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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 October 2014 (16.10.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/166522 A1

(51) International Patent Classification:
H04L 29/12 (2006.01) *H04L 12/24* (2006.01)
H04L 29/08 (2006.01)

(21) International Application Number:
PCT/EP2013/057351

(22) International Filing Date:
9 April 2013 (09.04.2013)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **ROBERT BOSCH GMBH** [DE/DE]; Postfach 30 02 20, 70442 Stuttgart (DE).

(72) Inventors: **SMAAK, Marc**; Scandinavistraat 9, NL-4614JR Bergen op Zoom (NL). **DE BROUWER, Tom**; Haagweg 268b, NL-4812XG Breda (NL). **VAN TIENEN, Stephan**; Rijnlaan 81, NL-4615CA Bergen op Zoom (NL).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

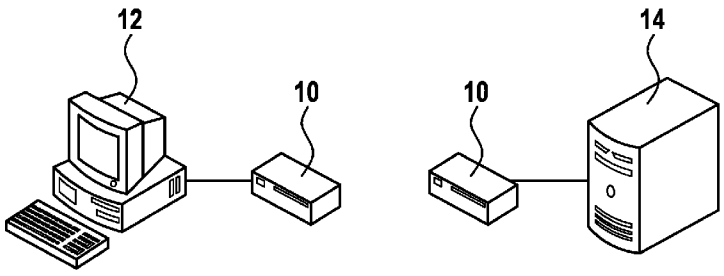
Published:

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

WO 2014/166522 A1

(54) Title: METHOD FOR NETWORK CHANGE TOLERANT SERVICE DISCOVERY IN A COMPUTER NETWORK

Fig. 1



(57) Abstract: Method and computer network for discovering services in a computer network using Domain Name System Service Discovery (DNS-SD), comprising as components at least a client and a server, the components can be linked by bridges and communicate by a network protocol, whereby the client and the server have a connection-oriented communication path between each other in the computer network, whereby in case of a connection loss one of the components being affected by the connection loss announces itself regularly using DNS-SD until the connection to the client is restored.

Description

Title

Method for network change tolerant service discovery in a computer network

Technical Field

The invention provides for a method of discovering services in a computer network being tolerant of network changes.

Background art

A computer network is a collection of computers and electronic devices interconnected by communication channels like the internet allowing for sharing of resources and information. Communication protocols define the rules and data formats for exchanging information in such a network. A well known communication protocol is the Internet Protocol Suite.

The Internet Protocol Suite is a set of communication protocols used for the Internet and similar networks, and generally the most popular protocol stack for wide area networks. It is commonly known as TCP/IP, because of its most important protocols: Transmission Control Protocol and Internet Protocol, which were the first network networking protocols defined in this standard.

In a network in which multiple TCP/IP-enabled systems operate, systems will typically offer services. In order to find out which system offers which service, DNS (Domain Name System)-based Service Discovery (DNS-SD) can be used. The Domain Name System Service Discovery (DNS-SD) is an extension on the common Domain Name System.

Disclosure of the invention

The invention provides for a method of network change tolerant service discovery in a computer network according to claim 1, and an arrangement according to claim 6. Subject matter of the dependent claims define embodiments of the invention.

It will be understood that the features mentioned above and those described hereinafter can be used not only in the combination specified but also in other combinations or on their own, without departing from the scope of the present invention.

The invention is diagrammatically illustrated in the drawings by means of embodiments by way of example, and is hereinafter explained in detail with reference to the drawings. It is understood that the description is in no way limiting on the scope of the present invention and is nearly an illustration of embodiments of the invention.

Brief description of the drawings

Figure 1 shows a computer network.

Figure 2 shows the computer network of figure 1 with connected bridges.

Figure 3 shows another computer network.

Figure 4 shows a computer network with an additional server.

Figure 5 shows another computer network.

Figure 6 shows the computer network of figure 5 with disconnected bridges.

Description of embodiments

The Domain Name System is a distributed naming system for any resource connected to the internet. The system associates various information with domain names assigned to each of the participants. Furthermore, it translates domain

names to the numerical IP addresses needed for locating computer services and devices.

DNS-SD can be used in two different ways.

Multicast DNS:

Multicast DNS is a standard for using Domain Name System programming interfaces, packet formats and operating without configuring a conventional DNS server.

With multicast DNS (mDNS) each server multicasts the services it offers. These offers will be sent with an exponential back-off timer with a maximum of 8 messages. Next to sending the broadcast, it will react on any explicit query for the service it offers.

A client can send a multicast query for a certain service to all servers, servers which offer requested service will react on this query. The query will have an exponential back-off timer with a suggested maximum of 60 minutes.

Using mDNS allows a client to setermine the IP address of a given host without the direct help of a centralised DNS server.

Unicast DNS:

Unicast DNS uses a server as storage location for the services offered within a network. Instead of multicast all servers now use unicast messaging to register which services they are offering. This is the more scalable solution since it involves less multicast traffic on the network.

A client now will set up a long lived query with the storage server for services it is interested in. This way it gets updates about device offering the service.

Both solutions have their limitations in keeping the lists of devices offering services catches up to date with respect to existence in the real world.

In a client-server based TCP/IP system, client will often communicate to one or multiple servers. The communication to these servers can be executed using a connection-less or connection-oriented protocol. In case of a connection-oriented protocol the client and servers are mutually aware of the fact that they can communivate with each other, i.e. they will notice when the communication path between each other is lost.

Multicast DNS

Problem

Figure 1 shows an example of an arrangement comprising bridges 10, a client 12, and a server 14, being stable for 52 minutes multicast query is sent out at 0:00:01, 0:00:03, 0:00:06, 0:00:12, 0:00:24, 0:00:48, 0:01:36, 0:03:12, 0:06:24, 0:12:48, 0:25:36, 0:51:12, 1:51:12, 2:51:12), only every hour the client 12 will send out a query due to the exponential back-off timers.

In case a connection is made between both bridges 10 after 0:51:13 as shown in Figure 2, it will take up to an hour before the client 12 will notice the server 14. This means, at time = 1:51:12 the client 12 will send out a query message for the service the server 14 offers, on which the server 14 will respond. The maximum wait time of one hour is usually not acceptable for users of the service.

Solution

In a centrally-controlled network, there will always be a connection-oriented path between the client (the central controller) and the server. The server can verify if this connection exists. If the server detects a connection loss, because the connection between the two bridges 10 is lost, it will announce itself regularly as it concludes that its nework connectivity has changed in a relevant way. According to the Internet-Draft, the server is allowed to update its records with a maximum of 10 times per minute.

In case the client detects the connection loss, also in case the connection between both bridges 10 is lost, it immediately removes the device from its DNS-SD

cache. Therefore, the client will not try to reconnect to the server until it is reported again.

In case the connection between both bridges is restored again the client will quickly discover the server and can reconnect to the service it is providing. The server will stop its regular announcements as it has concluded that its network connectivity is connected again.

Alternatively, the server always announces itself regularly if there is no connection to a client. This way quick discovery works as well as no connection was present between the bridges during startup of client and server.

The disadvantage of this is that there is no more network load when there is no connection between the client and the server since all servers will start announcing themselves frequently. However, this is no issue since no useful information is sent on the network when the controller is not present.

Unicast DNS - Network connectivity loss client (central controller) <-> DNS Storage server

Problem

The set-up in Figure 3 shows a correct network for unicast DNS with bridges 10, a client 12, a server 14, and a DNS storage server 16. As described before, the client will have an outstanding long lived query with the DNS storage server 16. These messages are delivered via UDP (User Datagram Protocol), which has no guarantee of delivery.

Figure 4 shows a system in which an additional server 18 is connected at the time no connection is available between the DNS storage server 16 and the client 12. The DNS storage server 16 will send out a long-lived query update to the client 12, this message will never arrive, the DNS storage server 16 will not get any feedback from this event so it will not retry it. The client 12 will not notice that there is no connection to the DNS storage server 16 and misses this event since it uses UDP.

Whenever the connection is restored between the two bridges 10, the newly added server 18 is never found, because only updates are sent.

Solution

At the time the client sets up an LLQ (Long-Lived Query) with the DNS storage server, it should set up as well a keep-alive mechanism. This means, it should send every x seconds a message on a separate connection-oriented communication path to the DNS storage server. The DNS storage server will answer the message. Whenever the message is missed for a few times, the client must wait for the connection to be re-established. Once the connection is re-established the client should refresh its DNS-SD cache by restarting the LLQ at which time the information at the client will be up-to-date again.

Unicast DNS - Network connectivity loss between Server <-> DNS Storage Server

Problem

The client in a system which uses a DNS storage server as record storage can never fully trust the cache of the DNS storage server. In Figure 5, a correct set-up is shown with bridges 100, a client 102, a server 104, and a DNS storage server 106.

The DNS storage server 106 will have the DNS records of the server 104. These records are stored with a certain time-to-live. The server 104 is responsible for refreshing the records at the DNS storage server 106. Only when the time-to-live is timed out, the records will be reported lost to the client 102. Whenever, as shown in Figure 6, the link is lost between the two bridges 100, the client 102 will lose the connection to the server 104. The DNS storage server 106 still has the record during the time the time-to-live is not aged out. Since this time to live is usually quite long, minutes or even hours, the client 102 will use the outdated cache information during this time.

When the link is restored after the record at the DNS storage server 106 is aged out, the client 102 received an update that the server 104 was lost. At the time

the link is restored again, the server 104 will update the DNS storage server 106 with its records at the default refresh time. Whenever the connection is restored within the aging out time, so before the DNS storage server 106 informs the client 102 that the server 104 is gone via the LLQ, no update will be received at the client side. Therefore, the client 102 does not know that it can reconnect to the server 104.

Solution

In a centrally-controlled network, there will always be a connection-oriented communication path between the client 102 (the central controller) and the server 104.

The server 104 will notice that its connection is lost. At the time the server 104 notices that the connection is lost, it should reannounce its records with the DNS storage server 106. It has to make sure that the remove and add of its records are received by the DNS storage 106 by receiving an acknowledgement. In this case, the server 104 knows that the client 102 did receive a remove event and an add event via the LLQ mechanism. The client 102 can reconnect to the server 104 after it has seen the remove and add event.

With implementing one, two or all of the mechanism described above the service discovery of services in a connection-oriented system is much more stable.

Claims

1. Method for discovering services in a computer network using Domain Name System Service Discovery (DNS-SD), comprising as components at least a client and a server, the components can be linked by bridges and communicate by a network protocol, whereby the client and the server have a connection-oriented communication path between each other in the computer network, whereby in case of a connection loss one of the components being affected by the connection loss announces itself regularly using DNS-SD until the connection to the client is restored.

2. Method according to claim 1, whereby using a Multicast DNS, in case the server detects the connection loss it regularly announces itself.

3. Method according to claim 1 or 2, whereby using a Multicast DNS, in case the client detects the connection loss it removes component to which connection is lost from its DNS-SD cache.

4. Method according to claim 1, whereby the computer network comprises as component a DNS storage server.

5. Method according to claim 4, whereby using a Unicast DNS and the DNS storage server, in case the server detects the connection loss to the client the server revokes its announcement regularly until the DNS storage server acknowledges the revocation.

6. Method according to claim 4 or 5, whereby using a Unicast DNS and the DNS storage server, the server announces itself to the DNS storage server until the DNS storage server acknowledges the announcement.

7. Method according to one of claims 4 to 6, whereby using Unicast DNS and the DNS storage server, the client monitors the presence of the DNS storage

server by sending messages to the DNS storage server to which the DNS storage server responds.

8. Method according to one of claims 4 to 7, whereby using Unicast DNS and the DNS storage server, in case the client misses the response of the DNS storage server for a few times, the client will continue sending messages to the DNS storage server and will update its DNS-SD cache upon receiving a response from the DNS storage server.

9. Computer network being adapted for a method according to the claims 1 to 8 for discovering services in the computer network using Domain Name System Service Discovery, comprising as components at least a client and a server, the components can be linked by bridges and communicate by a network protocol, whereby the client and the server have a connection-oriented communication path between each other in the computer network, whereby in case of a connection loss one of the components being affected by the connection loss announces itself regularly using DNS-SD until the connection to the client is restored

10. Computer network according to claim 9, whereby the computer network comprises a DNS storage server.

Fig. 1

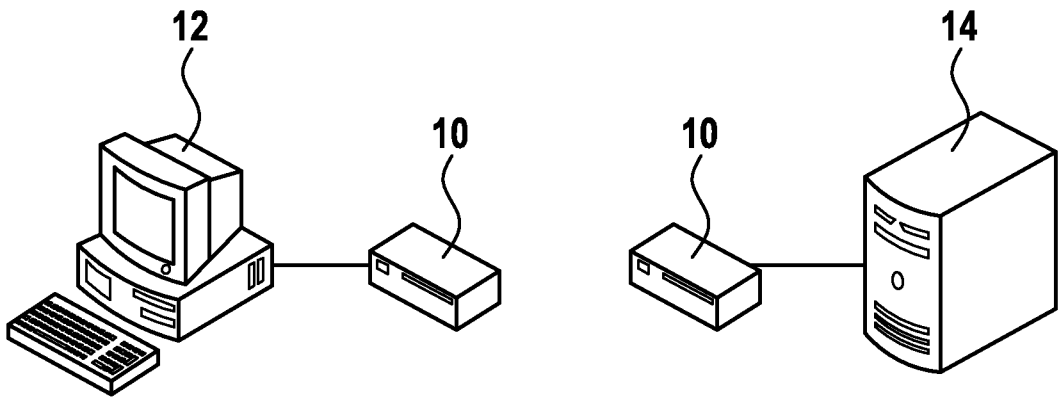


Fig. 2

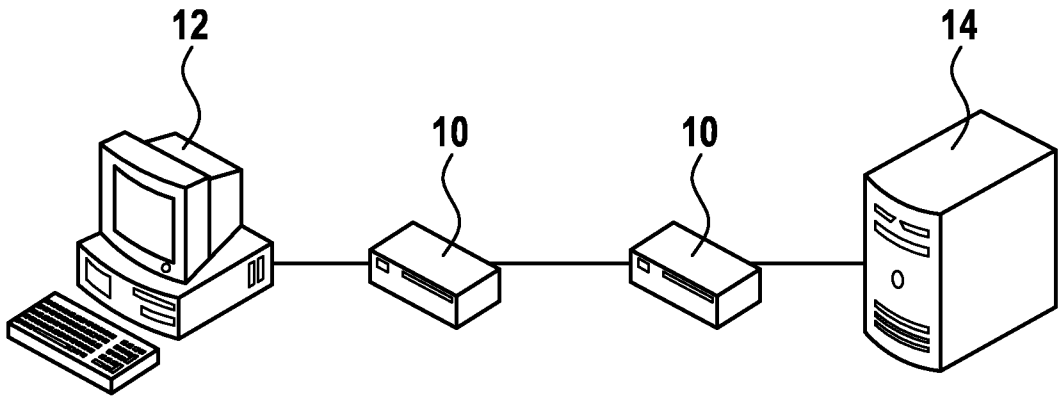


Fig. 3

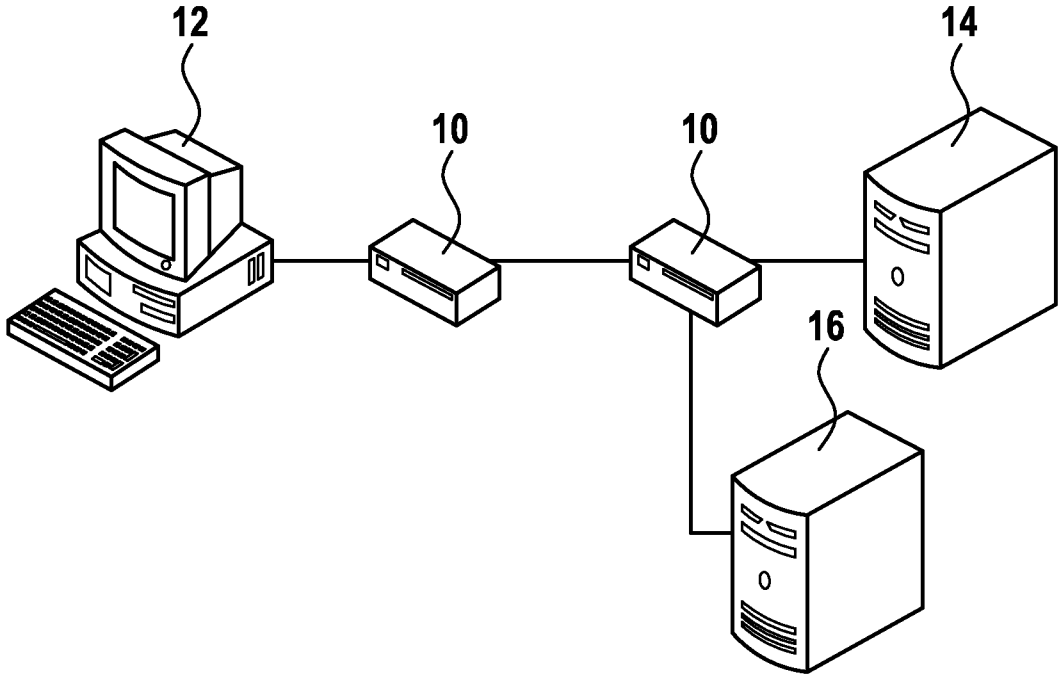


Fig. 4

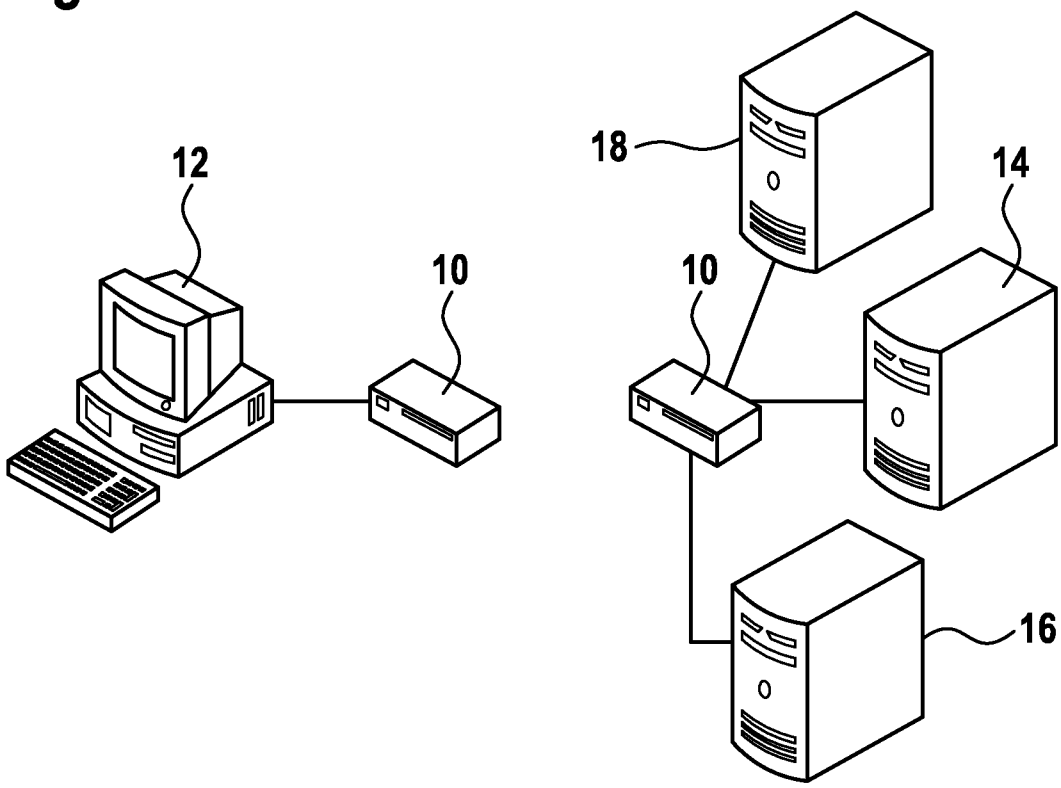


Fig. 5

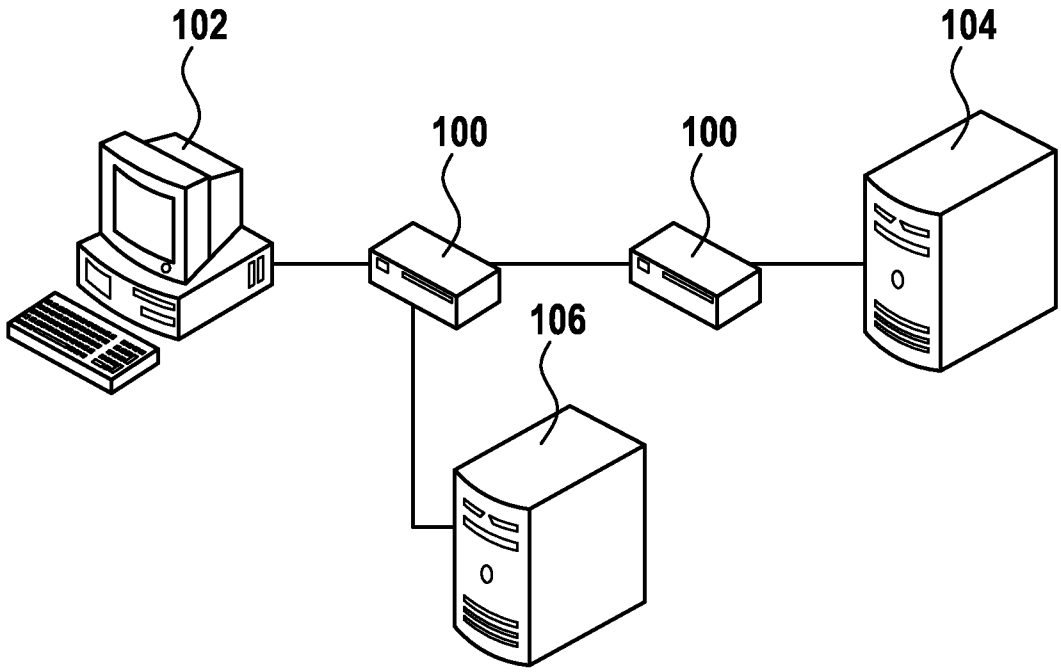
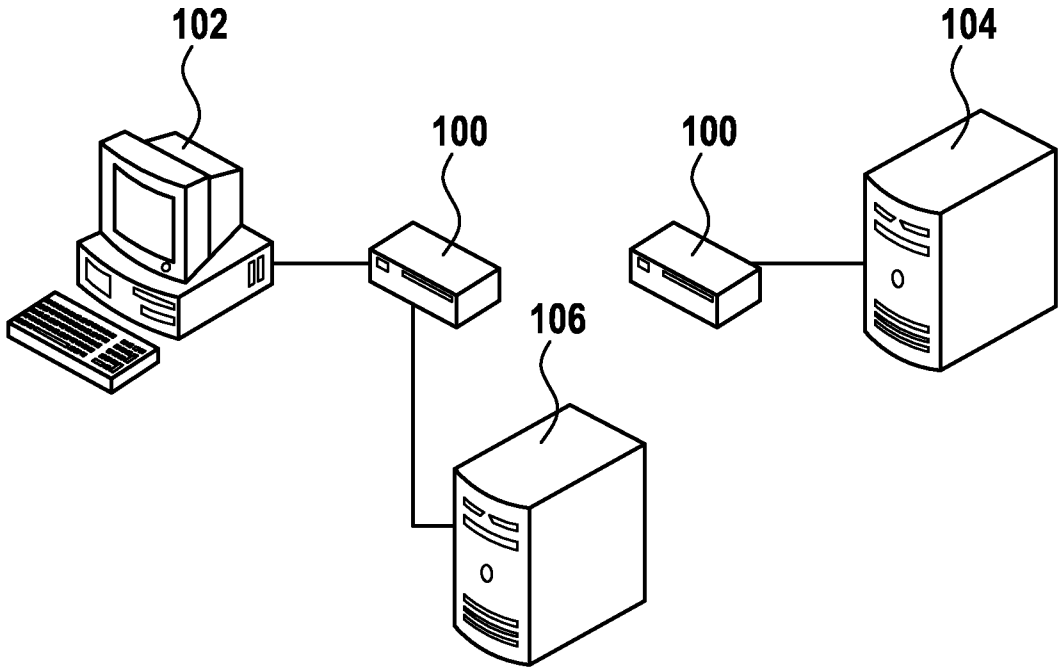


Fig. 6



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/057351

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/12 H04L29/08 H04L12/24
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.
Y	CHESHIRE M KROCHMAL APPLE INC S: "DNS-Based Service Discovery; rfc6763.txt", DNS-BASED SERVICE DISCOVERY; RFC6763.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARD, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, SWITZERLAND, 20 February 2013 (2013-02-20), pages 1-49, XP015090290, [retrieved on 2013-02-20] Chapters 1, 11. Appendix A, F ----- -/--	1-10

[X] Further documents are listed in the continuation of Box C.

[X] 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
26 November 2013	03/12/2013

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

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/057351

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CHESHIRE M KROCHMAL APPLE INC S: "Multicast DNS; rfc6762.txt", MULTICAST DNS; RFC6762.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARD, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, SWITZERLAND, 20 February 2013 (2013-02-20), pages 1-70, XP015090289, [retrieved on 2013-02-20] Chapters 1, 11.; abstract Appendix A, F Chapter 5.2 Chapter 8.	1-10
A	MOCKAPETRIS P: "RFC1035 - DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION", NETWORK WORKING GROUP REQUEST FOR COMMENTS, XX, XX, 1 November 1987 (1987-11-01), pages 1-55, XP000864261, Chapter 4.2.	1-10
A	US 2010/211878 A1 (SPIJKERBOSCH JOHANNES E [NL] ET AL) 19 August 2010 (2010-08-19) paragraph [0090] - paragraph [0098]	1-10
A	US 2009/259755 A1 (BOUCACHARD PHILIPPE [FR] ET AL) 15 October 2009 (2009-10-15) paragraph [0194] - paragraph [0204]	1-10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/057351

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010211878 A1	19-08-2010	EP 2201721 A2	30-06-2010
		JP 2011516930 A	26-05-2011
		US 2010211878 A1	19-08-2010
		WO 2009030759 A2	12-03-2009
US 2009259755 A1	15-10-2009	FR 2930100 A1	16-10-2009
		US 2009259755 A1	15-10-2009