



(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)

(21) International Application Number:
PCT/US2015/021515

(22) International Filing Date:
19 March 2015 (19.03.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/969,309 24 March 2014 (24.03.2014) US

(71) Applicant: THOMSON LICENSING [FR/FR]; 1-5 rue
Jeanne d'Arc, 92130 Issy Les Moulineaux (FR).

(72) Inventors: BETSCH, Jean-Sebastien; 5016 Bakman Ave,
#103, North Hollywood, California 91601 (US). RAMOS,
Adrian; 728 S. Marengo Ave, Apt. 2, Pasadena, California
91106 (US).

(74) Agents: SHEDD, Robert D. et al.; Thomson Licensing
LLC, 4 Research Way, 3rd floor, Princeton, New Jersey
08540 (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, 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, IR, IS, JP, KE, KG, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG,

[Continued on next page]

(54) Title: CONTENT SEGREGATION VIA LOGICAL UNIT NUMBER (LUN) MASKING

(57) Abstract: A method is described for performing content segregation by a network security system using logical unit number masking. Also described is a method including logging on to a client device by a first user, retrieving permissions from a database for the first user, spoofing a worldwide name for the first user into the client device host bus adapter, mapping logical unit numbers according to the first user's permissions and accessing content segregated network resources.

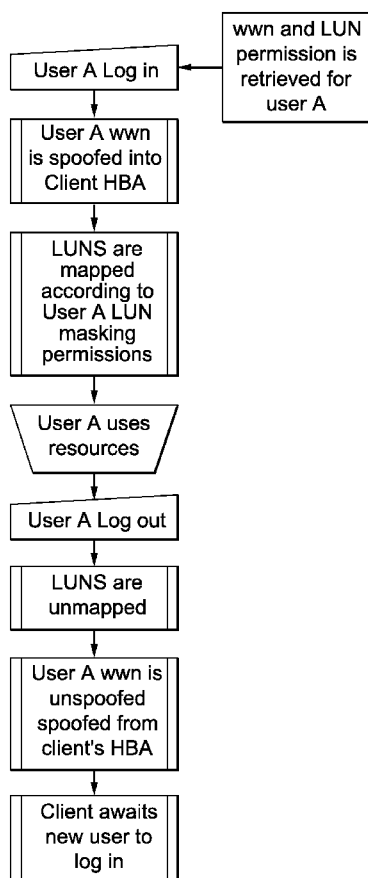


FIG. 5



MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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.

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, KM, ML, MR, NE, SN, TD, TG).

(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, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,

Published:

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

CONTENT SEGREGATION VIA LOGICAL UNIT NUMBER (LUN) MASKING

FIELD OF THE INVENTION

The present invention is related to providing a LUN masking at a user level
5 (i.e., users of a client) such that user access to volumes of a storage area network (SAN) can be restricted.

BACKGROUND OF THE INVENTION

In multicast and broadcast applications, data are transmitted from a server to
10 multiple receivers over wired and/or wireless networks. A multicast system as used herein is a system in which a server transmits the same data to multiple receivers simultaneously, where the receivers form a subset of all the receivers up to and including all of the receivers. A broadcast system is a system in which a server transmits the same data to all of the receivers simultaneously. That is, a multicast
15 system by definition can include a broadcast system.

In conventional Storage Area Networks (SANs) all data on the SAN is accessible to clients connected to the SAN. As used herein a client is an end device which is used by users. That is, in production type facilities,. A client (client device) may be used by any authorized user and is not restricted to any particular user.
20 Exemplary clients for Technicolor include internal production machines, each having a fiber card having worldwide name (WWN) that indicates to which SAN the fiber card has access. However, Technicolor customers (e.g., Disney and other studios) want to limit which clients have access to the customer's data on the SAN. For example, the customer may desire that only certain clients (i.e., certain production
25 machines) have access to the client's data on the SAN. An additional example is that the customer may also want to limit which Technicolor employees can access the customers data on the SAN (i.e., the customer may only want a single Technicolor employee to access the customer's data, may desire to limit the time of day or work shift during which the Technicolor employee can access the data, and the like).

30 A conventional approach to fulfilling the desire of Technicolor's customers would be to have a dedicated SAN for each Technicolor customer. However, SANs are expensive and this type of solution is cost prohibitive.

SUMMARY OF THE INVENTION

Traditional LUN (Logic Unit Number) masking is provided at a client device (e.g., production machine) level such that the client device is given access to specific folders or volumes within a Storage Area Network (SAN). The present invention is directed to providing a LUN masking at a user level (i.e., users of a client) such that
5 user access to volumes of a storage area network (SAN) can be restricted.

The present invention proposes content segregation by leveraging LUN masking as a mechanism for end user authentication and access. Therefore, organizing LUN masking at the user level instead of at the host bus adapter (HBA) hardware level (worldwide name).

10 The digital cinema industry is moving towards tighter security, which requires segregation of content. So far, this has been strictly physical segregation, but the present invention permits logical segregation as well.

BRIEF DESCRIPTION OF THE DRAWINGS

15 The present invention is best understood from the following detailed description when read in conjunction with the accompanying drawings. The drawings include the following figures briefly described below:

Fig. 1 is a schematic diagram showing conventional LUN masking.

Fig. 2 is a schematic diagram showing a simplified direct access to storage.

20 Fig. 3 is a schematic diagram showing the LUN masking of the present invention where the worldwide name is altered based on user login.

Fig. 4 is a simplified diagram of the operation of the present invention.

Fig. 5 is a flowchart of an exemplary implementation of the present invention.

25 Fig. 6 is a block diagram of an exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is described in terms of a content mastering system but is not so limited and may be used anywhere access to content may or must be segregated by user and in particular, where SANs are used for content storage.

5 A storage area network (SAN) is a dedicated storage fabric that provides access to clustered, block level data storage. SANs are primarily used to make volumes and file system storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of
10 storage devices that are generally not accessible through the local area network by other devices.

LUN masking is an authorization process that makes a Logical Unit Number available to some hosts and unavailable to other hosts. LUN masking is mainly implemented at HBA level. The security benefits of LUN masking
15 implemented at HBAs are limited, since with many HBAs it is possible to forge source addresses (WWNs/MACs/IPs) and compromise the access. Many storage controllers also support LUN masking. When LUN masking is implemented at storage controller level, controller itself enforces the access policies to the device which makes access more secure. However, it is mainly implemented not as a security
20 measure per se, but rather as a protection against misbehaving servers which may corrupt disks belonging to other servers. Conventional LUN masking is used to restrict a client's access to a specific volume on a Storage Area Network. Note that client device refers to a server/machine not a user. The server is identified by a worldwide name that is hard-coded in the fiber card of the server. As a result any user
25 logging on to the server will have the same access to the volumes. In the present invention, the user logs on to a server and overwrites the default server wwn with a personal wwn that refers to a user (person). Therefore, depending on who logs on to a server, the visibility of volumes is different. Thus, the present invention is a security protocol to restrict user visibility to a SAN.

30 A host bus adapter (HBA) connects a host system (the computer) to other network and storage devices. The terms are primarily used to refer to devices for connecting small computer system interface (SCSI), Fibre Channel and external serial advanced technology attachment (eSATA) devices. An eSATA is an external

computer bus interface that connects HBAs to mass storage devices such as hard disk drives and optical drives.

A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC
5 addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware
10 address (EHA), hardware address or physical address. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address.

A worldwide name (WWN) or worldwide identifier (WWID) is a unique identifier used in storage technologies including Fibre Channel, Advanced
15 Technology Attachment (ATA) or Serial Attached SCSI (SAS). A WWN may be employed in a variety of roles, such as a serial number or for addressability; for example, in Fibre Channel networks, a WWN may be used as a WWNN (worldwide node name) to identify a switch, or a WWPN (worldwide port name) to identify an individual port on a switch.

20 A network controller/metadata controller (or MDC) is a storage area network (SAN) technology for managing file locking, space allocation and data access authorization. This is needed when several clients are given block level access to the same disk volume. MDC examples include Data Direct Network Controller and Quantum D660.

25 The present invention provides an additional layer of software, which can provide an additional security mechanism that other (less burdensome, but more expensive, less flexible) solutions do not provide. That is, the present invention can provide logging, and easy, dynamic granting or denying access through user account management. This additional software layer also provides flexibility to meet further
30 security needs that might evolve in the future. The present invention promotes a secure, logged, user oriented, LUN masking mechanism that answers many of the security needs of studios (customers).

Fig. 1 is a schematic diagram showing conventional LUN masking. In Fig. 1 each client device is assigned a worldwide name. each client device is logged in to the network controller via an HBA. The network controller advises the fiber switch of the client logging in and the client's worldwide name. The client's worldwide name is mapped to a particular LUN or multiple LUNs by LUN masking. For example, client device 1 is assigned WWM1, which is mapped via LUN masking to LUN C only. Client device 1 logs on to the network controller via its HBA. The network controller advise the fiber switch of client device 1 logging in. The fiber switch only allows WWN1 to access LUN C only. Client device 2 is assigned WWN2 so when client device 2 logs on to the network controller via the HBA, the network controller advises the fiber switch of client device 2 logging in and the client device's worldwide name. The fiber switch allows WWN2 to access LUN A, LUN B and LUN C. Client device 3 is assigned WWM3, which is mapped via LUN masking to LUN A only. Client device 3 logs on to the network controller via its HBA. The network controller advise the fiber switch of client device 3 logging in. The fiber switch only allows WWN3 to access LUN A only. It does not matter which user is sitting at any of the client devices (work stations, client, server). It only matters what worldwide name is assigned to the client device (client, work station, server). In a content mastering environment, any user could sit at any work station (client, client device, server) and access whatever the worldwide name was authorized to access. By sitting a client device 2 a user that was not authorized by a particular studio to access the content of the particular studio would be granted access to the content simply based on which client (work station, client device, server) to which the user logged on. This is not acceptable to some studios. Some studios want access to their content restricted to one or a very small number of users or perhaps to a particular user or small number of users and further only at specified times (work shifts and/or work days).

A conventional approach to fulfilling the desire of studios (customers) would be to have a dedicated SAN for each customer (studio). However, SANs are expensive and this type of solution is cost prohibitive.

Fig. 2 is a schematic diagram showing a simplified direct access to storage. In the approach shown in Fig. 2, clients (client devices, work stations, servers) would have access to the LUN storage directly (probably via hard-wiring) to which their

worldwide name allowed access. This does not really solve the problem of controlling access by user rather than by client (client device, server, work station). As shown in Fig. 1 client device 1 has access only to LUN C. Client device 3 has access only to LUNA and client device 2 has access to LUN A, LUN B and LUN C.

5 Fig. 3 is a schematic diagram showing the LUN masking of the present invention where the worldwide name is altered based on user login. In Fig. 3 a user logs on to a client device. In the case shown in Fig. 3, user A logs on to client device 1. Upon login of user A (and proper identification of user A by some means known in the art such as user identification and password or biometric data such as fingerprint or iris scan), a script is executed which maps user A to WWN1. The implementation of software that captures the user credential and in turn allows the spoofing of the HBA's worldwide name to a worldwide name which is unique to each user. Therefore, carrying the LUN masking configuration, specific to a user on any machine the user is logged into.

15 Fig. 4 is a simplified diagram of the operation of the present invention. In Fig. 4 (1) user A logs in on client device 1 and accesses LUN C. In Fig. 4 (2) when user A is done, user A logs off of client device 1. In Fig. 4 (3) user B then logs in on client device 1 and access LUN A, LUN B and LUN C in accordance with user B's access permissions.

20 Fig. 5 is a flowchart of an exemplary implementation of the present invention. In Fig. 5 when user A logs in using a particular client device, the security database is accessed in order to retrieve the permissions for user A. A user's identity is verified or confirmed by using a user ID and password or biometric data. The wwn for user A is spoofed into client device HBA. The LUNs are mapped according to user A LUN masking permissions. User A uses the network resources to complete his/her work whereupon user A logs out/off of the particular client device. Network resources include LUNs of a SAN. Upon receiving the log out/off, the LUNs are unmapped by the security system of the present invention. User A wwn is unspoofed from the client device's HBA. The particular client device is now ready to accept a new user to log
25 in/on.
30

There is a need to establish a user priority protocol in order to resolve conflicts that will emerge from multiple users on client devices. Multiple users may login to a client device – whose wwn is used. If a user logs out while operations are in progress, what happens to the content and to the mapping (access) to the content?

5 When multiple users login to a client device (client, work station, server), the wwn name used to define access to the SAN is always be the one associated with the first user to login. This will define SAN access until the user logs out or is idle for a certain period of time and automatically logged off the client device. In case of several users logging in remotely, a hierarchy of users can be created and only users
10 with equal or superior credentials will be permitted to login alongside an existing user. The client device and, therefore, all users logged in will however keep the access level and wwn of the first user. A new wwn can only be spoofed when all users are logged off and new single user logs in.

 When a user logs off as operations are in process, the client device retains the
15 wwn and access level of the user until all operations are completed. It is only then that the user is “really” logged off of the client. This will prevent any interruption accessing data on the SAN. If another user tries to log in while operations are still in progress, the multiple user protocol is the same as multiple users described above. Once operations are completed and if another user has logged in while those
20 operations where in progress, he/she is prompted and given the choice to re-log in to spoof his own personal wwn.

 In the scenario shown in Fig. 3 above, if user B logs in while user A is logged in then user B is limited to LUN C unless user B is a super user (a user with superior security credentials and permissions). If user A then logs out then user B is still only
25 given access to LUN C. User B will, however, be prompted to logout and log back in again in order to receive full access to LUNS A, B and C. In the scenario depicted in Fig. 3, if user C logs in while user A is logged in then user C has no access unless user C is a super user. This is because user C only has access permission for LUN A and user A has no access to LUN A and user C is limited to user A’s access permissions.

30 The security protocol can also be tightened to only allow one user at a time with a super user who would be able to log in at any time and also force the log off of other users.

Fig. 6 is a block diagram of an exemplary embodiment of the present invention. Fig. 6 includes a network controller, which includes a number of modules. There is an I/O module for accepting users logging in/out (off) and is also used to provide for user identity verification (confirmation). This I/O module is in communication with a security database where users' permissions are stored including users' masking permissions in accordance with the principles of the present invention. The security database is in communication with a module which performs spoofing of a user's wwn into the client device onto which the user is logged on. This module also maps the LUNs according to the user's permissions. When the user logs out (off) then this module also unmaps the LUNs and unspoofs the user's wwn. This module is in communication with an access module which permits the user to access the content segregated network resources in accordance with the spoofing and mapping. The content is segregated on the various LUNs of one or more SANs.

It is to be understood that the present invention may be implemented in various forms of hardware, software, firmware, special purpose processors, or a combination thereof. Special purpose processors may include application specific integrated circuits (ASICs), reduced instruction set computers (RISCs) and/or field programmable gate arrays (FPGAs). Preferably, the present invention is implemented as a combination of hardware and software. Moreover, the software is preferably implemented as an application program tangibly embodied on a program storage device. The application program may be uploaded to, and executed by, a machine comprising any suitable architecture. Preferably, the machine is implemented on a computer platform having hardware such as one or more central processing units (CPU), a random access memory (RAM), and input/output (I/O) interface(s). The computer platform also includes an operating system and microinstruction code. The various processes and functions described herein may either be part of the microinstruction code or part of the application program (or a combination thereof), which is executed via the operating system. In addition, various other peripheral devices may be connected to the computer platform such as an additional data storage device and a printing device.

It is to be further understood that, because some of the constituent system components and method steps depicted in the accompanying figures are preferably implemented in software, the actual connections between the system components (or the process steps) may differ depending upon the manner in which the present

invention is programmed. Given the teachings herein, one of ordinary skill in the related art will be able to contemplate these and similar implementations or configurations of the present invention.

CLAIMS:

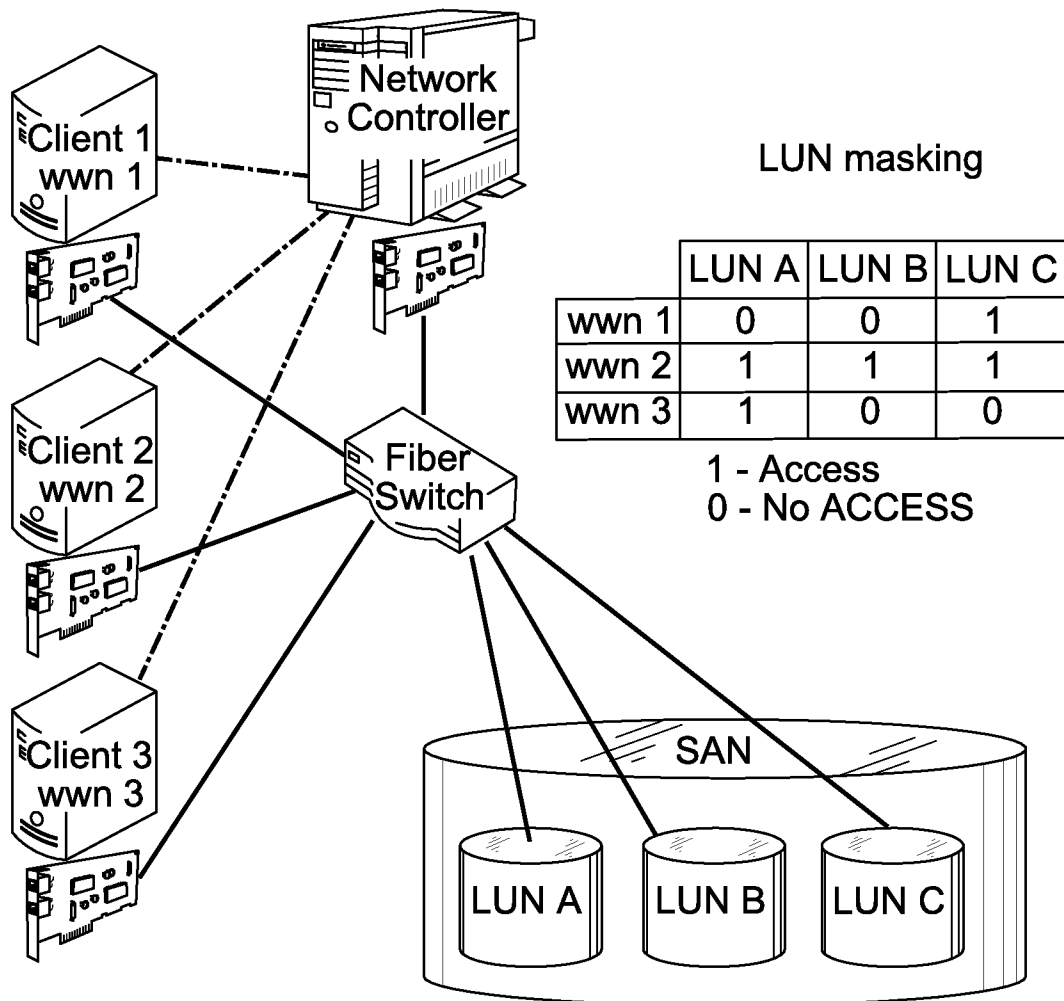
1. A method, said method comprising performing content segregation by a network security system using logical unit number masking.
2. A method, said method comprising:
 - 5 logging on to a client device by a first user;
 - retrieving permissions from a database for said first user;
 - spoofing a worldwide name for said first user into said client device host bus adapter;
 - mapping logical unit numbers according to said first user's
 - 10 permissions; and
 - accessing content segregated network resources.
3. The method according to claim 2, said method further comprising:
 - logging out of said first user from said client device;
 - unmapping said logical unit numbers; and
 - 15 unspoofing said worldwide name for said first user from said client device.
4. The method according to claim 2, wherein said database is a security database.
5. The method according to claim 2, wherein said permissions are masking permissions.
6. The method according to claim 2, wherein said network resources include
- 20 logical unit numbers of a storage area network.
7. The method according to claim 2, further comprising:
 - receiving a login request from a second user;
 - determining if said second user has permissions at least as great as said
 - 25 first user;
 - retrieving said worldwide name of said first user; and
 - limiting access to said network resources by said second user to access to said network resources granted to said first user.
8. The method according to claim 7, further comprising:
 - 30 logging out of said first user from said client device;
 - unmapping said logical unit numbers;
 - unspoofing said worldwide name for said first user from said client device; and

prompting said second user to log out and to re-login to gain full permissions of said second user.

9. The method according to claim 2, wherein said method is performed by a security system resident in a network controller.

5

1/6



PRIOR ART
FIG. 1

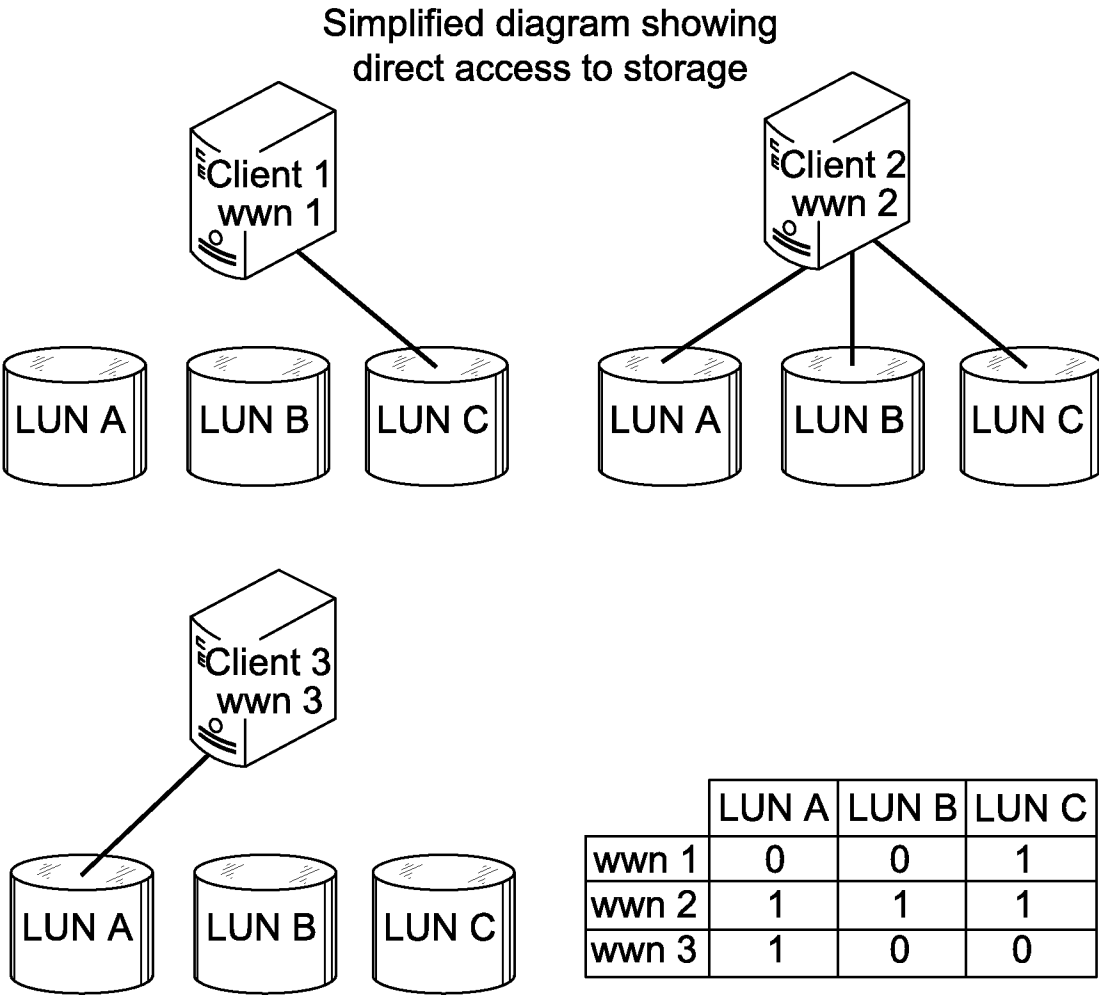


FIG. 2

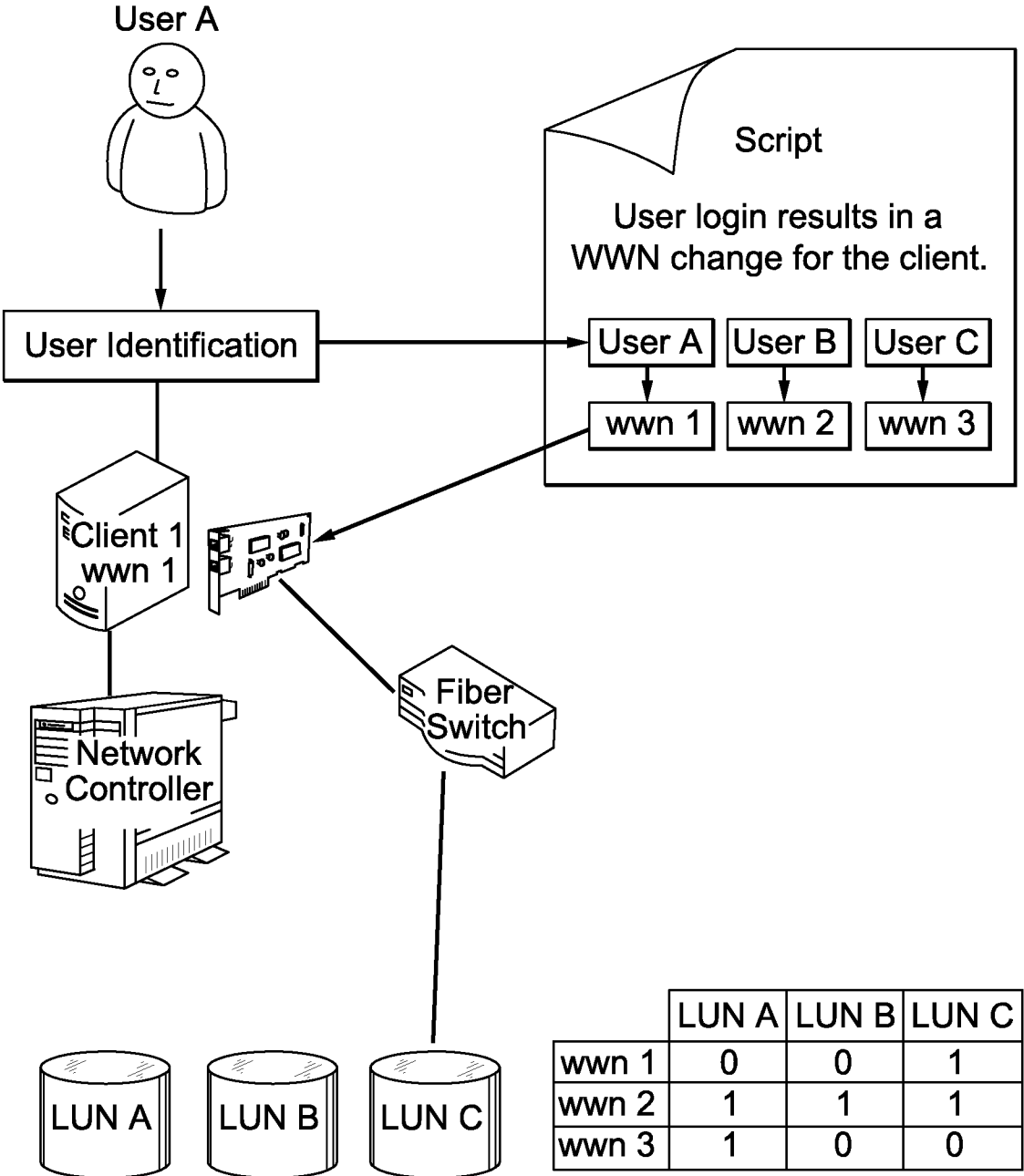
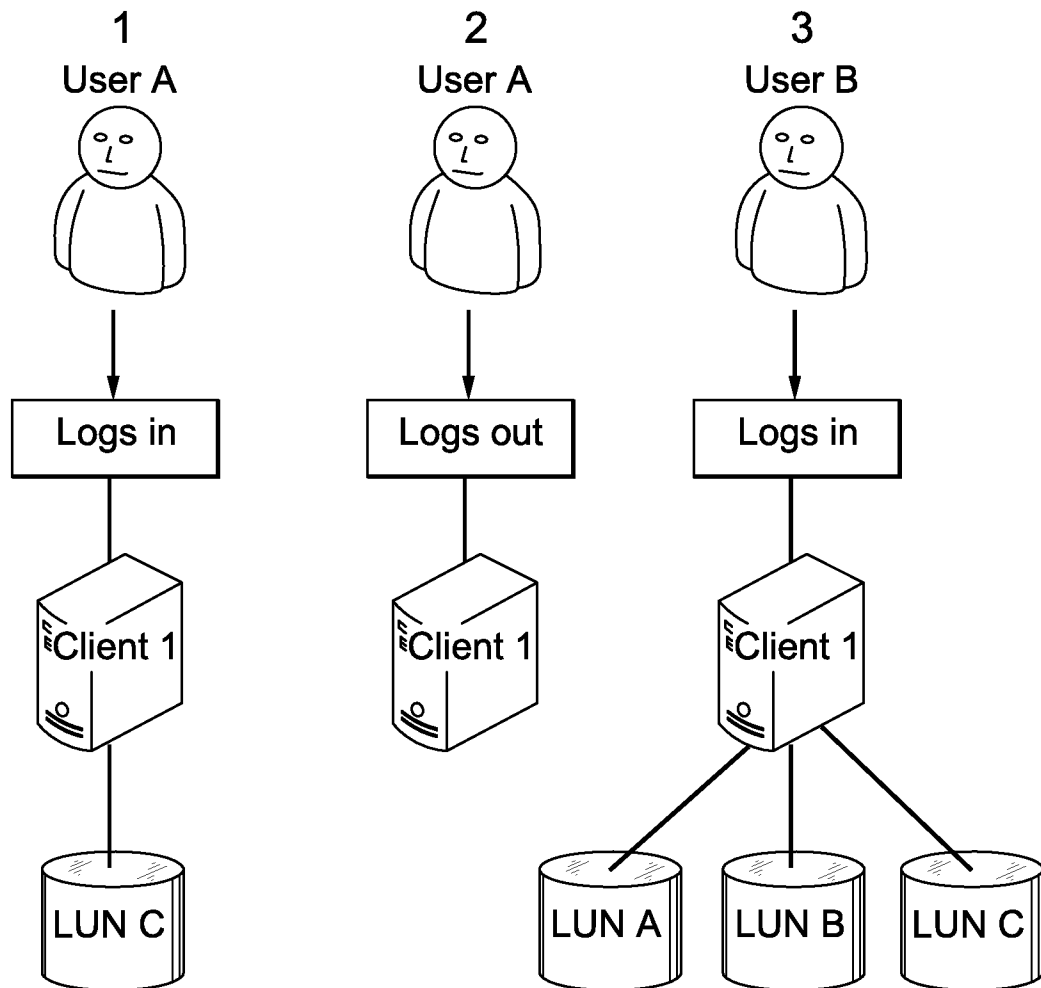
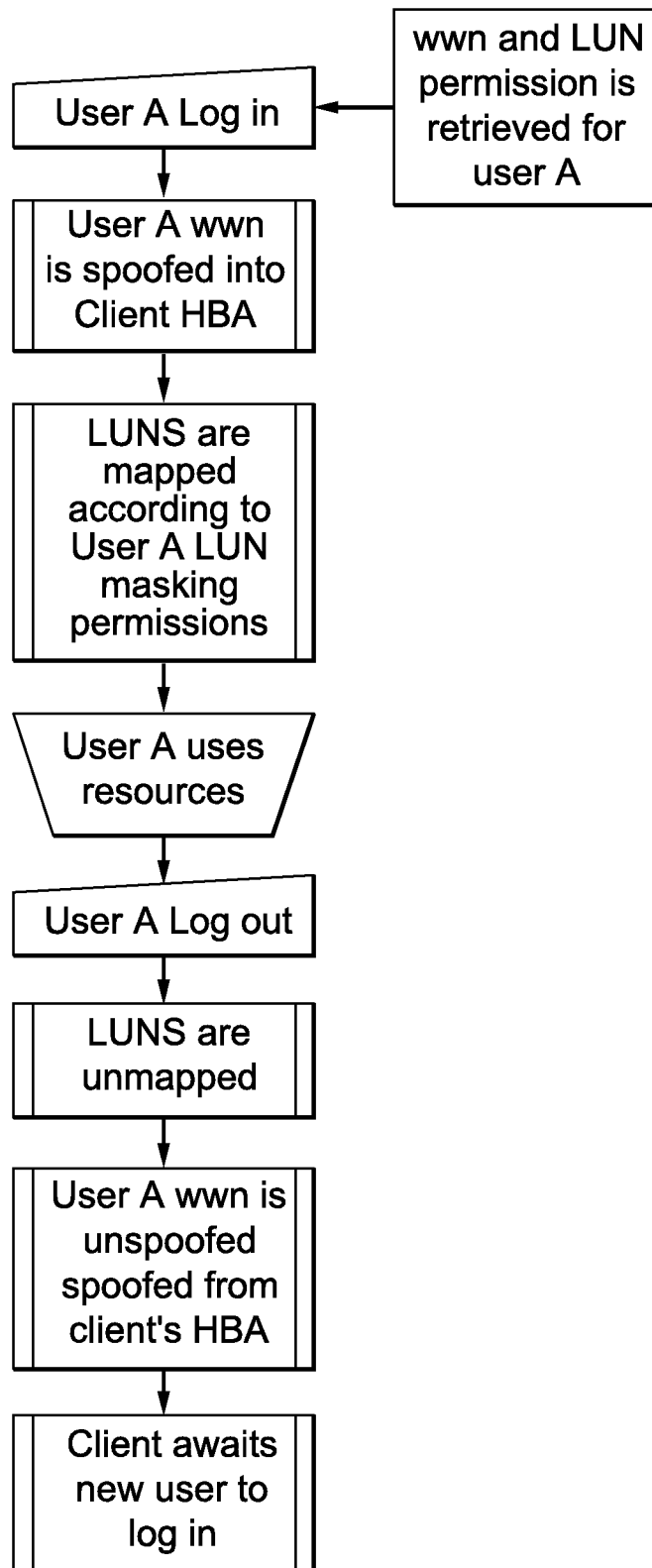


FIG. 3

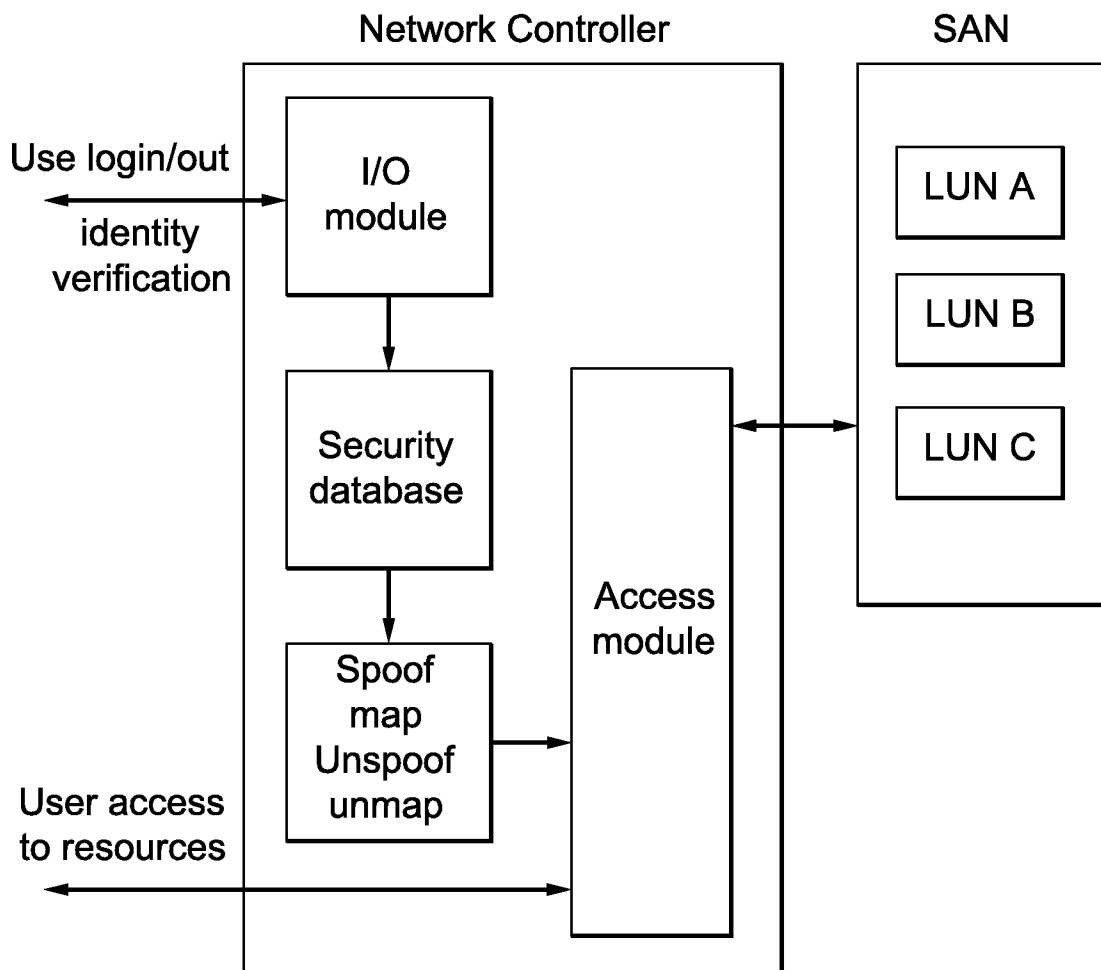
4/6

*FIG. 4*

5/6

*FIG. 5*

6/6

*FIG. 6*

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/021515

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 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 G06F

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/021727 A1 (MATSUNAMI NAOTO [JP] ET AL) 27 January 2005 (2005-01-27) figures 3,4 paragraphs [0007], [0039] - [0043] paragraphs [0045], [0053], [0058] paragraphs [0059], [0068], [0074] paragraph [0125]	1-9
X	US 2010/080237 A1 (DAI CHUNG [US] ET AL) 1 April 2010 (2010-04-01) paragraph [0088] ----- -/--	1-9



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

9 June 2015

Date of mailing of the international search report

17/06/2015

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Kufer, Léna

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/021515

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TECHNOMAGESINC: "Data Transport Processor Applications Overview", INTERNET CITATION, 8 September 2002 (2002-09-08), pages 1-12, XP002481539, Retrieved from the Internet: URL: http://web.archive.org/web/20020809071759/www.technomagesinc.com/papers/DTP_Apps.html [retrieved on 2008-05-26] figure 9 section 5.2	1-9
A	----- EP 1 509 021 A2 (MICROSOFT CORP [US]) 23 February 2005 (2005-02-23) paragraphs [0003], [0030], [0033] paragraphs [0039], [0043], [0044] -----	1-9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2015/021515

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2005021727	A1	27-01-2005	JP 3837953 B2 25-10-2006
			JP 2000259583 A 22-09-2000
			US 2005021727 A1 27-01-2005
			US 2007083635 A1 12-04-2007
			US 2008270608 A1 30-10-2008

US 2010080237	A1	01-04-2010	NONE

EP 1509021	A2	23-02-2005	CN 1585410 A 23-02-2005
			EP 1509021 A2 23-02-2005
			JP 2005071362 A 17-03-2005
			KR 20050020682 A 04-03-2005
			US 2005044244 A1 24-02-2005
			US 2012265880 A1 18-10-2012
