one Session Capturing Server (SCS). The at least one main server with IP address registered at DNS Server as highest priority server for serving a plurality of clients within communication network while the at least one redundant server takes over role of main server as next highest priority server and the at least one Session Capturing Server (SCS) registers and deregisters main server and redundant servers. Preferably, the at least one Session Capturing Server (SCS) maintains mapping table of redundant servers IP address with main servers IP address.

Further, the at least one Session Capturing Server (SCS) creates tunnel to redundant servers IP address to capture packets for main server and transmits the said packets to redundant servers via the said tunnel and destroys tunnel with redundant servers when mapping table entries are deleted. Preferably, the at least one redundant server further creates tunnel to at least one Session Capturing Server (SCS) when Registration Acceptance (RA) message is received from Session Capturing Server (SCS) and destroys tunnel with at least one Session Capturing Server (SCS) when deregistration message is received from main server.

Another aspect of the present invention provides a method for providing redundancy within communication network using IP address mobility. The method comprising steps of establishing communication session by main server as highest priority server within communication network, joining trusted virtual domain with next highest priority redundant servers to build mutual trust, sending probe messages by redundant backup server to main server for uplink status, taking over role of main server by next highest priority server within communication network when highest priority server is down, registering new main server with Session Capturing Server (SCS) and unregistering current main server with Session Capturing Server (SCS) when highest priority server is up.

A further aspect of the present invention provides a method for establishing communication session by main server as highest priority server within communication network. The method comprises steps of joining trusted virtual domain to build trust with back up servers and Session Capturing Server (SCS), receiving probe messages from redundant server and providing status update of main server to redundant server, sending deregistration message to redundant server when main server is down and configuring IP address of main server and deregistering binding with Session Capturing Server (SCS) when main server is up.

Further, the method of sending probe messages by redundant backup server to main server for uplink status further comprises steps of joining trusted virtual domain to build trust with main server, back up servers and Session Capturing Server (SCS), sending encrypted status probe messages to main server, continuously sending status messages to main server when status reports are received from main server, sending other messages based on user configuration or Registration Request (RR) messages to Session Capturing Server (SCS) when status reports are not received from main server, creating tunnel with Session Capturing Server (SCS) when Registration Acceptance (RA) message is received from Session Capturing Server (SCS) and destroying tunnel with Session Capturing Server (SCS) when deregistration message is received from main server.

The present invention consists of features and a combination of parts hereinafter fully described and illustrated in the accompanying drawings, it being understood that various changes in the details may be made without departing from the scope of the invention or sacrificing any of the advantages of the present invention.

BRIEF DESCRIPTION OF ACCOMPANYING DRAWINGS

To further clarify various aspects of some embodiments of the present invention, a more particular description of the invention will be rendered by references to specific embodiments thereof, which are illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail through the accompanying drawings where:

FIG. 1 illustrates a system for providing redundancy within communication network using IP address mobility.

FIG. 2 is a flowchart illustrating a method for providing redundancy within communication network using IP address mobility.

FIG. 3 is a flowchart illustrating a method for establishing communication session by main server as highest priority server within communication network.

FIG. 4 is a flowchart illustrating a method for configuring IP address of main server and deregistering binding with Session Capturing Server (SCS) when main server is up.

FIG. 5 is a flowchart illustrating a method for sending probe messages by redundant backup server to main server for uplink status.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides a system and method for providing redundancy within communication network using IP address mobility. Hereinafter, this specification will describe the present invention according to the preferred embodiments. It is to be understood that limiting the description to the preferred embodiments of the invention is merely to facilitate discussion of the present invention and it is envisioned without departing from the scope of the appended claims.

Reference is first made to FIG. 1 and FIG. 2 respectively. FIG. 1 illustrates a system for providing redundancy within communication network using IP address mobility and FIG. 2 is a flowchart illustrating a method for providing redundancy within communication network using IP address mobility. As illustrated in FIG.1, the system for providing redundancy within communication network using IP address mobility. The concept of IP mobility is associated with devices being mobile and changing point of attachment from one network to another. The principal of IP mobility of the present invention introduces IP address mobility rather than device mobility.

The system of the present invention comprising at least one trusted virtual domain (102). The said trusted virtual domain further comprising at least one main server (104), at least one redundant server (106) and at least one Session Capturing Server (SCS) (108). The main server obtains an address which is the same address registered in the DNS server. The at least one main server (104) with IP address registered at DNS Server as highest priority server serves a plurality of clients within communication network as clients access services offered by the server through the assigned IP in the DNS.

The at least one redundant server (106) takes over role of main server (104) as next highest priority server. The said redundant servers are backup servers. The redundant servers further creates tunnel to at least one Session Capturing Server (SCS) when Registration Acceptance (RA) message is received from Session Capturing Server (SCS) and destroys tunnel with at least one Session Capturing Server (SCS) when deregistration message is received from main server.

The at least one Session Capturing Server (SCS) (108) of the present invention registers and deregisters main server (104) and redundant servers (106). The at least one Session Capturing Server (SCS) (108) maintains mapping table of redundant servers (106) IP address with main servers (104) IP address. The said Session Capturing Server (SCS) (108) further creates tunnel to redundant servers IP address to capture packets for main server and transmits the said packets to redundant servers via the said tunnel and destroys tunnel with redundant servers when mapping table entries are deleted.

The methodology of the present invention which provides redundancy within communication network using IP address mobility comprising steps of establishing communication session by main server as highest priority server within communication network (202). The main server is a machine with higher capacity to handle multiple requests wherein it is therefore the highest priority server. Once in operation, the main server can choose one of the many available security association techniques to join a trusted virtual domain with the next highest priority redundant backup servers, who also join the trusted virtual domain of the main server to build mutual trust (204). When a trust has been built between the main server and the redundant server, the main server can rest assure that the backup server is authorized to take over its responsibilities. The redundant server sends probe messages to main server for uplink status (206) and redundant server as the next highest priority server takes over role of main server within communication network when highest priority server is down (208). Thereafter, the new main server is registered with Session Capturing Server (SCS) (210) and current main server is deregistered with Session Capturing Server (SCS) when highest priority server is up (212).

Reference is now being made to FIG. 3 and FIG. 4 respectively. FIG. 3 is a flowchart illustrating a method for establishing communication session by main server as highest priority server within communication network while FIG. 4 is a flowchart illustrating a method for configuring IP address of main server and deregistering binding with Session Capturing Server (SCS) when main server is up. As illustrated in FIG. 3, the method for establishing communication session by main server as highest priority server within communication network further comprises steps of joining trusted virtual domain to build trust with redundant servers and Session Capturing Server (SCS) (302). Thereafter, probe messages are received from redundant server (304) and status update of main

server is provided to redundant server (306). Deregistration message is sent to redundant server when main server is down (308) and IP address of main server is configured while binding is deregistered with Session Capturing Server (SCS) when main server is up (310).

As illustrated in FIG. 4, IP address of main server is configured and binding with Session Capturing Server (SCS) is deregistered when main server is up by requesting Session Capturing Server (SCS) to delete mapping table entries (402). Thereafter, deregistration request is sent to redundant server informing redundant server that main server is up (404) and tunnel between Session Capturing Server (SCS) and redundant server is destroyed when mapping table entries are deleted (406).

Reference is now being made to FIG. 5. FIG. 5 is a flowchart illustrating a method for sending probe messages by redundant backup server to main server for uplink status. Once a security association has been established, the backup server securely probes the main server to check if the main server is up and serving the clients. The main server then securely replies to the backup server. However, when the main server is down, the backup server does not get a reply and it concludes that the main server is down. Given the condition when no response is received from the main server, depending on the threshold level set by the administrator, the backup server may send another probe or conclude that the main server is down. Similarly the backup server for the next highest priority redundant backup server probes the next highest priority redundant backup server and so on. As illustrated in FIG. 5, in the operation of the redundant server, it joins the trusted virtual domain of the main server, backup servers and Session Capturing Server (SCS) (502). Thereafter, it sends out encrypted status probe message to the main server (504). As long as status reports are received from the main server, it continues to send out status messages to the main server (506). When a status report is not received, based on a user configurable threshold, it may send out another probe or sends a Registration Request (RR) message to the Session Capturing Server (SCS) (508). The RR message makes the SCS believe that the main server has physically moved to a new network location.

The Session Capturing Server (SCS) then creates a tunnel with the redundant server, send out a Registration Acceptance (RA) message and tunnels all the requests meant

for the main server to the redundant server (510). The redundant server then assumes the role of the main server and responds to the clients via the Session Capturing Server (SCS). When deregistration message is received from the main server, the redundant server knows that the main server is up again and it destroys the tunnel with the Session Capturing Server (SCS) (512). The redundant server again continues to probe the main server for uplink status.

The present invention provides for the Session Capturing Server (SCS) to maintain mapping table of redundant servers IP address with main servers IP address. Further, the Session Capturing Server (SCS) of the present invention is captured to ongoing sessions of the main server that has failed and the captured sessions is forwarded to a backup server for continuing services.

The present invention may be embodied in other specific forms without departing from its essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore indicated by the appended claims rather than by the foregoing description. All changes, which come within the meaning and range of equivalency of the claims, are to be embraced within their scope.

CLAIMS

1. A system (100) for providing redundancy within communication network using IP address mobility comprising:

   at least one trusted virtual domain (102) comprising at least one main server (104), at least one redundant server (106) and at least one Session Capturing Server (SCS) (108);

   the at least one main server (104) with IP address registered at DNS Server as highest priority server for serving a plurality of clients within communication network;

   the at least one redundant server (106) for taking over role of main server (104) as next highest priority server;

   the at least one Session Capturing Server (SCS) (108) for registering and deregistering main server (104) and redundant servers (106).

   characterized in that the at least one Session Capturing Server (SCS) (108) further maintains mapping table of redundant servers (106) IP address with main servers (104) IP address.

2. A system (100) according to Claim 1, wherein the at least one Session Capturing Server (SCS) (108) further:

   creates tunnel to redundant servers IP address to capture packets for main server and transmits the said packets to redundant servers via the said tunnel; and

   destroys tunnel with redundant servers when mapping table entries are deleted.

3. A system (100) according to Claim 1, wherein the at least one redundant server (106) further:

   creates tunnel to at least one Session Capturing Server (SCS) when Registration Acceptance (RA) message is received from Session Capturing Server (SCS); and

   destroys tunnel with at least one Session Capturing Server (SCS) when deregistration message is received from main server.

4. A system (100) according to Claim 1, wherein the said redundant servers (106) are backup servers.

5. A method (200) for providing redundancy within communication network using IP address mobility comprising steps of:

establishing communication session by main server as highest priority server within communication network (202);

joining trusted virtual domain with next highest priority redundant servers to build mutual trust (204);

sending probe messages by redundant server to main server for uplink status (206);

taking over role of main server by next highest priority server within communication network when highest priority server is down (208);

registering new main server with Session Capturing Server (SCS) (210); and

unregistering current main server with Session Capturing Server (SCS) when highest priority server is up (212).

6. A method (300) according to Claim 3, wherein establishing communication session by main server as highest priority server within communication network further comprises steps of:

joining trusted virtual domain to build trust with back up servers and Session Capturing Server (SCS) (302);

receiving probe messages from redundant server (304) and providing status update of main server to redundant server (306);

sending deregistration message to redundant server when main server is down (308); and

configuring IP address of main server and deregistering binding with Session Capturing Server (SCS) when main server is up (310).

7. A method (400) according to Claim 4, wherein configuring IP address of main server and deregistering binding with Session Capturing Server (SCS) when main server is up further comprises steps of:

requesting Session Capturing Server (SCS) to delete mapping table entries (402);

sending deregistration request to redundant server informing redundant server that main server is up (404); and

destroying tunnel between Session Capturing Server (SCS) and redundant server when mapping table entries are deleted (406).

8. A method (500) according to Claim 3, wherein sending probe messages by redundant server to main server for uplink status further comprises steps of:

joining trusted virtual domain to build trust with main server, back up servers and Session Capturing Server (SCS) (502);

sending encrypted status probe messages to main server (504);

continuously sending status messages to main server when status reports are received from main server (506);

sending other messages based on user configuration or Registration Request (RR) messages to Session Capturing Server (SCS) when status reports are not received from main server (508);

creating tunnel with Session Capturing Server (SCS) when Registration Acceptance (RA) message is received from Session Capturing Server (SCS) (510); and

destroying tunnel with Session Capturing Server (SCS) when deregistration message is received from main server (512).

9. A method according to Claim 6, wherein creating tunnel with Session Capturing Server (SCS) when Registration Acceptance (RA) message is received from Session Capturing Server (SCS) further comprises steps of taking over role of main server by redundant server and responding to clients via Session Capturing Server (SCS).

10. A method according to Claim 6, wherein destroying tunnel with Session Capturing Server (SCS) when deregistration message is received from main server further comprises steps of continuously sending messages to main server for uplink status.

100

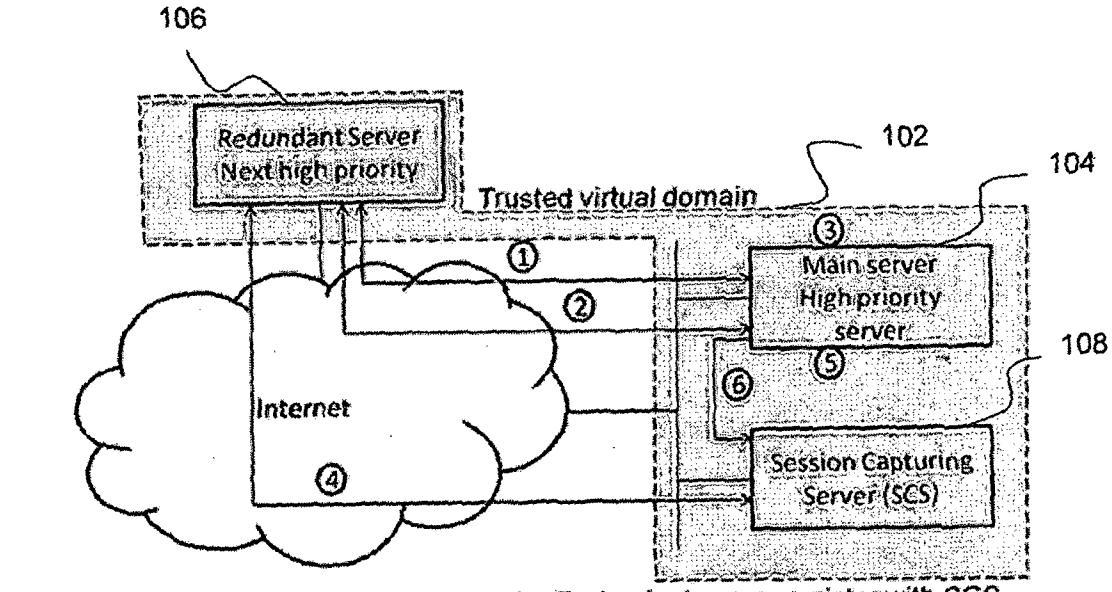

106
Redundant Server
Next high priority
Trusted virtual domain
102
104
Main server
High priority
server
108
Session Capturing
Server (SCS)
Internet
1 – Join trusted virtual domain
2 – Probe each other
3 – Main server is Down
4 – Redundant server register with SCS
5 – Main server is Up
6 – Main server de-register redundant server

FIG. 1

200

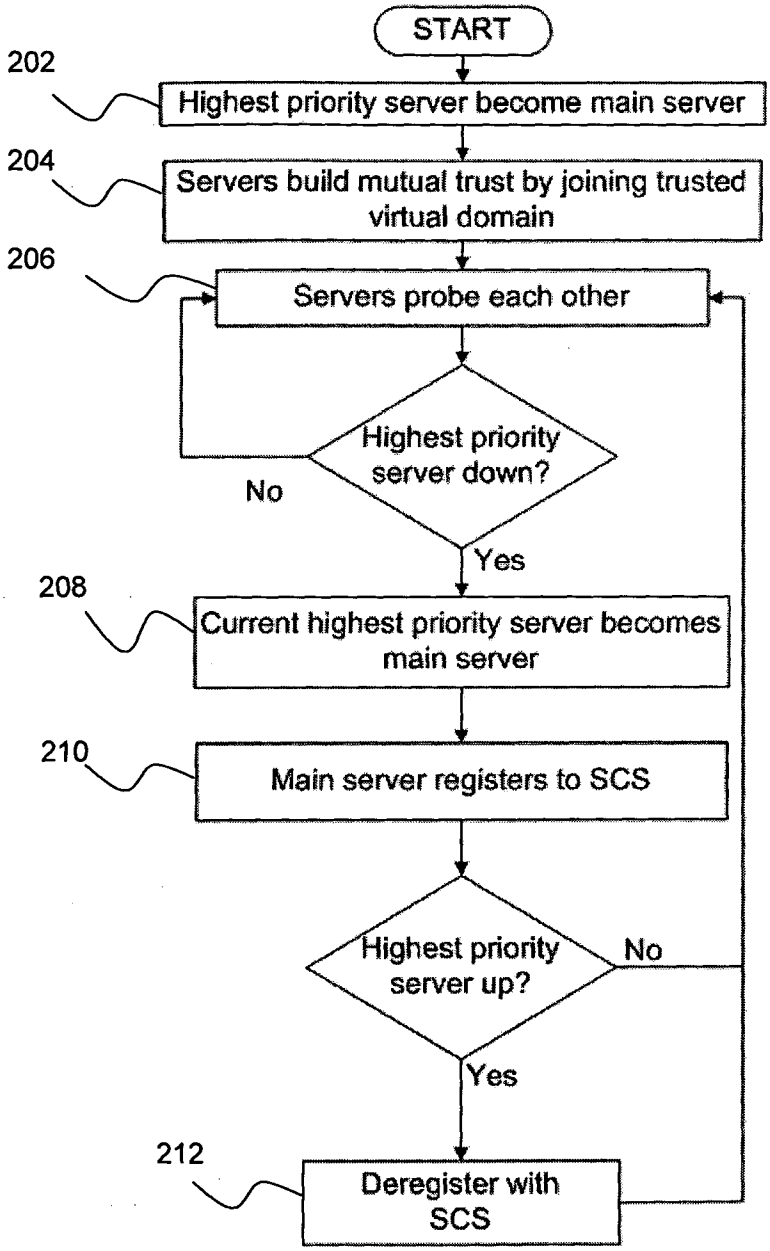

START
202
Highest priority server become main server
204
Servers build mutual trust by joining trusted virtual domain
206
Servers probe each other
Highest priority server down?
No
Yes
208
Current highest priority server becomes main server
210
Main server registers to SCS
Highest priority server up?
No
Yes
212
Deregister with SCS

FIG. 2

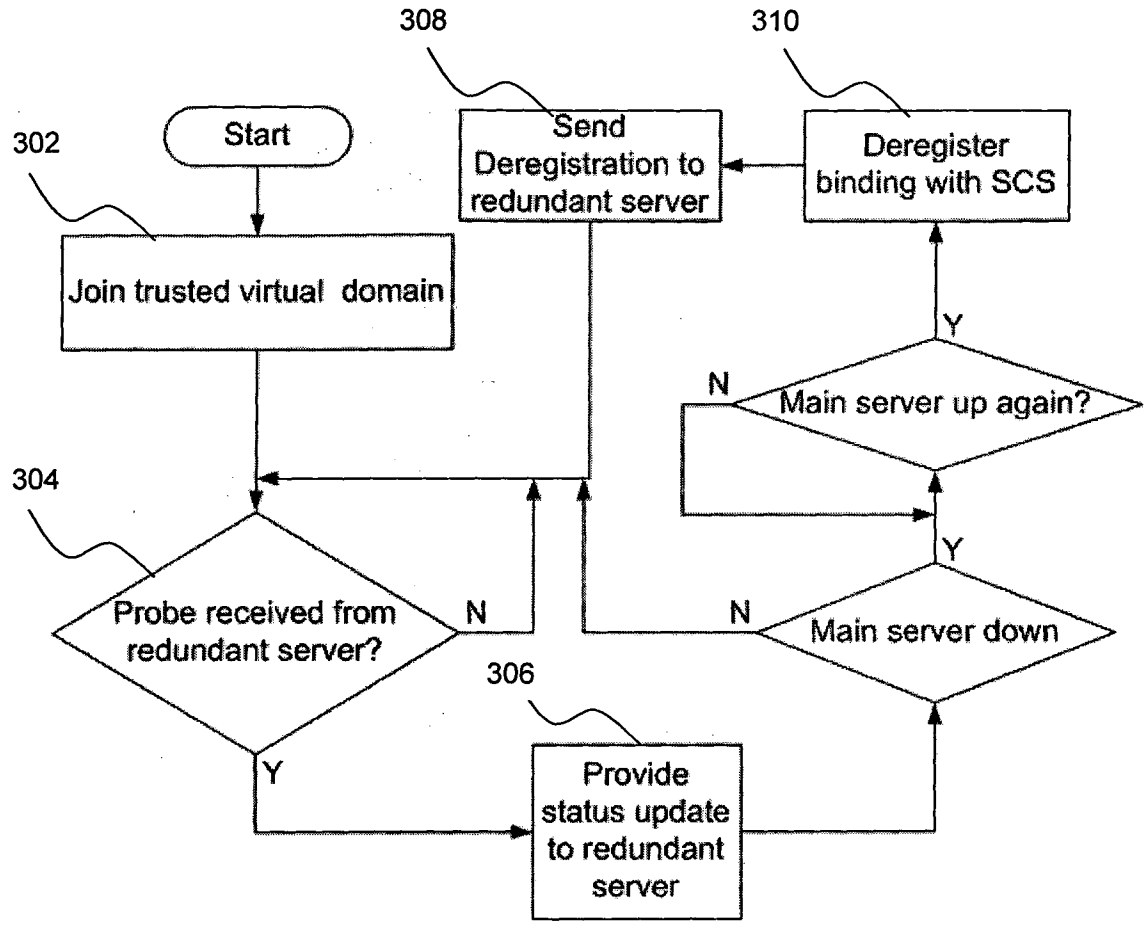

300
308
310
Start
302
Send Deregistration to redundant server
Deregister binding with SCS
Join trusted virtual domain
Y
N
Main server up again?
304
Y
Probe received from redundant server?
N
N
Main server down
306
Y
Provide status update to redundant server

FIG. 3

400

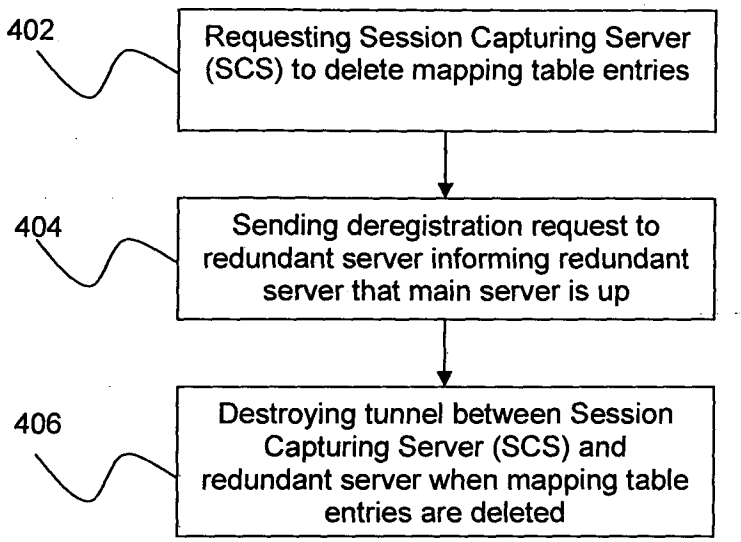

402
Requesting Session Capturing Server (SCS) to delete mapping table entries
404
Sending deregistration request to redundant server informing redundant server that main server is up
406
Destroying tunnel between Session Capturing Server (SCS) and redundant server when mapping table entries are deleted

FIG. 4

500

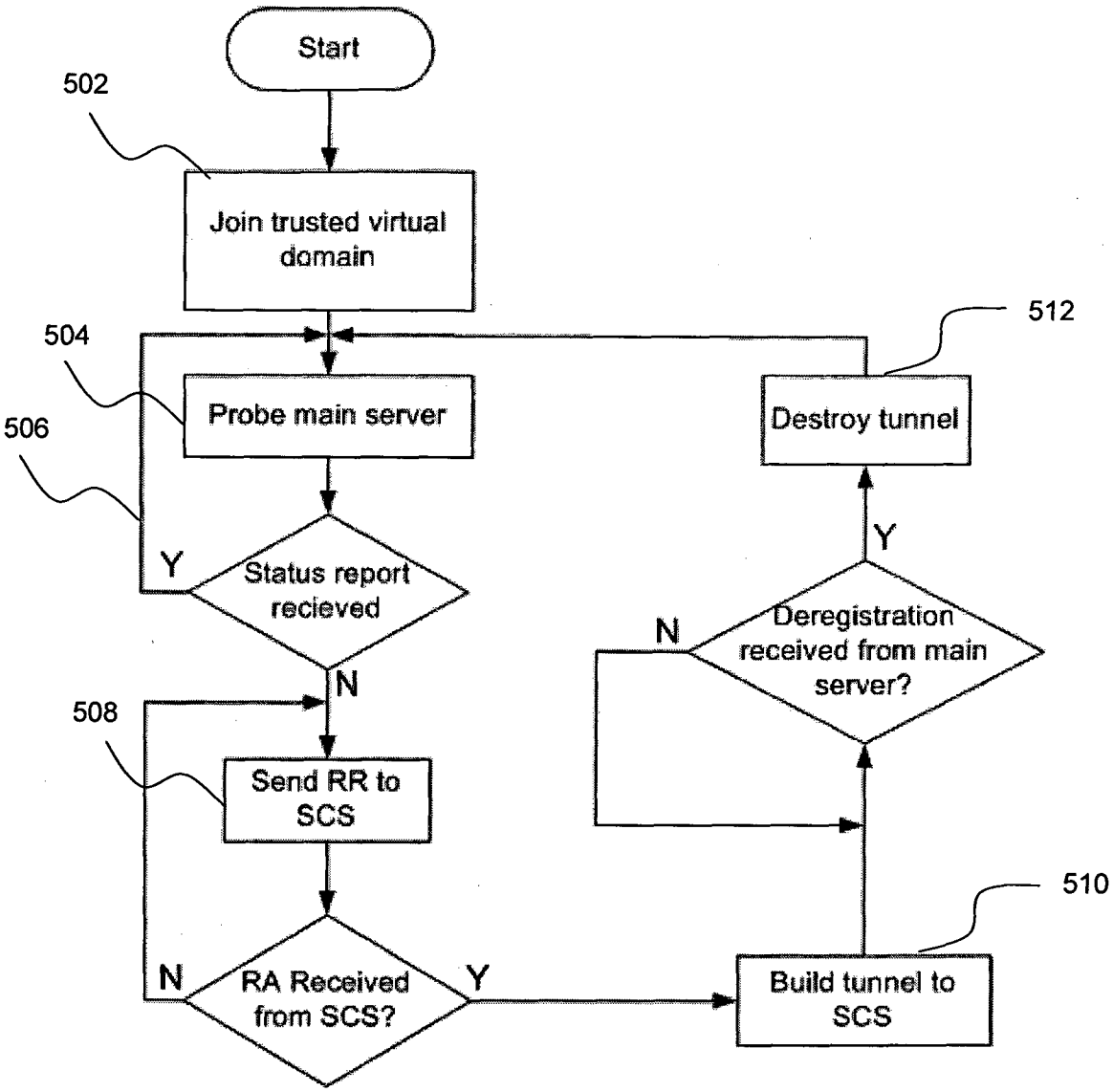

Start
502
Join trusted virtual domain
504
Probe main server
506
Status report recieved
Y
N
508
Send RR to SCS
RA Received from SCS?
N
Y
Build tunnel to SCS
510
Deregistration received from main server?
N
Y
Destroy tunnel
512

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/MY2012/000129

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/08
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, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 061 711 A2 (IDGATE CO LTD [JP]) 20 December 2000 (2000-12-20) abstract paragraph [0007] - paragraph [0011] paragraph [0017] - paragraph [0021] paragraph [0033] - paragraph [0039] figure 3	1,5
A	US 6 813 635 B1 (JORGENSON DANIEL SCOTT [US]) 2 November 2004 (2004-11-02) the whole document	1-10
A	WO 2004/036363 A2 (AKAMAI TECH INC [US]) 29 April 2004 (2004-04-29) the whole document	1-10

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

☒ See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 October 2012	02/11/2012

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	Pereira, Mafalda

4

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/MY2012/000129

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1061711 A2	20-12-2000	CA 2293880 A1	16-12-2000
		EP 1061711 A2	20-12-2000
		JP 3299521 B2	08-07-2002
		JP 2000357160 A	26-12-2000
		KR 20010005487 A	15-01-2001
		TW 463090 B	11-11-2001
US 6813635 B1	02-11-2004	US 6813635 B1	02-11-2004
		US 2005021848 A1	27-01-2005
WO 2004036363 A2	29-04-2004	AU 2003301473 A1	04-05-2004
		EP 1552413 A2	13-07-2005
		US 2004083283 A1	29-04-2004
		US 2007061440 A1	15-03-2007
		US 2008215730 A1	04-09-2008
		US 2012036238 A1	09-02-2012
		WO 2004036363 A2	29-04-2004