

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
5 February 2009 (05.02.2009)

PCT

(10) International Publication Number
WO 2009/017545 A1

(51) International Patent Classification:

G06F 15/00 (2006.01) **G06F 15/16** (2006.01)

(21) International Application Number:

PCT/US2008/007584

(22) International Filing Date: 17 June 2008 (17.06.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

11/830,106 30 July 2007 (30.07.2007) US

(71) Applicant (for all designated States except US):
HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. [US/US]; 20555 S.H. 249, Houston, Texas 77070 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **HANES, David, H.** [US/US]; 3404 East Harmony Road, Fort Collins, Colorado 80528-9599 (US).

(74) Agents: **WEBB, Steven, L.** et al.; Hewlett-Packard Company, Intellectual Property Administration, P.O. Box 272400, Mail Stop 35, Fort Collins, Colorado 80527-2400 (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, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, 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 the identity of the inventor (Rule 4.17(i))
- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

[Continued on next page]

(54) Title: FIRMWARE RETRIEVAL ACROSS A NETWORK

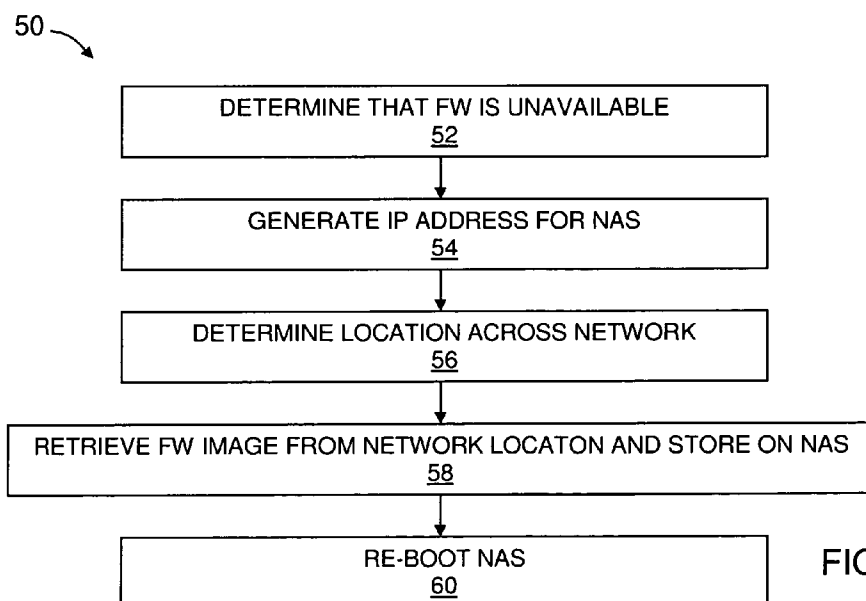


FIG. 3

(57) Abstract: A system (12) comprises a processor (32) and non-volatile storage (34) coupled to the processor. The non-volatile storage comprises firmware (36) that is executable by the processor. The processor determines whether the firmware is available to be executed. If the firmware is not available to be executed, the processor determines a location across a network and retrieves a second firmware image (18) from that location.



— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report*

FIRMWARE RETRIEVAL ACROSS A NETWORK

BACKGROUND

[0001] Networking various computers, printers, network-attached storage (NAS) devices, and other types of devices is ubiquitous. Implementing computer networks is becoming popular in small offices and home environments. The NAS device comprises a non-volatile storage medium such as a hard disk drive that is shareable by the various computers on the network. A NAS device has code (e.g., firmware) that is loaded during initialization of the NAS device and executed by a processor in the NAS device to bestow the NAS device with some, or all, of its functionality. The firmware may become unavailable due to, for example, corruption of the firmware itself or a malfunctioning of the hard drive on which the firmware is stored. If the firmware is unavailable, the NAS device is generally unusable.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] For a detailed description of exemplary embodiments of the invention, reference will now be made to the accompanying drawings in which:

[0003] Figure 1 shows a system in accordance with various embodiments;

[0004] Figure 2 shows a block diagram of a network-attached storage device in accordance with various embodiments; and

[0005] Figure 3 shows a method in accordance with various embodiments.

NOTATION AND NOMENCLATURE

[0006] Certain terms are used throughout the following description and claims to refer to particular system components. As one skilled in the art will appreciate, computer companies may refer to a component by different names. This

[0007]

[0008] document does not intend to distinguish between components that differ in name but not function. In the following discussion and in the claims, the terms “including” and “comprising” are used in an open-ended fashion, and thus should be interpreted to mean “including, but not limited to...”. Also, the term “couple” or “couples” is intended to mean either an indirect, direct, optical or wireless electrical connection. Thus, if a first device couples to a second device, that connection may be through a direct electrical connection, through an indirect electrical connection via other devices and connections, through an optical electrical connection, or through a wireless electrical connection. The term “system” refers to a combination of one or more components and comprises, for example, a computer, a subsystem within a computer, a network-attached storage device, a subsystem within a network-attached storage device, and a networked combination of one or more network devices.

DETAILED DESCRIPTION

[0009] Figure 1 shows a system 10 in accordance with various embodiments. As shown, system 10 comprises a network-attached storage (NAS) device 12, one or more client computers 14, and one or more server 16 coupled together via wide area network (WAN) 20. The NAS 12 comprises non-volatile storage which can be shared by any one or more client computers 14 over a local area network (LAN) 15. The NAS 12 communicates with the client computers 14 over the LAN 15 and to the server 16 via the WAN 20. In various embodiments, each client computer 14 comprises a desktop computer, a portable computer (e.g., a notebook computer, a handheld computer) or other type of computing device that, for example, can write data (e.g., files) to and retrieve data from NAS 12.

[0010] The embodiments described herein are presented in the context of NAS devices. However, the concepts herein apply to devices other than NAS devices. Examples of such devices to which the disclosed principles apply comprise digital media adapters or other network devices. This scope of this disclosure applies to all such devices, not just NAS devices.

[0011] Figure 2 shows an embodiment of NAS 12. The computers 14 and servers 16 may comprise the same or similar architecture. As shown in Figure 2,

[0012]

[0013] NAS 12 comprises a processor 32 coupled to a first non-volatile storage (NVS) 34, a second non-volatile storage 40, a network interface 42, and volatile storage (VS) 46. The network interface 42 provides connectivity to either or both of the LAN 15 and WAN 20. In at least some embodiments, the first non-volatile storage 34 comprises a hard disk drive. However in other embodiments, the non-volatile storage 34 may be other than a hard disk drive (e.g., Flash memory, compact disk read-only memory (CD ROM)). The non-volatile storage 34 comprises firmware 36. The firmware 36 is executable by the processor 32 and imparts some or all of the functionality of the NAS 12.

[0014] The second non-volatile storage 40 comprises, for example, Flash memory or any form of read-only memory (ROM) such as electrically-erasable programmable ROM (EEPROM). The second non-volatile storage 40 may comprise a hard disk drive or CD ROM in some embodiments. The non-volatile storage 40 stores a boot loader (BL) 44 and a subnet value 38. The boot loader 44 comprises code that is executable by the processor 32. During initialization of the NAS 12, the processor 32 begins execution of the boot loader 44. At least one of the functions performed by the boot loader 44 is to load the firmware 36 from the first non-volatile storage 34 into volatile storage 46. In at least some embodiments, volatile storage 46 comprises random access memory (RAM). A copy of firmware 36 is then executed from volatile storage 46.

[0015] It is possible that the firmware 36 becomes corrupted or that the non-volatile storage 34 on which the firmware 36 is stored becomes non-operative. In either case, the firmware 36 is not available for execution by the processor 32. The firmware 36 being unavailable for execution renders the NAS device 12 partially or entirely inoperative. In accordance with various embodiments, the boot loader 44 determines whether firmware 36 is available to be executed. If the boot loader determines that firmware 36 is not available to be executed, the boot loader 44 causes the processor to determine a location across a network to retrieve a copy of a firmware image to replace the unavailable firmware 36. The process is "automatic" in some embodiments, meaning that no user involvement is required. In some embodiments, the location across the network at which a

[0016]

[0017] copy of replacement firmware image is found may be at a location across the LAN 15 or WAN 20. The example of Figure 2 illustrates that a server 16 comprises a replacement firmware copy 18 that can be provided across WAN 20 to the NAS 12.

[0018] The boot loader 44 determines whether the firmware 36 is available in accordance with any suitable technique. In at least one embodiment, the boot loader 44 computes a checksum or hash of the firmware 36 and compares the computed value to a pre-stored value (a checksum or hash previously computed based on known good version of the firmware 36). If the values do not match (the newly computed checksum/hash and the previously pre-stored value), the firmware 36 is determined to be corrupted and thus unavailable for execution. Also or alternatively, the boot loader 44 may experience an error accessing the non-volatile storage 34 which may be indicative of an error with the non-volatile storage 34 itself. Further still, if the non-volatile storage 34 is new (e.g., the user replaced a defective non-volatile storage 34 with a new storage unit), the new non-volatile storage 34 may not have any firmware 36. The boot loader 44 detects the absence of firmware 36 and thus determines firmware 36 to be unavailable for execution.

[0019] In various embodiments, the replacement firmware copy (also referred to as an "image") located on the network may be a copy that is identical to the currently firmware 36 on the NAS. In other embodiments, the replacement firmware copy is not identical but is sufficient, at any rate, to enable the NAS device 12 to operate correctly. Once a replacement firmware copy is located and transmitted to the NAS device 12, the replacement firmware copy is loaded into non-volatile storage 34, and the NAS device is re-booted. Re-booting the NAS device 12 causes the boot loader 44 to load and begin execution of the newly replaced firmware.

[0020] In some embodiments, the boot loader 44 overwrites the current firmware 36, which may be corrupted, with the replacement firmware retrieved over the network. In other embodiments, the non-volatile storage 34 may be inoperative, and a user thus removes and replaces the non-volatile storage 34.

[0021]

[0022] The newly installed non-volatile storage 34 may not contain a firmware image 36 at all. In such embodiments, the boot loader 34 determines that no firmware 36 is present (i.e., firmware is unavailable for execution), retrieves a new copy of suitable firmware for execution on the NAS device 12, stores the retrieved firmware on the newly installed non-volatile storage 34, and re-boots the NAS 12 to thereby cause the newly loaded firmware to be executed.

[0023] In various embodiments, the boot loader 44 accesses (e.g., is encoded with or otherwise retrieves from any of the storages 34, 40, or 46) an identifying value that identifies the NAS 12 or its firmware 36. Examples of such a value comprise a serial number of the NAS device 12, a model number of the NAS 12, a revision identifier of the firmware 36, etc. The boot loader 44 uses this identifying value to locate a suitable replacement firmware copy on the network. Locations on the network (e.g., websites) store and make available one or more firmware copies to boot loaders 44 of NAS devices 12. Each firmware copy at such network locations also has an identifying value associated therewith that is indicative of the NAS device 12 or NAS device firmware 36 for which that firmware copy is suitable. In some embodiments, the boot loader 44 compares the NAS device's identifying value to the identifying value of the various firmware copies on the network and retrieves the firmware copy for which the identifying values match. In other embodiments, the boot loader submits a request to the network location for a firmware image that is suitable for use with the NAS device's identifying value (i.e., the NAS device's identifying value is part of the request by the boot loader 44). The network location (e.g., server 16) transmits back to the NAS device 12 the firmware image 18 whose identifying value matches the identifying value provided by the NAS device 12.

[0024] Because the firmware 36 of the NAS device 12 may be unavailable for execution, it is possible that the NAS device 12 will not have an assigned internet protocol (IP) address by the time that the boot loader 44 attempts to locate a replacement firmware image on the network. Without an IP address, communications over the network are difficult, if not impossible. In some

[0025]

[0026]

[0027] embodiments, the boot loader 44 uses Dynamic Host Configuration Protocol (DHCP) to allocate an IP address to the NAS device 12.

[0028] In other embodiments, the NAS device 12 comprises a subnet value 48 which is stored in the non-volatile storage 40. The subnet value 38 stored in the non-volatile storage 40 comprise the NAS device's last known subnet value (i.e., the subnet value last used by the NAS device in its operative state). For example, if the NAS device's most recently assigned IP address is "192.168.0.100," the subnet value is "198.168.0." In this example and for purposes of this disclosure, the ending '100' is referred to as an "extension." The NAS device's IP address may be static, in which case the IP address does not change, or dynamic, in which case the IP address changes over time (e.g., each time the NAS device initializes and connects to the network). Each time that the IP address changes for the NAS device 12, it is the extension that changes, not the subnet value. For example, the next time an IP address is assigned to the NAS device 12, the extension may change to "2," resulting in an IP address of "192.168.0.2."

[0029] In various embodiments, before the NAS device's boot loader 44 can access the network (e.g., server 16 across WAN 20), the boot loader 44 generates a suitable IP address for use by the NAS device 12 for use in retrieving a replacement firmware image on the network. The IP address generated by the boot loader 44 should be an IP address not already in use by another device on the network. In at least some embodiments, the boot loader 44 retrieves the subnet value 38 (which comprises some, but not all, of a suitable IP address for the NAS device 12), and tries different extensions until an extension is found that results in an IP address not already in use by another device. Continuing with the example above, the boot loader may initially try "192.168.0.1" (extension of "1") as an IP address. The boot loader 44 will broadcast a "ping" message using that IP address. If the boot loader 44 receives a response, which would occur if another device is already assigned IP address 192.168.0.1, then the boot loader 44 determines that 192.168.0.1 is not a suitable IP address for the NAS device 12 to use. The boot loader then increments the extension to "2" to generate a

[0030]

[0031] second IP address of 192.168.0.2 and again broadcasts a ping message, this time using 192.168.0.2 as its IP address. If the boot loader 44 again receives a response, then the boot loader 44 determines that 192.168.0.2 is not a suitable IP address for the NAS device 12 to use. The boot loader 44 repeats this process, each time incrementing the IP address extension until an IP address is found for which no response to a ping message is received. The boot loader 44 uses that IP address in its attempt to locate a replacement firmware image from the network.

[0032] Figure 3 illustrates a method 50 in accordance with various embodiments. The actions listed in Figure 3 can be performed in an order other than shown and two or more of the actions can be performed concurrently or be combined. At 52, the boot loader 44 determines that the NAS device's firmware 36 is not available for execution. At 54, the boot loader 44 generates a suitable IP address for use by the NAS device 12 (i.e., an IP address that is not in use by another device on the network). In some embodiments, the boot loader 44 generates the IP address after determining that the firmware 36 is unavailable. One suitable implementation of action 43 is discussed above. At 56, the boot loader determines a location to access on the network at which a possible replacement firmware image may be provided. In some embodiments, the IP address or uniform resource locator (URL) of the possible network location is encoded into the boot loader 44 itself. In other embodiments, the IP address or URL is stored in any of the storages 34, 40, or 46 of the NAS device 12. At 58, method 50 comprises a suitable replacement firmware image being found (e.g., using the identifying values as explained above), retrieved from the network location and stored on the NAS device 12. At 60, after loading the replacement firmware image onto the non-volatile storage 34 of the NAS device 12, the boot loader 44 causes the NAS device 12 to be re-booted to enable the newly retrieved and stored replacement firmware image to be executed.

[0033] The above discussion is meant to be illustrative of the principles and various embodiments of the present invention. Numerous variations and modifications will become apparent to those skilled in the art once the above

[0034]

[0035] disclosure is fully appreciated. It is intended that the following claims be interpreted to embrace all such variations and modifications.

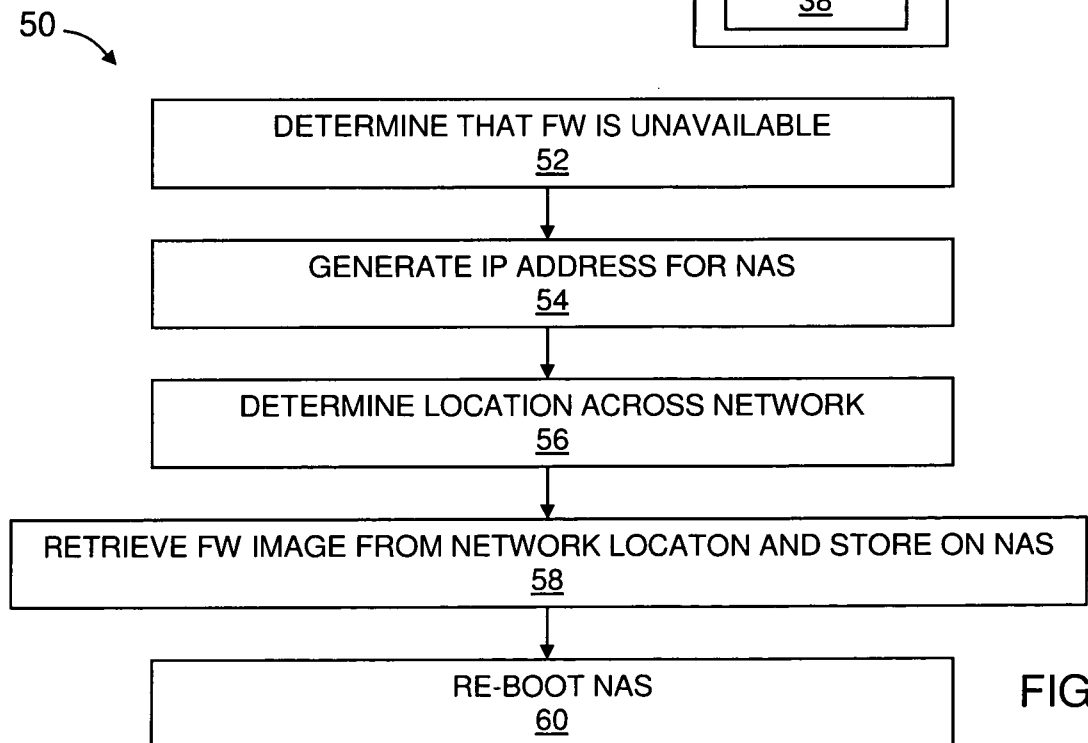
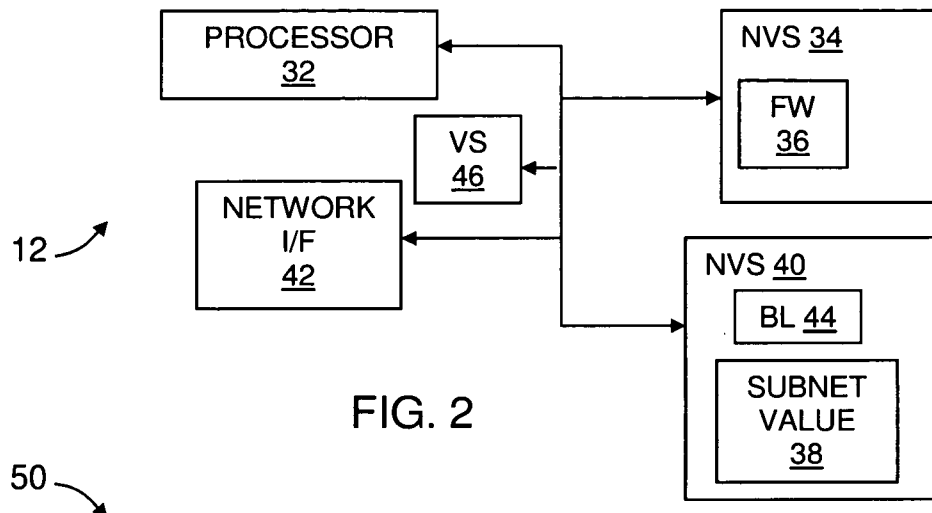
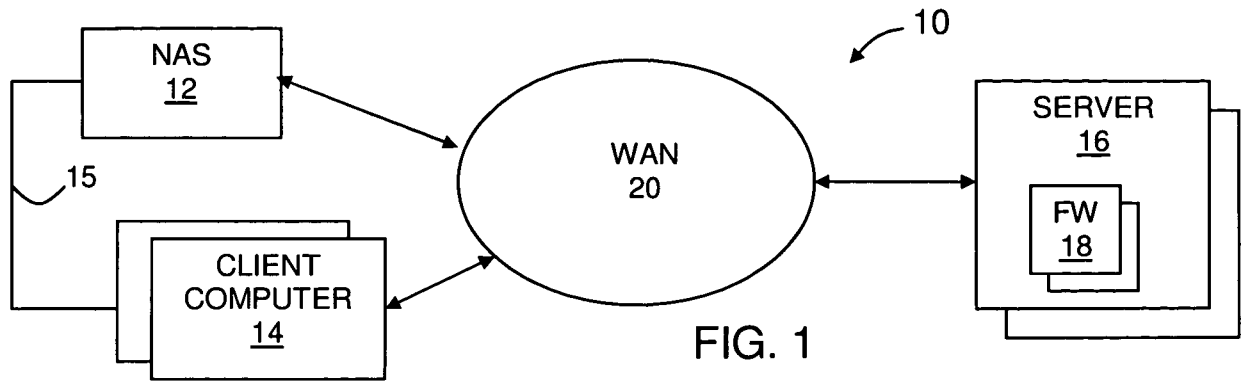
CLAIMS

What is claimed is:

1. A system (12), comprising:
a processor (32); and
non-volatile storage (34) coupled to said processor and comprising
firmware (36) that is executable by said processor;
wherein said processor determines whether the firmware is available to be
executed and, if the firmware is not available to be executed, said
processor determines a location across a network and retrieves a
second firmware image (18) from said location.
2. The system of claim 1 wherein said processor generates an internet
protocol (IP) address after determining that the firmware is unavailable.
3. The system of claim 1 wherein said processor determines the location by
retrieving an internet protocol (IP) address from non-volatile memory.
4. The system of claim 1 wherein said processor loads said retrieved second
firmware image in non-volatile storage.
5. The system of claim 1 wherein said processor compares an identifier
associated with said system to an identifier associated with the second firmware
image at said location.
6. A method, comprising:
determining (52) that firmware is unavailable to be executed;
determining (56) a location across a network; and
retrieving (58) a second firmware image from said location.
7. The method of claim 6 further comprising generating (54) an internet
protocol (IP) address after determining that the firmware is unavailable.

8. The method of claim 6 wherein determining the location comprises retrieving an internet protocol (IP) address from non-volatile memory.
9. The method of claim 6 further comprising loading said retrieved second firmware image in non-volatile storage.
10. The method of claim 6 further comprising comparing an identifier of the second firmware image at said location to an identifier associated with a system in which the firmware is unavailable.

1/1



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/007584**A. CLASSIFICATION OF SUBJECT MATTER****G06F 15/00(2006.01)i, G06F 15/16(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)

IPC 8 : G06F

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 since 1975

Japanese Utility Models and applications for utility models since 1975

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

eKIPASS(KIPO internal), IEEE xpl, Google, "backup", "remote", "firmware"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ----- Y	US 6986008 B2 (COLVIG ARTHUR JOHN et al.) 10 January 2006 See abstract, Figures 1-4, description row 35 column 3 - row 56 column 9, claims	1,6 ----- 2-5, 7-10
Y	US 6968369 B2 (VEPRINSKY ALEX et al.) 22 November 2005 See abstract, Figures 1-4, description row 9 column 2 - row 37 column 5, claims	2-5, 7-10
A	KR 10-2004-0091392 A (ATPIATEC CO., LTD.) 28 October 2004 See abstract, claims	1-10
A	US 7134044 B2 (FAIRCLOUGH DAY III KENETH et al.) 07 November 2006 See abstract, claims	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 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

08 OCTOBER 2008 (08.10.2008)

Date of mailing of the international search report

08 OCTOBER 2008 (08.10.2008)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-
gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

LEE, Jong Iek

Telephone No. 82-42-481-8373



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2008/007584

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6986008 B2	10.01.2006	CN 1836216 A	20.09.2006
		DE 602004003467 D1	11.01.2007
		EP 1584033 B1	29.11.2006
		JP 2006-518497 T	10.08.2006
		KR 10-2005-0088172	02.09.2005
		US 2004-139294 A1	15.07.2004
		WO 2004-063927 A1	29.07.2004
US 6968369 B2	22.11.2005	JP 2003-263352 A	19.09.2003
		JP 2007-282197 A	25.10.2007
		US 2003-061310 A1	27.03.2003
KR 10-2004-0091392 A	28.10.2004	NONE	
US 7134044 B2	07.11.2006	JP 7134044 A	23.05.1995