

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
6 August 2009 (06.08.2009)

PCT

(10) International Publication Number
WO 2009/096946 A1

(51) International Patent Classification:
G06F 12/16 (2006.01) **G06F 15/16** (2006.01)

Charles Martin [US/US]; 3404 E. Harmony Rd., Ft. Collins, 80528-9544 (US).

(21) International Application Number:
PCT/US2008/052313

(74) Agents: **O'MEARA, William** et al.; Hewlett-Packard Company, Intellectual Property Administration, Mail Stop 35, P.O. Box 272400, Fort Collins, Colorado 80527-2400 (US).

(22) International Filing Date: 29 January 2008 (29.01.2008)

(25) Filing Language: English

(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.

(26) Publication Language: English

(71) Applicant (*for all designated States except US*):
HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).

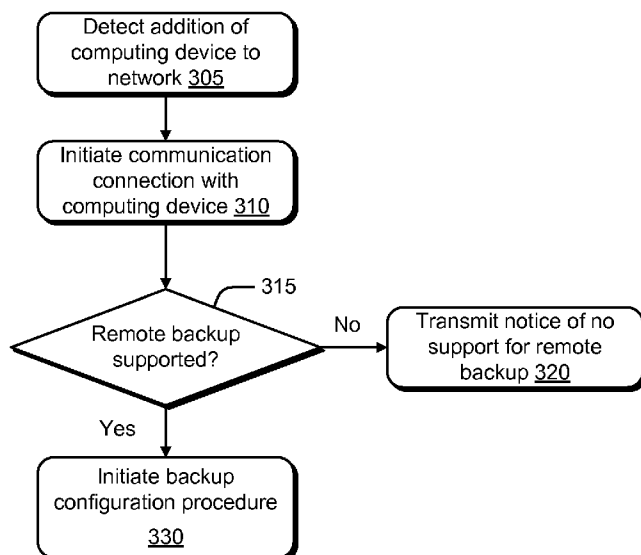
(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **CESARIO, Paul Michael** [US/US]; 3404 E. Harmony Rd., Ft. Collins, Colorado 80528-9544 (US). **HANES, David H.**; 3404 E. Harmony Rd., Ft. Collins, 80528-9544 (US). **McJILTON,**

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH,

[Continued on next page]

(54) Title: NETWORK ATTACHED STORAGE BACKUP



(57) Abstract: In one embodiment a network attached storage device comprises at least one storage media, a detection module to detect at least one computing device on a network, a configuration module to configure, in network attached storage device, backup settings, a coordination module to coordinate backup procedures, a network attached storage backup module to backup at least a portion of data from a computing device to the storage media, and a device backup module to backup only modified data from a computing device.

Fig. 3

WO 2009/096946 A1



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).

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

Published:

— *with international search report*

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

NETWORK ATTACHED STORAGE BACKUP

BACKGROUND

[0001] The term Network Attached Storage (NAS) refers to a dedicated data storage device(s) connected directly to a computer network to provide centralized data access and storage services to one or more network clients such as, e.g., a personal computer. In some circumstances it may be useful to back up data residing on the one or more network clients to a network attached storage device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] Fig. 1 is a schematic illustration of one embodiment of network attached storage environment.

[0003] Fig. 2 is a schematic illustration of an exemplary network attached storage device.

[0004] Fig. 3 is a flowchart illustrating operations in one embodiment of a backup configuration in network attached storage.

[0005] Fig. 4 is a flowchart illustrating operations in one embodiment of a backup procedure in network attached storage.

DETAILED DESCRIPTION

[0006] Described herein are exemplary systems and methods for data backup in network attached storage. The methods described herein may be embodied as logic instructions stored on a computer-readable medium. When executed on a processor, the logic instructions cause a general processor to be programmed as a special-purpose machine that implements the described methods. The processor, when configured by the logic instructions to execute the methods recited herein, constitutes structure for performing the described methods.

[0007] **Fig. 1** is a schematic illustration of one embodiment of network attached storage environment. Environment 100 may comprise one or more network attached storage devices 110a, 110b, 110c connected to one or more network clients 112a, 112b, 112c, 112d, 112e, 112f by a communication network 120.

[0008] Network attached storage devices 110a, 110b, 110c may be implemented as one or more communicatively connected storage devices. Exemplary storage devices may comprise, but are not limited to, the Media Vault™ line of storage devices commercially available from Hewlett-Packard Corporation of Palo Alto, California, USA. In some embodiments, at least a portion of communication network 120 may be implemented as a private, dedicated network such as, e.g., a local area network (LAN) or a wide area network (WAN). Alternatively, portions of communication network 120 may be

implemented using public communication networks such as, e.g., the Internet, pursuant to a suitable communication protocol such as, e.g. TCP/IP.

[0009] Network clients 112a, 112b, 112c, 112d, 112e, 112f may be implemented as computing devices such as, e.g., a networked computer 112a, a laptop computer 112b, a desktop computer 112c, a personal digital assistant (PDA) 112d, a smart phone 112e, other computing devices 112f or the like. Applications running on network clients 112a, 112b, 112c, 112d, 112e, 112f may initiate file access requests to access information stored in network attached storage devices 110a, 110b, 110c. Network attached storage devices 110a, 110b, 110c receive file access requests and, in response, locate and return the requested information to the network client that originated the request.

[0010] In some embodiments, a network attached storage device may monitor network traffic to identify any devices that may have been added to the network. In operation, a network attached storage device may detect a computing device on the network. The network attached storage device may then detect whether a computing device contains required firmware or software to allow for automatic configuration and backup. In some embodiments, a network attached storage device may also detect whether other network attached storage devices are on the network. In operation, the network attached storage device may then be configured to determine what data on a computing device is backed up, and when a backup is to be performed. In some embodiments, multiple network attached storage devices may be coordinated to distribute backup loads or as redundant backup. In operation, a

client may request a backup, or a network attached storage device may initiate a backup request depending on the configuration. In some embodiments, a network attached storage device may use key identifiers to label data so that identical data from various devices is only stored once. In operation, using a key identifier for backup data would comprise generating and assigning a key identifier to a block of data. The key identifier allows for the detection of the same key if one already exists. If the same data already exists elsewhere, a link to the storage location may be stored instead of the data. In some embodiments, a network attached storage device may perform an intelligent backup by only backing up data that has been modified since a previous backup.

[0011] **Fig. 2** is a schematic illustration of one embodiment of a network attached storage (NAS) device 200, which may be used to implement one or more of network attached storage devices 110a, 110b, 110c depicted in Fig. 1. Referring to Fig. 2, network storage device 200 comprises one or more network interfaces 210 which enables a communication connection with a network such as, e.g., network 120.

[0012] Network interface 210 may comprise an input/output (I/O) port to provide a physical connection with a network. For example, network interface 210 may comprise an Ethernet port. Network interface 210 may comprise a network interface card (NIC), also commonly referred to as a network adapter or a network card. The NIC manages I/O operations to enable NAS device 200 to communicate over a network. Alternatively, the operations of the NIC may be

implemented on a main circuit board such as, e.g., a motherboard of NAS device 200.

[0013] NAS device 200 further comprises at least one processor 212. As used herein, the term "processor" means any type of computational element, such as but not limited to, a microprocessor, a microcontroller, a complex instruction set computing (CISC) microprocessor, a reduced instruction set (RISC) microprocessor, a very long instruction word (VLIW) microprocessor, or any other type of processor or processing circuit.

[0014] NAS device 200 further comprises system random access memory and/or read-only memory 230. Memory 230 comprises an operating system 240 for managing operations of NAS device 200. In one embodiment, operating system 240 comprises a hardware interface module 254 that provides an interface to system hardware. The particular embodiment of operating system 240 is not critical to the subject matter described herein. Operating system 240 may be embodied as a UNIX operating system or any derivative thereof (e.g., Linux, Solaris, *etc.*) or as a Windows® brand operating system.

[0015] Operating system 240 comprises (or interfaces with) a file system(s) 250 that manages files used in the operation of NAS device 200. For example, file system(s) 250 may implement one or more file systems such as FAT, NTFS, ext3, reiser, or the like. In one embodiment, operating system 240 may comprise a file cache management system 244 interposed logically between the file system(s) 250 and underlying modules such as, e.g., the hardware interface module 254. File cache management system 244 interfaces

with the file system(s) 250 to manage the file cache 256 as a resource that may be shared between users of the computer system, e.g., on a per-workload basis.

[0016] Operating system 240 further comprises a system call interface module 242 that provides an interface between the operating system 240 and one or more application modules that execute on NAS device 200.

[0017] NAS device 200 further comprises storage media 280. For example, storage media 280 may be embodied as one or more arrays of magnetic disk drives, solid state drives or the like. Alternatively, storage media 280 may comprise optical, magneto-optical, or electro-optical storage media. Storage media 280 may be configured to implement RAID redundancy.

[0018] NAS device 200 further comprises a detection module 260. In some embodiments, a detection module is embodied as a software module that executes on processor(s) 212. By way of example and not limitation, a detection module may listen to network broadcast traffic to detect any devices that may be present on the network. When a device is detected, a detection module may connect to the device on a predetermined port to find out if the device contains required firmware and/or software to allow for automatic configuration for backup. In some embodiments, a detection module may also detect the presence of other NAS devices on the network and may establish peer-to-peer communication between NAS devices.

[0019] NAS device 200 further comprises a configuration module 262. In some embodiments, a configuration module is embodied as a software module

that executes on processor(s) 212. By way of example and not limitation, a configuration module controls backup settings by device category, type or the like, based on a rules engine and may be granular to device identifying information. By way of example and not limitation, a configuration module may control what data on a connected device is backed up and/or synchronized, when to perform backups, or the like. In some embodiments, the software in a configuration module is preconfigured with common computing device settings for backup. In some embodiments, a configuration module backup settings may be modified to fit a client's preference.

[0020] NAS device 200 further comprises a coordination module 264. In some embodiments, a coordination module is embodied as a software module that executes on processor(s) 212. By way of example and not limitation, a coordination module may coordinate backup activities with other NAS devices on the network. Coordination of a backup may be used to distribute computing workload, redundant backup or the like.

[0021] NAS device 200 further comprises a NAS backup module 266. In some embodiments, NAS backup module is embodied as a software module that executes on processor(s) 212. In some embodiments, a NAS backup module may receive backup communication requests from a client, can initiate backup requests to a client, or the like, depending on configuration. In some embodiments, a NAS backup module may use image/block level identifiers for data to backup so data from various devices is only stored once and therefore reducing duplicate data storage. By way of example and not limitation, an

identifier system may generate and assign key identifiers to a block of data thus allowing for detection of key identifiers already present in backup storage. In some embodiments, a NAS backup module may store a link to data already present in backup storage, as determined through a key identifier, as to reduce redundant storage.

[0022] NAS device 200 further comprises a device backup module 268. In some embodiments, a device backup module is embodied as a software module that executes on processor(s) 212. In some embodiments, a device backup module may initiate an intelligent backup and only backup modified data based on configurations provided by a NAS device.

[0023] Operations implemented by some embodiments of detection module 260, configuration module 262, coordination module 264, NAS backup module 266 and/or device backup module 268 are described with reference to Fig. 3 and Fig. 4.

[0024] **Fig. 3** is a flowchart illustrating operations in one embodiment of a method of backup configuration on a network attached storage device. In some embodiments, the operations depicted in Fig. 3 are implemented by the configuration module 262.

[0025] Referring to Fig. 3, at operation 305, a network attached storage device may detect the addition of one or more computing devices to a network. In some embodiments, detecting the addition of a computing device onto a network to which a network attached storage device is attached comprises: monitoring data traffic on the network, maintaining a list of computing devices

connected to the network, and comparing data identifying a source of data traffic with one or more entries on the list of computing devices connected to the network. In some embodiments, detection of connected devices may be accomplished by a network attached storage device listening to network traffic and determining what devices are present through monitoring data traffic on the network. In some embodiments, a network attached storage device may maintain a list of computing devices connected to the network. In some embodiments, a network attached storage device may compare data identifying a source of data traffic with one or more entries on a list of computing devices connected to the network to determine whether the device has been connected to the network previously.

[0026] At operation 310, a network attached storage device may initiate a communication connection with one or more computing devices that may have been added to the network. In some embodiments, initiating a remote backup configuration procedure to configure a computing device for remote backup operations comprises; determining a device type associated with a computing device, and entering the device type into a rules engine to obtain a backup configuration setting associated with the device type. By way of example and not limitation, a communication connection may be initiated by a client, by preset configurations on a network attached storage device or the like.

[0027] Once a network attached storage device has communicatively connected with one or more computing devices on a network, a network attached storage device must determine if computing devices connected to the

network allows for remote backup. In some embodiments, determining whether a computing device supports remote backup configuration comprises, detecting the presence of a firmware module on the computing device by accessing the contents of a predetermined memory location on the computing device. If at operation 315, one or more computing devices does not allow for remote backup, then at operation 320 notice is given that the computing device(s) do not support remote backup. By contrast, if at operation 315 one or more computing devices does allow for remote backup, then a network attached storage (NAS) device may initiate backup configuration procedures at operation 330. In some embodiments, configuring a backup procedure for at least one computing device connected to a network may comprise; detecting at least one additional network attached storage device connected to a network, and coordinating backup activities between multiple network attached storage devices.

[0028] In some embodiments, a NAS device may be configured to communicate with one or more remote server(s). In such embodiments, a NAS device may connect with the remote server(s) and download computing device configurations for data backup procedures. In some embodiments, a NAS device may maintain a table of configuration settings logically associated with computing device types. In some embodiments, a NAS device may periodically update a table of computing device configurations via a network connection to a remote server(s). In some embodiments, a network attached storage device may communicate with devices through prespecified ports to determine if the device contains the required firmware and/or software to allow for automatic

backup and/or synchronization. In some embodiments, multiple network attached storage devices are connected to a network and may coordinate to distribute backup procedure loads.

[0029] By way of example, and not limitation, a network attached storage device may detect an encoded flag in a computing device that may point to a predetermined memory location in the computing device.

[0030] **Fig. 4** is a flowchart illustrating operations in one embodiment of data backup on a network attached storage device. In some embodiments, the operations depicted in Fig. 4 are implemented by the detection module 260, the configuration module 262, the coordination module 264, the NAS backup module 266 and/or the device backup module 268.

[0031] At operation 400 a backup procedure is initiated. In some embodiments, the backup procedure may be initiated by a client. In some embodiments, a backup procedure may be initiated by a network attached storage device. In some embodiments, multiple network attached storage devices may be connected to a network and may be coordinated to share task responsibilities. In some embodiments, processing a backup procedure of at least a portion of data on connected computing devices may comprise using block level key identifiers for data to be backed up to avoid duplication of data storage. By way of example and not limitation, a network attached storage device may contain preset configurations of common computing devices that allow for remote backup.

[0032] If, at operation 405 the backup procedure is being performed for the first time, then at operation 410 a NAS device may generate and assign key identifiers to data blocks as it stores data during a backup procedure. In some embodiments, key identifiers may be sent to a client and stored in a memory location of a client computing device as well as on a network attached storage device. In some embodiments, a client may independently generate key identifiers for data blocks and transmit them to a network attached storage device. By way of example, and not limitation, when a backup procedure is performed on a computing device that does not contain much processing power, a network attached storage device may compute key identifiers for data blocks and transmit these key identifiers to the computing device.

[0033] In some embodiments, a client computing device and a network attached storage device may both generate and assign key identifiers to data blocks. In such embodiments, the client computing device and the network attached storage device may use the same function to generate the key identifiers to allow for synchronization during any subsequent backup procedures. By way of example and not limitation, key identifiers may be implemented as a hash function, a cyclic redundancy check (CRC) or any other mathematic function that may generate a unique value based on the contents of a memory block.

[0034] By contrast, if at operation 405 the backup procedure is not being performed for the first time, then a loop may be implemented to backup data blocks from computing devices at operation 415.

[0035] At operation 420 a network attached storage device may determine if a data block has a key identifier that matches data currently stored in backup. If, at operation 420, a data block has a matching key identifier present in a network attached storage device backup, then that data block is current (Operation 425), and the backup procedure may move to the next data block (Operation 430). In some embodiments, a link is provided to allow for access to data blocks already stored elsewhere in a network attached storage device backup storage. In some embodiments, linking to preexisting data blocks allows for reduction of storage of duplicate data which may be helpful in situations such as, but not limited to backing up operating system files from various devices.

[0036] By contrast, if at operation 420, a data block key identifier does not have a matching key identifier in a backup storage, then the data block is not current (Operation 435). At operation 440, a network attached storage device may generate and assign a key identifier to the data block and at operation 445, the data is stored.

[0037] Finally, at operation 450, key identifiers may be transmitted to a client and/or client computing device and the backup procedure may move to the next data block to be processed.

[0038] Some embodiments may be provided as computer program products, which may comprise a machine-readable or computer-readable medium having stored thereon instructions used to program a computer (or other electronic devices) to perform a process discussed herein. The machine-

readable medium may comprise, but is not limited to, floppy diskettes, hard disk, optical disks, CD-ROMs, magneto-optical disks, ROMs, RAMs, erasable programmable ROMs (EPROMs), electrically erasable EPROMs (EEPROMs), magnetic or optical cards, flash memory, or other suitable types of media or computer-readable media suitable for storing electronic instructions and/or data. Moreover, data discussed herein may be stored in a single database, multiple databases, or otherwise in select forms (such as in a table).

[0039] Reference in the specification to “one embodiment” or “an embodiment” means that a particular feature, structure, or characteristic described in connection with the embodiment is comprised in at least an implementation. The appearances of the phrase “in one embodiment” in various places in the specification are not necessarily all referring to the same embodiment.

CLAIMS

What is claimed is:

1. A method to manage backup services for remote clients of a network attached storage device, comprising:
 - detecting, in the network attached storage device, the addition of a computing device onto a network to which the network attached storage device is connected;
 - initiating, in the network attached storage device, a communication connection with the computing device;
 - determining whether the computing device supports remote backup configuration; and
 - in response to a determination that the computing device supports remote backup configuration, initiating, in the network attached storage device, a remote backup configuration procedure to configure the computing device for remote backup operations.
2. The method of claim 1, wherein detecting, in the network attached storage device, the addition of a computing device onto a network to which the network attached storage device is attached comprises:
 - monitoring, in the network attached storage device, data traffic on the network;
 - maintaining, in the network attached storage device, a list of computing devices connected to the network; and
 - comparing data identifying a source of data traffic with one or more entries on the list of computing devices connected to the network.
3. The method of claim 1, wherein determining whether the computing device supports remote backup configuration comprises:
 - detecting the presence of a firmware module on the computing device by accessing the contents of a predetermined memory location on the computing device.

4. The method of claim 1, wherein initiating, in the network attached storage device, a remote backup configuration procedure to configure the computing device for remote backup operations comprises:

- determining a device type associated with the computing device; and
- entering the device type into a rules engine to obtain a backup configuration setting associated with the device type.

5. The method of claim 1, wherein configuring, by the network attached storage device, backup procedure for at least one computing device connected to a network comprises:

- detecting at least one additional network attached storage device connected to a network; and
- coordinating backup activities between multiple network attached storage devices.

6. The method of claim 1, further comprising:

- processing, by the network attached storage device, a backup procedure of at least a portion of data on connected computing devices comprises using block level key identifiers for data to be backed up to avoid duplication of data storage.

7. The method of claim 6, wherein using block level identifiers comprises:

- generating a key identifier for a block of data;
- assigning the key identifier to the block of data; and
- storing a link to existing data located through the key identifier.

8. A computer program product comprising logic instructions stored on a computer-readable medium which, when executed by a computer processor, configure the processor to:

detect, in the network attached storage device, the addition of a computing device onto a network to which the network attached storage device is connected;

initiate, in the network attached storage device, a communication connection with the computing device;

determine whether the computing device supports remote backup configuration; and

in response to a determination that the computing device supports remote backup configuration, initiate, in the network attached storage device, a remote backup configuration procedure to configure the computing device for remote backup operations.

9. The computer program product of claim 8, further comprising logic instructions stored on a computer-readable medium which, when executed by a computer processor, configure the processor to:

monitor, in the network attached storage device, data traffic on the network;

maintain, in the network attached storage device, a list of computing devices connected to the network; and

compare data identifying a source of data traffic with one or more entries on the list of computing devices connected to the network.

10. The computer program product of claim 8, further comprising logic instructions stored on a computer-readable medium which, when executed by a computer processor, configure the processor to:

detect the presence of a firmware module on the computing device by accessing the contents of a predetermined memory location on the computing device.

11. The computer program product of claim 8, further comprising logic instructions stored on a computer-readable medium which, when executed by a computer processor, configure the processor to:

- determine a device type associated with the computing device; and
- consult entering the device type into a rules engine to obtain a backup configuration setting associated with the device type.

12. The computer program product of claim 8, further comprising logic instructions stored on a computer-readable medium which, when executed by a computer processor, configure the processor to:

- detect at least one additional network attached storage device connected to a network; and
- coordinate backup activities between multiple network attached storage devices.

13. The computer program product of claim 8, wherein logic instructions stored on a computer-readable medium which, when executed by a computer processor, configure the processor to process a backup procedure of at least a portion of data on connected computing devices comprises using block level identifiers for data to be backed up to avoid duplication of data storage.

14. The computer program product of claim 8, wherein logic instructions stored on a computer-readable medium which, when executed by a computer processor, configure the processor to use block level identifiers to:

- generate a key identifier for a block of data;
- assign the key identifier to the block of data; and
- store a link to existing data located through the key identifier.

15. A network attached storage device, comprising:
 - at least one storage media;
 - a detection module to detect at least one computing device on a network;
 - a configuration module to configure, in network attached storage device, backup settings;
 - a coordination module to coordinate backup procedures;
 - a network attached storage backup module to backup at least of portion of data from a computing device to the storage media; and
 - a device backup module to backup only modified data from a computing device.
16. The network attached storage device of claim 15, wherein the detection module is further configured to:
 - scan for presence of at least one other network attached storage device on a network; and
 - use at least two network attached storage devices on a network to distribute backup process tasks.
17. The network attached storage device of claim 15, wherein the configuration module is further configured with specified backup settings for a number of common devices.
18. The network attached storage device of claim 15, wherein the network attached storage backup module is further configured to use data key identifiers to avoid redundant backup.
19. The network attached storage device of claim 15, wherein the device backup module is configured to limit data backup to data that has been modified since a prior backup.

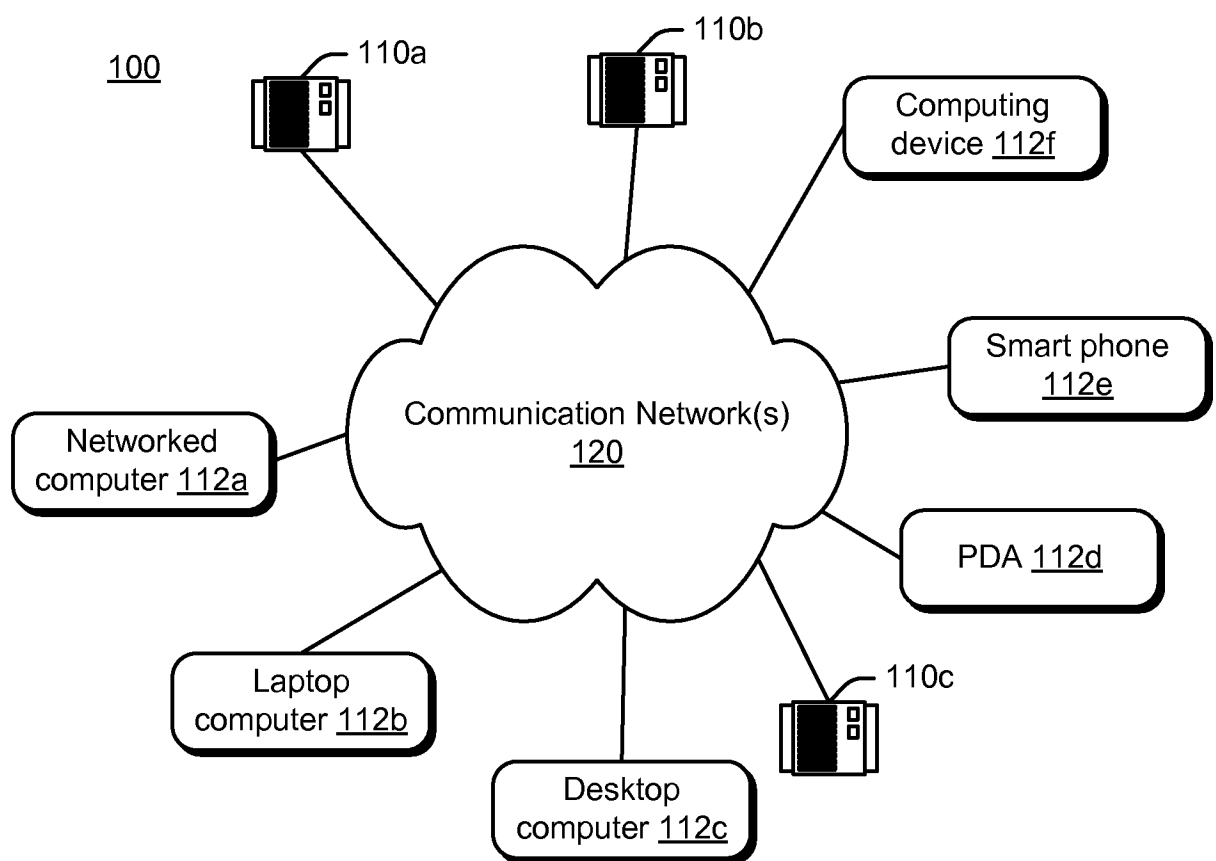
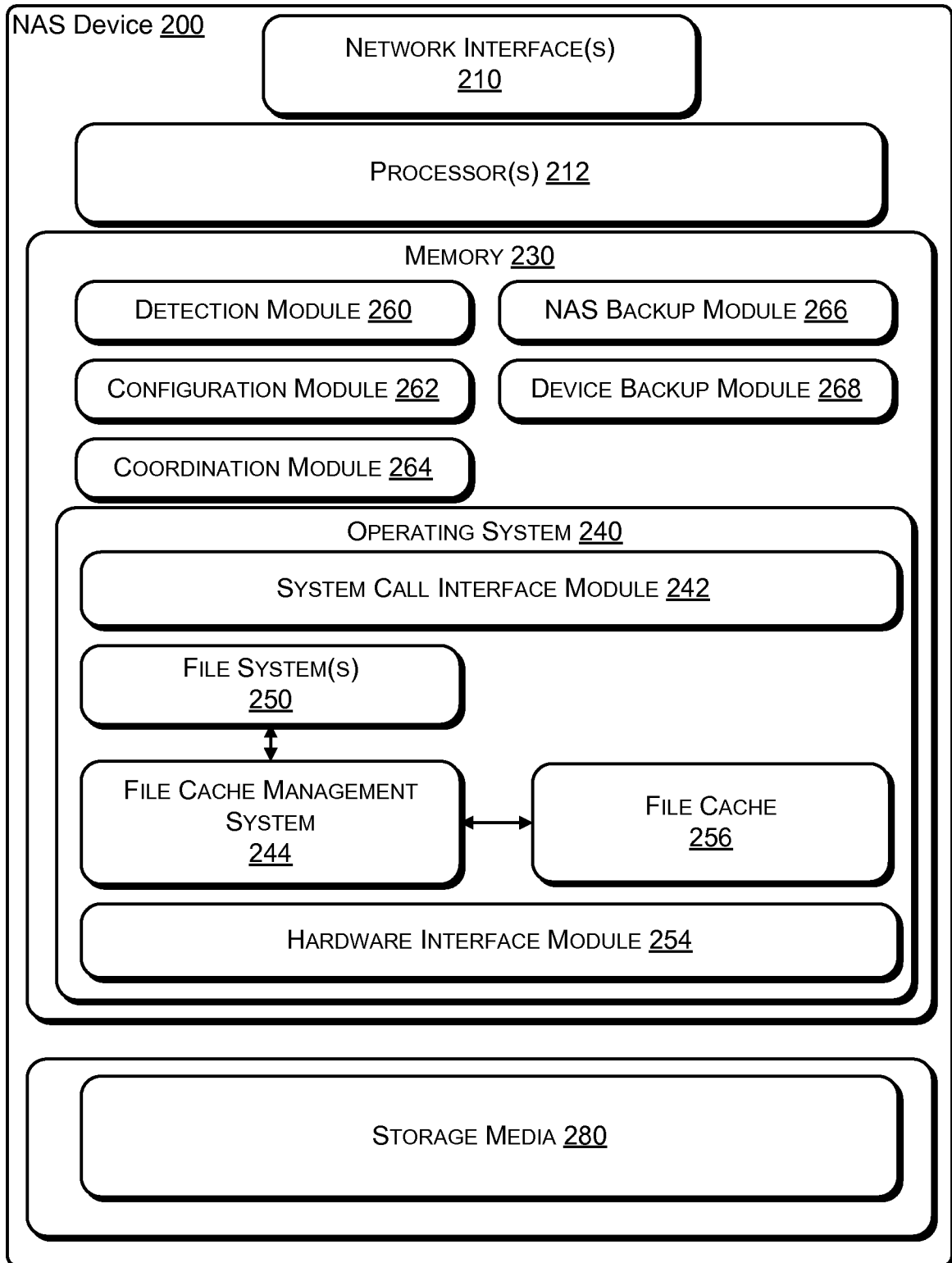
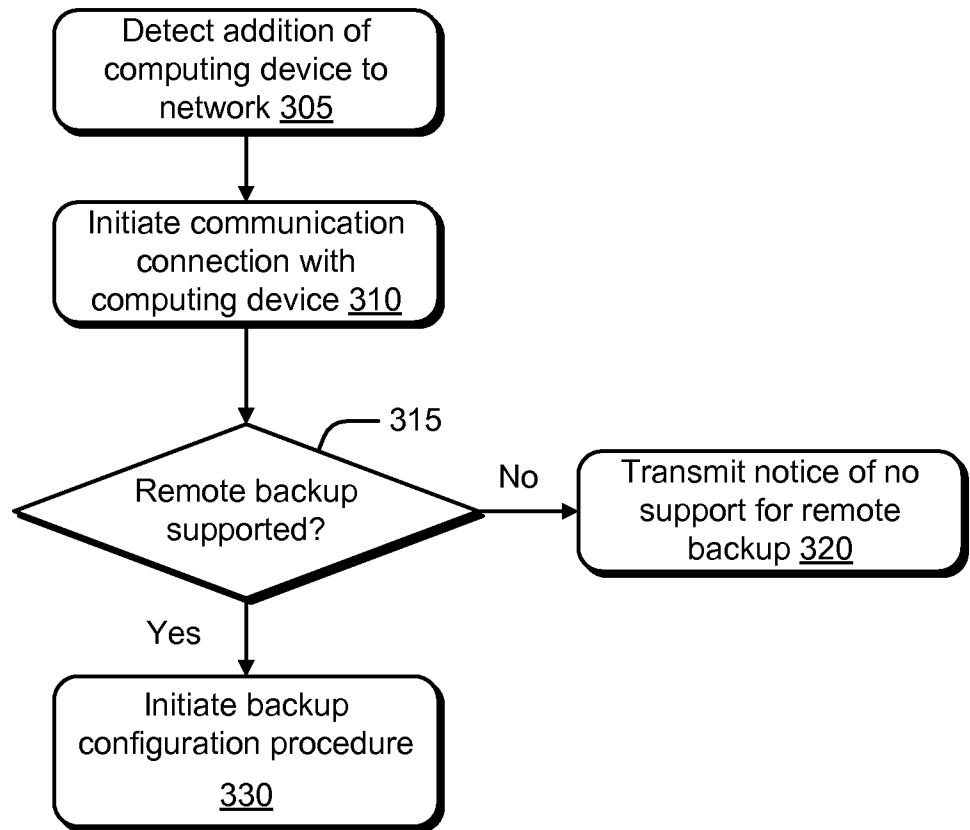


Fig. 1

**Fig. 2**

**Fig. 3**

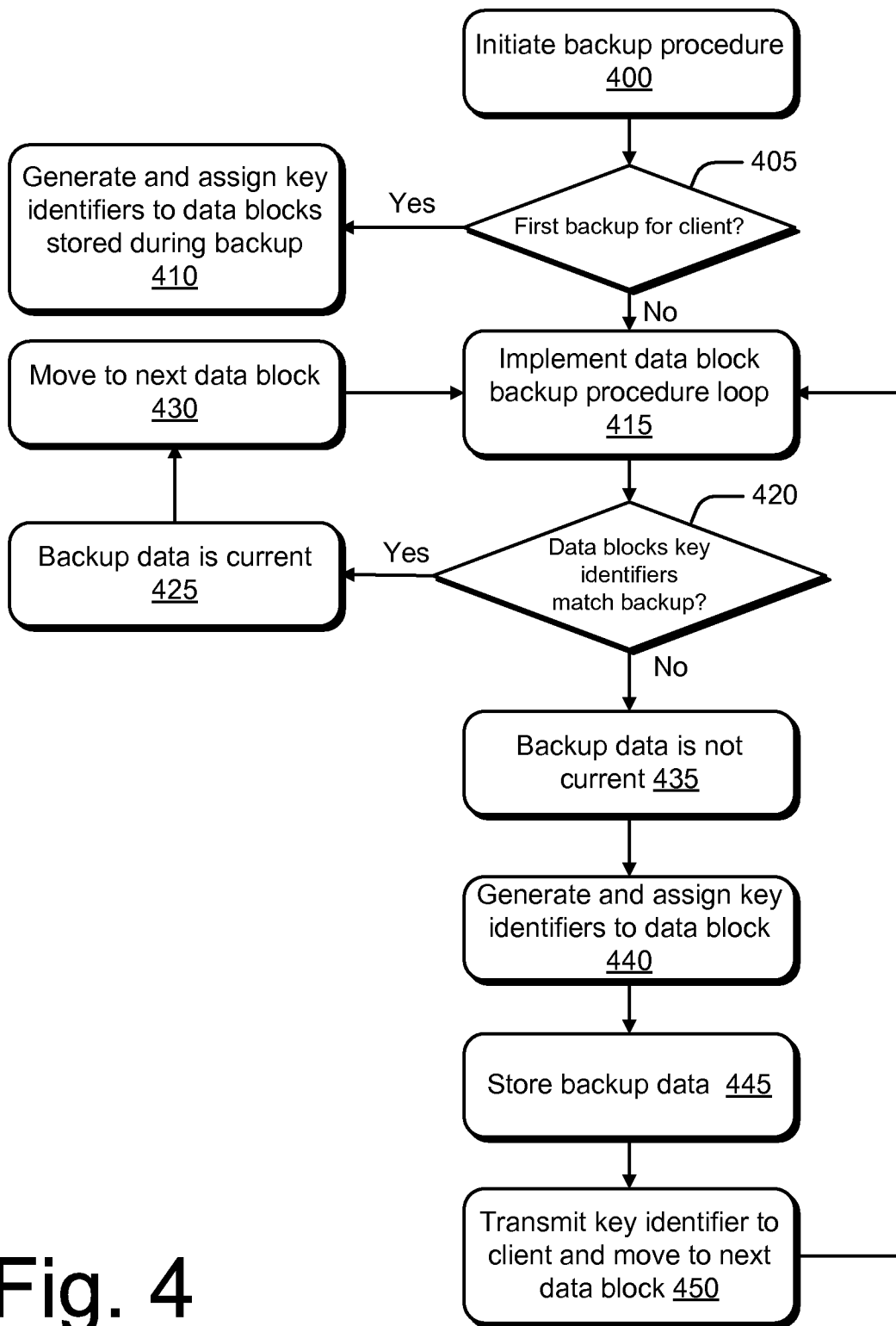


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2008/052313**A. CLASSIFICATION OF SUBJECT MATTER****G06F 12/16(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 12/16, G06F 15/16

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 application 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) "network, storage, backup, configuration"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004-0162900 A1 (TIM BUCHER et al.) 19 August 2004 See abstract; paragraphs [0057]-[0070]; fig.4, fig.5	1-19
A	US 2004-0143657 A1 (YU-TE WU et al.) 22 July 2004 See abstract; paragraphs [0021]-[0042]; fig.5, fig.8	1-19
A	US 6622220 B2 (STUART YOSHIDA et al.) 16 September 2003 See column 5, line 38 - column 11, line 16; fig.3	1-19
A	US 6892264 B2 (MICHAEL LOREN LAMB) 10 May 2005 See abstract; column 21, line 26 - column 84, line 8	1-19

☐ 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

15 OCTOBER 2008 (15.10.2008)

Date of mailing of the international search report

16 OCTOBER 2008 (16.10.2008)

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

Son, Yoon Sik

Telephone No. 82-42-481-5720



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2008/052313

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004-0162900 A1	19.08.2004	AU 2003-303432 A1 CA 2510116 A1 EP 1586043 A1 EP 1586043 A4 JP 2006-510991 A	22.07.2004 15.07.2004 19.10.2005 22.03.2006 30.03.2006
US 2004-0143657 A1	22.07.2004	JP 2004-227572 A TW 583538 B TW 583538 A	12.08.2004 11.04.2004 11.04.2004
US 6622220 B2	16.09.2003	US 2002-0174307 A1	21.11.2002
US 6892264 B2	10.05.2005	US 2003-0149753 A1	07.08.2003