



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/546,247	07/25/2017	Joseph E. RUBENSTEIN	2210592.02085US2

CONFIRMATION NO. 9030

POWER OF ATTORNEY NOTICE



OC000000063893396

23483
WILMERHALE/BOSTON
60 STATE STREET
BOSTON, MA 02109

Date Mailed: 11/01/2023

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/24/2023.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/kkdouglas/



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
15/546,247	07/25/2017	Joseph E. RUBENSTEIN	2210592.02085US2

CONFIRMATION NO. 9030

146018
Gardella Grace P.A.
80 M Street SE, 1st Floor
Washington, DC 20003

POA ACCEPTANCE LETTER



OC000000063893451

Date Mailed: 11/01/2023

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/24/2023.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/kkdouglas/

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

☒ Practitioners associated with Customer Number: **146018**

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number

Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

☒ The address associated with Customer Number: **146018**

OR

☐ Firm or individual name		
Address		
City	State	Zip
Country		
Telephone		Email

Assignee name and address: UMBRA Technologies Ltd.
Suite 2006, 20th Floor, Hua Qin International Building
340 Queen's Road Central, Hong Kong

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee.

Signature /Jorn Knutsen/	Date September 21., 2023
Name Jorn Knutsen	Telephone +47 97034 755
Title Chief Executive Officer	

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0035. Public burden for this form is estimated to average 18 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.** If filing this completed form by mail, send to: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013). <https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf>

Routine uses of the information in this record may include disclosure to: 1) law enforcement, in the event that the system of records indicates a violation or potential violation of law; 2) a Federal, state, local, or international agency, in response to its request; 3) a contractor of the USPTO having need for the information in order to perform a contract; 4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record; 5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record; 6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations; 7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals; 8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)); 9) the Office of Personnel Management (OPM) for personnel research purposes; and 9) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Additional Uses

Additional USPTO uses of the information in this record may include disclosure to: 1) the International Bureau of the World Intellectual Property Organization, if the record is related to an international application filed under the Patent Cooperation Treaty; 2) the public i) after publication of the application pursuant to 35 U.S.C. 122(b), ii) after issuance of a patent pursuant to 35 U.S.C. 151, iii) if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections, or an issued patent, or iv) without publication of the application or patent under the specific circumstances provided for by 37 CFR 1.14(a)(1)(v)-(vii); and/or 3) the National Archives and Records Administration, for inspection of records.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: UMBRA Technologies Ltd.
Application No./Patent No.: 10,630,505 Filed/Issue Date: April 21, 2020
Titled: SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK
UMBRA Technologies Ltd., a corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is ____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 044091, Frame 0171, or for which a copy thereof is attached.

- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/James E. Harris/

October 24, 2023

Signature

Date

James E. Harris

40,013

Printed or Typed Name

Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #
15/546,247

RECEIPT DATE / TIME
10/24/2023 01:50:26 PM ET

ATTORNEY DOCKET #
2210592.02085US2

Title of Invention

SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK

Application Information

APPLICATION TYPE Utility - U.S. National Stage under 35 USC 371

PATENT # 10630505

CONFIRMATION # 9030

FILED BY Jon Bhatti

PATENT CENTER # 63065102

FILING DATE 07/25/2017

CUSTOMER # 23483

FIRST NAMED INVENTOR Joseph E. RUBENSTEIN

INTL. APPLICATION # -

INTL. FILING DATE -

CORRESPONDENCE ADDRESS -

AUTHORIZED BY James Harris

Documents

TOTAL DOCUMENTS: 4

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
2023-10-24 UMBRA P50512US01 Fee Address Indication form.pdf	2	Maintenance Fee Address Change	264 KB
2023-10-24 UMBRA P50512US01 Correspondence change form.pdf	2	Change of Address	271 KB
2023-10-24 UMBRA P50512US01 POA-3.73 Statement.pdf	5	-	1718 KB

2023-10-24 UMBRA P50512US01 POA-3.73 Statement-PA...pdf	(1-2)	2	Power of Attorney	1607 KB
2023-10-24 UMBRA P50512US01 POA-3.73 Statement-R3.73.pdf	(3-5)	3	Assignee showing of ownership per 37 CFR 3.73	138 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
2023-10-24 UMBRA P50512US01 Fee Address Indication form.pdf	3725F8D52B5E2D9B6C0301AB890A06A556F98C3753566EDD4 5BD6E6D9397B6CC8CDD85E8A33FA15E8C4F6AE383CD474D3 B93F74BCB3DCE5372D289D30F10C35F
2023-10-24 UMBRA P50512US01 Correspondence change form.pdf	24F5DAE14688CB09B6F17A43DC9BD08B824F77C13A7C5D1B 16E4CAF2740BD6C923998283890D67CA03B7CA70322BB6226 369AD1EEB97AABA0C3223BA29E4AA34
2023-10-24 UMBRA P50512US01 POA-3.73 Statement.pdf	31AAC1A619ADF3A6AC0E7352E156E028A8A8090C5C39ABE5 FF51AE3D386996BBB7AF3406BCD20E8D0DDBEF7BAB772416 FEB5668E1BAC566BA424CA5187EB582B
2023-10-24 UMBRA P50512US01 POA-3.73 Statement-PA...pdf	3E1B03A194B07B192FCBD9C0178E377FD6BA89C09BB571DA0 FD6274FBBDB0233FB071706F70D7F7D159DA594AA325FCFB0 C331F85423C1B701B7087A19974E55
2023-10-24 UMBRA P50512US01 POA-3.73 Statement-R3.73.pdf	ADE382467711F5100FDA064A8E466AD83F88A6E54B8646E963 26873C4A4B362A9CBF45F7A1BF8C06E0A463314BB2E0E3576 0AC180BDBB075D4C090A2B264BDD6

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless it displays a valid OMB control number.

"FEE ADDRESS" INDICATION FORM	
Address to: Mail Stop Maintenance Fee Director of the United States Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	
-OR-	
Fax to: 571-273-6500	
INSTRUCTIONS: The issue fee must have been paid for the application(s) listed on this form. In addition, only an address represented by a Customer Number can be established as the fee address for maintenance fee purposes (hereafter, fee address). A fee address should be established when correspondence related to maintenance fees should be mailed to a different address than the correspondence address for the application. When to check the first box below: If you have a Customer Number to represent the fee address. When to check the second box below: If you have no Customer Number representing the desired fee address, in which case a completed Request for Customer Number (PTO/SB/125) must be attached to this form. For more information on Customer Numbers, see the Manual of Patent Examining Procedure (MPEP) § 403.	
For the following listed application(s), please recognize as the "Fee Address" under the provisions of 37 CFR 1.363 the address associated with: ☒ Customer Number: 146018 OR ☐ The attached Request for Customer Number form (PTO/SB/125)	
PATENT NUMBER (if known)	APPLICATION NUMBER
10,630,505	
Completed by (check one): ☐ Applicant/Inventor ☒ Attorney or Agent of record 40,013 Reg. No. ☐ Assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(c) (Form PTO/AIA/96) is enclosed or was filed on _____ (Date) <u>/James E. Harris/</u> Signature <u>James E. Harris</u> Typed or printed name <u>703-547-8704</u> Requester's telephone number <u>October 24, 2023</u> Date	
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. If the assignee is a juristic entity, this form must be signed by a patent practitioner (attorney or agent) of record. Submit multiple forms if more than one signature is required, see below*.	
☒ *Total of <u>1</u> forms are submitted	

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-0016. Public burden for this form is estimated to average 5 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.** SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013). <https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf>

Routine uses of the information in this record may include disclosure to: 1) law enforcement, in the event that the system of records indicates a violation or potential violation of law; 2) a Federal, state, local, or international agency, in response to its request; 3) a contractor of the USPTO having need for the information in order to perform a contract; 4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record; 5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record; 6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations; 7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals; 8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)); 9) the Office of Personnel Management (OPM) for personnel research purposes; and 9) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Additional Uses

Additional USPTO uses of the information in this record may include disclosure to: 1) the International Bureau of the World Intellectual Property Organization, if the record is related to an international application filed under the Patent Cooperation Treaty; 2) the public i) after publication of the application pursuant to 35 U.S.C. 122(b), ii) after issuance of a patent pursuant to 35 U.S.C. 151, iii) if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections, or an issued patent, or iv) without publication of the application or patent under the specific circumstances provided for by 37 CFR 1.14(a)(1)(v)-(vii); and/or 3) the National Archives and Records Administration, for inspection of records. <https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf>

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**CHANGE OF
CORRESPONDENCE ADDRESS
Patent**Address to:
Mail Stop Post Issue
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Patent Number	10,630,505
Issue Date	April 21, 2020
Application Number	15/546,247
Filing Date	July 25, 2017
First Named Inventor	Joseph E. RUBENSTEIN
Attorney Docket Number	P50512US01

Please change the Correspondence Address for the above-identified patent to:

☒ The address associated with Customer Number:

146018

OR☐ **Firm or
Individual Name****Address****City****State****ZIP****Country****Telephone****Email**

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

This form will not affect any "fee address" provided for the above-identified patent. To change a "fee address" use the "Fee Address Indication Form" (PTO/SB/47).

I am the:

☐ Patentee.☐ If the Patentee was not the applicant for patent (37 CFR 1.42), then a Statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is enclosed or was filed on _____. See 37 CFR 3.71.☒ Attorney or agent of record. Registration Number 40,013.☐ Patent practitioner acting in a representative capacity whose correspondence address is the correspondence address of record. Notice has been given to the patentee or owner. Registration Number 40,013.

Signature /James E. Harris/

Typed or
Printed Name James E. Harris

Date October 24, 2023

Telephone 703-547-8704

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

A Federal agency may not conduct or sponsor, and a person is not required to respond to, nor shall a person be subject to a penalty for failure to comply with an information collection subject to the requirements of the Paperwork Reduction Act of 1995, unless the information collection has a currently valid OMB Control Number. The OMB Control Number for this information collection is 0651-00**. Public burden for this form is estimated to average ** hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the information collection. Send comments regarding this burden estimate or any other aspect of this information collection, including suggestions for reducing this burden to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 or email InformationCollection@uspto.gov. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. If filing this completed form by mail, send to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. The United States Patent and Trademark Office (USPTO) collects the information in this record under authority of 35 U.S.C. 2. The USPTO's system of records is used to manage all applicant and owner information including name, citizenship, residence, post office address, and other information with respect to inventors and their legal representatives pertaining to the applicant's/owner's activities in connection with the invention for which a patent is sought or has been granted. The applicable Privacy Act System of Records Notice for the information collected in this form is COMMERCE/PAT-TM-7 Patent Application Files, available in the Federal Register at 78 FR 19243 (March 29, 2013). <https://www.govinfo.gov/content/pkg/FR-2013-03-29/pdf/2013-07341.pdf>

Routine uses of the information in this record may include disclosure to: 1) law enforcement, in the event that the system of records indicates a violation or potential violation of law; 2) a Federal, state, local, or international agency, in response to its request; 3) a contractor of the USPTO having need for the information in order to perform a contract; 4) the Department of Justice for determination of whether the Freedom of Information Act (FOIA) requires disclosure of the record; 5) a Member of Congress submitting a request involving an individual to whom the record pertains, when the individual has requested the Member's assistance with respect to the subject matter of the record; 6) a court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel in the course of settlement negotiations; 7) the Administrator, General Services Administration (GSA), or their designee, during an inspection of records conducted by GSA under authority of 44 U.S.C. 2904 and 2906, in accordance with the GSA regulations and any other relevant (i.e., GSA or Commerce) directive, where such disclosure shall not be used to make determinations about individuals; 8) another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)); 9) the Office of Personnel Management (OPM) for personnel research purposes; and 9) the Office of Management and Budget (OMB) for legislative coordination and clearance.

If you do not furnish the information requested on this form, the USPTO may not be able to process and/or examine your submission, which may result in termination of proceedings, abandonment of the application, and/or expiration of the patent.

Additional Uses

Additional USPTO uses of the information in this record may include disclosure to: 1) the International Bureau of the World Intellectual Property Organization, if the record is related to an international application filed under the Patent Cooperation Treaty; 2) the public i) after publication of the application pursuant to 35 U.S.C. 122(b), ii) after issuance of a patent pursuant to 35 U.S.C. 151, iii) if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections, or an issued patent, or iv) without publication of the application or patent under the specific circumstances provided for by 37 CFR 1.14(a)(1)(v)-(vii); and/or 3) the National Archives and Records Administration, for inspection of records.

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court for the Western District of Texas on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 1:23-cv-904	DATE FILED 8/2/2023	U.S. DISTRICT COURT for the Western District of Texas
PLAINTIFF UMBRA TECHNOLOGIES LTD.(UK), UMBRA TECHNOLOGIES LIMITED (CN) & UMBRA TECHNOLOGIES (US) INC., dba UMBRA TECHNOLO		DEFENDANT VMWARE, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 US 10,574,482 B2	2/25/2020	UMBRA Technologies Ltd.
2 US 10,630,505 B2	4/21/2020	UMBRA Technologies Ltd.
3 US 11,108,595 B2	8/31/2021	UMBRA Technologies Ltd.
4 US 11,146,632 B2	10/12/2021	UMBRA Technologies Ltd.
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading		
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK	
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
 Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/546,247	04/21/2020	10630505	2210592.02085US2	9030
23483	7590	04/01/2020		
WILMERHALE/BOSTON 60 STATE STREET BOSTON, MA 02109				

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 23 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

UMBRA Technologies Ltd., Hong Kong, CHINA;
Joseph E. RUBENSTEIN, Beijing, CHINA;
Jørn Allan Dose KNUTSEN, Oslo, NORWAY;
Thibaud Auguste Bernard Jean SAINT-MARTIN, Aubignan, FRANCE;
Carlos Eduardo ORÉ, Saint-Herblain, FRANCE;
Fred BROUSSARD, Indianapolis, IN;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23483 7590 12/11/2019
WILMERHALE/BOSTON
60 STATE STREET
BOSTON, MA 02109

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/546,247	07/25/2017	Joseph E. RUBENSTEIN	2210592.02085US2	9030

TITLE OF INVENTION: SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	03/11/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
POLLACK, MELVIN H	2445	709-249000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list

- (1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
- (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1. Wilmer Cutler Pickering
2. Hale and Dorr LLP
3. _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

UMBRA TECHNOLOGIES LTD.

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

HONG KONG, CHINA

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

- ☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 08-0219

5. Change in Entity Status (from status indicated above)

- ☐ Applicant certifying micro entity status. See 37 CFR 1.29
- ☐ Applicant asserting small entity status. See 37 CFR 1.27
- ☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Yu Yang/ Date March 10, 2020

Typed or printed name Yu Yang Registration No. 68,839

Electronic Patent Application Fee Transmittal				
Application Number:		15546247		
Filing Date:		25-Jul-2017		
Title of Invention:		SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK		
First Named Inventor/Applicant Name:		Joseph E. RUBENSTEIN		
Filer:		Yu Yang/Lori Roman		
Attorney Docket Number:		2210592.02085US2		
Filed as Small Entity				
Filing Fees for U.S. National Stage under 35 USC 371				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	500	500

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				500

Electronic Acknowledgement Receipt	
EFS ID:	38833615
Application Number:	15546247
International Application Number:	
Confirmation Number:	9030
Title of Invention:	SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK
First Named Inventor/Applicant Name:	Joseph E. RUBENSTEIN
Customer Number:	23483
Filer:	Yu Yang/Lori Roman
Filer Authorized By:	Yu Yang
Attorney Docket Number:	2210592.02085US2
Receipt Date:	11-MAR-2020
Filing Date:	25-JUL-2017
Time Stamp:	16:42:13
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 500
RAM confirmation Number	E20203AG43142801
Deposit Account	080219
Authorized User	Lori Roman
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.20 (Post Issuance fees)	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	2085US2_Issue_Fee_transmittal.PDF	440808	no	1
			a76268a837be474595402fcfa140dde5f3eb05ec		
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30582	no	2
			bf46cff2ae09dfd70ae2000c20efbc47149e1f92		
Warnings:					
Information:					
Total Files Size (in bytes):			471390		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23483 7590 12/11/2019
WILMERHALE/BOSTON
60 STATE STREET
BOSTON, MA 02109

EXAMINER

POLLACK, MELVIN H

ART UNIT

PAPER NUMBER

2445

DATE MAILED: 12/11/2019

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/546,247	07/25/2017	Joseph E. RUBENSTEIN	2210592.02085US2	9030

TITLE OF INVENTION: SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	03/11/2020

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23483 7590 12/11/2019
WILMERHALE/BOSTON
60 STATE STREET
BOSTON, MA 02109

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/546,247	07/25/2017	Joseph E. RUBENSTEIN	2210592.02085US2	9030

TITLE OF INVENTION: SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	03/11/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
POLLACK, MELVIN H	2445	709-249000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☐ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/546,247	07/25/2017	Joseph E. RUBENSTEIN	2210592.02085US2	9030
23483	7590	12/11/2019	EXAMINER	
WILMERHALE/BOSTON			POLLACK, MELVIN H	
60 STATE STREET			ART UNIT	PAPER NUMBER
BOSTON, MA 02109			2445	
DATE MAILED: 12/11/2019				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 15/546,247	Applicant(s) RUBENSTEIN et al.	
	Examiner MELVIN H POLLACK	Art Unit 2445	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the RCE filed 11/21/19.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 1-20 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
a) ☒ All b) ☐ Some *c) ☐ None of the:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)	5. ☐ Examiner's Amendment/Comment
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 11/21/19.	6. ☐ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.	7. ☐ Other _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.	

/MELVIN H POLLACK/ Primary Examiner, Art Unit 2445	
---	--

Issue Classification 	Application/Control No. 15/546,247	Applicant(s)/Patent Under Reexamination RUBENSTEIN et al.
	Examiner MELVIN H POLLACK	Art Unit 2445

CPC						
Symbol					Type	Version
H04L	/	12	/	4633	F	2013-01-01
H04L	/	45	/	64	I	2013-01-01
H04L	/	45	/	12	I	2013-01-01
H04L	/	61	/	1511	I	2013-01-01
H04L	/	63	/	02	I	2013-01-01

CPC Combination Sets					
Symbol				Type	Set

NONE (Assistant Examiner) (Date)		Total Claims Allowed: 20	
/MELVIN H POLLACK/ Primary Examiner, Art Unit 2445 (Primary Examiner) (Date)		02 December 2019 (Date)	O.G. Print Claim(s) 1
			O.G. Print Figure 15

U.S. Patent and Trademark Office

Part of Paper No.: 20191202

Issue Classification 	Application/Control No. 15/546,247	Applicant(s)/Patent Under Reexamination RUBENSTEIN et al.
	Examiner MELVIN H POLLACK	Art Unit 2445

INTERNATIONAL CLASSIFICATION			
CLAIMED			
G06F		15	16
NON-CLAIMED			

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
709	249

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/MELVIN H POLLACK/ Primary Examiner, Art Unit 2445	02 December 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	15

U.S. Patent and Trademark Office

Part of Paper No.: 20191202

Issue Classification 	Application/Control No. 15/546,247	Applicant(s)/Patent Under Reexamination RUBENSTEIN et al.
	Examiner MELVIN H POLLACK	Art Unit 2445

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47															
CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	10	10	19	19										
2	2	11	11	20	20										
3	3	12	12												
4	4	13	13												
5	5	14	14												
6	6	15	15												
7	7	16	16												
8	8	17	17												
9	9	18	18												

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 20	
/MELVIN H POLLACK/ Primary Examiner, Art Unit 2445 (Primary Examiner) _____ (Date) _____		02 December 2019 O.G. Print Claim(s) 1	O.G. Print Figure 15

U.S. Patent and Trademark Office

Part of Paper No.: 20191202

<i>Search Notes</i> 	Application/Control No. 15/546,247	Applicant(s)/Patent Under Reexamination RUBENSTEIN et al.
	Examiner MELVIN H POLLACK	Art Unit 2445

CPC - Searched*		
Symbol	Date	Examiner
east	02/15/2019	mhp
update	08/16/2019	mhp
update	12/02/2019	mhp

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
709	249	02/15/2019	MHP
	update	08/16/2019	MHP
	update	12/02/2019	mhp

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

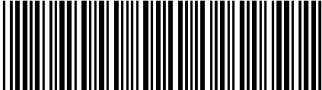
Search Notes		
Search Notes	Date	Examiner
east	02/15/2019	MHP
update	08/16/2019	MHP
update	12/02/2019	MHP

/MELVIN H POLLACK/ Primary Examiner, Art Unit 2445	
---	--

<i>Search Notes</i> 	Application/Control No. 15/546,247	Applicant(s)/Patent Under Reexamination RUBENSTEIN et al.
	Examiner MELVIN H POLLACK	Art Unit 2445

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
	EAST	08/16/2019	MHP
	update	12/02/2019	MHP

/MELVIN H POLLACK/ Primary Examiner, Art Unit 2445	
---	--

<i>Index of Claims</i> 	Application/Control No. 15/546,247	Applicant(s)/Patent Under Reexamination RUBENSTEIN et al.
	Examiner MELVIN H POLLACK	Art Unit 2445

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS									
☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47									
CLAIM		DATE							
Final	Original	02/14/2019	08/16/2019	12/02/2019					
1	1	✓	=	=					
2	2	✓	=	=					
3	3	✓	=	=					
4	4	✓	=	=					
5	5	✓	=	=					
6	6	✓	=	=					
7	7	✓	=	=					
8	8	✓	=	=					
9	9	✓	=	=					
10	10	✓	=	=					
11	11		=	=					
12	12		=	=					
13	13		=	=					
14	14		=	=					
15	15		=	=					
16	16		=	=					
17	17		=	=					
18	18		=	=					
19	19		=	=					
20	20		=	=					

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	15/546,247-Conf. #9030
				Filing Date	July 25, 2017
				First Named Inventor	Joseph E. RUBENSTEIN
				Art Unit	2445
				Examiner Name	M. H. Pollack
Sheet	1	of	2	Attorney Docket Number	2210592.02085US2

U. S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
	AA	US-2013/0308471-A1	11-21-2013	Krzanowski et al.	
	AB	US-7,801,030	09-21-2010	Aggarwal et al.	
	AC	US-2009/0122990-A1	05-14-2009	Gundavelli et al.	
	AD	US-2013/0259465-A1	10-03-2013	Blair	
	AE	US-2015/0222637-A1	08-06-2015	HUNG et al.	
	AF	US-2016/0028586-A1	01-28-2016	BLAIR	
	AG	US-2003/0233551-A1	12-18-2003	Kouznetsov et al.	
	AH	US-6,879,995	04-12-2005	Chinta et al.	
	AI	US-2006/0031407-A1	02-09-2006	Dispensa et al.	
	AJ	US-2008/0091598-A1	04-17-2008	Fauleau	
	AK	US-2008/0168377-A1	07-10-2008	Stallings et al.	
	AL	US-2008/0260151-A1	10-23-2008	Fluhrer et al.	
	AM	US-2010/0017603-A1	01-21-2010	Jones	
	AN	US-8,069,258	11-29-2011	Howell	
	AO	US-2014/0101036-A1	04-10-2014	Phillips et al.	
	AP	US-2014/0278543 A1	09-18-2014	Kasdon	
	AQ	US-2002/0087447 A1	07-04-2002	McDonald et al.	
	AR	US-2008/0301794 A1	12-04-2008	Lee	
	AS	US-2014/0149552-A1	05-29-2014	Carney et al.	
	AT	US-2003/0195973-A1	10-16-2003	Savarda	
	AU	US-2010/0316052-A1	12-16-2010	Petersen	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T ⁶
		Country Code ³ -Number ⁴ -Kind Code ⁵ (if known)				
	BA	EP-2154834-A1	02-17-2010	Juniper Networks, Inc		
	BB	EP-1498809-A1	01-19-2005	Fujitsu Ltd		

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.H.P./

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	15/546,247-Conf. #9030
				Filing Date	July 25, 2017
				First Named Inventor	Joseph E. RUBENSTEIN
				Art Unit	2445
				Examiner Name	M. H. Pollack
Sheet	2	of	2	Attorney Docket Number	2210592.02085US2

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
	CA	"Open Radio Equipment Interface (ORI); ORI Interface Specification; Part 2: Control and Management (Release 4)," Group Specification, European Telecommunications Standards Institute (ETSI), 650, Route des Lucioles; F-06921 Sophia-Antipolis; France, vol. ORI, No. V4.1.1, October 1, 2014 (185 pages)	
	CB	Robert Russell, "Introduction to RDMA Programming," Copyright 2012, retrieved from the Internet: URL:web.archive.org/web/20140417205540/http://www.cs.unh.edu/~rdr/rdma-intro-module.ppt, 2012 (76 pages)	

Examiner Signature	/MELVIN H POLLACK/	Date Considered	12/02/2019
-----------------------	--------------------	--------------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.H.P./

Doc code: RCEX

Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (02-18)

Approved for use through 11/30/2020. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL **(Submitted Only via EFS-Web)**

Application Number	15546247	Filing Date	2017-07-25	Docket Number (if applicable)	2210592.02085US2	Art Unit	2445
First Named Inventor	Joseph E. RUBENSTEIN			Examiner Name	Melvin H. POLLACK		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.

Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☐ Other _____

☒ Enclosed

☐ Amendment/Reply

☒ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
 (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

☒ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to
 Deposit Account No 08-0219

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

Doc code: RCEX

Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (02-18)

Approved for use through 11/30/2020. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	Yu Yang/	Date (YYYY-MM-DD)	2019-11-21
Name	Yu Yang	Registration Number	68839

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Docket No.: 2210592.02085US2
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: UMBRA Technologies Ltd. Confirmation No.: 9030
Application No.: 15/546,247 Art Unit: 2445
Filed: July 25, 2017 Examiner: M. H. Pollack
Title: SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK

MS RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT (IDS)

Dear Commissioner:

Pursuant to 37 C.F.R. §§ 1.56, 1.97, and 1.98, the attention of the United States Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of the above-identified application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement, pursuant to 37 C.F.R. § 1.114(c), accompanies the Request for Continued Examination (37 C.F.R. § 1.114) submitted herewith.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), copies of U.S. patents and U.S. patent application publications are not submitted. Submitted herewith are copies of foreign patents and non-patent literature in accordance with 37 C.F.R. § 1.98(a)(2).

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98, and the Examiner is respectfully requested to consider the listed references.

Application No.: 15/546,247

Docket No.: 2210592.02085US2

In the event the U.S. Patent and Trademark Office determines that a fee is required, Applicant petitions for any required relief including extensions of time and authorizes the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to Deposit Account No. 08-0219, under Order No. 2210592.02085US2 from which the undersigned is authorized to draw.

Respectfully submitted,

Dated: November 21, 2019

/Yu Yang/
Yu Yang
Registration No.: 68,839
Attorney for Applicant(s)

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000 (telephone)
(617) 526-5000 (facsimile)

Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	15/546,247-Conf. #9030
				Filing Date	July 25, 2017
				First Named Inventor	Joseph E. RUBENSTEIN
				Art Unit	2445
				Examiner Name	M. H. Pollack
Sheet	1	of	2	Attorney Docket Number	2210592.02085US2

U. S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. ¹	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number-Kind Code ² (if known)			
	AA	US-2013/0308471-A1	11-21-2013	Krzanowski et al.	
	AB	US-7,801,030	09-21-2010	Aggarwal et al.	
	AC	US-2009/0122990-A1	05-14-2009	Gundavelli et al.	
	AD	US-2013/0259465-A1	10-03-2013	Blair	
	AE	US-2015/0222637-A1	08-06-2015	HUNG et al.	
	AF	US-2016/0028586-A1	01-28-2016	BLAIR	
	AG	US-2003/0233551-A1	12-18-2003	Kouznetsov et al.	
	AH	US-6,879,995	04-12-2005	Chinta et al.	
	AI	US-2006/0031407-A1	02-09-2006	Dispensa et al.	
	AJ	US-2008/0091598-A1	04-17-2008	Fauleau	
	AK	US-2008/0168377-A1	07-10-2008	Stallings et al.	
	AL	US-2008/0260151-A1	10-23-2008	Fluhrer et al.	
	AM	US-2010/0017603-A1	01-21-2010	Jones	
	AN	US-8,069,258	11-29-2011	Howell	
	AO	US-2014/0101036-A1	04-10-2014	Phillips et al.	
	AP	US-2014/0278543 A1	09-18-2014	Kasdon	
	AQ	US-2002/0087447 A1	07-04-2002	McDonald et al.	
	AR	US-2008/0301794 A1	12-04-2008	Lee	
	AS	US-2014/0149552-A1	05-29-2014	Carney et al.	
	AT	US-2003/0195973-A1	10-16-2003	Savarda	
	AU	US-2010/0316052-A1	12-16-2010	Petersen	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. ¹	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T ⁶
		Country Code ³ -Number ⁴ -Kind Code ⁵ (if known)				
	BA	EP-2154834-A1	02-17-2010	Juniper Networks, Inc		
	BB	EP-1498809-A1	01-19-2005	Fujitsu Ltd		

Examiner Signature		Date Considered	
-----------------------	--	--------------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language Translation is attached.

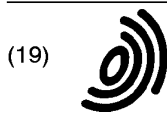
Substitute for form 1449/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(Use as many sheets as necessary)</i>				Complete if Known	
				Application Number	15/546,247-Conf. #9030
				Filing Date	July 25, 2017
				First Named Inventor	Joseph E. RUBENSTEIN
				Art Unit	2445
				Examiner Name	M. H. Pollack
Sheet	2	of	2	Attorney Docket Number	2210592.02085US2

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
	CA	"Open Radio Equipment Interface (ORI); ORI Interface Specification; Part 2: Control and Management (Release 4)," Group Specification, European Telecommunications Standards Institute (ETSI), 650, Route des Lucioles; F-06921 Sophia-Antipolis; France, vol. ORI, No. V4.1.1, October 1, 2014 (185 pages)	
	CB	Robert Russell, "Introduction to RDMA Programming," Copyright 2012, retrieved from the Internet: URL:web.archive.org/web/20140417205540/http://www.cs.unh.edu/~rdr/rdma-intro-module.ppt, 2012 (76 pages)	

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached.



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) **EP 1 498 809 A1**

(12)

EUROPEAN PATENT APPLICATION
published in accordance with Art. 158(3) EPC

(43) Date of publication:
19.01.2005 Bulletin 2005/03

(51) Int Cl.7: **G06F 3/06**, G06F 12/08,
G06F 13/10, G06F 12/00

(21) Application number: **02758854.0**

(86) International application number:
PCT/JP2002/008359

(22) Date of filing: **20.08.2002**

(87) International publication number:
WO 2003/075147 (12.09.2003 Gazette 2003/37)

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR**

• **WATANABE, Takashi, c/o FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211-8588 (JP)

(30) Priority: **06.03.2002 WOPCT/JP02/02063**

(71) Applicant: **FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211-8588 (JP)

(74) Representative: **Stebbing, Timothy Charles**
Haseltine Lake,
Imperial House,
15-19 Kingsway
London WC2B 6UD (GB)

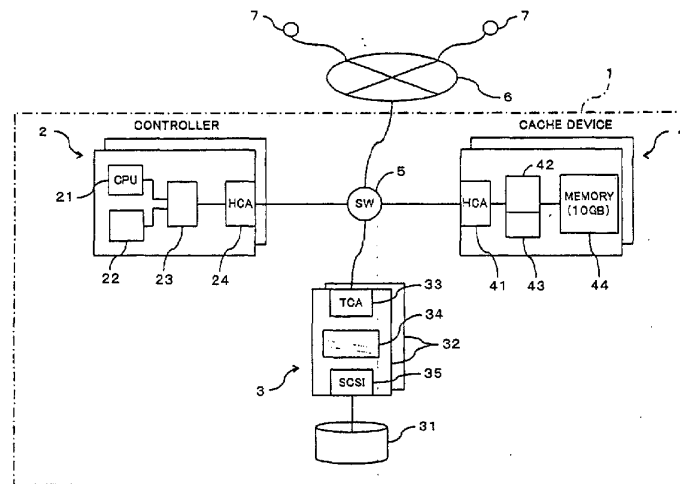
(72) Inventors:
• **OE, Kazuichi, c/o FUJITSU LIMITED**
Kawasaki-shi, Kanagawa 211-8588 (JP)

(54) **STORAGE SYSTEM AND DATA TRANSFER METHOD FOR THE SYSTEM**

(57) Upon receipt of an access request from a client device (7) by way of an internal network (5), a controller (2) issues a data transfer instruction to a cache device (4) or a storage device (3). The cache device (4) or the storage device (3), which has received the data transfer instruction, carries out a direct negotiation required for

data transfer with the client device (7) in accordance with the instruction, thereby directly transferring data to the client device (7). As a result, an attempt can be made to significantly curtail latency of a storage system (1) and improve a throughput [i.e. securing of a band at which performance of the internal network (5) can be exhibited sufficiently].

FIG. 1



Description

Technical Field

5 [0001] The present invention relates to a storage system and a data transfer method for use in the system, and more particularly, to a technique for accessing an external input/output device of a disk drive or the like, by way of a node device such as a personal computer (PC) or a workstation (WS) or the like.

Background

10 [0002] Fig. 26 shows an example of an existing storage system. As shown in Fig. 26, this system includes a node device 100 (hereinafter simply called a "node 100") such as a PC and an input/output (I/O) device 200 connected to the node 100 by way of an SCSI (Small Computer System Interface) bus 300. The node 100 is equipped with a CPU 101, a main storage section (main memory) 102, an SCSI card 103, or the like, which are connected so as to be communicable with each other by way of an internal bus 104. The I/O device 200 is equipped with a disk controller 201, a buffer 202, and a disk drive 203.

15 [0003] There is a case where the SCSI bus 300 is connected with a plurality of I/O devices 200. There is also a case where another interface, such as a fiber channel (FC), is used for connection between the node 100 (the main memory 102) and the I/O device 200.

20 [0004] In such a system, when data are transferred between the node 100 (the main memory 102) and the I/O device 200 (the disk drive 203), the node 100 must activate the disk controller 201 of the I/O device 200 by means of an SCSI protocol. For instance, when a file system 105 writes data into the disk drive 203, procedures such as those provided below are executed.

25 [0005] Specifically, as shown in Figs. 26 and 27, the file system 105 of the node 100 requests an SCSI driver 106 to perform writing of a disk (step A1). The file system 105 and the SCSI driver 106 are usually incorporated as a single function of an OS (operating system) or the like. The CPU 101 operates by reading file system data and driver data, which are stored in the main memory 102, thereby implementing the respective functions.

30 [0006] The SCSI driver 106, having received the disk write request, conducts negotiation with the disk controller 201 several times so as to determine a data transfer rate, or the like, in the SCSI bus 300, to thus establish a connection (step A2); initiates real transfer of data; and requests the disk controller 201 to write the data (step A3). When writing of the data into the disk drive 203 within the I/O device 200 involves excessive consumption of time, the SCSI driver 106 temporarily terminates the connection to the disk controller 201.

35 [0007] In the I/O device 200, after having temporarily stored into the buffer 202 the data received from the node 100 by way of the SCSI bus 300 (step A4), the disk controller 201 writes the data into the disk drive 203 (step A5). When internal processing (writing of the data) of the I/O device 200 has been completed (steps A6, A7), the disk controller 201 reports to the SCSI driver 106 that transfer (writing) has been completed, by making an interrupt (step A8), and the SCSI driver 106 reports completion of transfer operation to the file system 105 (step A9).

40 [0008] However, such a conventional system must start the disk controller 201 of the I/O device 200 by use of a protocol output from the node 100, such as an SCSI or an FC. Moreover, operations which would have been required until data are actually transferred are also complicated (because negotiation must be performed several times between the node 100 and the disk controller 200). Hence, there is a problem of large latency.

45 [0009] In relation to the band of transfer (a transfer rate) between the node 100 and the I/O device 200, improvements have been made on FC as well as on SCSI (up to 160 MB/s). However, if an Infiniband (IB) is introduced as an internal network, the transfer rate of the internal bus 104 of the node 100 can be increased up to the level of gigabytes per second (GB/s) or thereabouts. However, existing interface standards, such as SCSI and FC, have large latency as mentioned previously, and hence performance of the Infiniband cannot be exhibited sufficiently.

50 [0010] The present invention has been conceived in view of these problems and aims at providing a storage system and a data transfer method for use in the system, which can diminish latency by making an attempt to distribute a data transfer operation and ensure a data transfer band (rate) enabling sufficient exhibition of performance of an IB network when the IB network is introduced.

Disclosure of the Invention

55 [0011] To achieve the object, a storage system of the present invention is characterized by comprising: a storage device storing data; a cache device capable of caching the data stored in the storage device; a controller controlling access to at least the storage device and the cache device; and an internal network interconnecting the storage device, the cache device, and the controller so as to be enable communications therebetween, wherein the controller includes transfer instruction issuing means which issues a data transfer instruction to one of the cache device and the storage

device upon receipt of an access request transmitted, by way of the internal network, from a client device connected to the internal network in an accessible manner; and at least one of the storage device and cache device which receives the data transfer instruction includes direct transfer means for performing direct transfer of data to the client device by means of directly carrying out negotiation required for data transfer with the client device in accordance with the data transfer instruction from the controller.

[0012] In the storage system having such a configuration, the client device issues an access request to the controller byway of the internal network (an access request issuing step). Upon receipt of the access request, the controller issues a data transfer instruction to the cache device or the storage device (a transfer command issuing step).

[0013] In accordance with a data transfer instruction output from the controller, the cache device or the storage device conducts a negotiation required to transfer data to the client device, thereby directly transferring data to the client device (a direct transfer step). This enables an attempt to diminish latency of the storage system and increase a data throughput significantly.

[0014] Here, the controller generates a message required to conduct negotiation between the client device and the cache device or the storage device and transmits the thus-generated message to the cache device along with the data transfer instruction. The cache device or the storage device can carry out transfer of data to the client device using the message generated by the controller. This enables the controller to intensively manage generation of a message and issue of the data transfer instruction, thereby simplifying data transfer control.

[0015] As a matter of course, the controller may transmit, to the cache device or the storage device, message information required to generate a message to be used in conducting negotiation between the client device and the cache or storage device along with the data transfer instruction. The cache device or the storage device may generate the message in accordance with the message information. This reduces the processing load on the controller associated with transfer of the data.

[0016] After completion of data transfer, the cache device or the storage device issues an acknowledgement message to the controller by way of the internal network. Upon receipt of the acknowledgement message from the cache device or the storage device, the controller may issue, to the client device, a reply message indicating completion of data transfer by way of the internal network. Thus, on the supposition that the controller generates an acknowledgment message to be issued to the client device, the processing load on respective devices can be lessened as compared with a case where the controller, the cache device, or the storage device intensively generates and issues all the messages required to conduct negotiation with the client device.

[0017] In a case where two or more cache devices are provided, the controller generates a message required for negotiation to be carried out between the client device and the respective cache devices and transmits the message to the respective cache devices along with the data transfer instruction. After the respective cache devices have transferred data to the client device through use of the message generated by the controller, any of the cache devices may transmit a message indicating completion of the data transfer to the client device by way of the internal network. This obviates a necessity of all the cache devices transmitting the reply message to the client device, which in turn significantly curtails the number of messages exchanged by way of the internal network.

[0018] As a matter of course, each of the cache devices may transmit the reply message indicating completion of data transfer to the client device by way of the internal network, and the client device may receive the respective reply messages output from the respective cache devices, thereby completing data transfer.

[0019] In a case where two or more cache devices are provided, the controller generates a message required for the negotiation to be carried out between the client device and the cache devices and transmits the message to the cache devices along with the data transfer instruction, as well as transmitting data copy destination cache device information to the cache devices. The cache devices transfer data to the client device through use of the message received from the controller. Subsequently, the cache device having received the data through data transfer may copy the received data to another cache device specified by the data copy destination cache device information received from the controller.

[0020] This enables realization of so-called mirroring in the system, thereby enhancing the reliability of the system.

[0021] The controller may instruct any one of the cache devices caching the same data to transfer the data to the storage device. The cache device having received the instruction may transfer the data to the storage device by way of the internal network and delete the data which have been stored redundantly along with the other cache device, thereby releasing a memory area thereof. This enables effective utilization of memory capacity of the cache device, and hence the memory capacity required by the cache device can be curtailed.

[0022] A storage system of the present invention is characterized by comprising a plurality of storage devices for storing data; a controller controlling access to the storage device; and an internal network interconnecting the storage device and the controller so as to enable communications therebetween. The controller and the storage devices further comprise the means provided below.

• Controller

[0023]

5 (1) Virtual storage management means which manages memory areas of a plurality of the storage devices as a virtual storage area of specific size by means of collectively managing the memory areas of a plurality of the storage devices through use of a virtual storage address; and
 (2) Transfer instruction issuing means which issues a data transfer instruction to the storage device having the memory area specified by the virtual storage management means on the basis of a certain virtual storage address
 10 upon receipt, by way of the internal network, of a request for access to the virtual storage area using the virtual storage address from a client device accessibly connected to the internal network.

• Storage Device

15 [0024] (1) Direct transfer means which carries out a direct negotiation required for data transfer with the client device in accordance with the data transfer instruction from the controller, thereby directly transferring data to the client device.
 [0025] Therefore, according to the storage system, data can be directly transferred between the storage device and the client device 7 without passing through the controller 2. Even in this case, in addition to enabling an attempt to greatly curtail latency and significantly improve a data throughput (ensure a band at which the performance of the
 20 internal network can be exhibited sufficiently), the storage system can provide a function comparable to that of the conventional virtual storage system.

Brief Description of the Drawings

25 [0026]

Fig. 1 is a block diagram showing the configuration of a storage system which is an embodiment of the present invention;
 Fig. 2 is a functional block diagram showing the configuration of the principal section of a controller shown in Fig. 1;
 30 Fig. 3 is a block diagram showing the configuration of the principal section of a cache device shown in Fig. 1;
 Fig. 4 is a block diagram showing the configuration of the principal section of a storage device shown in Fig. 1;
 Fig. 5 is a view for describing operation of the storage system shown in Fig. 1 (when data to be transferred are present in the cache device);
 Fig. 6 is a view for describing operation of the storage system shown in Fig. 1 (when data to be transferred are present in the storage device);
 35 Fig. 7 is a view for describing a first modification of operation of the storage system shown in Fig. 1;
 Fig. 8 is a view for describing a second modification of operation of the storage system shown in Fig. 1;
 Fig. 9 is a view for describing a third modification of operation of the storage system shown in Fig. 1;
 Fig. 10 is a view for describing a fourth modification of operation of the storage system shown in Fig. 1;
 40 Figs. 11 and 12 are views for describing a fifth modification of operation of the storage system shown in Fig. 1;
 Fig. 13 is a view for describing a sixth modification of operation of the storage system shown in Fig. 1;
 Fig. 14 is a view for describing a seventh modification of operation of the storage system shown in Fig. 1;
 Fig. 15 is a view showing a specific example of a management table (a virtual storage/real storage conversion map) showing a correlation between a virtual storage region and a real storage region according to an eighth
 45 modification of the present embodiment;
 Fig. 16 is a view showing a specific example of a management table (a cache map) showing a correlation between a virtual storage region and a cache region according to the eighth modification of the present embodiment;
 Fig. 17 is a view for describing an example case where the data held in real sectors of a disk drive in the storage system according to the eighth modification of the present embodiment are transferred directly to a client;
 50 Fig. 18 is a view for describing an example case where the data held in real sectors of the cache device in the storage system according to the eighth modification of the present embodiment are transferred directly to a client;
 Fig. 19 is a view for describing a case where a "mirroring" is realized in the storage system according to the eighth modification of the present embodiment;
 Fig. 20 is a view for describing a case where "striping" is realized in the storage system according to the eighth
 55 modification of the present embodiment;
 Fig. 21 is a view for describing virtual storage management employed in a case where storage devices are added to the storage system according to the eighth modification of the present embodiment;
 Fig. 22 is a view for describing virtual storage management when storage devices are added to the storage system

that realizes the "mirroring" shown in Fig. 19;

Fig. 23 is a view for describing virtual storage management when storage devices are added to the storage system that realizes the "striping" shown in Fig. 20;

Fig. 24 is a view for describing operation when data are transferred directly to the storage device from the cache device in the storage system according to the eighth modification of the present embodiment;

Fig. 25 is a view for describing operation when data are transferred directly to the cache device from the storage device in the storage system according to the eighth modification of the present embodiment;

Fig. 26 is a view showing an example existing storage system; and

Fig. 27 is a sequence diagram for describing data transfer processing to be performed by the storage system shown in Fig. 26.

Best Modes for Implementing the Invention

[0027] Fig. 1 is a block diagram showing the configuration of a storage system which is an embodiment of the present invention. A storage system 1 shown in Fig. 1 includes a controller (Control Machine) 2, a storage device 3, and a cache device 4. These devices 2, 3, and 4 are interconnected so as to be communicable with each other by way of an Infiniband (IB) network (IB switch) 5 serving as an internal network (such a configuration is called a WSS (Wire Speed Storage) architecture).

[0028] The devices 2, 3, and 4 are provided in respective numbers, as required. The controller 2 and the cache device 4 are constituted in the form of, e.g., network cards for use with the IB network 5. Moreover, the IB switch 5 is connected to an LAN (Local Area Network) 6 or the like constituted of one or more client devices (nodes) 7. The client devices 7 (hereinafter described simply as "clients 7") can access the storage system 1 by way of the LAN 6.

[0029] As shown in Figs. 1 and 4, the storage device 3 includes a disk drive (or possibly a tape unit) 31 for storing necessary data, e.g., file data; and an interface card (network card) 32 for controlling access to the disk drive 31. This interface card 32 is further equipped with a target channel adapter (TCA: Target Channel Adapter) 33 having the function of the IB network controller; a protocol conversion section (Protocol Transition Unit) 34; and a SCSI interface 35 having the function of a disk controller. The interface card 32 is prepared in required numbers equal to the number of disk drives 31 provided.

[0030] The protocol conversion section 34 can transfer necessary data directly to the client 7 by way of the IB network 5 by means of interpreting a message transmitted from the controller 2 over the IB network 5; making an access to the disk drive 31 to be accessed, by way of the SCSI interface 35 to which the disk drive 31 is connected, in accordance with details of the message; and making an RDMA (Remote Direct Memory Access) to the client 7 and returning the result of access as a reply message to the same.

[0031] Specifically, the protocol conversion section 34 serves as direct transfer means which transfers data directly to and from the client 7 by means of carrying out negotiation required for data transfer directly with the client 7 in accordance with a transfer instruction from the controller 2.

[0032] Also, the cache device 4 can transfer data directly to the client 7 in accordance with the instruction output from the controller 2. In the embodiment, as shown in Figs. 1 and 3, the cache device is constituted of a target channel adapter (TCA) 41 having the function of, e.g., an internal network controller; a memory area management section 42; a protocol handler 43; and a memory device 44 (hereinafter described simply as "memory 44") such as large-capacity RAM (of, e.g., 10 gigabytes or thereabouts).

[0033] Here, the memory area management section 42 is for manage allocation of areas (memory areas) of the memory 44 in the cache device 4 to the respective controllers 2 serving as cache regions capable of caching data pertaining to the respective disk drives 31. The protocol handler (protocol processing section) 43 interprets the message sent from the controller 2, accesses the memory 44 in accordance with details of the message, and makes the RDMA to the client 7 and returns a reply message to the client 7, thereby transferring the necessary data directly to the client 7.

[0034] In the cache device 4, the protocol handler 43 serves as direct transfer means which transfers data directly to the client 7 by means of carrying out negotiation required for data transfer directly to and from the client 7 in accordance with the transfer instruction output from the controller 2.

[0035] The controller 2 is for intensively managing (controlling) accesses to the cache device 4 and the storage device 3. For instance, the controller is realized by installing system management processes (programs), as software or firmware, into a workstation comprising, e.g., a CPU (Central Processing Unit) 21, memory 22, a chipset 23, a host channel adapter (HCA) 24, and the like.

[0036] The "system management processes" are for managing a location where data are reserved, such as where the entity of file data is reserved in the system 1 (the storage device 3 or the cache device 4), and also for receiving a request from the client device (hereinafter simply called "client") 7.

[0037] Specifically, as a result of the CPU 21 reading, e.g., the "system management processes" stored in the memory 22, the controller 2 is designed to exhibit the functions of a DAFS protocol handler (Direct Access File System Protocol

Handler) 21-1, an internal protocol handler 21-2, a real storage area management section (Real Storage Manager) 21-3, a cache area management section (Cache Machine Memory Manager) 21-4, a virtual storage management section (Virtual Storage Manager) 21-5, and a message transceiving section (Message Transition Unit) 21-6, or the like, as shown in, e.g., Fig. 2.

[0038] The DAFS protocol handler 21-1 performs DAFS protocol processing and has the function of receiving a DAFS processing request sent from the client 7 and issuing a transfer instruction (data transfer instruction) to the cache device 4 or the storage device 3, which manages data of interest.

[0039] Specifically, the DAFS protocol handler 21-1 has the function of transfer instruction issuing means which issues a transfer instruction to the cache device 4 or the storage device 3 upon receipt of the access request sent from the client 7 accessible to the IB network 5 by way of the IB network 5.

[0040] The internal protocol handler (internal protocol processing section) 21-2 is for performing control, such as flow control, required for continuing communication within the system 1. The real storage area management section 21-3 is for managing information about a network address and capacity of the storage device 3 (disk drive' 31) present in the system 1. The cache area management section 21-4 is for managing a memory area of the cache device 4 (memory 44) and has information about the network address and capacity of the cache device 4 (memory 44) and assigns the memory area in accordance with a request output from the virtual storage management section 21-5. Put another way, the cache area management section 21-4 collectively manages the memory areas of the cache device 4 through use of virtual storage addresses.

[0041] Furthermore, the virtual storage management section 21-5 manages memory areas of the plurality of storage devices 3 as virtual storage areas of specific sizes, by means of collectively managing memory areas of the plurality of storage devices 3 (disk drives 31) through use of the virtual storage addresses, as well as managing where the data requested by the client 7 (requested through use of the virtual storage address) are reserved in the system 1. In the present embodiment, such management is embodied by retaining management tables (data of table format), such as Tables 1 and 2 provided below.

Table 1

Map of Virtual Storage and Real Areas of Storage Device			
Virtual Storage ID	Virtual Sector Range	Real Storage ID	Sector Range of Real Storage
00	0-999	00	0-999
	1000-1999	01	0-999
	2000-2999	02	0-999
01	0-999	10	0-999
	0-999	11	0-999
02	Striping	20	0-999
		21	0-999
		22	0-999

Table 2

Map of Virtual Storage and Real Areas of Cache Device						
IB Address	Memory Address	Virtual Storage ID	Virtual Sector	Real Storage	Real Storage Sector	Flag
#0	10	00	0	00	0	
#1	01	01	0	10	200	

[0042] The management tables shown in Tables 1 and 2 manage, in an associated manner, a storage image provided to the client 7 by the controller 2 and which of the storage device 3 or the cache device 4 actually stores the entity of data against the storage image. For instance, the management table shown in Table 1 shows a map correlating the virtual storage and the memory area ((sector) of the disk drive 31) of real storage, thereby showing a correspondence between a sector of the virtual storage and a sector of the disk drive 31.

[0043] A virtual storage ID = 00 signifies that three disk drives 31 (real storage IDs = 00, 01, 02) are taken as a single virtual storage sequentially having sector groups (0 to 999) of the disk drives as virtual sector groups (in other words, the three disk drives 31 are seen as a single virtual disk by the client 7). Further, a virtual storage ID = 01 shows the

case of so-called "mirroring." A virtual storage ID = 02 shows a case of so-called "striping."

[0044] Meanwhile, Table 2 is a management table for managing the data cached in the cache device 4 among the data managed by the management table shown in Table 1. For instance, a first row of Table 2 signifies that the data stored in a virtual sector = 0 (sector = 0 of the real storage ID = 00) of the virtual storage (formed from the three disk drives 31) specified by the virtual storage ID = 00 are cached in a memory address = 10 of the memory 44 within the cache device 4 specified by an IB address = #0.

[0045] More detailed specific examples of the management tables will be described later by reference to Figs. 15 and 16.

[0046] After having retrieved and specified a location where the data are present, on the basis of the management tables provided in Tables 1 and 2 in synergy with the virtual storage management section 21-5, the DAFS protocol handler 21-1 issues a data transfer instruction (hereinafter simply called a "transfer instruction") to a corresponding component (the cache device 4 or the storage device 3).

[0047] First, the DAFS protocol handler 21-1 retrieves the cached data by reference to Table 2. If the cache data are present, the transfer instruction is issued to the cache device 4 that retains the cache data. If not, the transfer instruction is issued to the storage device 3.

[0048] The message transceiving section 21-6 generates a message, such as the transfer instruction and the RDMA (Remote Direct Memory Access), and sends the message to the IB network 5. The message transceiving section 21-6 also receives a message, such as the DAFS processing request transferred from the IB network 5 and an acknowledgment (Acknowledgment) output from the storage device 3 or the cache device 4.

[0049] Operation of the storage system 1 of the present embodiment having the foregoing configuration will be described hereinbelow.

(1) When the data to be transferred are present in the cache device 4

[0050] As shown in Fig. 5, the DAFS processing request (a request for access to a file A: Request File A) is assumed to have been issued from a certain client 7 to the controller 2 by way of the IB network 5 (step S1: an access-request-issuing step). In the controller 2, when the message transceiving section 21-6 has received the access request, the DAFS protocol handler 21-1 analyzes the received message, to thus ascertain contents of the message (the request for access to the file A).

[0051] Next, the DAFS protocol handler 21-1 determines whether or not the file A for which the request has been issued is cached in the cache device 4, by retrieving the management table shown in Table 2 in synergy with the virtual storage management section 21-4. On the assumption that the file A is cached in the cache device 4, the DAFS protocol handler 21-1 issues, to the cache device 4, a transfer instruction for transferring the file A to the client 7 (specified by an IP (Internet Protocol) address or the like) that has originally issued the request for access to the file A (step S2: a transfer-instruction-issuing step).

[0052] At this time, the DAFS protocol handler 21-1 also generates a message (a reply message 51 or an RDMA message 52) required by the cache device 4 to transfer data, by means of carrying out negotiation directly with the client 7, and sends the message to the cache device 4 along with the transfer instruction. At least the position in the cache device 4 where the file A is stored (memory address) and information about the size of the file A (sector range) are stored in the RDMA message 52.

[0053] When the cache device 4 has received the transfer instruction from the controller 2, the protocol handler 43 analyzes details of the transfer instruction and, consequently, ascertains that the instruction specifies transfer of the file A to the client 7. Then, the protocol handler 43 reads the target file A by means of reading data equal to a specified size from the storage position specified by the RDMA message 52, in synergy with the memory area management section 42.

[0054] The protocol handler 43 transfers the read file A directly to the client 7 by way of the IB network 5 by means of the RDMA message (step S3: a direct transfer step) and completes transfer of the file A by sending the reply message 52 received from the controller 2 (step S4).

(2) When the data to be transferred are present in the storage device 3.

[0055] As shown in Fig. 6, the DAFS processing request (a request for access to a file B: Request File B) from a certain client 7 is sent to the controller 2 by way of the IB network 5 (step S11). In the controller 2, when the message transceiving section 21-6 receives the transfer instruction, the DAFS protocol handler 21-1 analyzes the received message, thereby ascertaining contents of the message (the request for access to the file B).

[0056] Next, the DAFS protocol handler 21-1 determines whether or not the file A for which the request has been issued is cached in the cache device 4, by retrieving the management table shown in Table 2 in synergy with the virtual storage management section 21-4. On the assumption that the file B is not cached in the cache device 4, the DAFS

protocol handler 21-1 further retrieves the management table shown in Table 1 in synergy with the virtual storage management section 21-4, thereby specifying the storage device 3 (disk drive 31) reserving the file B for which the request has been issued.

[0057] The DAFS protocol handler 21-1 issues, to the cache device 4, a transfer instruction for transferring the file B to the client 7 (specified by an IP (Internet Protocol) address or the like) that has originally issued the request for access to the file B (step S12).

[0058] At this time, the DAFS protocol handler 21-1 also generates a message (the reply message 51, the RDMA message 52, and storage access information (a message) 53 showing the position in the disk drive 31 where the file B is stored) required by the storage device 3 to transfer data, by means of carrying out negotiation directly with the client 7, and sends the message to the storage device 3 along with the transfer instruction. The position of a leading sector of the file B in the disk drive 31 and information about the size of the file B are stored in the storage access information 53.

[0059] When the storage device 3 has received the transfer instruction from the controller 2, the protocol conversion section 34 interprets the transfer instruction. In accordance with details of the instruction, the SCSI interface 35 accesses the disk drive 31 on the basis of the storage access information 53, thereby reading from the disk drive 31 the file B specified by the information about the position of the leading sector and the size (step S13).

[0060] The SCSI interface 35 transfers the result of access (the file B), by way of the protocol conversion sections 34 and the TCA 33, directly to the client 7 in the form of the RDMA message over the IB network 5 (step S14) and returns the reply message to the client 7 again over the IB network 5 (step S15).

[0061] As mentioned above, the cache device 4 having the large-capacity memory 44 is mounted in the storage system 1 of the present embodiment, and the request (access request) output from the client 7 is received by the controller 2. However, real transfer processing and real processing of a reply to the client 7 are performed directly by the cache device 4 (or the storage device 3) while bypassing the controller 2. Therefore, there is enabled an attempt to significantly diminish latency and greatly improve a data throughput (ensure a band where the performance of the IB network 5 can be sufficiently exhibited).

[0062] In the aforementioned embodiment, the controller 2 intensively generates and issues the transfer instruction, the reply message 51, and the RDMA message 52, and hence the data transfer control to be performed in the system 1 is simplified, and the system has an advantage in terms of maintenance.

(3) First Modification

[0063] In the embodiment described by reference to Fig. 5, the controller 2 prepares the replay message 51 and the DRAM message 52 and passes the messages to the cache device 4. However, these messages may be prepared by the cache device 4.

[0064] Specifically, as shown in Fig. 7, the controller 2 (DAFS protocol handler 21-1) sends positional information about the file A—for which the access request has been issued—(the memory address of the cache device 4) directly to the cache device 4 while attaching the information to the transfer instruction to be delivered to the cache device 4 (step S2'). The cache device 4 originally generates a message (the RDMA message, the reply message, or the like) required for negotiation with the client 7, from the information sent from the controller 2 by means of the protocol handler 43 and performs processing for transferring the requested file A to the client 7 (steps S3', S4').

(4) Second Modification

[0065] Similarly, even in the embodiment described by reference to Fig. 6, the reply message 51 and the RDMA message 52 may be prepared by the storage device 3 rather than by the controller 2.

[0066] Specifically, as shown in Fig. 8, the controller 2 (DAFS protocol handler 21-1) sends positional information about the file B—for which the access request has been issued—directly to the storage device 3 while attaching the information to the transfer instruction to be delivered to the storage device 3 (step S12'). The storage device 3 reads the file B from the disk drive 41 in accordance with the information 53 sent from the controller 2 (step S13); originally generates the message (the RDMA message, the reply message, or the like) required for negotiation with the client 7 by means of the protocol conversion section 34; and performs processing for transferring the file B to the client 7 (steps S14', S15').

[0067] By means of the first and second modifications, the processing load on the controller 2 can be distributed to the cache device 4 or the storage device 3. Therefore, the system 1 is expected to be established inexpensively by means of miniaturizing and reducing costs of the controller by means of, e.g., curtailing the performance required by the controller 2.

(5) Third Modification

[0068] In the embodiment previously described by reference to Fig. 5, the controller 2 sends to the cache device 4 only a transfer instruction pertaining to the file A associated with the RDMA message 52, thereby causing the cache device 4 to make the RDMA to the client 7. The controller 2 can also be caused to perform remaining processing operations (generation and delivery of the reply message 51).

[0069] Specifically, as shown in Fig. 9, when the controller 2 (the DAFS protocol handler 21-1) has received the request for access to the file A from the client 7 (step S1), the DAFS protocol handler 21-1 generates the RDMA message 52 as a message which is required by the cache device 4 to perform data transfer by means of carrying out negotiation directly with the client 7 and sends the message to the cache device 4 along with the transfer instruction pertaining to the file A (step S21). Even in this case, at least a position in the cache device 4 where the file A is stored (memory address) and the size information (sector range) about the file A are stored in the RDMA message 52.

[0070] When the cache device 4 has received the transfer instruction from the controller 2, the protocol handler 43 analyzes details of the instruction and reads the object file A from the storage position specified by the RDMA message 52 in synergism with the memory area management section 42. The thus-read message is transferred directly to the client 7 by way of the IB network 5 by means of the RDMA message (step S22).

[0071] After completion of transfer operation, the protocol handler 43 generates an acknowledgment message addressed to the controller 2 and sends the thus-generated message to the controller 2 by way of the IB network 5 (step S23). In the controller 2 having received the acknowledgment message, the DAFS protocol handler 21-1 generates a reply message addressed to the client 7 and sends the message to the client 7 by way of the IB network 5 (step S24).

(6) Fourth Modification

[0072] Similarly, even in the embodiment described by reference to Fig. 6, the controller 2 sends to the storage device 3 only a transfer instruction pertaining to the file B associated with the RDMA message 52 and the storage access information 53, thereby causing the storage device 3 to make the RDMA to the client 7. The controller 2 can also be caused to perform remaining processing operations (generation and delivery of the reply message 51).

[0073] Specifically, as shown in Fig. 10, when the controller 2 has received the request for access to the file B from the client 7 (step S11), the DAFS protocol handler 21-1 in the controller 2 analyzes details of the received message and specifies the storage device where the requested file B is reserved (the disk drive 31) in synergism with the virtual storage management section 21-4.

[0074] The DAFS protocol handler 21-1 sends, to the specified storage device 3, the RDMA message 52 and the storage access information 53 while attaching the messages to the transfer instruction pertaining to the file B (step S21'). Even in this case, information about the position of the leading sector of the file B in the disk drive 31 and the size of the same is stored in the storage access information 53.

[0075] When the storage device 3 has received the transfer instruction from the controller 2, the protocol conversion section 34 interprets the transfer instruction. In accordance with details of the instruction, the SCSI interface 35 accesses the disk drive 31 on the basis of the storage access information 53, thereby reading from the disk drive 31 the file B specified by the information about the position of the leading sector and the size (step S22').

[0076] The SCSI interface 35 transfers the result of access (the file B), by way of the protocol conversion sections 34 and the TCA 33, directly to the client 7 in the form of the RDMA message over the IB network 5 (step S23'). After completion of the transfer operation, the protocol conversion section 34 sends a report to this effect to the controller 2 by way of the IB network 5 by means of the acknowledgment message (step S24'). Upon receipt of this report (acknowledgment message), the controller 2 generates the reply message 51 addressed to the client 7, by means of the DAFS protocol handler 21-1 and sends the message to the client 7 by way of the IB network 5 (step S25').

[0077] As in the case of the above-described third and fourth modifications, when compared with the embodiment shown in Figs. 5 and 6, the processing load on the controller 2 can be distributed to the cache device 4 or the storage device 3 by burdening the cache device 4 or the storage device 3 with a part of generation of the message required for negotiation with the client 7.

(7) Fifth Modification

[0078] Next will be described transfer processing performed by the system 1 when the plurality of cache devices 4 retain the same data redundantly with a view toward enhancing the reliability of data (so-called mirroring).

[0079] As shown in Fig. 11, a request (a write access) for access to the file A is assumed to have been issued from the client 7 to the controller 2 by way of the IB network 5 (step S31).

[0080] When the controller 2 has received the access request, the DAFS protocol handler 21-1 analyzes the received message and specifies (selects) cache devices 4A and 4B where the requested file A is to be reserved, in synergism

with the virtual storage management section 21-4. The DAFS protocol handler 21-1 generates, for the respective cache devices 4A, 4B, the messages (the reply messages 51 and the RDMA messages 52) required for communication with the client 7 and sends the messages to the cache devices 4A, 4B while attaching the messages to the transfer instruction (step S32). In this case, each of the RDMA messages 52 requires information about the memory addresses and sizes of the respective cache devices 4A, 4B where the file A is to be retained.

[0081] When the cache devices 4A, 4B have received the transfer instruction from the controller 2 as mentioned previously, the protocol handler 43 analyzes details of the instruction; receives the file A directly from the client 7 by way of the IB network 5 through use of the RDMA messages 52 received from the controller 2 in synergism with the memory area management section 42; and writes the files into the memory 44 (step S33).

[0082] Subsequently, after the client 7 has finished making the RDMA to the respective cache devices 4A, 4B, the protocol handlers 43 of the respective cache devices 4A, 4B return replies to the client 7 by means of the replay messages 51 received from the controller 2 (step S34). The client 7 terminates the transfer operation (the mirroring) upon receipt of the replies from all the cache devices 4A, 4B.

[0083] As mentioned above, according to the modifications, even when the mirroring is performed, the respective cache devices 4 carry out negotiation required for data transfer (exchange of the messages) with the client 7 in accordance with the transfer instruction from the controller 2. Real data transfer and reply processing are performed directly between the client 7 and the plurality of cache devices 4 while bypassing the controller 2. Hence, an attempt can be made to enhance reliability while curtailing the latency of the system 1 and improving a data throughput.

[0084] In the foregoing example, it may be the case that the transfer operation is completed when any one of the cache devices 4A, 4B has returned a reply. In such a case, the necessity for all the cache devices 4 sending the reply message to the client 7 is obviated. Hence, it may be the case that only some of the cache devices 4 send both the reply message 51 and the RDMA message 52, and the remaining cache devices 4 send only the RDMA message 52.

[0085] Specifically, as shown in Fig. 12, when the controller 2 has received the request for access to the file A from the client 7, the controller 2 sends the transfer instruction having the reply message 51 and the RDMA message 52 attached thereto to one cache device; e.g., the cache device 4A (step S32) and sends to the remaining cache device 4B the transfer instruction having only the RDMA message 52 attached thereto (step S32').

[0086] Thereby, after the respective cache devices 4A, 4B have made RDMA to the client 7 in connection with the file A (step S33), only the cache device 4A having received the reply message 51 from the controller 2 sends the reply message 51 to the client 7 (step S34).

[0087] Through the foregoing operations, the processing load on the controller 2 can be reduced, and the processing load on some of the cache devices 4 can also be lessened.

(8) Sixth Modification

[0088] Next, a modification of transfer processing to be performed during the "mirroring" will be described. In this case, the controller 2 does not issue any transfer instruction to all the cache devices 4 but issues a transfer instruction to one of the cache devices 4. The same data are copied from that cache device 4 to the other cache devices 4, thereby realizing mirroring.

[0089] Specifically, as shown in Fig. 13, when the request (write request) for access to the file A is assumed to have been issued by the client 7 to the controller 2 (step S41), the DAFS protocol handler 21-1 of the controller 2 issues, to the cache device 4A, for example, the transfer instruction used by the cache device 4A to receive the file A from the client 7 by way of the IB network 5 (step S42).

[0090] At this time, the DAFS protocol handler 21-1 generates the reply message 51 and the RDMA message 52, as well as generating the address information 54 about the cache device 4B which is the destination of copy of the file A. These messages and information are attached to the transfer instruction addressed to the cache device 4A. Even in this case, the RDMA message 52 requires the memory address of the cache device 4 and information about the size of the file A.

[0091] The cache device 4A having received the transfer instruction from the controller 2 receives the file A transferred from the client 7 by means of the RDMA message 52 generated by the controller 2 (step S43). When the transfer operation has been completed, the reply is sent back to the client 7 by means of the reply message 53 received from the controller 2 (step S44). The cache device 4A specifies the cache device 4B, which is a destination of copy, on the basis of the address information 54 received from the controller 2. The file A received from the client 7 is copied to the memory 44 of the cache device 4B (step S45). The copying can be performed by means of RDMA.

[0092] By means of the above-described operation, the number of messages exchanged within the system 1 is curtailed, so that the "mirroring" for enhancing the reliability of the system 1 can be realized without involving a decrease in the data throughput of the system 1.

(9) Seventh Modification

[0093] As mentioned previously by reference to Figs. 11 to 13, when the "mirroring" is performed by means of the plurality of cache devices 4, the data redundantly retained by some of the cache devices 4 are transferred to the storage device 3 at a certain time, thereby releasing the memory areas of the memory 44 of the cache device 4.

[0094] Specifically, as shown in Fig. 14, the controller 2 issues, to at least one of the cache devices 4A and 4B redundantly retaining the same file A, an instruction for transferring the file A to the storage device 3 at a certain time (step S51). As a matter of course, information specifying the storage device 3 and the disk drive 31, which are destinations of transfer, is attached to the transfer instruction at this time.

[0095] The cache device 4A having received the transfer instruction transfers the file A to the disk drive 31 of the storage device 3 by means of the RDMA (step S52). After having completed the transfer operation, the cache device sends a report to this effect to the controller 2 by means of the acknowledgment message (step S53) and deletes the redundantly-stored file A from the memory 44, to thus release the memory area (step 54).

[0096] By means of the foregoing operation, redundant data involving a low frequency of access are saved from the cache device 4 to the storage device 3, thereby enabling such a control operation that redundant data involving a high frequency of access are left in the cache device 4 in a prioritized manner. Consequently, the memory capacity of the cache device 4 can be used in the most effective manner. Even when mirroring is performed, the memory capacity required by the cache device 4 can be curtailed.

(10) Eighth Modification

[0097] Operation—which pays attention to the function of the previously-described virtual storage management section 21-5 and that of the cache area management section 21-4—will now be described hereinbelow.

[0098] As mentioned previously, the virtual storage management section 21-5 and the cache area management section 21-4 embody the virtual storage system, by means of collectively managing a correlation between a virtual storage area and a real storage area (the memory area of the storage device 3 (the disk drive 31)) and a correlation between the virtual storage area and a cache area (the memory area of the cache device 4), through use of the management table shown in Table 1 and the management table (map) shown in Table 2.

[0099] More specifically, the correlation between the virtual storage area and the real storage area is managed by a management table (a virtual storage/real storage conversion map) 211, such as that shown in Fig. 15. The correlation between the virtual storage area and the cache area is managed by a management table (cache map) 212, such as that shown in Fig. 16. As a matter of course, when no cache device 4 is present in the system, the cache area management section 21-4 (the cache map 212) is not necessary.

[0100] The virtual storage/real storage conversion map 211 retains a correlation among a "virtual storage ID," a "virtual sector," a "mode," a "real storage network address," a "real storage sector," a "stripe width," and the like. The cache map 212 retains a correlation among the "virtual storage ID," the "virtual sector," the "real storage network address," the "real storage sector," a "cache storage network address," a "cache local address," a flag, and the like.

[0101] For instance, it is meant that a "virtual storage ID" = a virtual storage of A (hereinafter often described as a "virtual storage A") is configured as a first entry of the virtual storage/real storage conversion map 211 by means of a "virtual sector" = "0-1999"; that the respective virtual sectors "0-999" of these sectors correspond to sectors (real storage sectors) = "2000-2999" of the storage device 3 (disk drive 31) specified by "real storage network address" = "10.25.180.3"; and that remaining virtual sectors "1000-1999" correspond to sectors (real storage sectors) = "4000-4999" of the storage device 3 (the disk drive 31) specified by the "real storage network address" = "10.25.180.4."

[0102] Here, "mode" = "jbod" signifies a "concatenation." In this case, the mode means that the virtual storage A is formed from concatenation between the sector "2000-2999" of one disk drive 31 and the sector "4000-4999" of another disk drive 31. Here, the "real storage network address" is taken as data (ID) of IP address format. However, as a matter of course, an ID of another format is also available.

[0103] Next, it is meant that a "virtual storage ID" = a virtual storage of B is configured as a second entry of the virtual storage/real storage conversion map 211 by means of a "virtual sector" = "0-3999"; that the respective virtual sectors "0-1999" of these sectors correspond to sets of "real storage sector" = "0-1999" and "3000-4999" of the two disk drives 31 (sets are denoted by "aa" and "ab" in Fig. 19) specified by the "real storage network address" = "10.25.180.10" and "10.25.180.11"; and that the "mirroring" specified by the "mode" is performed through use of the set of real storage sectors.

[0104] Similarly, it is meant that the respective sectors "2000-3999" correspond to sets of "real storage sector" = "0-1999" and "0-1999" (sets denoted as "aa" and "ab" in Fig. 19) of two disk drives 31 specified by "real storage network address" = "10.25.180.12" and "10.25.180.13"; and that the "mirroring" specified by the "mode" is performed through use of one set of real storage sectors.

[0105] In other words, the virtual storage management 21-5 is considered to have the function of mirroring means

which effects mirroring by means of managing a virtual storage address assigned to a specified area of the virtual storage area and real addresses assigned to the memory areas of the plurality of storage devices 3 in an associated manner. In this case, when the access request has been issued by the client 7, the data transfer instruction is issued to the respective storage devices 3, whereupon data are transferred directly between the client 7 and the storage devices 3.

[0106] Moreover, it is meant that a "virtual storage ID" = a virtual storage of C is configured as a third entry of the virtual storage/real storage conversion map 211 by means of a "virtual sector" = "0-7999"; that the respective virtual sectors "0-7999" of these sectors correspond to sets of "real storage sector" = "0-3999" and "1000-4999" of the two disk drives 31 specified by the "real storage network address" = "10.25.180.20" and "10.25.180.21"; and that the "striping" of "stripe width = 2" specified by the "mode" is performed through use of the real storage sectors.

[0107] Specifically, as shown in, e.g., Fig. 20, the correlation between the "virtual sector" and the "real sector" is assumed to be C#0=aa#0, C#1=ab#0, C#2=aa#1, C#3=ab#1, C#4=aa#2, C#5=ab#2, C#6=aa#3, ..., accesses to the disks 31a, 31b are made by access requests to virtual sectors C#0 → C#1 → C#2 → C#3 → C#4 → C#5 → C#6 → ... in sequence of a real sector aa#0 of the disk drive 31a → a real sector ab#0 of the disk drive 31b → a real sector aa#1 of the disk drive 31a → a real sector ab#1 of the disk drive 31b → a real sector aa#2 of the disk drive 31a → a real sector ab#2 of the disk drive 31b → a real sector aa#3 of the disk drive 31a → ...

[0108] Put another way, in this case, the virtual storage management section 21-5 comes to have the function of striping means. The striping means implements striping, by means of managing the virtual storage addresses and the real addresses assigned to the memory areas of the plurality of storage devices 3 in an associated manner such that consecutive divided areas resulting from division of a single virtual storage area (ID=C) by a predetermined size (a stripe width) are assigned to areas within different storage devices 3 (disk drives 31).

[0109] A first entry of the cache map 212 shown in Fig. 16 means that a "virtual storage ID" = a "virtual sector" of A = "2000" corresponds to a "real sector" = "4000" of the disk drive 31 specified by a "real storage network address" = "10.25.180.3" as well as to a "cache local address" (memory address) = "0x80000" of the cache device 4 specified by a "cache network address" = "10.25.180.20."

[0110] Similarly, a second entry of the cache map 212 means that the "virtual storage ID" = the "virtual sector" of A = "2001" corresponds to a "real sector" = "5000" of the disk drive 31 specified by the "real storage network address" = "10.25.180.3" as well as to the "cache local address" (memory address) = "0x40000" of the cache device 4 specified by the "cache network address" = "10.25.180.21."

[0111] Specifically, the cache area management section 21-4 is also arranged to collectively manage the memory areas of the cache device 4 by means of the virtual storage addresses.

[0112] "Flag" = "coherent" means that the data stored in the "real sector" coincide with the data stored in the "cache local address." "Flag" = "dirty" means that a mismatch exists between the data (the data stored in the cache device 4 are new). The "flags" further include "empty," which means that the cache area has already been assigned to the cache device 4 but effective data have not yet been stored in that area.

[0113] Now, in the case of "flag" = "dirty," consecutive processing such as that shown in, e.g., Fig. 24, is performed. Specifically, the controller 2 (the virtual storage management section 21-5) issues, to the cache device 4, a synchronization instruction for making the data (hereinafter also called "real data") retained in the "real sector" (aa) of the disk drive 31 match the latest data held in the "cache local address" (aaa) (step S61).

[0114] The cache device 4 having received the instruction transfers the data directly to the disk drive 31 by way of the IB network 5, thereby updating the data held in the "real sector" (aa) of the disk drive 31 to the latest data (step S62) and returning a report indicating completion of synchronization to the controller 2 as a reply (step S62). The controller 2 (the virtual storage management section 21-5) having received the reply updates the "flag" of the entry of the cache map 212 to "coherent" (step S63).

[0115] When the data are written into the cache device 4 from the disk drive 31 with the "flag" = "empty," consecutive processing such as that shown in, e.g., Fig. 25, is performed. Specifically, the controller 2 (the virtual storage device 21-5) issues to the storage device 3 an instruction for writing the data retained in the "real sector" (aa) of the disk drive 31 into the "cache local address" (aaa) of the cache device 4 (step S71).

[0116] The storage device 3 having received the instruction transfers the data stored in the "real sector" (aa) of the disk drive 31 directly to the cache device 4 by way of the IB network 5 to thereby write the data into the area of the "cache local area" (aaa) of the cache device 4 (step S72); and returns to the controller 2 a report indicating completion of writing operation (step S72). The controller 2 having received the response (the virtual storage management section 21-5) updates the "flag" of that entry of the cache map 212 to "coherent" (step S73).

[0117] Thus, the controller 2 issues an instruction to the storage device 3 or the cache device 4 on the basis of the entry of the cache map 212, thereby transferring data directly between the storage device 3 and the cache device 4 and enabling synchronization of the cache data with the real data and uploading the real data to the cache device 4 at high speed.

[0118] As mentioned above, in the present embodiment, direct transfer of data (including "mirroring" and "striping")

between the client 7 and the storage device 3 or the cache device 4 in the virtual storage system becomes feasible by means of managing the maps 211, 212 by means of the controller 2 (the virtual storage management section 21-5).

[0119] Specifically, as shown in Figs. 17 and 18, when a certain client 7 issues, to the controller 2, a request for (read) access to a certain virtual storage (through use of a virtual storage address) by way of the IB network 5, the controller 2 specifies a real storage area (real sector) retaining the requested data, in accordance with entry details of the entries of the maps 211, 212. The controller passes, to the storage device 3 or the cache device 4 managing the real sector, the information required to directly transfer data to the client 7, thereby enabling direct transfer of data between the client 7 and the storage device 3 or the cache device 4 while bypassing the controller 2.

[0120] Fig. 17 shows a case where the data retained in the real sector "aa" of the disk drive 31 are transferred directly to the client 7, and Fig. 18 shows a case where the data retained in the real sector "aaa" of the cache device 4 are transferred directly to the client 7. Detailed operations performed after the real storage areas have been specified are the same as those shown in Figs. 5 and 6.

[0121] Next will be described a case where disk drives 31 are additionally connected to the IB network 5.

[0122] As shown in, e.g., Fig. 21, consideration is given to a case where a new disk drive 31b is provided while a disk drive 31a has already been connected to a certain interface card 32. In this case, the controller 2 (the virtual storage management section 21-5) retains, as a map 211 obtained before addition, entries associating the "virtual sectors" ("0-999") with the "real sectors" (aa = "2000-2999") of the disk drive 31a. After addition of the disk drive, entries associating the "virtual sectors" ("1000-1999") with the "real sectors" (bb = "4000-4999") of the added disk drive 31b are appended to the map 211.

[0123] As mentioned above, addition of only new entries to the map 211 enables allocation of areas (real sectors) in the storage device 3 (the disk drive 31b) corresponding to the new virtual storage areas (the virtual sectors "1000-1999") additionally to the allocated virtual storage areas (the virtual sectors "0-999").

[0124] Addition of the virtual storage areas can also be effected even in the case of the "mirroring" or "striping" configuration, by means of addition of corresponding entries to the map 211 in the same manner.

[0125] For instance, as shown in Fig. 22, when two disk drives 31c, 31d are newly added to the controller 2 (the virtual storage management section 21-5) under the situation where the entries associating the "virtual sectors" (e.g., "0-1000") with the "real sectors" (e.g., aa = "2000-3000," bb = "4000-5000") of the two disk drives 31a, 31b have already been registered in the map 211 and where "mirroring" has been realized through use of the areas (aa = "2000-3000," bb = "4000-5000") within the two disk drives 31a, 31b, the only requirement is to add, to the map 211, entries associating newly-required "virtual sectors" (e.g., "1001-2000") with "real sectors" (e.g., ba = "0-999") of the disk drive 31c and the "real sectors" (e.g., bb = "2000-2999") of the disk drive 31d.

[0126] This enables "mirroring" using the areas (ba = "0-999," and bb = "2000-2999") within the newly-added two disk drives 31c, 31d.

[0127] Similarly, as shown in Fig. 23, when the two disk drives 31c, 31d are newly added to the controller 2 (the virtual storage management section 21-5) under the situation where the entries associating the "virtual sectors" (e.g., "0-1000") with the "real sectors" (e.g., aa = "0-499," bb = "1000-1500") of the two disk drives 31a, 31b have already been registered in the map 211 and where "striping" having a strip width b=2 has been realized through use of the areas (aa = "0-499," bb = "1000-1500") within the two disk drives 31a, 31b, the only requirement is to add, to the map 211, entries associating newly-required "virtual sectors" (e.g., "1001-2000") with "real sectors" (e.g., ba = "1000-1499") of the disk drive 31c and the "real sectors" (e.g., bb = "3000-3499") of the disk drive 31d.

[0128] This enables "striping" that uses the areas (ba = "1000-1499," and bb = "3000-3499") within the newly-added two disk drives 31c, 31d and has a stripe width (b = 2). The stripe width of the disk drives 31a, 31b achieved before addition may change from that of the disk drives 31c, 32d achieved after addition.

[0129] It goes without saying that, even when some of the storage devices 3 are deleted (reduced) from the IB network 5, deletion can be realized by changing only the entries of the map 211.

[0130] Specifically, the virtual storage management section 21-5 has the function of virtual storage address Change means which change associations between the virtual storage addresses of the virtual storage area and the real addresses of the memory areas of the storage device 3 in accordance with an increase or decrease in the number of storage devices 3 connected to the IB network 5.

[0131] As mentioned above, in the foregoing embodiments, direct transfer of data between the storage device 3 or the cache device 4, and the client 7 while bypassing the controller 2 enables an attempt to significantly curtail latency and improve a data throughput (assurance of a band where the performance of the IB network 5 can be sufficiently exhibited) as well as providing a function which won't be subordinate to the conventional virtual storage system.

(11) Others

[0132] The present invention is not limited to the previously-described embodiments and, needless to say, can be carried out while being modified in various manners falling within the scope of the gist of the invention.

[0133] For instance, the foregoing embodiments are based on the premise that the access request issued from the client 7 by way of the IB network 5 is based on DAFS. However, the same working effect can be yielded even when the access request is based on another protocol [e.g., SRP (SCSI RDMA Protocol)].

[0134] Formats of the various messages exchanged within the IB network 5 can be changed, as required.

Industrial Applicability

[0135] As has been described, according to the present invention, the cache device (or the storage device) provided in the storage system directly transfers data by carrying out negotiation required for data transfer with the client device in accordance with the instruction from the controller. Therefore, latency of the system can be diminished, and a significant improvement in the data throughput can be achieved. For instance, a high-speed, high-performance data center or the like can be constructed, and the center is considered to have extremely high usefulness.

Claims

1. A storage system comprising:

a storage device (3) storing data;
 a cache device (4) capable of caching said data stored in said storage device (3);
 a controller (2) controlling access to at least said storage device (3) and said cache device (4); and
 an internal network (5) interconnecting said storage device (3), said cache device (4), and said controller (2) so as to be enable communications therebetween, wherein
 said controller (2) includes transfer instruction issuing means (21-1) which issues a data transfer instruction to one of said cache device (4) and said storage device (3) upon receipt of an access request transmitted, by way of said internal network (5), from a client device (7) connected to said internal network (5) in an accessible manner; and
 at least one of said storage device (3) and cache device (4) which receives said data transfer instruction includes direct transfer means (34 or 43) for performing direct transfer of data to said client device (7) by means of directly carrying out negotiation required for data transfer with said client device (7) in accordance with said data transfer instruction from said controller (2).

2. A data transfer method for use in a storage system having a storage device (3) storing data, a cache device (4) capable of caching said data stored in said storage device (3), a controller (2) controlling access to at least said storage device (3) and said cache device (4), and an internal network (5) interconnecting said storage device (3), said cache device (4), and said controller (2) so as to be enable communications therebetween, the method comprising:

an access request issuance step (S1) of a client device (7) connected to said internal network (5) in an accessible manner, that issues an access request to said controller (2) by way of said internal network (5);
 a transfer instruction issuance step (S2) of said controller (2) that issues a data transfer instruction to either said cache device (4) or said storage device (3) upon receipt of said access request; and
 a direct transfer step (S3) of one of said cache device (4) and said storage device (3) carrying out direct negotiation required for transfer of data with respect to said client device (7), thereby transferring data directly to said client device (7).

3. The data transfer method for use in a storage system according to claim 2, wherein said controller (2), in said transfer instruction issuance step (S2), generates a message for said negotiation to be carried out between said client device (7) and said cache device (4) and transmits said message to said cache device (4) along with said data transfer instruction; and

said cache device (4), in said data transfer step (S3), transfers data to said client device (7) through use of said message generated by said controller (2).

4. The data transfer method for use in a storage system according to claim 2, wherein said controller (2), in said transfer instruction issuance step (S2), generates a message for said negotiation to be carried out between said client device (7) and said storage device (3) and transmits said message to said storage device (3) along with said data transfer instruction; and

said storage device (3), in said data transfer step (S3), transfers data to said client device (7) using said

message generated by said controller (2).

- 5 5. The data transfer method for use in a storage system according to claim 2, wherein said controller (2), in said transfer instruction issuance step (S3), generates a message for said negotiation to be carried out between said client device (7) and said cache device (4) and transmits said message to said cache device (4) along with said data transfer instruction; and
said cache device (4), in said data transfer step (S3), generates said message on the basis of said message information transmitted from said controller (2) and transfers data to said client device (7) through use of said message.
- 10 6. The data transfer method for use in a storage system according to claim 2, wherein said controller (2), in said transfer instruction issuance step (S2), transmits a message required for establishing said negotiation between said client device (7) and said storage device (3) to said cache device (4) along with said data transfer instruction; and
15 said storage device (3), in said data transfer step (S3), generates said message on the basis of said message information transmitted from said controller (2) and transfers data to said client device (7) through use of said message.
- 20 7. The data transfer method for use in a storage system according to claim 3 or 5, wherein said cache device (4) issues an acknowledgment message to said controller (2) by way of said internal network (5) when said data transfer pertaining to said direct transfer step (S3) has been completed; and
said controller (2) issues a reply message indicating completion of data transfer to said client device (7) by way of said internal network (5) upon receipt of said acknowledgment message from said cache device (4).
- 25 8. The data transfer method for use in a storage system according to claim 4 or 6, wherein said storage device (3) issues an acknowledgment message to said controller (2) by way of said internal network (5) when said data transfer pertaining to said direct transfer step (S3) has been completed; and
said controller (2) issues a reply message indicating completion of data transfer to said client device (7) by way of said internal network (5) upon receipt of said acknowledgment message from said storage device (3).
- 30 9. The data transfer method for use in a storage system according to claim 2, wherein, in a case where two or more cache devices (4) are provided, said controller (2), in said transfer instruction issuance step (S2), generates a message required for said negotiation to be carried out between said client device (7) and said cache devices (4A, 4B) and transmits said message to said cache devices (4) along with said data transfer instruction;
35 said cache devices (4A, 4B), in said direct transfer step (S3), transfer data to said client device (7) through use of said message generated by said controller (2); and
any one of said cache devices (4A, 4B) transmits a message indicating completion of said data transfer to said client device (7) by way of said internal network (5).
- 40 10. The data transfer method for use in a storage system according to claim 2, wherein, in a case where two or more cache devices (4) are provided, said controller (2), in said transfer instruction issuance step (S2), generates a message required for said negotiation to be carried out between said client device (7) and said cache devices (4A, 4B) and transmits said message to said cache devices (4A, 4B) along with said data transfer instruction;
45 said cache devices (4A, 4B), in said direct transfer step (S3), transfer data to said client device (7) through use of said message generated by said controller (2);
any one of said cache devices (4A, 4B) transmits a message indicating completion of said data transfer to said client device (7) by way of said internal network (5); and
said client device (7) completes said data transfer upon receipt of said reply message from said respective cache devices (4A, 4B).
- 50 11. The data transfer method for use in a storage system according to claim 2, wherein, in a case where two or more cache devices (4) are provided, said controller (2), in said transfer instruction issuance step (S2), generates a message required for said negotiation to be carried out between said client device (7) and said cache devices (4A, 4B), transmits said message to said cache device (4) along with said data transfer instruction, and transmits data copy destination cache device information to said cache device (4A);
55 said cache device (4A), in said direct transfer step (S3), transfers data to said client device (7) through use of said message received from said controller (2); and
said cache device (4A) copies said received data to another cache device (4B) specified by said data copy

destination cache device information received from said controller (2).

12. The data transfer method for use in a storage system according to any one of claims 9 through 11, wherein said controller (2) instructs any one of said cache devices (4A, 4B) caching the same data to transfer said data to said storage device (3); and
said cache device (4A) having received said instruction transfers said data to said storage device (3) by way of said internal network (5) and deletes said data which have been stored redundantly along with the other cache device (4B), thereby releasing a memory area thereof.
13. A storage system comprising:
a plurality of storage devices (3) for storing data;
a controller (2) controlling access to said storage device (3); and
an internal network (5) interconnecting said storage device (3) and said controller (2) so as to enable communications therebetween, wherein
said controller (2) comprises
virtual storage management means (21-5) managing memory areas of a plurality of said storage devices (3) as a virtual storage area of specific size by means of collectively managing said memory areas of a plurality of said storage devices (3) through use of a virtual storage address; and
transfer instruction issuing means (21-1) which issues a data transfer instruction to said storage device (3) having said memory area specified by said virtual storage management means (21-5) on the basis of a certain virtual storage address upon receipt, by way of said internal network (5), of a request for access to said virtual storage area using said virtual storage address from a client device (7) accessibly connected to said internal network (5); and wherein
said storage device (3) has direct transfer means (34) which carries out a direct negotiation required for data transfer with said client device (7) in accordance with said data transfer instruction from said controller (2), thereby directly transferring data to said client device (7).
14. The storage system according to claim 13, further comprising a cache device (4) capable of caching said data stored in said storage device (3), wherein
said controller (2) further comprises cache area management means (21-4) for collectively managing a memory area of said cache device (4) through use of said virtual storage address; and
said transfer instruction issuing means is configured to issue said data transfer instruction to one of said storage device (3) and said cache device (4) having a memory area which can be specified by one of said virtual storage management means (21-5) and said cache area management means (21-4) on the basis of said virtual storage address.
15. The storage system according to claim 14, wherein the cache device (4) has direct transfer means (43) which carries out a direct negotiation required for data transfer with said client device (7) in accordance with said data transfer instruction from said controller (2), thereby directly transferring data to said client device (7).
16. The storage system according to claim 13, wherein said virtual storage management means (21-5) has mirroring means which effects mirroring by means of managing a virtual storage address assigned to a specific area of said virtual storage area and real addresses assigned to memory areas of a plurality of said storage devices in an associated manner.
17. The storage system according to claim 13, wherein said virtual storage management means (21-5) has striping means which effects striping by means of managing said virtual storage address and real addresses assigned to memory areas of a plurality of said storage devices (3) in an associated manner such that consecutive split areas obtained when said virtual storage area is divided into areas of given size are allocated to said memory areas of a plurality of said storage devices (3).
18. The storage system according to claim 13, 15, or 16, wherein said virtual storage management means (21-5) further includes virtual storage address change means for changing association of said virtual storage addresses of said virtual storage area with real addresses of increased or decreased memory areas of said storage devices (3) in accordance with an increase or decrease in the number of said storage devices (3) corresponding to said internal network.

EP 1 498 809 A1

19. The storage system according to claim 14, wherein said cache area management means (21-4) of said controller (2) comprises cache data instruction issuing means issuing, to said cache device (4) or said storage device (3), a data transfer instruction to be used for directly transferring data between said cache device (4) and said storage device (3).

5

10

15

20

25

30

35

40

45

50

55

FIG. 1

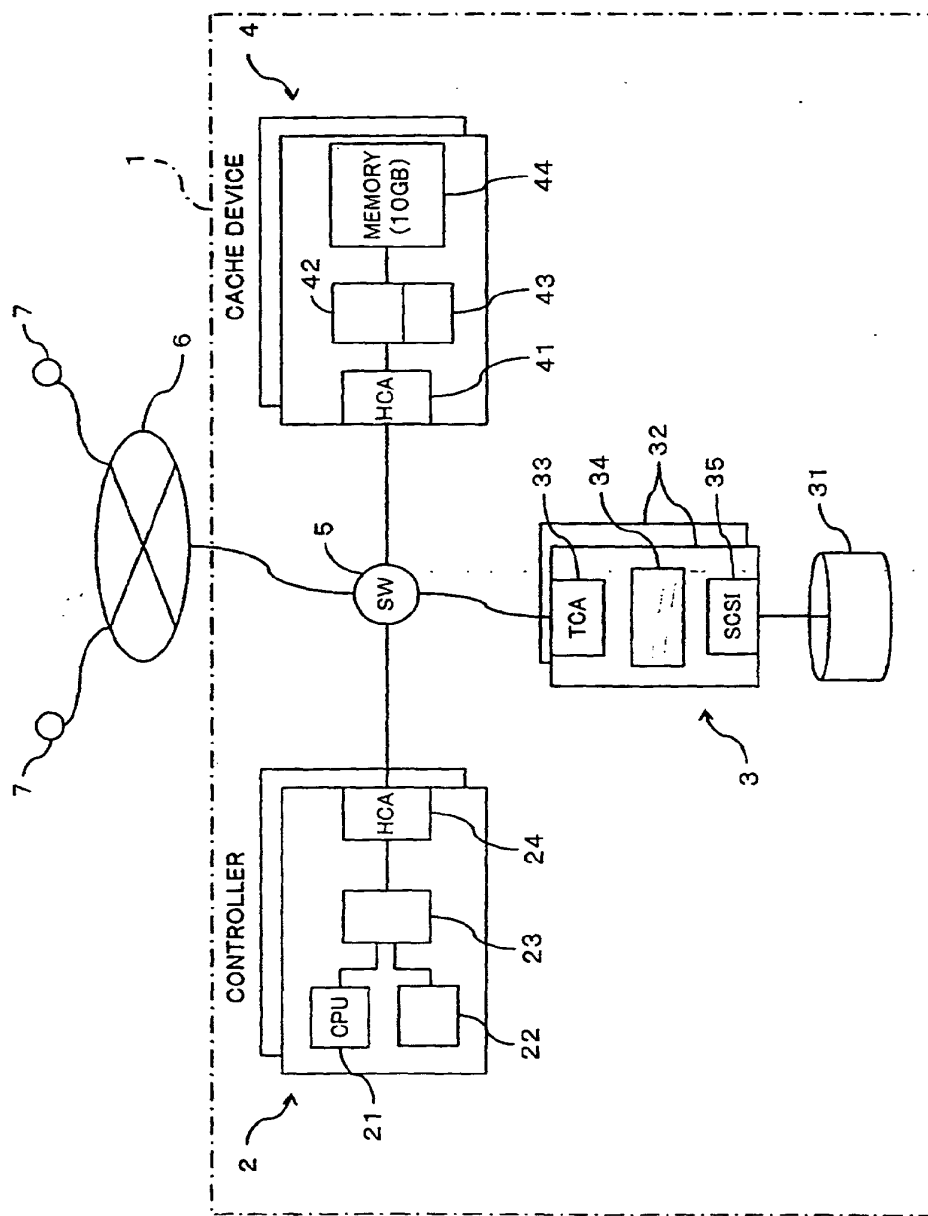


FIG. 2

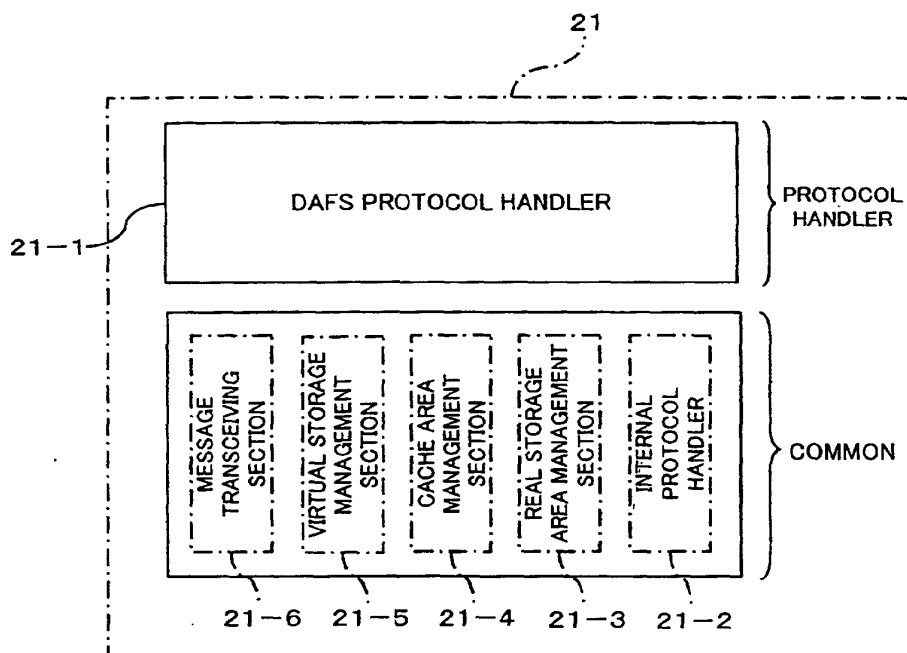


FIG. 3

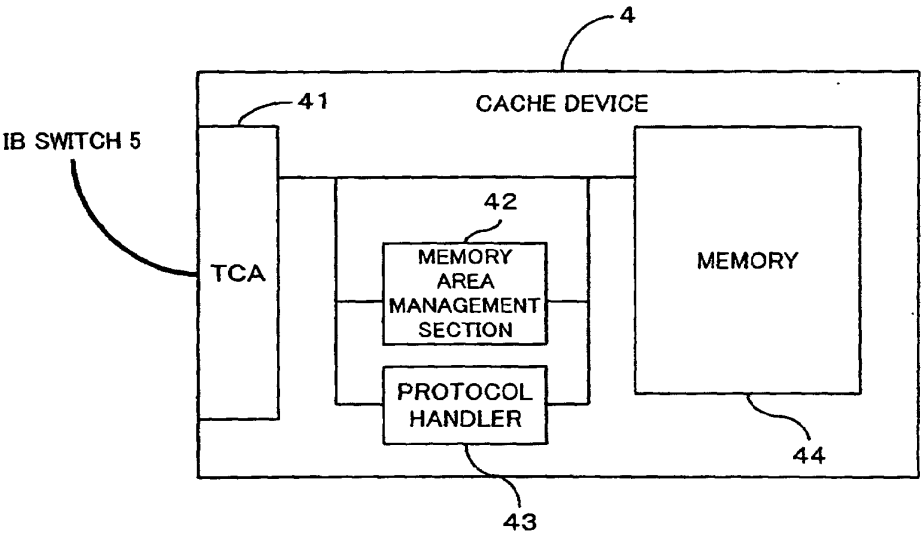


FIG. 4

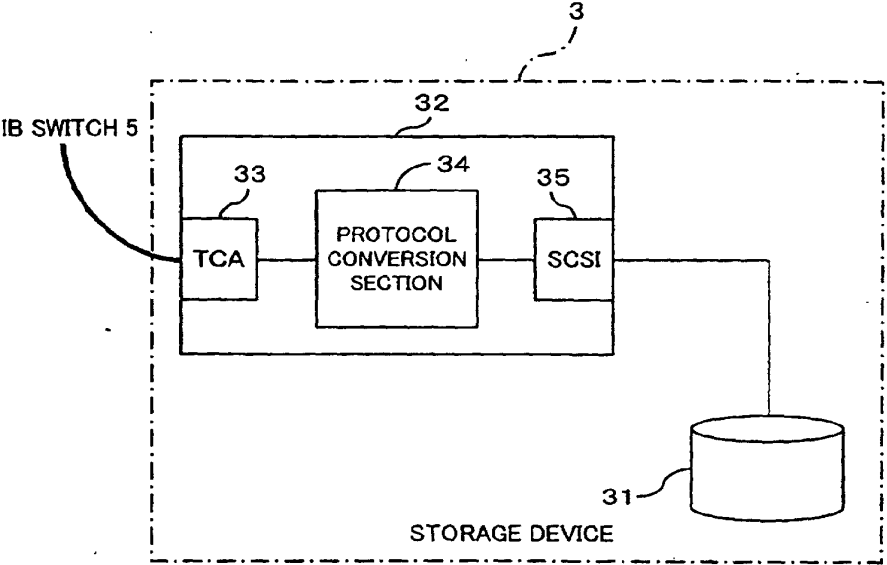


FIG. 5

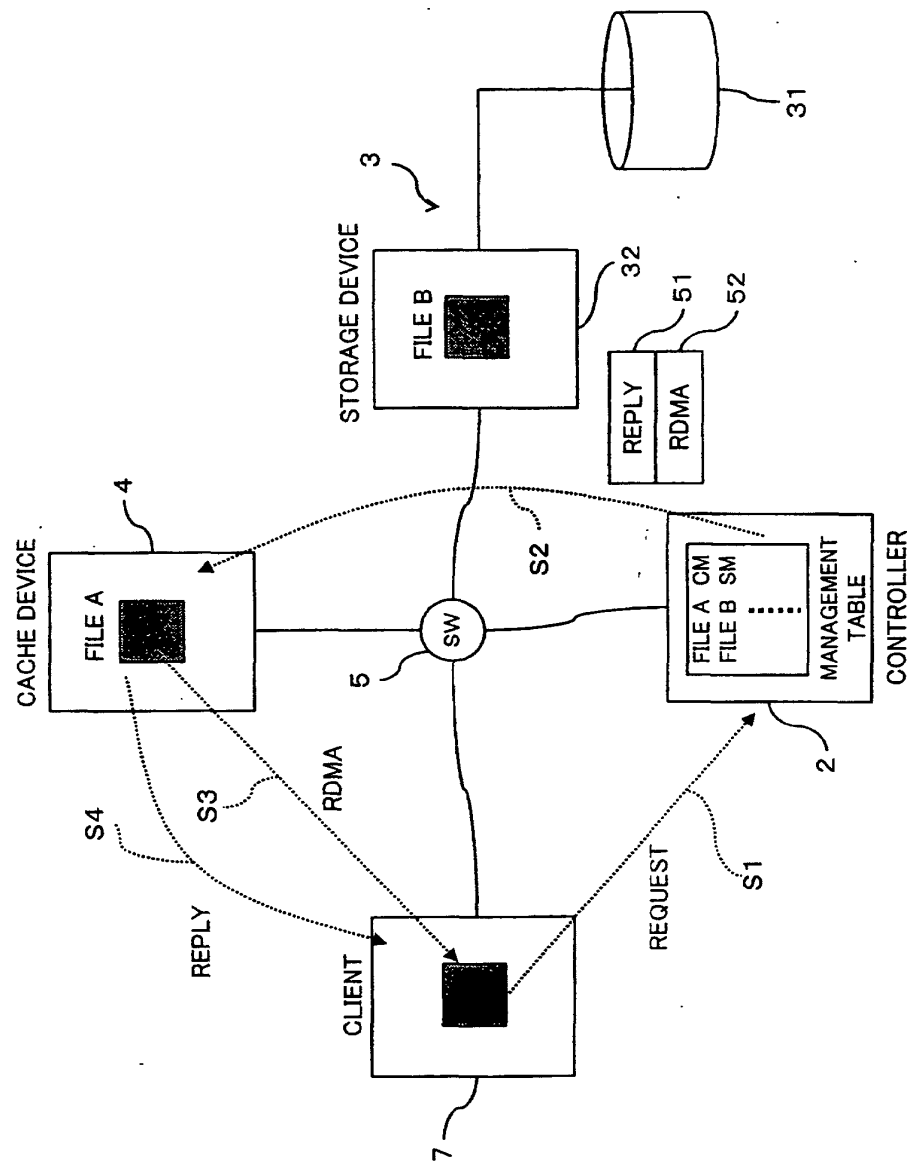


FIG. 6

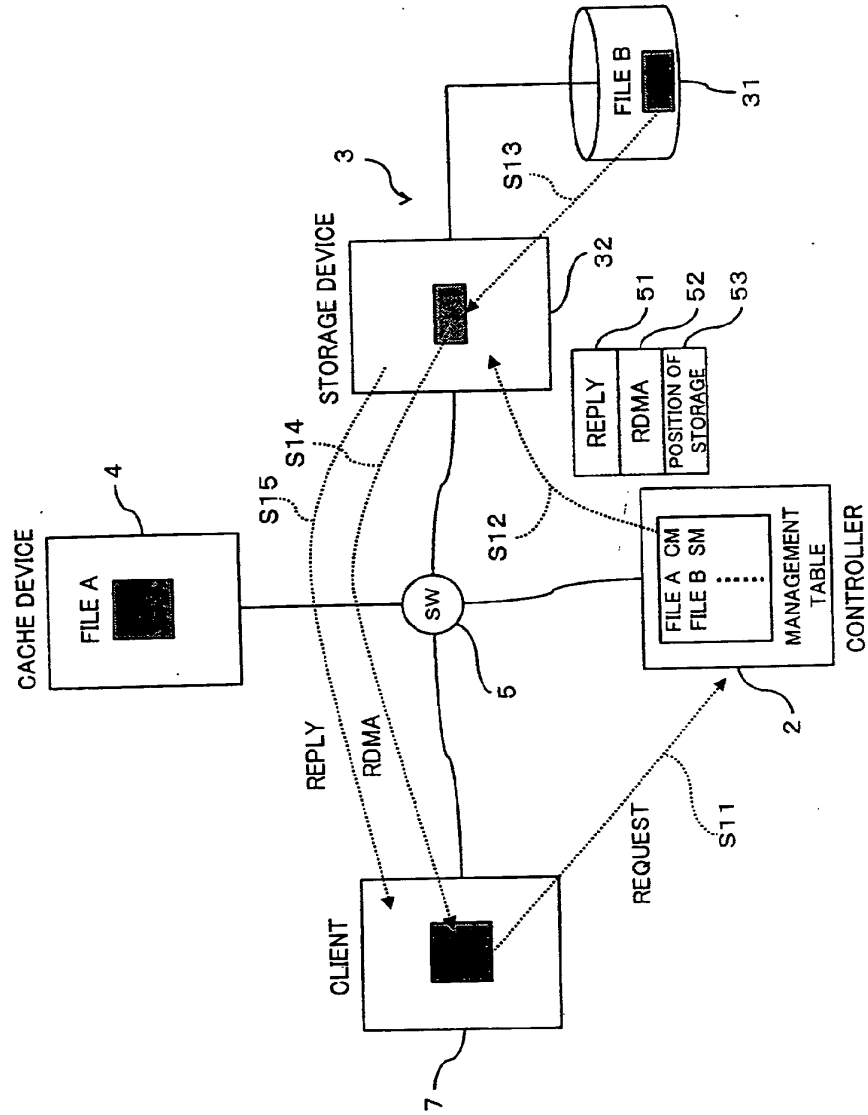


FIG. 7

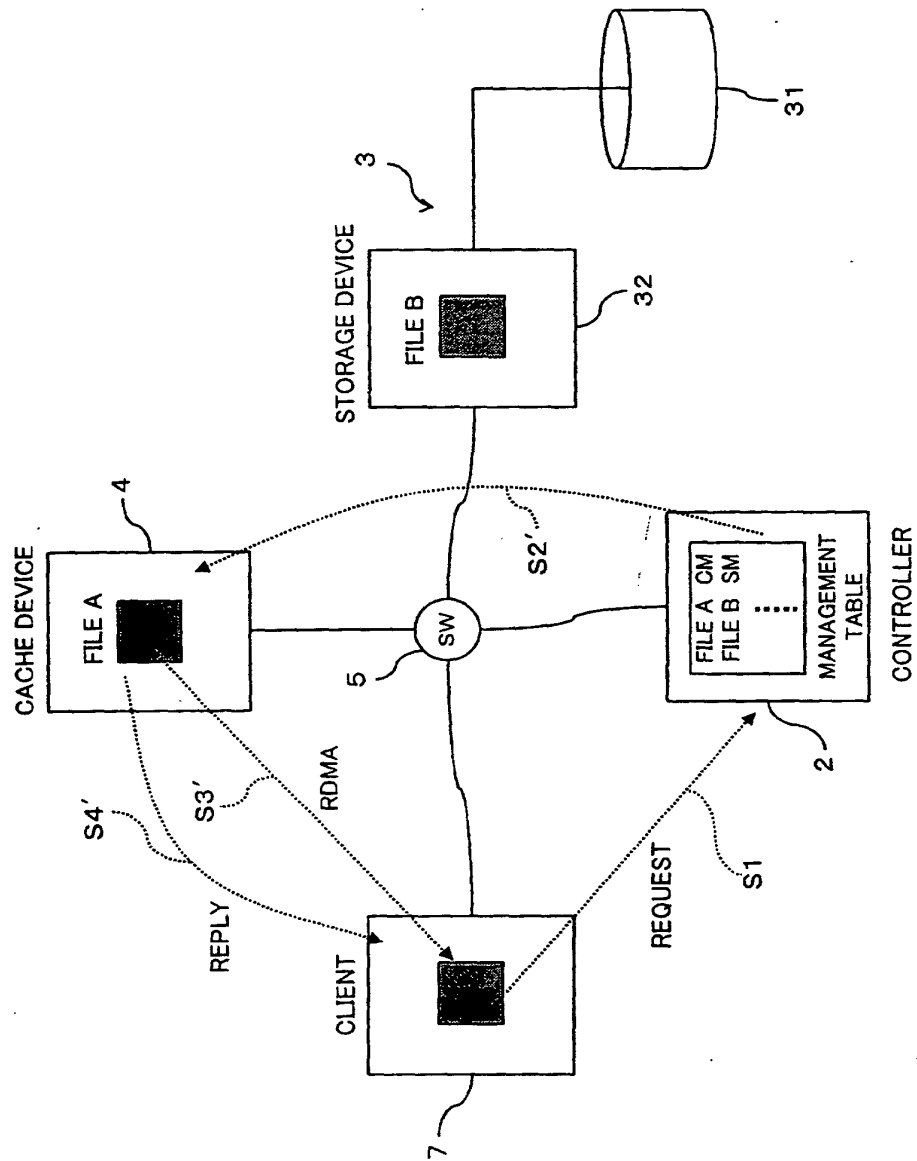


FIG. 8

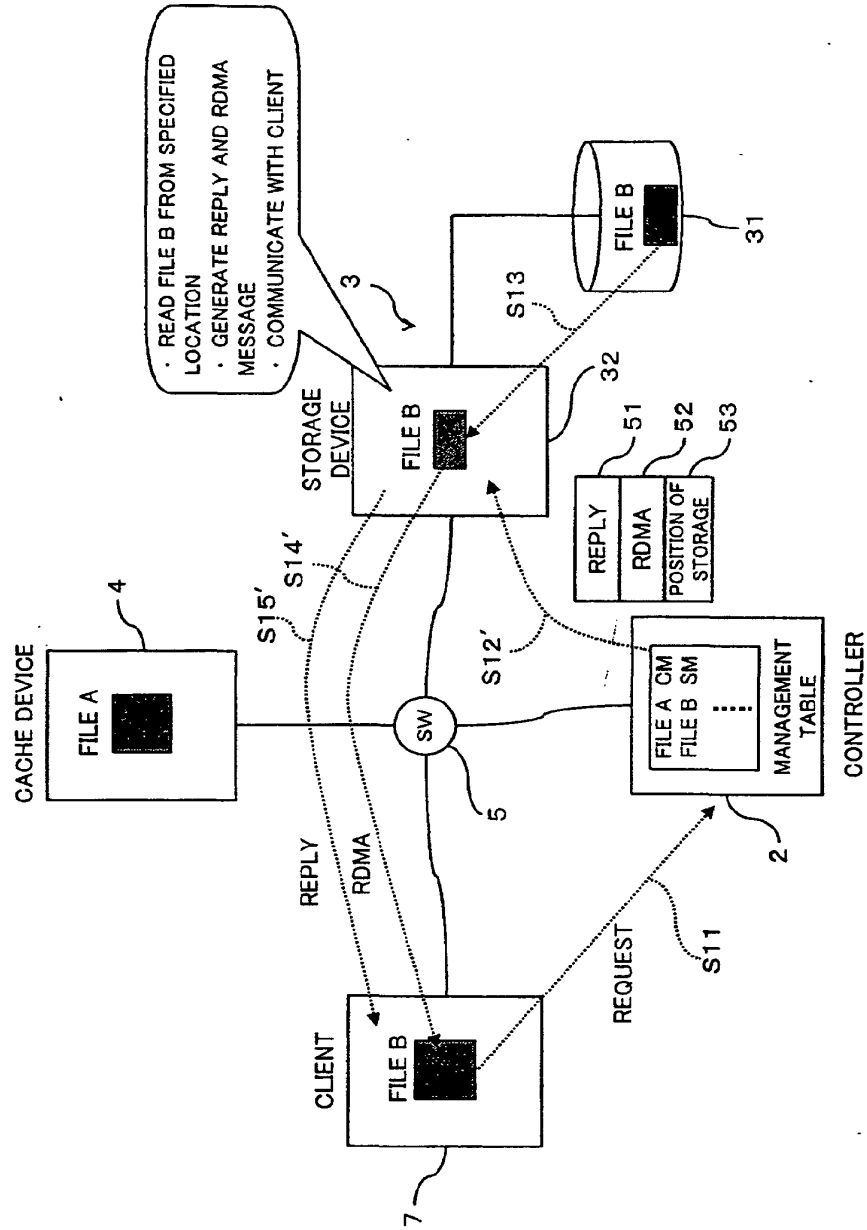


FIG. 9

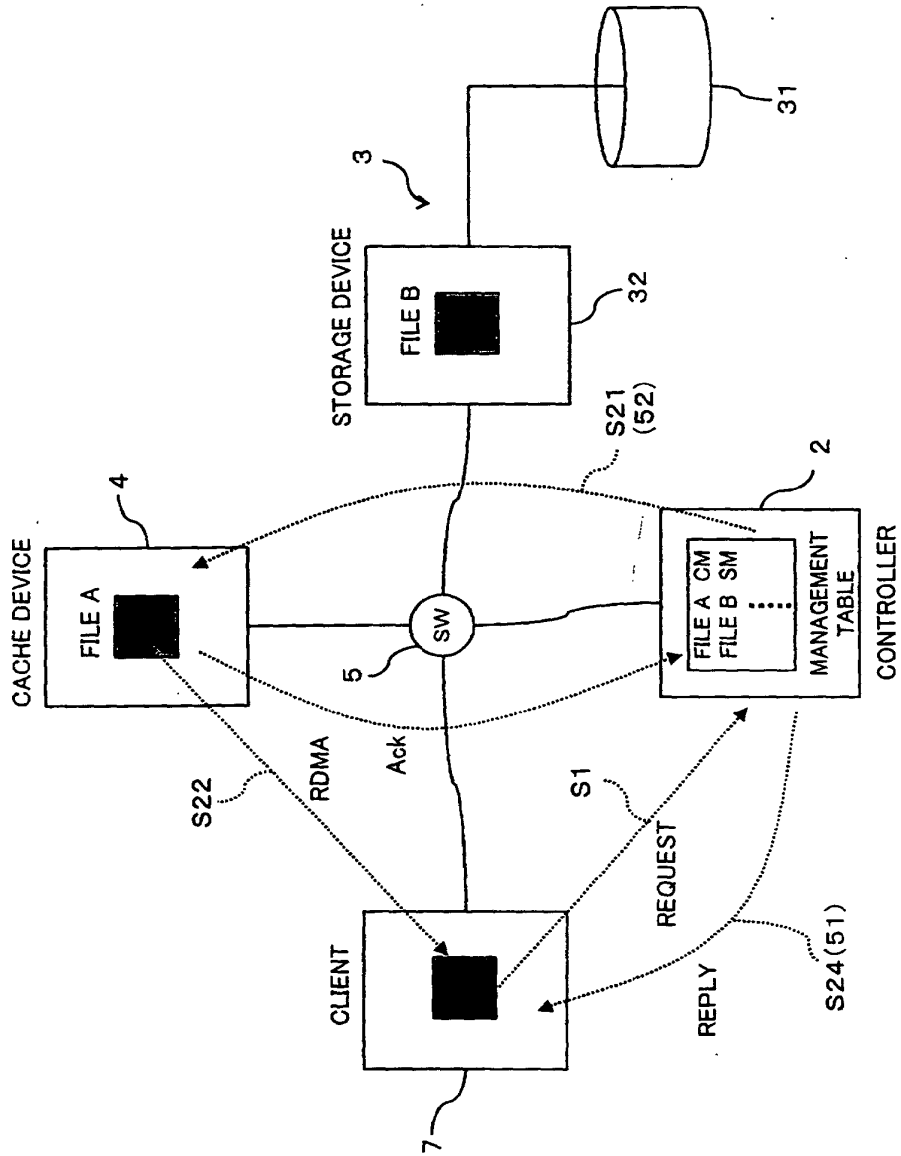


FIG. 10

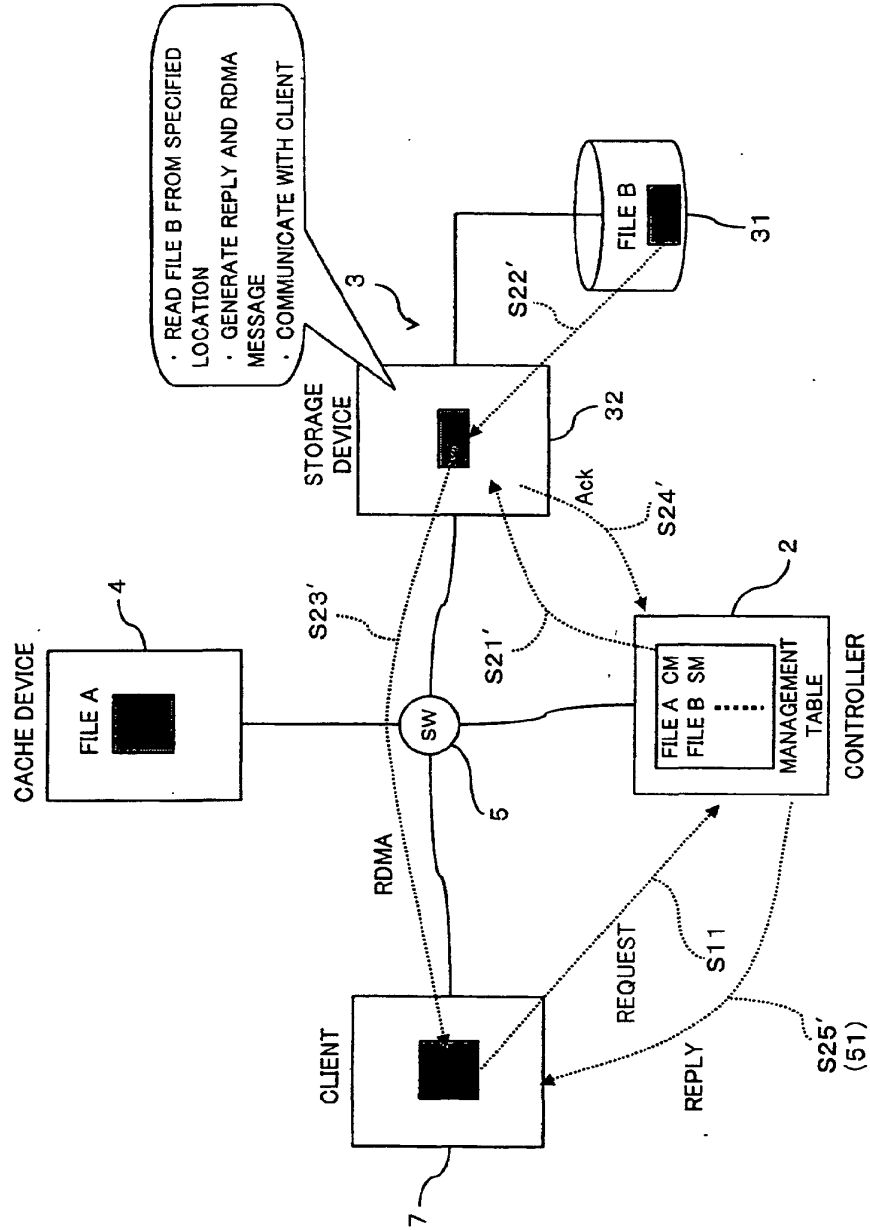


FIG. 11

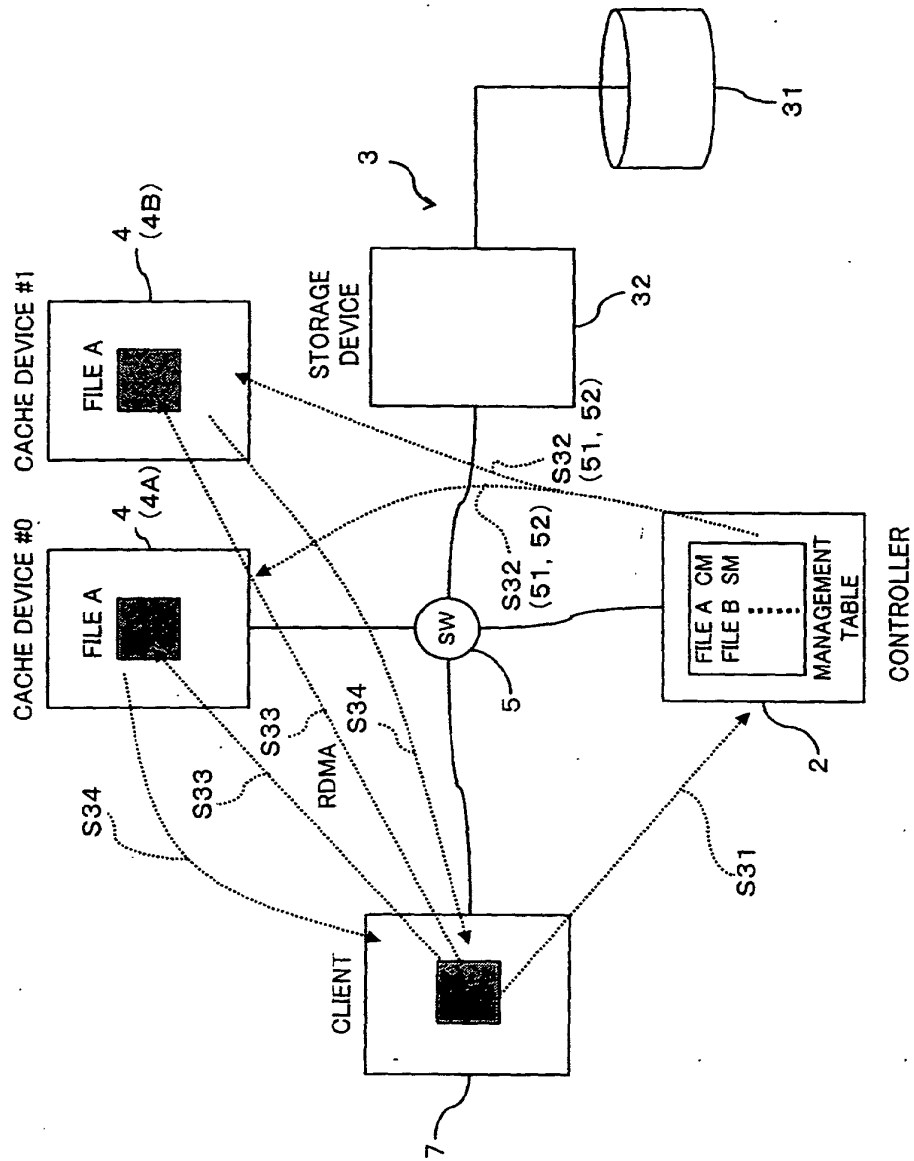


FIG. 12

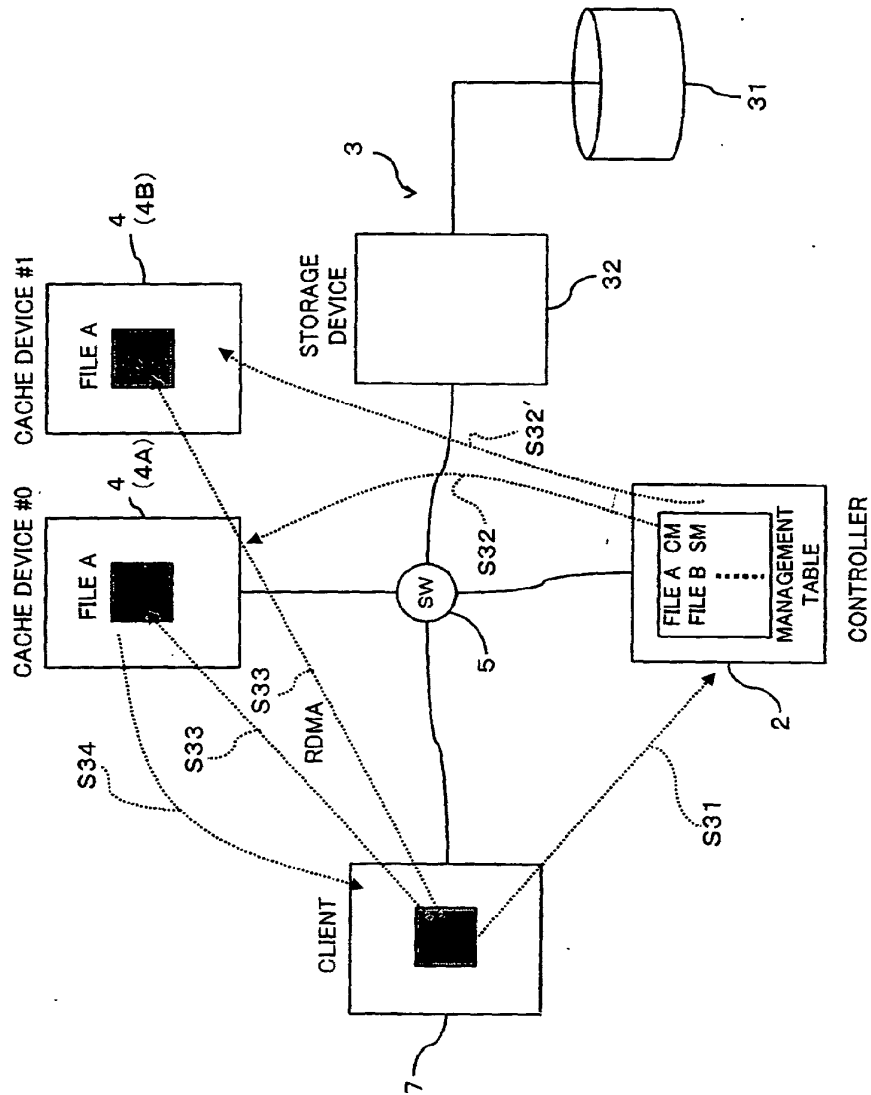


FIG. 13

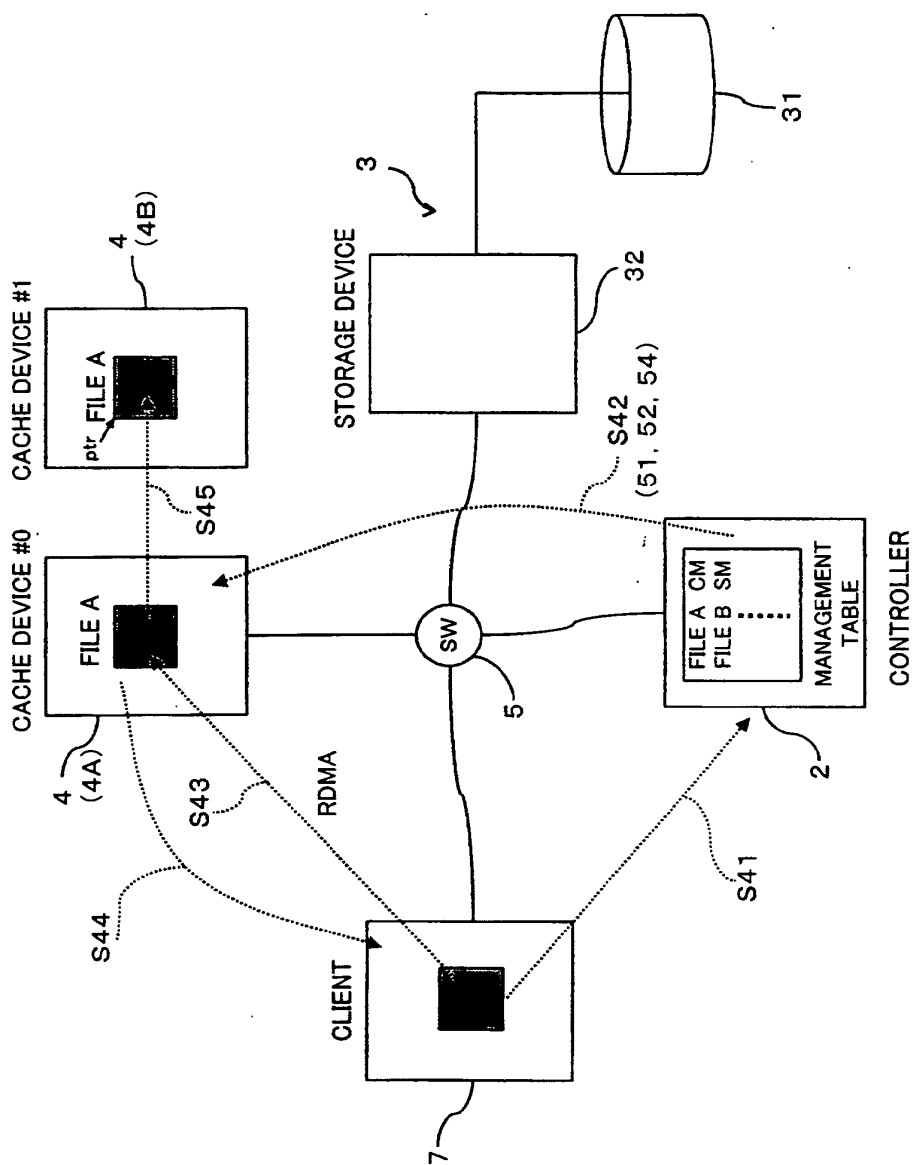


FIG. 14

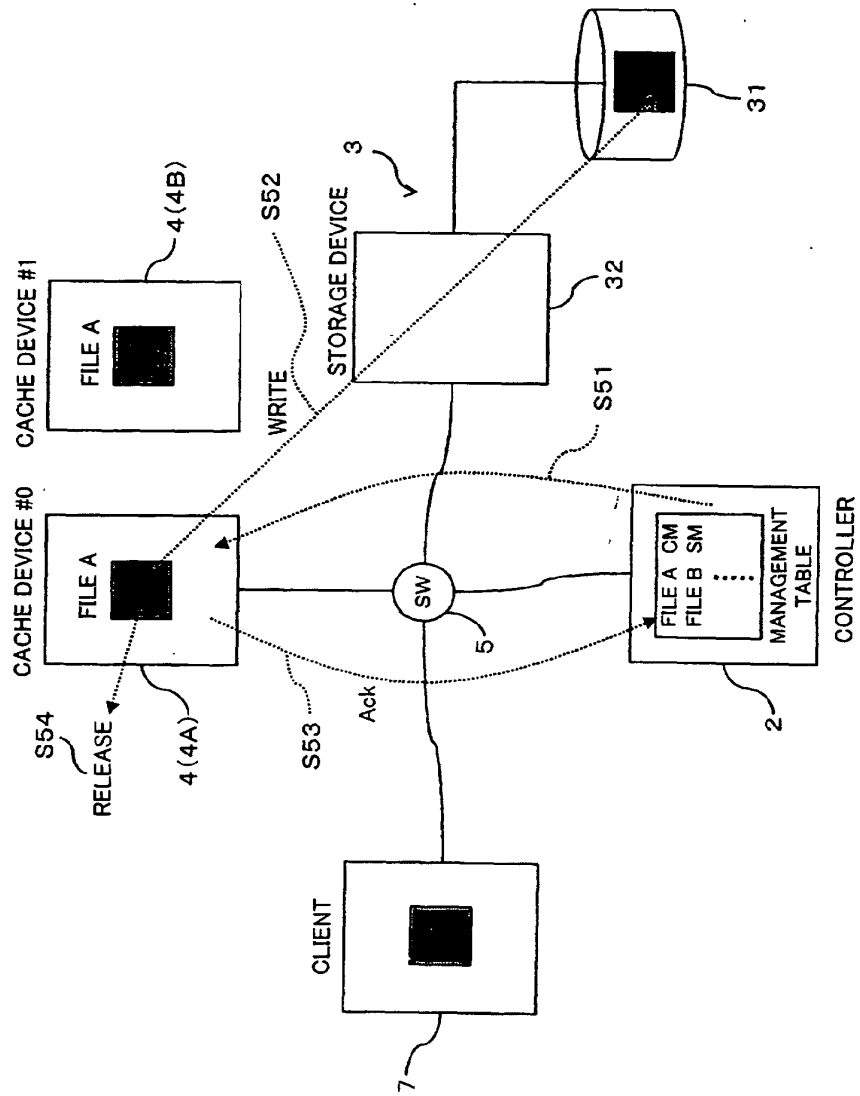


FIG. 15

211
↓

VIRTUAL STORAGE ID	VIRTUAL SECTOR	MODE	REAL STORAGE NETWORK ADDRESS	REAL STORAGE SECTOR	STRIPE WIDTH
A	0-999 1000-1999	jpod	10.25.180.3 10.25.180.4	2000-2999 4000-4999	—
B	0-1999 2000-3999	MIRROR	10.25.180.10 10.25.180.11 10.25.180.12 10.25.180.13	0-1999 3000-4999 0-1999 0-1999	—
C	0-7999	STRIPE	10.25.180.20 10.25.180.21	0-3999 1000-4999	2
⋮	⋮	⋮	⋮	⋮	⋮

FIG. 16

212

VS ID	VS SECTOR	REAL NETWORK ADDRESS	REAL SECTOR	CACHE NETWORK ADDRESS	CACHE LOCAL ADDRESS	FLAG
A	2000 2001	10.25.180.3 10.25.180.3	4000 5000	10.25.180.20 10.25.180.21	0x80000 0x40000	COHERENT DUTY
⋮	⋮	⋮	⋮	⋮		⋮

FIG. 17

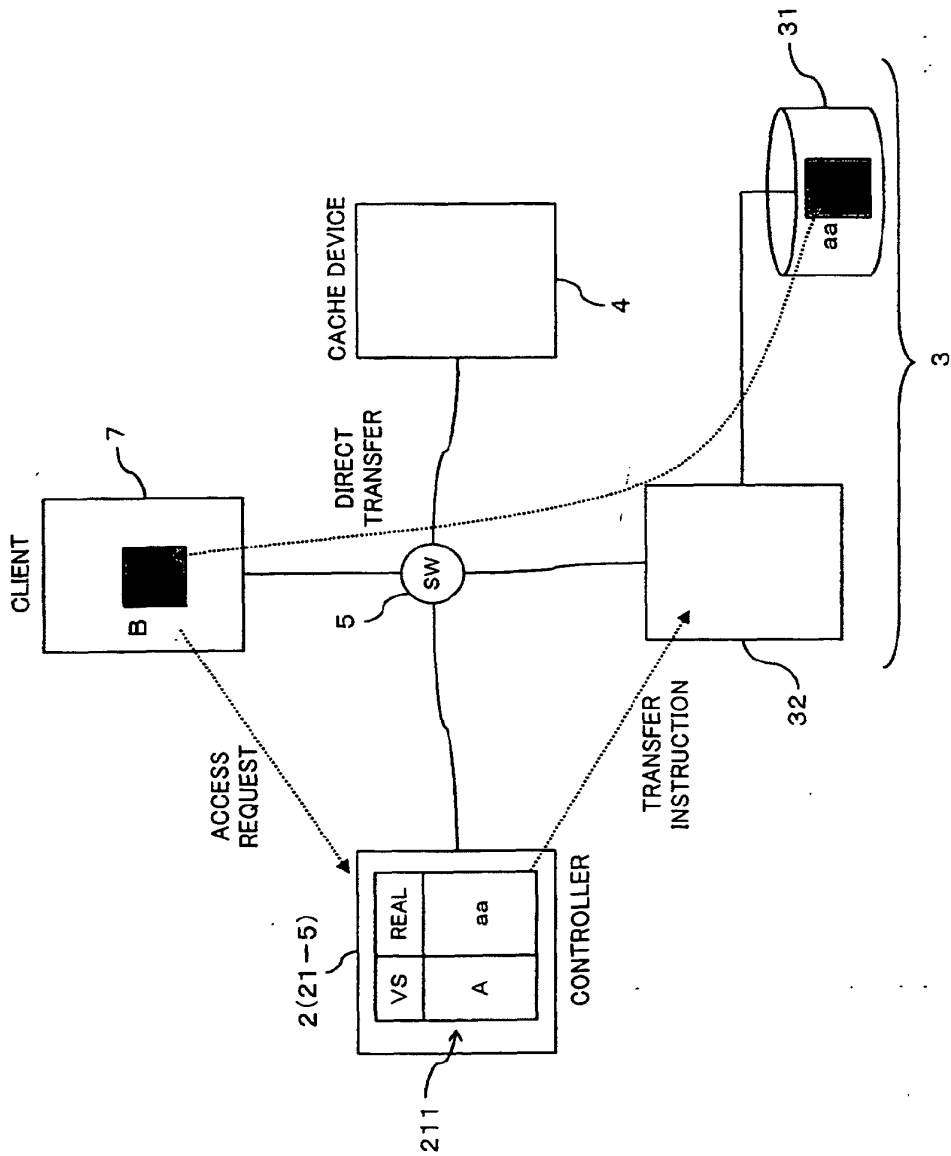


FIG. 18

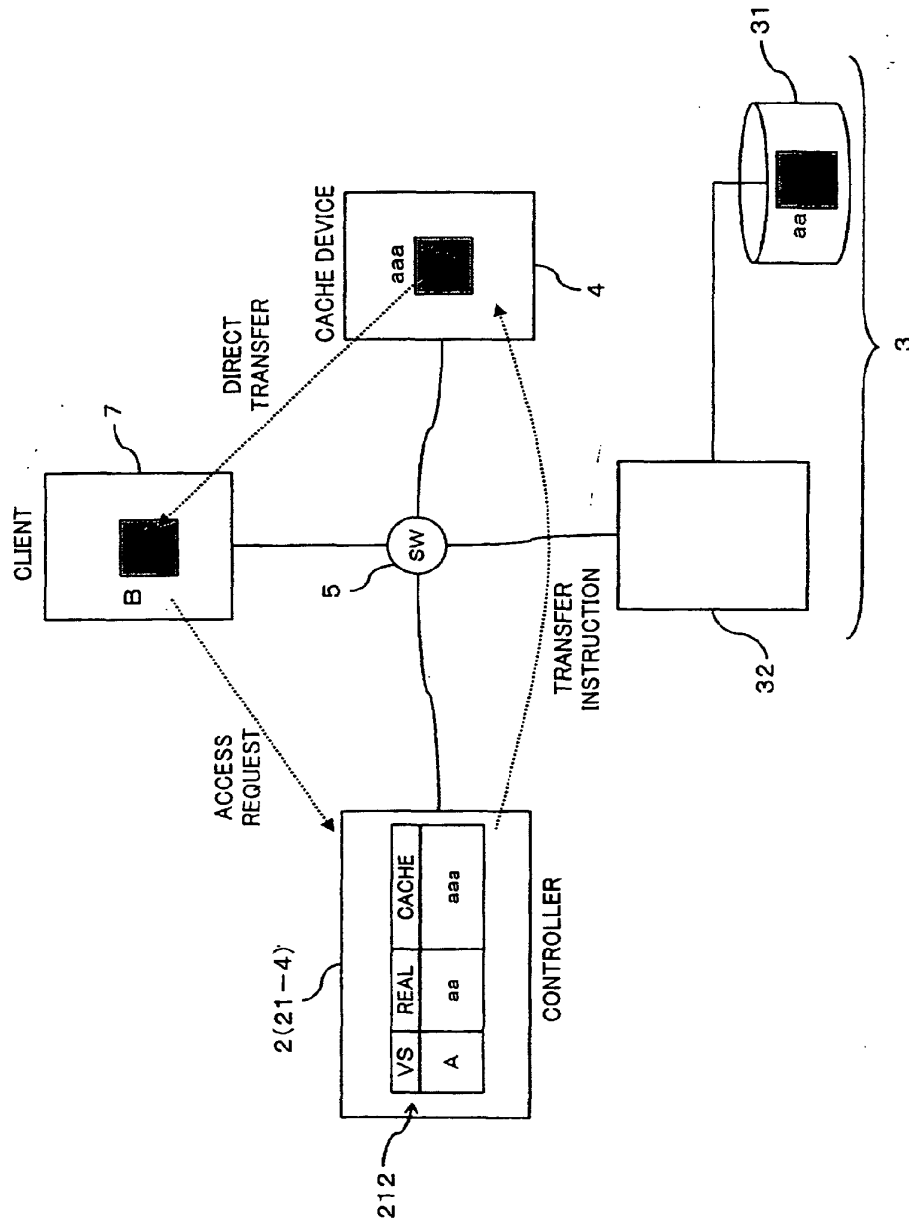
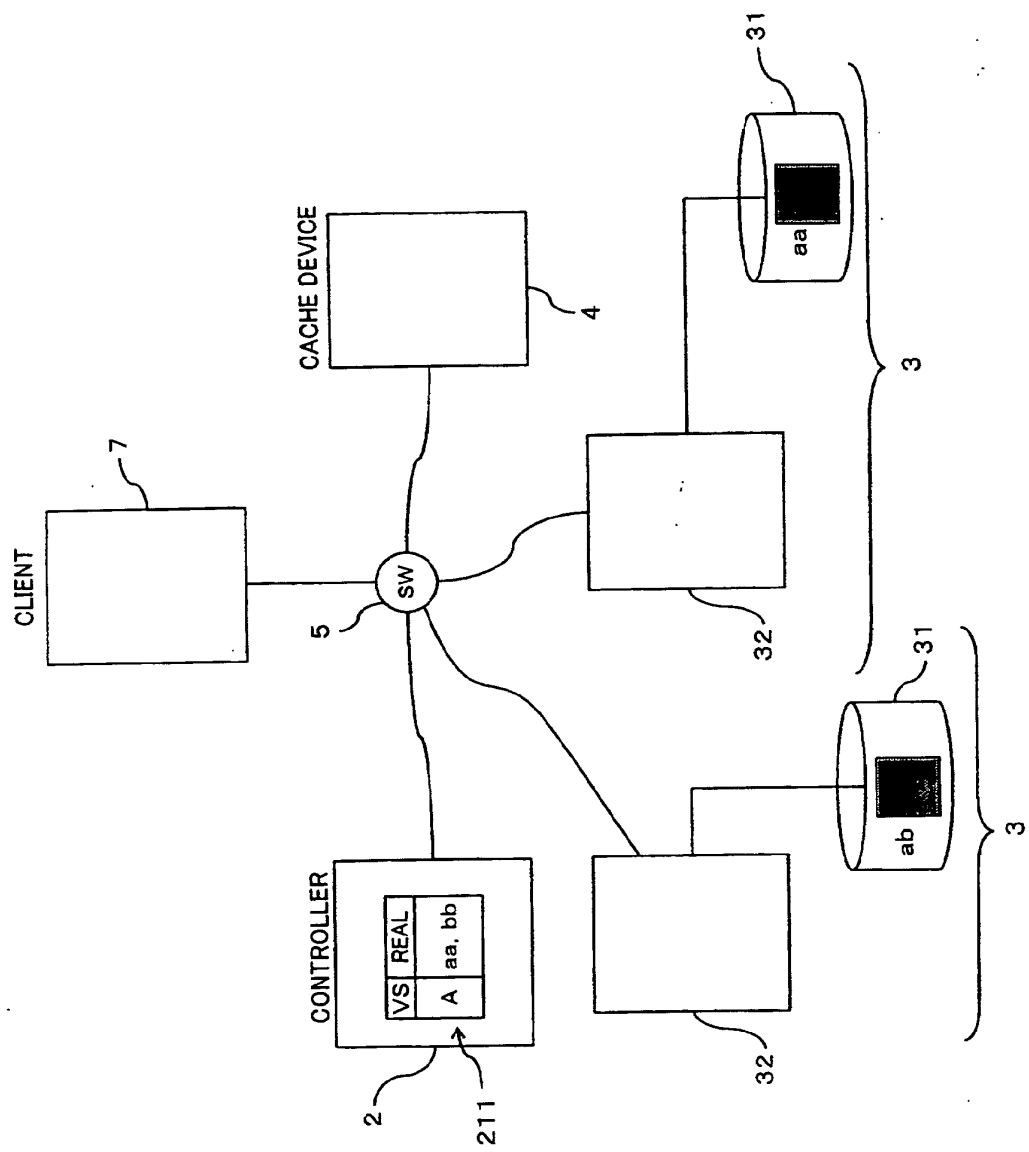


FIG. 19



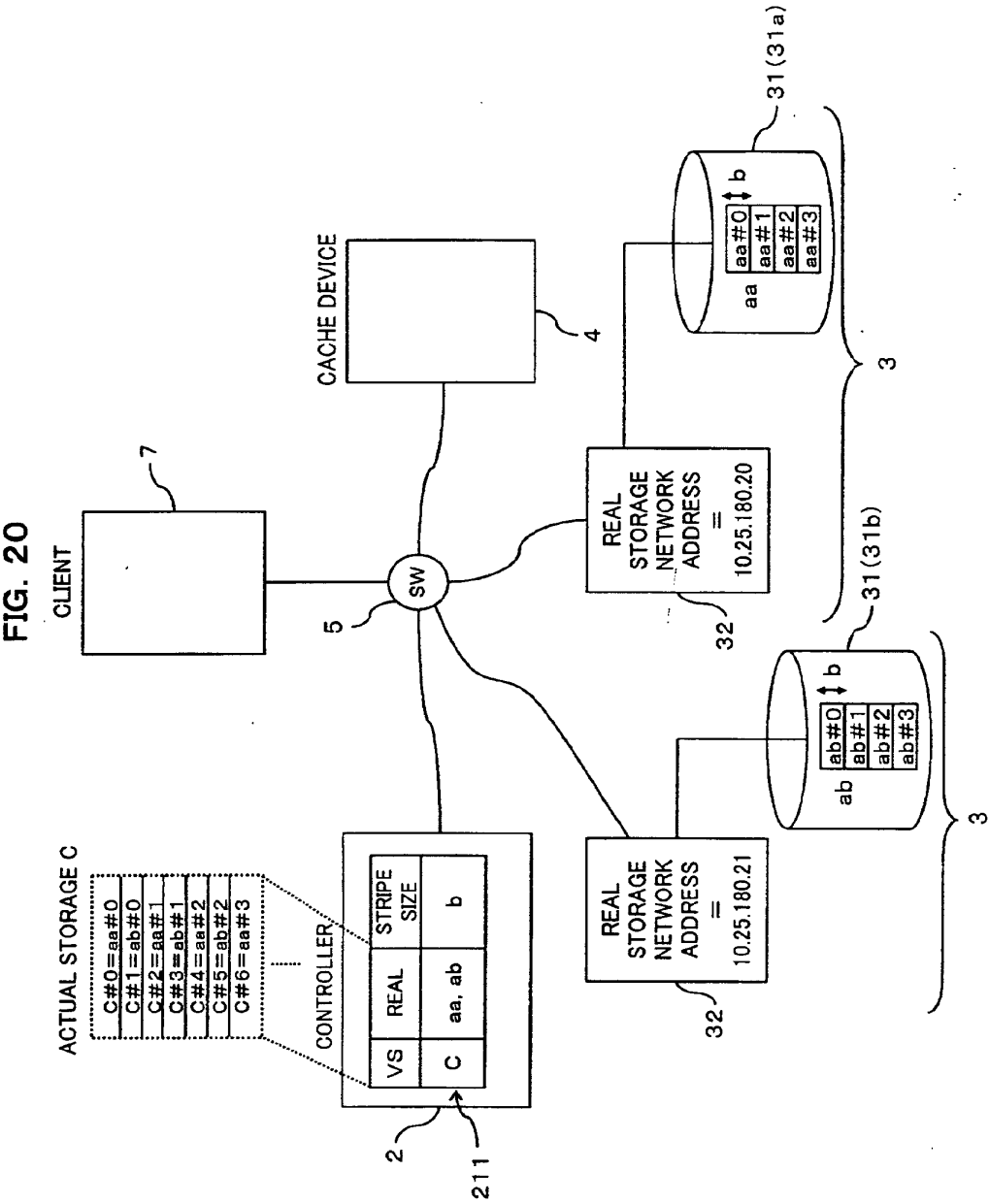


FIG. 21

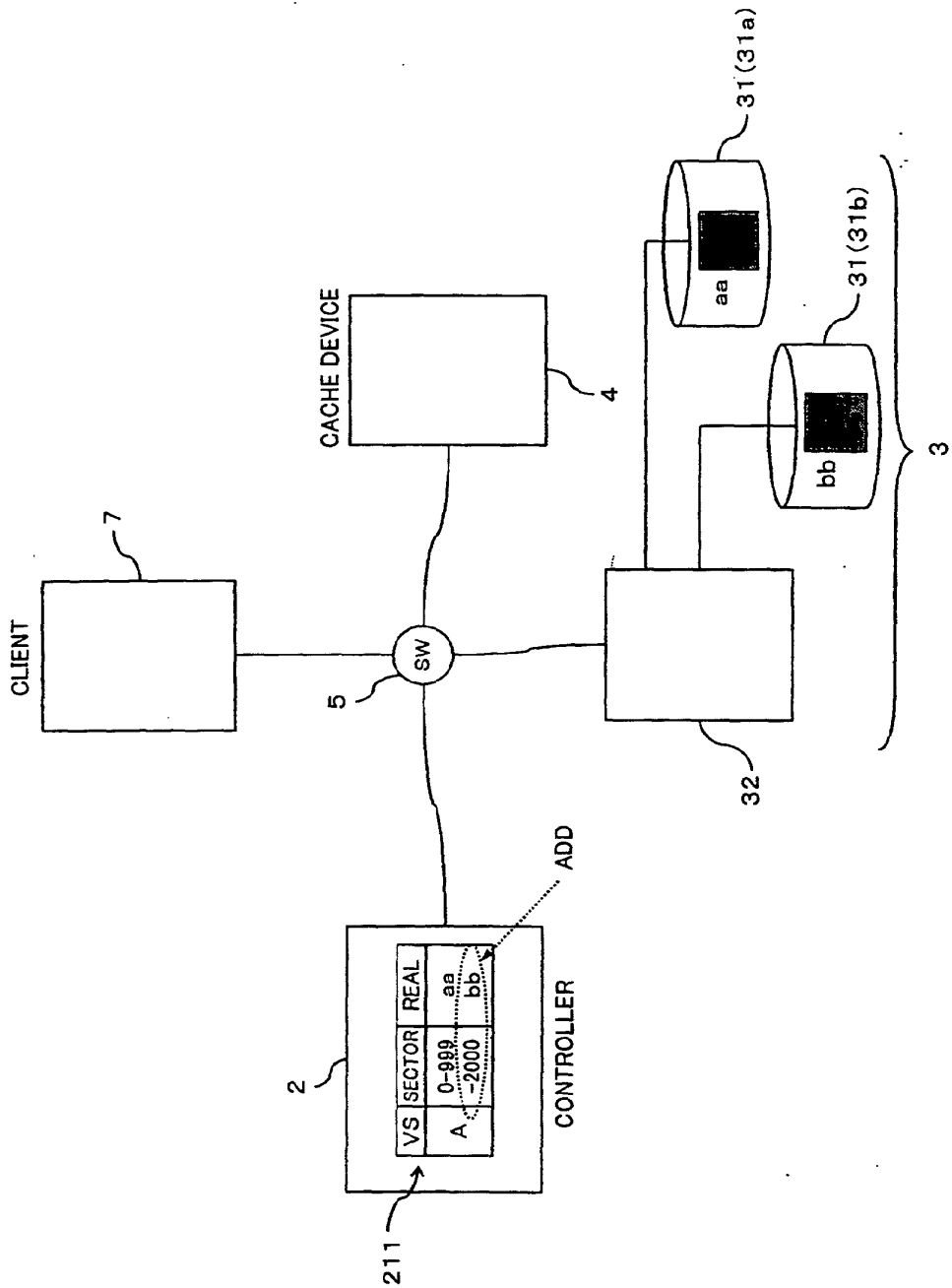


FIG. 22

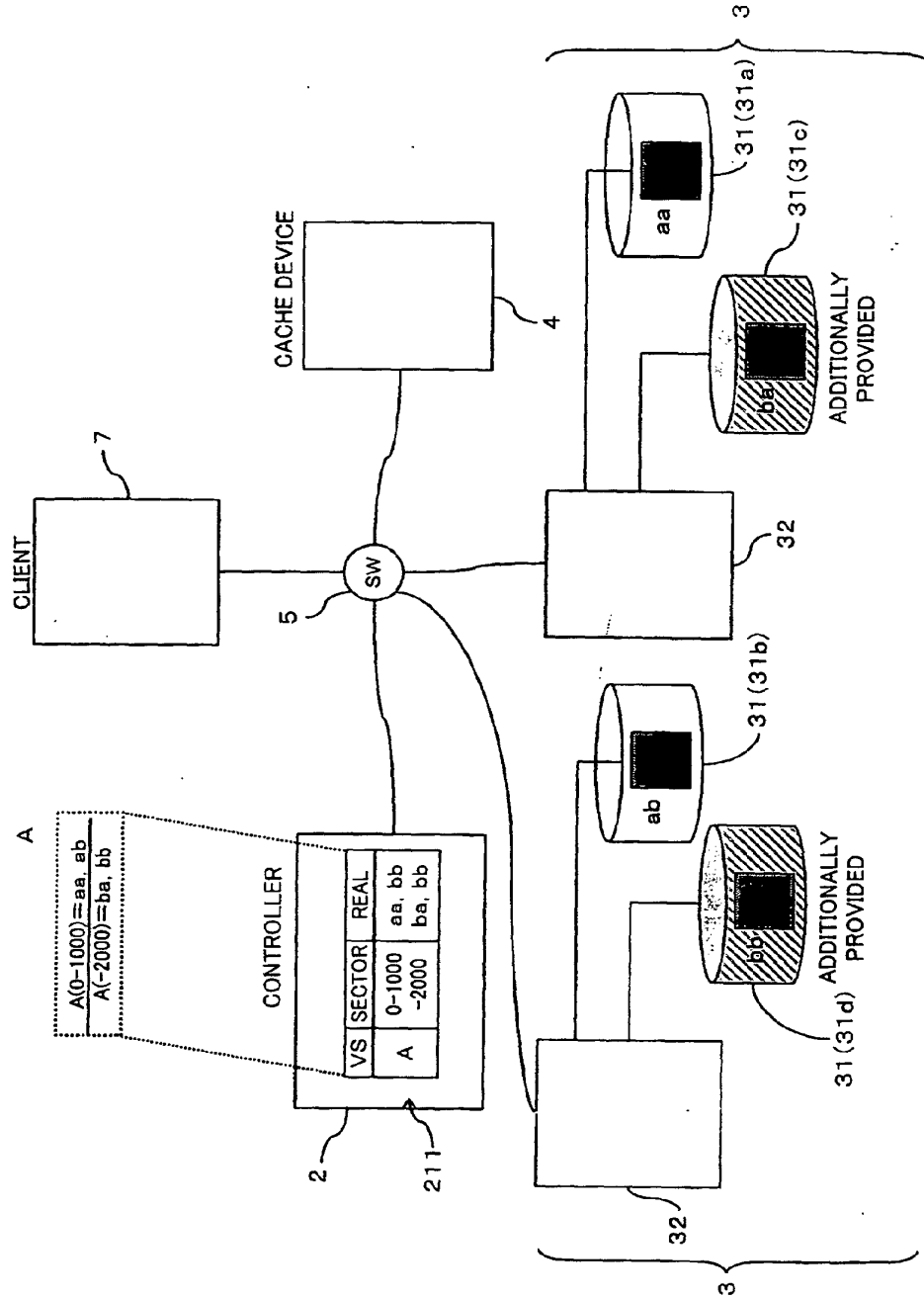


FIG. 23

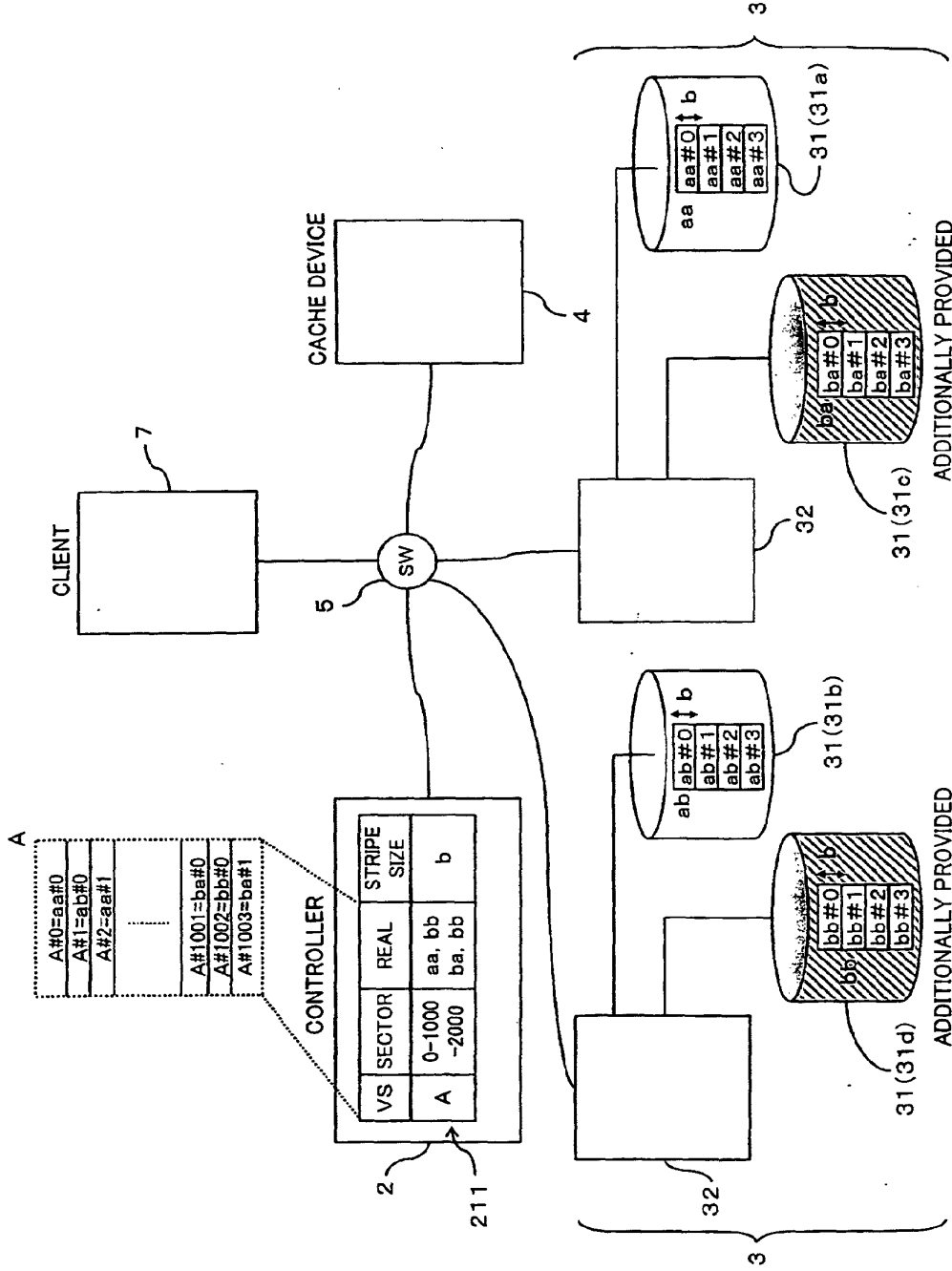


FIG. 24

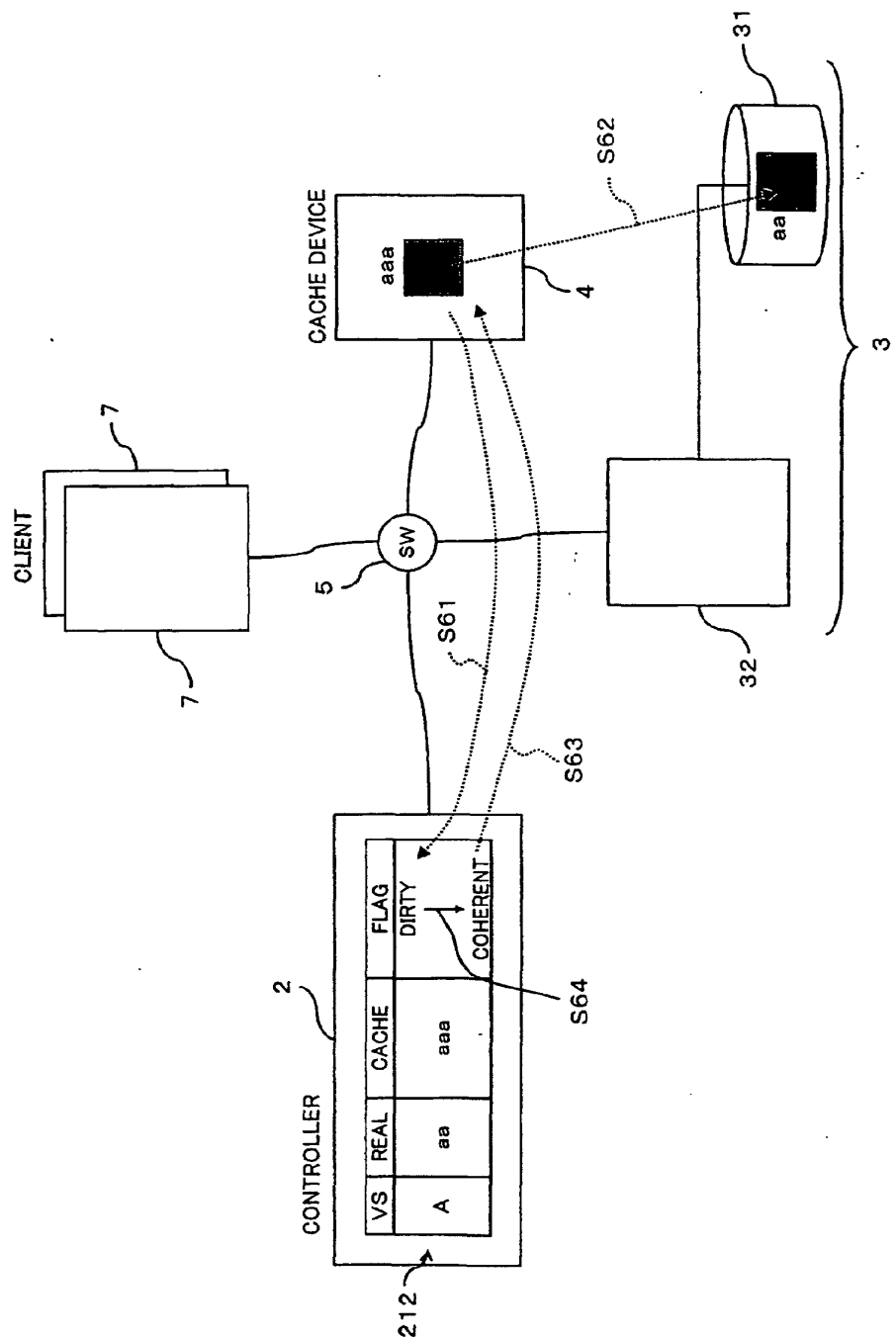


FIG. 25

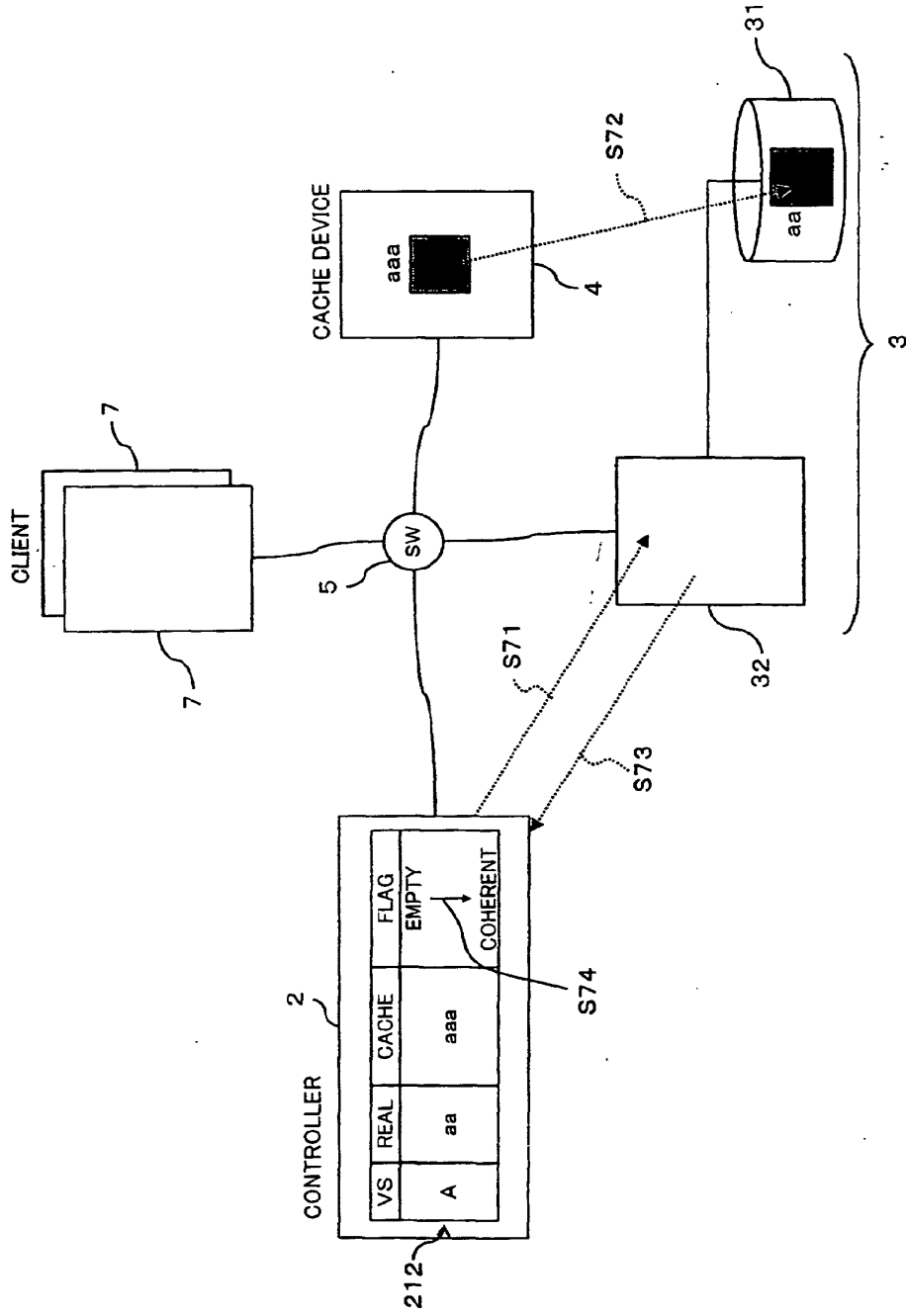


FIG. 26

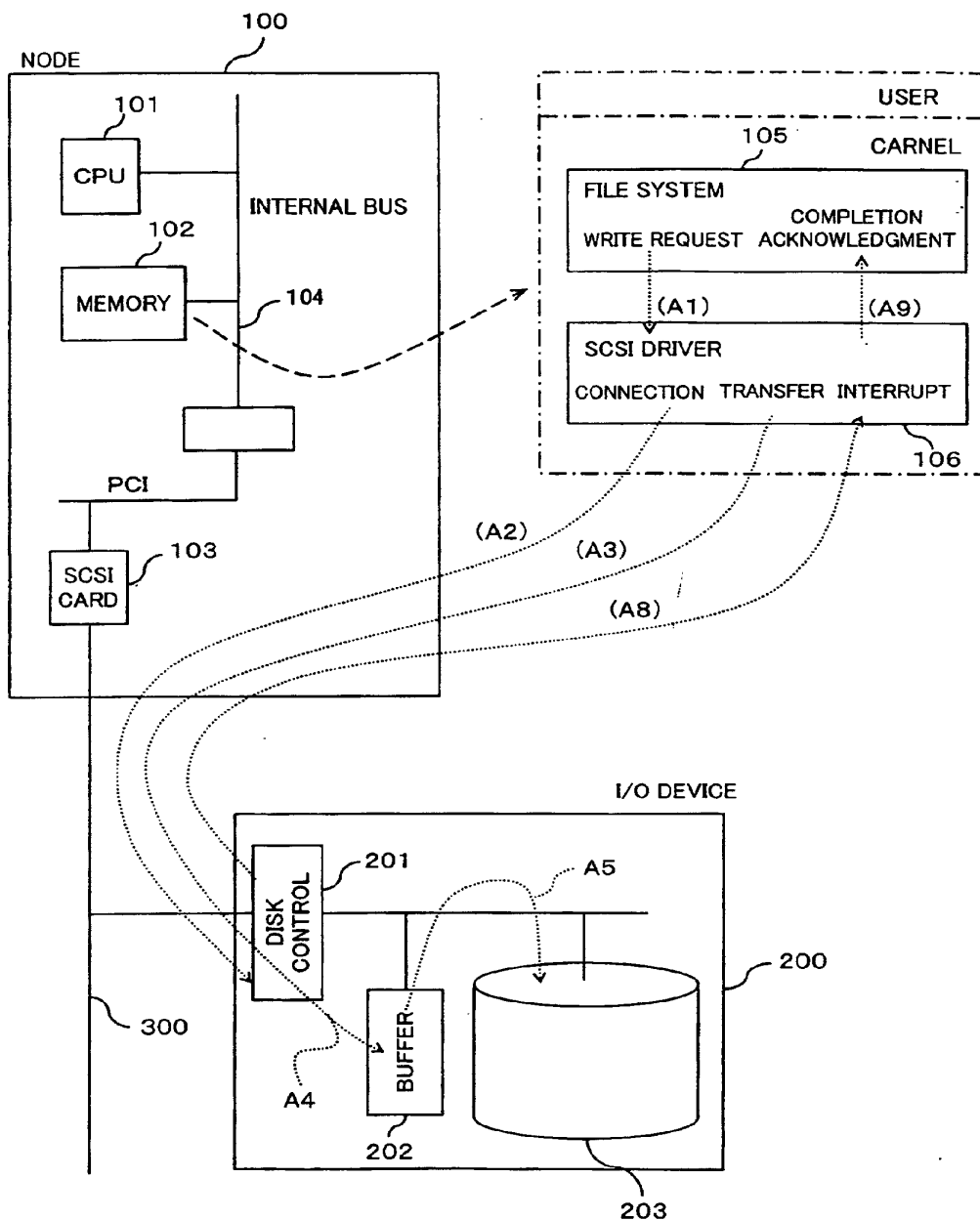
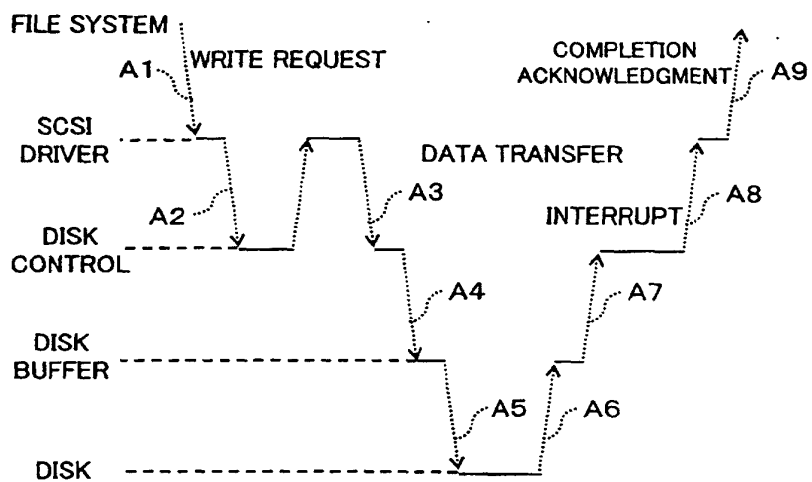


FIG. 27



INTERNATIONAL SEARCH REPORT		International application No. PCT/JP02/08359
A. CLASSIFICATION OF SUBJECT MATTER Int.Cl ⁷ G06F3/06, G06F12/08, G06F13/10, G06F12/00		
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) Int.Cl ⁷ G06F3/06, G06F12/08, G06F13/10, G06F12/00		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2002 Kokai Jitsuyo Shinan Koho 1971-2002 Jitsuyo Shinan Toroku Koho 1996-2002		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 5-308366 A (Ricoh Co., Ltd.), 19 November, 1993 (19.11.93), Full text; all drawings (Family: none)	1-19
A	JP 2002-63060 A (Hitachi, Ltd.), 28 February, 2002 (28.02.02), Full text; all drawings & US 2001/51994 A1	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 document 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 15 November, 2002 (15.11.02)		Date of mailing of the international search report 03 December, 2002 (03.12.02)
Name and mailing address of the ISA/ Japanese Patent Office		Authorized officer
Facsimile No.		Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)



(11) **EP 2 154 834 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
17.02.2010 Bulletin 2010/07

(51) Int Cl.:
H04L 12/46 (2006.01) H04L 29/06 (2006.01)

(21) Application number: **09167142.0**

(22) Date of filing: **04.08.2009**

(84) Designated Contracting States:
**AT BE BG CH CY CZ DE DK EE ES FI FR GB GR
HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL
PT RO SE SI SK SM TR**
Designated Extension States:
AL BA RS

(72) Inventors:
• **Varadhan, Kannan**
San Jose, CA 95129 (US)
• **Gomes, Joao Campelo F.N.**
Bristol, BS1 6XF (GB)

(30) Priority: **14.08.2008 US 88916 P**
14.11.2008 US 271605

(74) Representative: **Harrison Goddard Foote**
Belgrave Hall
Belgrave Street
Leeds
LS2 8DD (GB)

(54) **Routing device having integrated MPLS-Aware firewall**

(57) An MPLS-aware firewall allows firewall security policies to be applied to MPLS traffic. The firewall, which may be integrated within a routing device, can be configured into multiple virtual security systems. The routing device provides a user interface by which a user specifies one or more zones to be recognized by the integrated firewall when applying stateful firewall services to the packets. The user interface allows the user to define different zones and policies for different ones of the virtual security systems. In addition, the user interface supports a syntax that allows the user to define the zones for the firewall by specifying the customer VPNs as interfaces associated with the zones. The routing device generates mapping information for the integrated firewall to map the customer VPNs to specific MPLS labels for the MPLS tunnels carrying the customer's traffic.

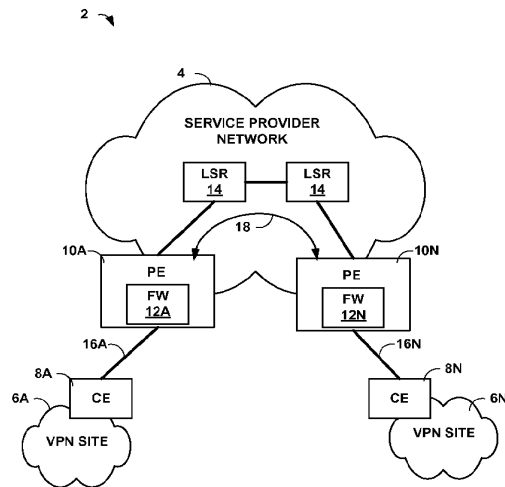


FIG. 1

EP 2 154 834 A1

Description**TECHNICAL FIELD**

5 [0001] The invention relates to computer networks and, more specifically, network devices that route packets within computer networks.

BACKGROUND

10 [0002] A computer network is a collection of interconnected computing devices that exchange data and share resources. In a packet-based network, such as the Internet, the computing devices communicate data by dividing the data into small blocks called packets. The packets are individually routed across the network from a source device to a destination device. The destination device extracts the data from the packets and assembles the data into its original form. Dividing the data into packets enables the source device to resend only those individual packets that may be lost during transmission.

15 [0003] A private network may include a number of devices, such as computers, owned or administered by a single enterprise. These devices may be grouped into a number of site networks, and these sites in turn may be geographically distributed over a wide area. Each site network may include one or more local area networks (LANs) connecting the devices at the particular site.

20 [0004] With the advent of Virtual Private Network (VPN) technology, enterprises can now securely share data between site networks over a public network, such as the Internet. For example, a hub or central VPN site may be the network at the headquarters of the enterprise, while spoke site networks are typically networks at geographically distributed branch offices, sales offices, manufacturing or distribution facilities, or other remote site of the enterprise.

25 [0005] In some instances the remote sites may establish VPN tunnels to hub site or between the remote sites to allow the computing devices within the remote sites to securely communicate with each other or with devices at the hub site through the Internet or another public network infrastructure of a network service provider. A number of communication protocols have been developed for establishing a VPN tunnel. In general, these protocols allow network devices to establish the VPN tunnel as one or more secure data flows across the public network infrastructure. For example, Internet Protocol Security (IPSec) protocols and Secure Sockets Layer (SSL) protocols make use of cryptographic technology to establish network "tunnels." These tunnels allow packets conforming to other network protocols, such as Internet Protocol (IP) packets, to be encapsulated within encrypted packet streams flowing between the sites.

30 [0006] Commonly, each customer site may include a customer edge router that is coupled via a network link to a corresponding provider edge router within the service provider network. The provider edge routers provide VPN services so that the customer's traffic is securely communicated between the VPN sites through the service provider's network and possibly other intermediate networks. One common form of VPN services provided by the network service provider is a multiprotocol label switching (MPLS) VPN. Specifically, an MPLS VPN utilizes creates label switched paths (LSPs) for carrying the customer's VPN traffic through the intermediate networks via defined paths. That is, the routers of the service provider's network support MPLS and establish LSPs between the customer's sites for carrying the customer's VPN traffic.

40 [0007] Due to increasing importance of network security, it has become common for service providers to deploy security devices at the border between each VPN site and the service provider network or other intermediate public networks connecting the VPN sites. One example of a commonly deployed security device is a firewall network device. A firewall, for example, is typically a dedicated device that is configured to permit or deny traffic flows based on the service provider's security policies.

45 [0008] Conventional firewalls, however, have difficulty applying security services to MPLS traffic for various reasons. For example, MPLS traffic flowing through a firewall typically has no state in the data plane. That is, MPLS traffic consists of MPLS labels attached to encapsulated traffic, such as IP traffic. When passing through the firewall, the MPLS labels attached to MPLS packets typically have no meaning to the firewall. As such, the firewall device is unable to provide stateful analysis of the MPLS traffic, such as application of deep packet inspection using assembled application layer data.

50 [0009] For this reason, service providers commonly deploy a separate firewall device between each customer edge router and the corresponding provider edge router that provides ingress and egress for the MPLS tunnels. In this way, the firewall devices are located entirely outside of the MPLS core of the service provider network and are able to apply firewall policies to Internet-Protocol (IP)-based traffic from each customer site external to the MPLS core. However, deployment of these firewall devices increases the number of devices that the service provider must manage and deploy.

55 This increases the configuration and management burden on the service provider, as well as creates power, thermal, cooling, rack space and other issues for the administrator.

SUMMARY

[0010] In general, an MPLS-aware firewall is described that allows firewall security policies to be applied to MPLS traffic. Moreover, the MPLS-aware firewall may be integrated within a routing device, thus allowing a single device to provide both routing functionality, including MPLS support, as well as firewall services. As one example, a service provider may deploy a single device as described herein to provide MPLS VPN services to customers as well as apply firewall policies to the customer's MPLS VPN traffic. In this manner, the techniques described herein may allow the service providers to avoid the requirement to deploy separate routers and non-MPLS aware firewalls when providing MPLS VPN services.

[0011] Further, the techniques described herein may be applied to achieve zone-based firewall services that allow zone-based security policies to be defined and applied for the different network interfaces of the firewall. For example, in addition to allowing zones to be defined based on physical interfaces, the device described herein allows security zones to be defined for VPN tunnels carrying communications for customer VPNs. That is, the device provides a user interface by which VPN tunnels can be defined as logical interfaces for purposes of security policies, and these logical interfaces can be used like other physical interfaces to define zones to which policies are to be applied by the device.

[0012] In one embodiment, the invention is directed to a network router comprising a plurality of interfaces configured to send and receive packets, and a routing engine having a control unit that executes a routing protocol to maintain routing information specifying routes through a network, wherein the control unit executes at least one protocol to establish VPN tunnels for one or more customer VPNs. The network router further includes a forwarding engine configured by the routing engine to select next hops for the packets in accordance with the routing information, the forwarding plane having a switch fabric to forward the packets to the interfaces based on the selected next hops. The network router also includes a firewall integrated within the network router, the firewall configured to apply security functions to the packets. Upon receiving packets from the network, a flow control module of the forwarding engine directs one or more of the packets to the integrated firewall for application of the stateful firewall services. Further, the network router provides a user interface by which a user specifies one or more zones to be recognized by the firewall when applying the stateful firewall services to the packets. The example user interface supports a text-based syntax that allows the user to define the zones by specifying the customer VPNs as interfaces associated with the zones. In other examples, a graphical user interface may readily be used. Moreover, the user interface may be remotely accessed or deployed by a web browser, a management and provisioning system, or other device.

[0013] In another embodiment, a method includes executing, with a routing engine of a router, at least one protocol to establish virtual private (VPN) tunnels for customer VPNs. The method further includes presenting, with the network router, a user interface by which a user specifies one or more zones to be recognized by a firewall integrated within the router, wherein the user interface supports a syntax that allows the user to define the zones by specifying one or more of the VPN tunnels for the customer VPNs as interfaces associated with the zones. The method further includes receiving, from a network, packets at a plurality of interfaces of the router; directing, with a flow control module of a forwarding engine of the router, one or more of the received packets to the firewall for application of stateful firewall services; and applying stateful firewall services to the packets with the firewall of the network router based on the zones specified by the user. Further, the method includes, after applying stateful firewall services, forwarding at least some of the packets from the firewall to the forwarding engine; selecting next hops for the packets within the network with the forwarding engine; and forwarding the packets to the interfaces in accordance with the selected next hops.

[0014] The integrated router and MPLS-aware firewall described herein may have certain advantages over conventional firewalls. For example, device is able to provide firewall services that require deep packet inspection using assembled application layer data even though the VPN traffic may be encapsulated with one or more labels and, thus, typically has no state in the data plane. For example, the integrated router and MPLS-aware firewall can apply intrusion detection and prevention, virus scanning, layer seven application layer security services and other services that require stateful analysis of the MPLS traffic carried over a VPN.

[0015] Moreover, the integrated router and MPLS-aware firewall may have certain advantages when deployed at the edge of a service provider network that provides MPLS-based VPN services. For example, in this situation the MPLS-aware firewall is able to apply firewall services even though it operates on asymmetric traffic, i.e., IP traffic and MPLS traffic, at the interface to and from the MPLS VPN core provided by the service provider network. Further, the device the integrated router and MPLS-aware firewall can easily service multiple customers of the service provider network.

[0016] In addition, the MPLS-aware firewall may support virtual security systems. That is, the firewall may be logically partitioned into multiple virtual security systems to provide multi-tenant security services. The virtual security systems represent logically partitioned firewall instances providing separate security services, including MPLS-aware zone-based firewall services. The router may present the virtual security systems as logically independent firewalls that can be independently configured even though the virtual security systems may share computing resources of the integrated firewall. The router presents a user interface that allows a root system administrator or an administrator authorized for a specific virtual security system to define different zones and policies for different ones of the virtual security systems.

[0017] The details of one or more embodiments of the invention are set forth in the accompanying drawings and the description below. Other features, objects, and advantages of the invention will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF DRAWINGS

[0018] FIG. 1 is a block diagram illustrating an example network environment in which a router includes an integrated MPLS-aware firewall.

[0019] FIG. 2 is a block diagram illustrating in further detail an example router that includes an integrated MPLS-aware firewall.

[0020] FIG. 3 is a chart illustrating an example configuration of a router having an integrated MPLS-aware firewall for providing zone-based firewall services to MPLS and other network traffic.

[0021] FIG. 4 is a block diagram illustrating an example router that integrates a routing component and an MPLS-aware firewall using a shared forwarding plane.

[0022] FIG. 5 is a flowchart illustrating example operation of router of FIG. 4 in accordance with the principles of the invention.

[0023] FIG. 6 is a block diagram illustrating in further detail an example router that integrates a routing component and an MPLS-aware firewall using a shared forwarding plane.

[0024] FIG. 7 is a flowchart further illustrating example operation of an MPLS-aware firewall router.

[0025] FIG. 8 illustrates example mapping information provided by a routing component to an integrated firewall of a network device enabling security services to be applied to MPLS tunnels.

[0026] FIG. 9 is a block diagram illustrating an example router having support for virtual security systems and integrating a routing component and an MPLS-aware firewall using a shared forwarding plane.

[0027] FIG. 10 is a flowchart further illustrating example operation of an MPLS-aware firewall router having support for virtual security systems.

[0028] FIG. 11 illustrates example mapping information provided by a routing component to an integrated firewall of a network device enabling security services to be applied to MPLS tunnels for different virtual security systems.

[0029] FIG. 12 is a block diagram showing an inter-provider deployment of the MPLS, aware, zone-based firewall described herein.

DETAILED DESCRIPTION

[0030] FIG. 1 is a block diagram illustrating an example network environment 2 in which a service provider network 4 provides connectivity between customer virtual private network (VPN) sites 6A-6N (collectively, VPN sites 6). In the example of FIG. 1, VPN sites 6 includes customer edge (CE) routers 8A-8N connected to provider edge (PE) routers 10A-10N of service provider network 4 via network links 16A-16N.

[0031] In one example, service provider network 4 supports provider-provisioned VPNs (PPVPNs). PE routers 10A-10N (collectively, PE routers 10) transport communications of customer VPN sites 6 through service provider network 4 and possibly other intermediate networks. Service provider network generally includes a set of PE routers 10 at the edge of the network interconnected with internal routers and other network devices via high-speed network links. As shown in FIG. 1, the internal routers may be label switched routers (LSRs) 14 that provide a Multi-protocol Label Switching (MPLS) MPLS core network. PE routers 10 and LSRs 14 execute one or more routing protocols, such as Intermediate System to Intermediate System (ISIS) for distributing routing information. In addition, PE routers 10 may execute the Multi-Protocol Border Gateway Protocol (mpBGP) for exchanging VPN routes associated with VPN sites 6 as well as VPN labels to be applied to the VPN communications. For example, administrators associated with service provider network 4 may configure PE routers 10 so as to provision VPN services for one or more customer VPNs. At this time the administrators define a VPN identifier for each customer VPN (e.g., VPN_CUSTOMER_A), and PE routers 10 allocate VPN labels, VPN addresses, a router target, a router distinguisher, and all other state information necessary for the VPN. In the example of FIG. 1, PE routers 10 exchange this information via mpBGP so as to form one or more end-to-end VPN tunnels 18.

[0032] In addition, PE routers 10 may communicate with LSRs 14 to establish one or more MPLS tunnels in the form of one or more end-to-end label switch paths (LSPs) for transporting the VPN communications through service provider network 4 and possibly other intermediate networks. Traffic flowing along network links 16 to and from VPN sites 6 may take the form of Internet Protocol (IP) packets, and may be secured using Internet Protocol Security (IPSec) protocols, Secure Sockets Layer (SSL) protocols or other protocols that make use of cryptographic technology. PE routers 10 provide ingress and egress for the IP traffic with respect to the Multi-protocol Label Switching (MPLS) services provided within service provider network 4. That is, PE routers 10 operate as ingress and egress LSRs for communicating the IP packets of VPN sites 6 as encapsulated VPN packets traversing VPN tunnels 18 and optionally one or more LSPs. For

example, PE router 10A may receive IP traffic from VPN site 6A, and may then prepend a VPN label based on the corresponding customer VPN associated with the traffic. The VPN traffic may then be viewed as flowing along a VPN tunnel through service provider network 4, and the VPN tunnel 18 may be viewed as a form of an MPLS tunnel. One or more of these VPN tunnels 18 (i.e., packet flows having VPN labels prepended to each packet) may then further be encapsulated within a label stack of additional MPLS labels so as to flow along one or more LSPs. For example, PE router 10A may further prepend one or more MPLS labels to form an outer label stack on top of the VPN label of each VPN packet, and forward the VPN packets along one or more dedicated LSPs through service provider network 4. PE routers 10 and LSRs 14 may use any type of label switching protocol to establish the LSPs, such as MPLS protocols like Resource Reservation Protocol (RSVP) and the Label Distribution Protocol (LDP).

[0033] As shown in FIG. 1, each of PE routers 10 includes an integrated firewall (FW) 12A-12N (collectively, FWs 12). As described in further detail below, each of FWs 12 is an MPLS-aware firewall that allows service provider network 4 to apply firewall security policies at the IP-MPLS interface. That is, FWs 12 allow firewall security policies to be applied at the point where IP traffic enters or exits VPN tunnels 18. Moreover, as illustrated in FIG. 1, the MPLS-aware FWs 12 may be integrated within routing device (e.g., PE routers 12), thus allowing a single device to provide both routing functionality, including MPLS support, as well as firewall services. In this manner, the techniques described herein may allow the service provider to avoid the requirement to deploy separate non-MPLS aware firewalls between PE routers 10 and CE routers 8.

[0034] Further, FWs 12 of PE routers 10 may provide zone-based firewall services that allow zone-based security policies to be defined and applied for the different network interfaces of the PE router. For example, in addition to allowing zones to be defined based on physical interfaces, the PE routers 10 provide a user interface that allows the service provider to define security zones with respect to customer VPNs that are supported by service provider network 4. That is, each of PE routers 10 may provide a user interface having a command syntax that allows individual customer VPNs to be defined and recognized by FWs 12 as logical interfaces, and these logical interfaces can be used like other physical interfaces of the PE routers to define zones and corresponding security policies to be applied to those zones.

[0035] FIG. 2 is a block diagram illustrating an example of an MPLS-enabled router, such as PE routers 10 of FIG. 1, that includes an integrated MPLS-aware firewall (FW) 22. In this example, FW 22 provides zone-based firewall services that allow zone-based security policies to be defined and applied for the different network interfaces of the router. In the example of FIG. 2, router 20 includes physical interfaces 27 for sending and receiving IP traffic 28 to and from VPN sites 24 via physical network links. Router 20 provides a user interface that allows the service provider to define zones and corresponding security policies with respect to those physical interfaces. In addition, the user interface of router 20 allows the service provider to define security zones with respect to individual customer VPNs 30 that are used to securely tunnel communications through the service provider network. For example, as shown in FIG. 2, the system administrator may interact with the user interface to specify logical interfaces 29 or other identifiers for one or more of the established customer VPNs. In addition, the user interface supports a command syntax that allows the logical interfaces for the individual customer VPNs 30 to be used in conjunction with the physical interfaces 27 of router 20 to define zones and corresponding security policies to be applied by FW 22 to those zones. As explained herein, router 20 maintains mapping information to allow router 20 to apply zone-based security services to customer traffic associated with VPN labels and optionally additional MPLS labels, thereby providing a router having integrated MPLS-aware firewall.

[0036] FIG. 3 is a chart illustrating an example configuration of FW 22 of router 20 for providing zone-based firewall services. In the chart of FIG. 3, the vertical axis represents all of the input interfaces of router 20, including N physical input interfaces (any of interfaces 27 of FIG. 2 for input links) as well as Y input VPNs (any of logical interfaces 29 for VPNs of which router 20 is the egress). The horizontal axis represents all of the output interfaces of router 20, including X physical output interfaces (any of interfaces 27 of FIG. 2 for output links) as well as Z output VPNs (any of logical interfaces 29 for VPNs of which router 20 is the ingress). In this example, a system administrator for the service provider network has interacted with the user interface of router 20 to define three distinct zones: (1) a first zone 30 for all MPLS traffic received via VPN 1, (2) a second zone 34 for all IP traffic output on physical interface OUTPUT INT X, and (3) a third zone 34 for all IP traffic received on physical interface INPUT INT 1.

[0037] Router 20 may, for example, provide a text-based command line interface by which the system administrator or software agent provides configuration data in conformance with a command syntax as follows:

```
zone ZONE_NAME {
  interface INTERFACE_NAME;
  ...
  interface INTERFACE_NAME;
  vpn VPN_NAME;
  ...
  vpn VPN_NAME;
}
```

EP 2 154 834 A1

In the above example, the keyword "zone" indicates that the administrator is defining a new security zone, and the bracket delimiters enclose a collection of interfaces that define that zone. For example, any physical interfaces that fall within that zone can be specified using the keyword "interface." In addition, logical interfaces for VPNs carrying VPN communications through the service provider network can be easily specified by the "vpn" keyword followed by a string identifier for a customer VPN, listed as "VPN_NAME" in the syntax above. In this way, the administrator is able to easily identify customer VPNs that utilize VPN services of the service provider, and router 20 resolves the strings provided within the configuration data to VPNs provisioned through the service provider network. This allows the administrator to view the VPN tunnels as a logical interface for purposes of defining zones to which to apply firewall policies, even though many of those VPN tunnels may traverse the same physical interface. In this way, the administrator may define a plurality of zones (e.g., zones 30, 32 and 34 of FIG. 3), and for each zone may specify a collection of physical interfaces, VPNs or combinations thereof, that are to be considered by FW 22 as within that zone. The above syntax is merely illustrative. For example, in other embodiments the keywords "interface" or "vpn" may be omitted, or other keywords may be used. [0038] In addition, the user interface of router 20 provides a syntax for defining security policies to be applied with respect to the defined zones. For example, router 20 may support a syntax as follows:

```
15      policy from-zone ZONE_NAME to-zone ZONE_NAME {
          match {
              source-address <s>;
              destination-address <d>;
20          source-port <sp>;
              destination-port <dp>;
              application protocol <any>;
          }
          then {
25              actions;
          }
      }
```

In the example syntax above, the keyword "policy" indicates that the administrator is defining zone-based security policy to be applied by FW 22. The keyword "from-zone" indicates that the subsequent text specifies a defined zone from which traffic must be received for the policy to apply. The keyword "to-zone" indicates that the subsequent text specifies a defined zone to which the traffic must be destined for the policy to apply. As shown above, the policy includes a keyword "match" that allows the administrator to specify packet flow criteria, such as source network address, destination network address, source port, destination port, application protocol or other criteria. In addition, the policy specifies one or more actions to be applied to network traffic that is received via the "from-zone" for output on the "to-zone" and that matches any packet flow criteria specified in the policy. FW 22 then applies the actions enumerated in the policy to network traffic satisfying those conditions. Example actions including packet filtering, packet logging, intrusion detection and prevention, virus scanning, network address translation (NAT), policy-based authentication, and the like.

[0039] In accordance with the example syntax, an administrator may provide configuration data as follows:

```
40      zone untrust {
          vpn VPN-A; /* VPN carrying traffic from VPN site VPN-A*/
          vpn VPN-B; /* VPN carrying traffic from VPN site VPN-B*/
      }
      zone trust {
45          interface ge-0/0/0.1; /*Physical interface for link to client site A*/
          interface so-2/4/2.0; /*Physical interface for link to client site B*/
      }
      policy from-zone untrust to-zone trust {
          then {
50              apply virus_scanning;
          }
      }
```

In this example, the administrator has defined two firewall zones, "untrust" and "trust." For the zone "untrust," the administrator has indicated that the zone includes VPN traffic carried by two VPN tunnels, VPN-A and VPN-B. For the zone "trust," the administrator has indicated that the zone includes a collection of two interfaces for forwarding traffic to client sites A and B. Further, the administrator has defined a policy for application to traffic received from an interface within the zone untrust and directed to an interface within the zone trust (e.g., VPN traffic from the MPLS core via VPN-A or VPN-B and directed to the client sites A or B as IP traffic). For such traffic, the policy requires FW 22 to apply stateful

virus scanning algorithms to application layer data assembled from the packets.

[0040] FIG. 4 is a block diagram illustrating an example router that integrates a routing component and an MPLS-aware firewall. Router 40 may, for example, be a high-end router capable of deployment within a service provider network. Moreover, forwarding plane 42 may be provided by dedicated forwarding integrated circuits normally associated with high-end routing and forwarding components of a network router. U.S. Patent Application 2008/0044181, entitled MULTI-CHASSIS ROUTER WITH MULTIPLEXED OPTICAL INTERCONNECTS, describes a multi-chassis router in which a multi-stage switch fabric, such as a 3-stage Clos switch fabric, is used as a high-end forwarding plane to relay packets between multiple routing nodes of the multi-chassis router. The entire contents of U.S. Patent Application 2008/0044181 are incorporated herein by reference.

[0041] As shown in the example embodiment of FIG.4, router 10 integrates an MPLS-aware firewall 44 and a routing plane 46 that utilize a shared forwarding plane 42. Forwarding plane 42 is a rich and dynamic shared forwarding plane, optionally distributed over a multi-chassis router. Moreover, forwarding plane 42 may be provided by dedicated forwarding integrated circuits normally associated with high-end routing components of a network router. Consequently, routing plane 46 and forwarding plane 42 operate as a high-end router, and firewall 44 has been tightly integrated within router 40 (e.g., by way of service cards 64) so as to use forwarding plane 42 of the routing components in a shared, cooperative manner. Further details of one example embodiment of router 40 can be found in U.S. Provisional Patent Application 61/054,692, filed May 20, 2008, entitled "STREAMLINED PACKET FORWARDING USING DYNAMIC FILTERS FOR ROUTING AND SECURITY IN A SHARED FORWARDING PLANE," which is incorporated herein by reference.

[0042] Routing plane 46 provides a routing engine 68 that is primarily responsible for maintaining a routing information base (RIB) 72 to reflect the current topology of a network and other network entities to which router 40 is connected. For example, routing engine 68 provides an operating environment for execution of routing protocols 70 that communicate with peer routers and periodically update RIB 72 to accurately reflect the topology of the network and the other network entities. Example protocols include routing and label switching protocols, such as mpBGP, ISIS, RSVP-TE and LDP, to establish VPNs, LSPs and for exchanging labels.

[0043] In accordance with RIB 72, forwarding component 80 maintains forwarding information base (FIB) 74 that associates network destinations or MPLS labels with specific next hops and corresponding interface ports of output interface cards of router 40. Routing engine 68 typically processes RIB 72 to perform route selection and generate FIB 74 based on selected routes and allocated MPLS labels. In this way, routes as well as labeling information can be programmed into forwarding plane 42. Routing engine 68 may generate FIB 74 in the form of a radix tree having leaf nodes that represent destinations within the network. U.S. Patent 7,184,437 provides details on an exemplary embodiment of a router that utilizes a radix tree for route resolution, the contents of which is incorporated herein by reference in its entirety.

[0044] When forwarding a packet, forwarding component 80 traverses the radix tree to a leaf node based on information within a header of the packet to ultimately select a next hop and output interface to which to forward the packet. Based on the selection, forwarding component may output the packet directly to the output interface or, in the case of a multi-stage switch fabric of a high-end router, may forward the packet to subsequent stages for switching to the proper output interface.

[0045] Network services process (NSP) 73 of routing engine 46 communicates with and programs service cards 64 of firewall 44. For example, routing engine may present a user interface (UI) 77 as described above so as to receive configuration data from administrator 79 defining firewall zones and policies with respect to physical interfaces, sub-interfaces or MPLS tunnels. In response, NSP 73 programs services cards 64 with corresponding configuration data, causing the service cards of firewall 44 to recognize the defined zones and apply the security policies when processing packets from forwarding plane 42. Each service card 64 may, for example, execute a microkernel that operates as a consumer of state information and listens for communications from NSP 73.

[0046] In this way, routing plane 46 and firewall 44 interact so that firewall 44 is made aware of state information associated with the MPLS traffic flowing through the routing device. For example, NSP 73 of routing engine 68 programs the service cards with information that associates customer VPNs with specific VPN labels and optionally one or more additional MPLS labels that have been used for tunneling the corresponding VPN traffic through the service provider network. NSP 73 may query protocols 70 and RIB 72 to provide the service cards 64 of firewall 44 with information maintained with the RIB for the VPN. For example, for VPN traffic that may be received by router 40 from a customer VPN, NSP 73 may provide information that identifies a VPN tag and optionally one or more MPS tags may will be affixed to the header of the packet and mapping information to associate this these labels with a customer VPN identifier (e.g., a text string or other identifier) that may be utilized by the administrator when defining input zones and policies. For VPN traffic that may be output by router 40 to the MPLS core, NSP 73 may provide mapping information that identifies a VPN label and optionally one or more MPLS labels to be applied by forwarding component 80 to IP traffic destined for the customer VPN, a corresponding next hop identifier for the traffic and a mapping to associate this <VPN label, next hop identifier> pair with a customer VPN identifier (e.g., a text string or other identifier) that may be utilized by the administrator when defining firewall zones and policies. Alternatively, the mapping information may provide other information useful

in uniquely identifying the customer VPN, such as a route designator, a route target or other information.

[0047] Forwarding plane 42 may include a flow control unit 75 to selectively direct packets to firewall 44 for processing. For example, flow control unit 75 receives incoming packet flows 78 (e.g., IP traffic or VPN-encapsulated traffic) and determines whether to send the packets through the firewall 44 for processing within one or more of service cards 64, or whether to bypass the firewall 44. Service cards 24 receive packets from flow control unit 75, selectively provide firewall services to the packets in accordance with the defined zones and policies, and relay the packet or any response packets to forwarding plane 42 for forwarding by forwarding component 80 in accordance with FIB 74.

[0048] Service cards 24 within firewall 44 may be installed along a backplane or other interconnect of router 40 to perform a variety of firewall services on the packets received from forwarding plane 42, such as filtering, logging, Intrusion Detection and Prevention (IDP) analysis, virus scanning, deep packet inspection. In some cases, service card 24 may issue commands 36 to dynamically configure a flow table (not shown) within flow control unit 75 of forwarding plane 42. For example, when flow control unit 75 receives a packet and determines that the packet belongs to a new packet flow that does not match any of its filters, flow control unit 75 may send the packet to service cards 64 for processing. Upon receiving and processing the packet or packets of a packet flow, service cards 64 may issue a command 69 to install a dynamic filter within the flow table, such as an exact match filter that indicates particular actions to be performed when a packet is received that matches the filter. In the case that service cards 64 determine no further firewall services need be applied to a packet flow (e.g., after determining that the packet flow is trusted or benign), service cards 64 may install a filter within flow control unit 75 to specify that subsequent packets of this packet flow session may be processed on a straight path that bypasses firewall 44. When flow control unit 75 receives a subsequent packet of the same packet flow, flow control unit 75 checks the flow table, determines that the packet matches the new dynamic filter, and directs the packet on the appropriate path according to the dynamic filter.

[0049] In this example, routing and firewall services are integrated within a single router 40 that uses a shared forwarding plane 42 suitable for high-speed forwarding functions required by MPLS routers, such as PE routers 10 of FIG. 1.

[0050] FIG. 5 is a flowchart illustrating example operation of router 40 of FIG. 4 in accordance with the principles of the invention. Initially, routing engine 68 executes protocols 70, such as mpBGP to exchange VPN information, including VPN identifiers, VPN routes and VPN labels (81). In addition, routing engine may optionally utilize RSVP-TE, LSP or other mPLS protocols to establish one or more MPLS tunnels (i.e., LSPs) for carrying the VPN traffic through the service provider network for various customer VPN sites (81). At this time, routing engine 68 updates RIB 72 and programs forwarding component 80 in accordance with the VPN routes, VPN labels as well as any additional MPLS labels allocated to carry the VPN traffic. In addition, NSP 73 of routing engine 46 programs service cards 64 of firewall 44 with a mapping that associates the customer VPN information with the specific VPN labels, and optionally any additional MPLS labels, used in communicating VPN traffic to and from the next hop(s) within the service provider network (82, 85). Further, NSP programs service cards 64 with configuration data received from the administrator defining firewall zones and policies with respect to either physical interfaces or the individual customer VPNs, causing the service cards of firewall 44 to recognize the defined zones and applying the security policies when processing packets from forwarding plane 42 (83, 85).

[0051] After configuration and establishment of the VPN tunnels, router 40 receives a packet, which may be IP traffic from a VPN site or VPN traffic from a VPN tunnel (optionally carried by an LSP) through the service provider network (84). In one optional example, a flow control unit 75 of the forwarding plane 42 analyzes the received packet to identify a packet flow associated with the packet (86), e.g., using a flow-based provisioning logic to identify a five-tuple based on information carried in the header or body of the packet. Upon identifying the packet flow, flow control unit 75 references an internal flow table to determine whether belongs to a new packet flow or a packet flow already recognized by the router (88).

[0052] If flow control unit 75 does not find a match in the flow table (NO branch of 88), which indicates that the packet belongs to a new packet flow, the flow control unit directs the packet to service cards 64 of firewall 44 for firewall services (90). When the packet is directed to firewall 44, one of service cards 64 applies stateful firewall services to the packet (92). For example, the service cards 64 may extract and assemble application layer data from the packet, and a deep packet inspection (DPI) engine may perform Intrusion Detection and Prevention (IDP) analysis and/or virus scanning to filter out bad packets. As a further example, the service card 24 may perform ciphering, NAT or authentication services.

[0053] After applying firewall services, service cards 64 then inject the packet into forwarding plane 42 for forwarding by forwarding component 80 in accordance with FIB 74 (96). At this time, service cards 64 of firewall 44 may signal flow control unit 75 and direct the flow control unit to install criteria in its internal flow table designating whether subsequent packets of the packet flow should be trusted such that firewall services need not be applied, or whether the subsequent packets should continue to be directed to firewall 44.

[0054] If, however, flow control unit 75 finds a match in the flow table (YES branch of 88) for the received packet and the matching entry directs the packet onto a straight path for processing (YES branch of 94), flow control module 20 does not forward the packet to firewall 44 but signals forwarding component 80 that the packet can immediately be forwarded in accordance with FIB (74).

[0055] If the matching entry of the flow table indicates that firewall services are to be applied to the recognized packet flow (NO branch of 94), then flow control unit 75 directs the packet to service cards 64 of firewall 44 for firewall services (90, 92) and subsequent forwarding by forwarding component 88 (98).

[0056] FIG. 6 is a block diagram illustrating in further detail an example router 100 that integrates a routing engine 104 and an MPLS-aware firewall 123 using a shared forwarding plane provided by forwarding engine 106. Features of router 100 may, for example, be incorporated within any of PE routers 10, router 20, or router 30 described above.

[0057] Router 100 comprises a control unit 102 that includes a routing engine 104 and a forwarding engine 106. Routing engine 104 is primarily responsible for maintaining routing information base (RIB) 88 to reflect the current topology of a network and other network entities to which it is connected. In particular, routing engine 104 periodically updates RIB 108 to accurately reflect the topology of the network and other entities. Routing engine 104 also includes routing protocols 89 that perform routing operations, including protocols for establishing VPNs and optionally LSPs through a network.

[0058] UI module 105 represents software executing on routing engine 104 that presents a command line interface (e.g., via a shell or Telnet session) for receiving configuration data as described herein, including firewall configuration data defining zones and zone-based policies for application by service cards 120 of firewall 123. NSP 73 of routing engine 46 communicates with and programs service cards 64 of firewall 123 as described above.

[0059] In accordance with RIB 108, forwarding application specific integrated circuits (ASICs) 90 of forwarding engine 106 maintain forwarding information base (FIB) 122 that associates network destinations or MPLS labels with specific next hops and corresponding interface ports. For example, control unit 102 analyzes RIB 108 and generates FIB 122 in accordance with RIB 108. Router 100 includes interface cards 114A-114N ("IFCs 114") that receive and send packets via network links 116 and 117, respectively. IFCs 114 may be coupled to network links 116, 117 via a number of interface ports.

[0060] Generally, flow control unit 118 of forwarding engine 106 may relay certain packets received from IFCs 94 to service cards 120A-120M ("service cards 120") in accordance with a flow filter table 124. Service cards 120 receive packets from flow control unit 118, selectively provide firewall services in accordance with information within the packet, and relay the packet or any response packets to control unit 102 for forwarding by forwarding ASICs 120. Forwarding ASICs 120 may comprise one or more dedicated packet forwarding integrated circuits.

[0061] Flow control unit 118 includes flow-based provisioning logic 102 that distinguishes between packet flow sessions based on a five-tuple found within a header of each received packet and steers packets of the same flows to the same one of service cards 120 for application of stateful firewall services. Flow control unit 118 references flow filter table 104 as described above to determine whether a received packet corresponds to a trusted packet flow that may be processed via a straight path (i.e., bypassing service cards 120 entirely), or whether the received packet corresponds to an unknown or untrusted packet flow session and should therefore be sent to one of service cards 120 for further inspection and application of firewall services. Upon application of firewall services, service cards 120 may provide feedback to flow control unit 118 via service card communication module 106 (SERVICE CARD COMM. MODULE 106) to dynamically update flow table 124. That is, service cards 120 may update flow filter table 124 via commands 121 to service card communication module 108.

[0062] In one embodiment, each of forwarding engine 106 and routing engine 104 may comprise one or more dedicated processors, hardware, ASICs or the like, and may be communicatively coupled by a data communication channel. The data communication channel may be a high-speed network connection, bus, shared-memory or other data communication mechanism. Router 100 may further include a chassis (not shown) for housing control unit 102. The chassis has a number of slots (not shown) for receiving a set of cards, including IFCs 94 and service cards 120. Each card may be inserted into a corresponding slot of the chassis for electrically coupling the card to control unit 102 via a bus, backplane, or other electrical communication mechanism.

[0063] Router 100 may operate according to program code having executable instructions fetched from a computer-readable storage medium (not shown). Examples of such media include random access memory (RAM), read-only memory (ROM), non-volatile random access memory (NVRAM), electrically erasable programmable read-only memory (EEPROM), flash memory, and the like. The functions of router 100 may be implemented by executing the instructions of the computer-readable storage medium with one or more processors, discrete hardware circuitry, firmware, software executing on a programmable processor, or a combination of any of the above.

[0064] FIG. 7 is a flowchart illustrating exemplary operation of an MPLS-aware firewall, e.g., any of firewalls 12, 22, 44, 123 described above. For exemplary purposes, the flowchart of FIG. 7 will be explained in reference to firewall 123 and its one or more service cards 120 illustrated in FIG. 6.

[0065] Upon receiving a packet from packet from forwarding engine 106 (130), firewall 123 processes the packet to identify the input interface by which the packet was initially received by router 100 (132). In one example, either the IFC 114 upon which the packet was received or the forwarding engine 106 determines the specific input interface upon which the packet was received by router 100 and attaches information to the packet identifying the particular interface prior to relaying the packet to firewall 123 for processing.

[0066] Next, firewall 123 analyzes the header of the packet to determine if the input packet is an IP packet and not a VPN packet that has a VPN label and that was received from the service provider network via a VPN. If so, then firewall 123 accesses its internal configuration data and determines whether the administrator has defined any input zone that includes the physical interface upon which the packet was received (136).

5 **[0067]** If, however, the packet is an VPN packet having either a single VPN label or an MPLS stack in which the VPN label is the inner label, firewall 123 accesses the configuration data and determines whether the administrator has defined an input zone that for the customer VPN from which the packet was received (138). That is, firewall 123 reads the packet's inner VPN label and accesses the mapping information provided by NSP 103 of routing engine 104 to map the in VPN label to a customer VPN identifier, e.g., string or numerical identifier. The inner label of the received packet, i.e.,
10 the VPN label, is typically a label previously allocated by the router using mpBGP and issued to an upstream LSR along the VPN tunnel. Thus, routing engine 104 has knowledge of this VPN label, and the mapping information provided to firewall 123 by NSP 103 maps this VPN label to the particular customer VPN identifier, thereby allowing the administrator to specify that customer VPN in policies and zones within the firewall configuration data. Upon identifying the customer VPN from the inner VPN label based on the mapping information from NSP 103, firewall 123 parses the configuration
15 data to determine whether the administrator has defined any input zone that includes the customer VPN within the zone's collection of interfaces.

[0068] After determining the input zone, firewall 123 determines whether the packet matches an existing packet flow session currently being processed by firewall 123 (140). If so, firewall 123 may place the packet on fast path processing for immediate forwarding by forwarding engine 106. For example, when fast path processing the packet, firewall 123
20 need not perform the computationally intensive task of initializing and updating session information for the new packet. Moreover, firewall 123 need not apply policies to the packet as such policies may have already been applied to the packet flow.

[0069] If the packet does not match an existing packet flow (NO branch of 140), firewall 123 performs a route lookup on the packet to determine a next hop and, based on the next hop, an output interface for the packet (144). For example,
25 one or more of service cards 120 of firewall 123 may be programmed by routing engine 104 and installed with a copy of all or a portion of FIB 122 as used by forwarding ASICs 120. Alternatively, FIB 122 of forwarding ASICs 130 may be stored in a shared memory accessible via service cards 120. In either case, firewall 123 traverses the FIB based on information within the packet so as to determine the next hop and corresponding output interface for the packet. Further, based on information installed within the copy of the FIB, firewall 123 determines based on the route lookup whether
30 the packet will be output as IP traffic or as VPN traffic to be injected into the service provider network (146).

[0070] If the route lookup indicates that the packet will not be output as a VPN packet having a VPN label and optionally one or more outer MPLS labels, but instead the packet will be output as an IP packet, then firewall 123 accesses the configuration data and determines whether the administrator has defined any output zone that includes the output interface to which the IP packet is destined (148).

35 **[0071]** If, however, the route lookup indicates that the packet is to be encapsulated and output by forwarding engine 106 as an VPN packet, firewall 123 accesses the configuration data and determines whether the administrator has defined any output zone that includes the customer VPN to which the packet will be output (150). That is, based on the route lookup, firewall 123 determines the inner forwarding equivalence class (FEC) label, i.e., the VPN label that will ultimately be prepended to the packet by the forwarding engine 106 when forwarding the packet. In addition, firewall
40 123 determines, based on the route lookup, the next hop to which the VPN packet will be forwarded. Next, firewall 123 accesses the mapping data provided by NSP 103 of routing engine 104 to map the data pair < VPN label, next hop> to a specific customer VPN identifier. Firewall 123 uses both the VPN label to be applied to the packet as well as the next hop since, for VPN traffic leaving router 100 and entering the MPLS core of the service provider network, the VPN labels have likely been allocated by upstream routers along the VPN tunnels and, as such, may be duplicative. Thus, for egress
45 VPN traffic to be injected into a VPN tunnel, firewall 123 identifies the correct customer VPNs to which the packet is destined by indexing the mapping information provided by NSP 103 based on the unique pair: <VPN label, next hop> learned in the route lookup for the packet. Other information may be used, such as route designators and/or route targets for the customer VPNs. Upon resolving the customer VPN identified from the mapping, firewall 123 accesses its configuration data to identify any output zone that the administrator has defined that includes the customer VPN to which
50 the packet is destined.

[0072] Next, having determined the input zone and the output zone for the packet, firewall 123 accesses its configuration data to identify any policy that has been defined for traffic traveling between the zones. At this time, firewall 123 also applies any packet flow criteria that have been defined by the policies. Upon identifying the matching policies, firewall 123 applies to the packet the actions specified by those policies (152).

55 **[0073]** After applying the policies, firewall 123 processes the packet along a "first path" by initializing and creating session information to maintain state for the packet flow. Finally, firewall 123 injects the packet into forwarding engine 106 for forwarding in accordance with FIB 122 (154). In this example, router 100 integrates MPLS-aware, zone-based firewall security features in single network device. Moreover, a full mesh of zone-based policies can be defined and

applied seamlessly with respect to physical interfaces as well as customer VPNs.

[0074] FIG. 8 illustrates example mapping information 160 provided by a routing component to an integrated firewall of a network device (e.g., from NSP 73 of routing engine 68 to firewall 44 of router 40) to enable security services to be applied to MPLS-based customer VPNs. Alternatively, the forwarding plane 42 can dynamically identify the VPN tunnel, e.g., by the customer interface on which the traffic arrived, and communicate mapping information to firewall 44 and/or routing engine 68. In any event, as shown in FIG. 8, the example mapping information 160 includes a plurality of entries, each entry listing a customer VPN identifier 162 (e.g., a text string or other identifier) that was provided by the administrator when defining input zones and policies via interaction with a user interface, such as UI 75.

[0075] For example, the first and second entries of mapping information include a customer VPN identifier "VPN_customer_A" representing a string specified by the administrator when defining an interface for an input zone for the firewall, as shown in the examples discussed above. In response to the use of a new customer VPN identifier within the configuration data for the firewall, the routing component (e.g., NSP 73 of routing engine 68) creates two entries in mapping information 160. The first entry maps the customer VPN identifier to an MPLS label to be applied by the router's forwarding component (e.g., forwarding component 80) when encapsulating IP traffic destined for that particular customer's VPN site as well as a corresponding next hop identifier for the traffic. The second entry maps that same customer VPN identifier to a VPN label that is expected to be affixed to inbound traffic received from the customer's VPN site, optionally as an inner label of an MPLS label stack.

[0076] For example, the first entry of mapping information 160 maps the string "VPN_Customer_A" to an <VPN label 100, next hop identifier 10.1.1.1> pair. In this way, the first entry resolves the string utilized in the firewall configuration data to a specific inner VPN label to be used for outbound VPN traffic to be injected into the service provider network, optionally along an LSP. The second entry of mapping information 160 maps the string "VPN_Customer_A" to a VPN label 750 previously allocated by the router and expected to be affixed to VPN traffic received by the inbound VPN tunnel for that customer VPN site. Mapping information 160 may be input by the administrator to resolve the firewall configuration information to specific VPN tunnels and next hops where necessary, or the routing component may determine this information dynamically based on the RIB and corresponding FIB utilized for routing and forwarding purposes. Other information may be used in addition to or in place of the next hop, such as a route designator or route target for the customer VPN.

[0077] FIG. 9 is a block diagram illustrating another example of a router 200 that integrates a routing plane 206 and an MPLS-aware firewall 208 using a shared forwarding plane 204. Features of router 200 may, for example, be incorporated within any of PE routers 10, router 20, router 30 or router 100 described above.

[0078] In the example of FIG. 9, firewall 208 has been logically partitioned into multiple virtual security systems 240A-240X to provide multi-tenant security services. That is, virtual security systems 240 represent logically partitioned firewall instances providing separate security services, including MPLS-aware zone-based firewall services, that are applied by firewall 208. Router 200 presents virtual security systems 240 as logically independent firewalls that can be independently configured even though the virtual security systems may share computing resources of service cards 224.

[0079] For example, a root-level administrator 207 ("ROOT ADMIN 207") is a central, overarching security and system administrator that may control and administer a ROOT one of virtual security systems 240. In this way, root-level administrator 207 can access and configure any custom VSYS specific security resources, as well as manage any shared security resources, such as a SHARED-UNTRUST zone, which is a commonly shared connection to the Internet used by multiple internal security zones. The root-level administrator 207 also controls the initial assignment of interfaces and zones.

[0080] For example, a root-level administrator 207 may interact with UI 215 to provide configuration data to define virtual security systems 240 and, for each of the virtual security systems, specify one or more virtual security system (VSY) administrators 209 ("VSY ADMINS 209"). Each of virtual security systems 240 is presented to the corresponding VSY administrator 209 as a unique security domain, and the VSY administrator 209 for each virtual system 240 can individualize their security domain by defining specific zones and policies to be applied to traffic associated with that virtual system 240. Each virtual security system 240 can be configured to have its own totally separated set of security zones, policy rule set and management domain. In this way, virtual security systems 240 logically segment integrated MPLS-aware firewall 208 into multiple security devices. Each VSY administrator 209 may interact with UI 215 in the manner described herein so as to provide configuration data for a specific virtual system 240, including defining firewall zones and policies with respect to physical interfaces, sub-interfaces, or customer VPNs. Management interfaces presented by UI 215 are specific to the particular virtual security system 240 being configured and managed, and each of the virtual security systems 240 appears as a discrete security device to the individual VSY administrator 209. This means that each distinct virtual security system 240 may have, for example, its own web interface, operational management connections and views. The VSY administrator 209 of one virtual security systems 240 is isolated to the configuration and operation of his or her own virtual system.

[0081] As one example, user interface 215 of router 200 provides a syntax for defining security policies to be applied with respect to the defined zones for specific virtual security systems 240. For example, router 200 may support a syntax

EP 2 154 834 A1

as follows:

```
vsys VSYS-IDENTIFIER {  
    zone ZONE_NAME {  
5         interface INTERFACE_NAME;  
         interface INTERFACE_NAME;  
         vpn VPN_NAME;  
         vpn VPN_NAME;  
    }  
10    policy from-zone ZONE_NAME to-zone ZONE_NAME {  
        match {  
            source-address <s>;  
            destination-address <d>;  
            source-port <sp>;  
            destination-port <dp>;  
15            application protocol <any>;  
        }  
        then {  
            actions;  
        }  
20    }  
}
```

In the example above, the keyword "vsys" indicates that the subsequent configuration data applies to a specific one of virtual security systems 240. This outer information may be omitted by vsys administrators 209 and the corresponding one of virtual security system 40 may be automatically determined by UI 215. In any case, the administrator may define zones and policies using the keywords "zone" and "policy," as described above, for the particular virtual system 240. The above syntax is merely illustrative.

[0082] In accordance with an example syntax, an administrator may provide configuration data as follows:

```
vsys Customer-A {  
30    zone untrust {  
        vpn VPN-A; /* VPN carrying traffic for VPN site VPN-A*/  
        vpn VPN-B; /* VPN carrying traffic for VPN site VPN-B*/  
    }  
    zone trust {  
35        interface ge-0/0/0.1; /*Physical interface for link to client site A*/  
        interface so-2/4/2.0; /*Physical interface for link to client site B*/  
    }  
    policy from-zone untrust to-zone trust {  
        then {  
40            apply virus_scanning;  
        }  
    }  
}
```

This example is similar to the example above, and the administrator has defined two firewall zones, "untrust" and "trust." For the zone "untrust," the administrator has indicated that the zone includes VPN traffic carried by two customer VPNs, VPN-A and VPN-B. For the zone "trust," the administrator has indicated that the zone includes a collection of two interfaces for forwarding traffic to client sites A and B. Further, the administrator has defined a policy for application to traffic received from an interface within the zone untrust and directed to an interface within the zone trust (e.g., VPN traffic from the MPLS core via VPN-A or VPN-B and directed to the client sites A or B as IP traffic). For such traffic, the policy requires the virtual security system identified as "Customer-A" (e.g., virtual security system 240) of FW 208 to apply stateful virus scanning algorithms to application layer data assembled from the packets that correspond to that particular virtual security system and forwarded in accordance with its specific FIB 214.

[0083] As virtual security systems, each of virtual security systems 240 may share the same hardware resources provided by service cards 224. For example, computing resources provided by service cards 224 may apply security policies for any of virtual security systems 240 to the network traffic associated with that particular virtual system. Further, weightings, time quotas or percentages of CPU or other hardware usage can be allocated and enforced so as to ensure fair usage by virtual security systems 240 so that consumption of hardware resources by one of the virtual system, such as in response to a denial of service attack, does not impact the performance of all of the other virtual security systems.

Alternatively or in addition, virtual security systems 240 may be allocated to specific service cards 224.

[0084] In addition, in response to creation of virtual security systems 240, router 200 may manage resources of routing engine 211 and forwarding plane 204 so as to provide a plurality of virtual routers, where each virtual security system 240 may optionally map to a different virtual router. A virtual router is a separate routing instance within router 200, and each instance may execute its own routing protocol and maintain its own settings, route table (RIB), and routing updates. Each virtual router participates in its own routing domain; multiple virtual routers allow a single device (e.g., router 200) to participate in multiple routing domains completely separated from each other. That is, routing engine 211 may maintain a logically separate RIB 212 for each virtual security system 240. Further, for each RIB 212, routing engine 211 programs forwarding component 220 with a corresponding FIB 214 in accordance with the routes, as well as the MPLS labels associated with the routes, for the virtual system 240. In other words, routing engine 211 may program forwarding component 220 with logically isolated FIBs 212, one for each virtual security system 240, and forwarding component 220 applies the appropriate FIB when making packet forwarding decisions.

[0085] In a manner similar to that described above with respect to FIG. 4, NSP 213 programs firewall 208 with configuration data. In this case, NSP 213 programs configuration data for each of virtual security systems 240, causing the service cards 224 of firewall 208 to recognize the zones and security policies defined for the different virtual security systems when processing packets from forwarding plane 204. Each service card 224 may, for example, execute a microkernel that operates as a consumer of state information and listens for communications from NSP 213. In this way, routing plane 206 and firewall 208 interact so that firewall 208 provides support for multiple virtual security systems and is made aware of state information associated with the VPN traffic flowing through the routing device.

[0086] For example, NSP 213 of routing engine 211 programs the service cards 224 with information that creates virtual security systems 240 and then, for each of the virtual security system, associates customer VPNs for that virtual security system with specific VPN labels that have been used for tunneling the corresponding VPN traffic through the service provider network. NSP 213 may query the corresponding protocols 210 and RIB 212 for the respective virtual security system 240 to provide the service cards 224 of firewall 208 with information maintained with that specific RIB for that specific virtual security system. For example, for VPN traffic that may be received by router 200 for a virtual security system 240, NSP 213 may provide information that identifies one or more VPN tags that will be affixed to the header of the packet and mapping information to associate this VPN label with a customer VPN identifier (e.g., a text string or other identifier) that may be utilized by the VSYS administrator 209 when defining input zones and policies for that particular virtual security system. For VPN traffic that may be output by router 200 to the service provider network in association with a virtual security system 240, NSP 213 may provide mapping information that identifies any one or more VPN labels to be applied by forwarding component 220 to IP traffic destined for the customer VPN, a corresponding next hop identifier for the traffic and a mapping to associate this <VPN label, next hop identifier> pair with a customer VPN identifier (e.g., a text string or other identifier) that may be utilized by the VSYS administrator 209 when defining firewall zones and policies for that virtual security system.

[0087] Forwarding plane 204 may include a flow control unit 215 that operates in a manner similar to flow control unit 75 (FIG. 4) to selectively direct packets to firewall 208 for processing. Service cards 224 may issue commands 219 to install dynamic filters within flow control unit 215 to control packet diversion to firewall 208.

[0088] FIG. 10 is a flowchart illustrating exemplary operation of an MPLS-aware firewall, e.g., any of firewalls 12, 22, 44, 123, 200 described above. For exemplary purposes, the flowchart of FIG. 10 will be explained in reference to firewall 200 and its one or more service cards 224 illustrated in FIG. 9.

[0089] Upon receiving a packet from packet from forwarding plane 204 (230), firewall 208 first classifies the packet into one of virtual security systems 240 based on source and/or destination information for VLAN, interfaces, IP address or combinations thereof. Next, one or more of service cards 244 associated with the virtual security system 240 to which the packet is classified (associated) processes the packet to identify the input interface by which the packet was initially received by router 200 (232). In one example, either the IFC upon which the packet was received or the forwarding plane 204 determines the specific input interface upon which the packet was received by router 200 and attaches information to the packet identifying the particular interface prior to relaying the packet to firewall 208 for processing.

[0090] Next, firewall 208 (i.e., the particular one or more service cards 224 of firewall 208 providing the execution environment for the virtual security system 240 for the packet) analyzes the header of the packet to determine if the input packet is an IP packet and not a VPN packet that was received from the service provider network via a VPN tunnel. If so, then firewall 208 accesses root configuration data as well as configuration data for the specific virtual security system 240 associated with the packet to determine whether either the root administrator 207 or the VSYS administrator 209 has defined any input zone, for that specific virtual security system 240, that includes the physical interface upon which the packet was received (236).

[0091] If, however, the packet is a VPN packet having a VPN label (optionally as an inner label of an MPLS label stack), firewall 208 accesses root configuration data as well as configuration data for the specific virtual security system 240 associated with the packet to determine whether either the root administrator 207 or the VSYS administrator 209 has defined any input zone for that specific virtual security system 240 that includes the customer VPN from which the

packet was received (238). That is, firewall 208 reads the packet's inner VPN label and accesses the mapping information provided by NSP 213 of routing engine 211 to map the inner VPN label to a customer VPN identifier, e.g., string or numerical identifier, used within the RIB 212 for that particular virtual security system 240.

[0092] After determining the input zone, firewall 208 determines whether the packet matches an existing packet flow session currently being processed by firewall 208 (240). If so, firewall 208 may place the packet on fast path processing for immediate forwarding by forwarding component 220. For example, when fast path processing the packet, firewall 208 need not perform the computationally intensive task of initializing and updating session information for the new packet. Moreover, firewall 208 need not apply policies to the packet as such policies may have already been applied to the packet flow.

[0093] If the packet does not match an existing packet flow (NO branch of 241), firewall 208 performs a route lookup on the packet to determine a next hop and, based on the next hop, an output interface for the packet (244). For example, the service cards 224 to which virtual security systems 240 are allocated may be programmed by routing engine 211 and installed with a copy of all or a portion of FIBs 214 for the respective virtual system. Alternatively, FIBs 214 may be stored in a shared memory accessible via service cards 224. In either case, when performing a route lookup, firewall 208 selects the FIB 214 for the virtual security system 240 associated with the packet and traverses that FIB based on information within the packet so as to determine the next hop and corresponding output interface for the packet. Further, based on information installed within the copy of the corresponding FIB, firewall 208 determines based on the route lookup whether the packet will be output as IP traffic or as VPN traffic having a prepended VPN label (246).

[0094] If the route lookup indicates that the packet will not be output as a VPN packet on a VPN tunnel but instead the packet will be output as an IP packet, then firewall 208 accesses the root configuration data and the configuration data for the particular virtual security system 240 to determine whether the root administrator 207 or the corresponding VSYS administrator 209 has defined any output zone that includes the output interface to which the IP packet is destined (248).

[0095] If, however, the route lookup indicates that the packet is to be encapsulated and output by forwarding component 220 as a VPN packet on a VPN tunnel, firewall 208 accesses the root configuration data and the configuration data for the particular virtual security system 240 to determine whether the root administrator 207 or the corresponding VSYS administrator 209 has defined any output zone that includes the customer VPN to which the packet will be output (250). That is, based on the route lookup, firewall 208 determines the outer forwarding equivalence class (FEC) label, the VPN label that will ultimately be prepended to the packet by forwarding component 220 when forwarding the packet using the FIB 214 for the particular virtual security system 240. In addition, firewall 208 determines, based on the route lookup using the copy of the appropriate FIB 214, the next hop to which the VPN packet will be forwarded. Next, firewall 208 accesses the mapping data provided by NSP 213 of routing engine 211 to map the data pair < VPN label, next hop> to a specific customer VPN. Firewall 208 uses both the MPLS label to be applied to the packet as well as the next hop since, for VPN traffic leaving router 200 and entering the MPLS core, the VPN labels have likely been allocated by upstream LSRs along the VPN tunnels and, as such, may be duplicative. Thus, for egress VPN traffic to be placed on the VPN, firewall 208 identifies the correct customer VPNs to which the packet is destined by indexing the mapping information provided by NSP 103 based on the unique pair: <VPN label, next hop> learned in the route lookup for the packet. Based on the customer VPN identified from the mapping, firewall 208 accesses its root configuration data as well as the configuration data for the specific virtual security system 240 to identify any zone that either root administrator 207 or the VSYS administrator 209 has defined that includes the customer VPN to which the packet is destined.

[0096] Next, having determined the input zone and the output zone for the packet, firewall 208 accesses the root configuration data and the configuration data for the specific virtual security system 240 to identify any policy that either root administrator 207 or the VSYS administrator 209 has defined for traffic traveling between those zones. At this time, firewall 208 also applies any packet flow criteria that have been defined by the policies. Upon identifying the matching policies, firewall 208 applies to the packet the actions specified by those policies (252). In this way, zone and policy selection by firewall 208 is dependent on the particular virtual security system 240 to which the packet belongs.

[0097] After applying the policies, firewall 208 processes the packet along a "first path" by initializing and creating session information to maintain state for the packet flow. Finally, firewall 208 injects the packet into forwarding component 220 for forwarding in accordance with the particular FIB 214 corresponding to the virtual security system 240 (254). In this example, router 200 integrates MPLS-aware, zone-based firewall security features in single physical network device that provides support for multiple virtual security systems. Moreover, each virtual security system can logically apply a full mesh of zone-based policies can be defined and applied seamlessly with respect to physical interfaces as well as customer VPNs.

[0098] FIG. 11 illustrates example mapping information 300 provided by a routing component to an integrated firewall of a network device having support for virtual security devices (e.g., from NSP 213 of routing engine 211 to firewall 208 of router 200) to enable security services to be applied to MPLS tunnels. For exemplary purposes, FIG. 11 will be described with respect to router 200 of FIG. 9.

[0099] As shown in FIG. 11, the example mapping information 300 includes a plurality of entries, each entry listing a

virtual security system identifier 301 (e.g., a text string or other identifier) that was provided by root administrator 207 when defining virtual security systems 240. In addition mapping information 300 stores a customer VPN identifier 302 (e.g., a text string or other identifier) that was provided by either the root administrator 207 or the authorized VSYS administrator 209 when defining input zones and policies for the corresponding one of virtual security systems 240 via interaction with a user interface 215.

[0100] For example, the first and second entries of mapping information include a customer VPN identifier "VPN_customer_A" representing a string specified by the administrator when defining an interface for an input zone for the firewall, as shown in the examples discussed above. In response to the use of a new customer VPN identifier within the configuration data for the firewall, the routing component (e.g., NSP 73 of routing engine 211) creates two entries in mapping information 300. The first entry maps the customer VPN identifier to a VPN label to be applied by the router's forwarding component (e.g., forwarding component 220) when encapsulating IP traffic destined for that particular customer's VPN site as well as a corresponding next hop identifier for the traffic. The second entry maps that same customer VPN identifier to a VPN label that is expected to be affixed as the inner label to inbound MPLS traffic received from the customer's VPN site.

[0101] For example, the first four entries of mapping information 300 correspond to a first virtual security system (VSYS_customer_A) and the last two entries correspond to a second virtual security system (VSYS_customer_B). Thus, this example illustrates mapping information 300 for a router having two virtual security systems currently defined.

[0102] The first entry of mapping information 300 is applicable only to virtual security system "VPN_Customer_A" and maps a VPN identifier "VPN_OFFICE" to an <VPN label 100, next hop identifier 10.1.1.1> pair. In this way, the first entry resolves the "VPN_OFFICE" string utilized in the firewall configuration data by the VSYS_administrator to a specific outbound VPN tunnel recognized within the first virtual security system.

[0103] The second entry of mapping information 300 is also only applicable to virtual security system "VPN_Customer_A" and maps the VPN identifier "VPN_OFFICE" to an VPN label 750 previously allocated by the router for this virtual security system. That is, MPLS label 750 is expected to be affixed to VPM traffic received by the inbound VPN tunnel for that customer VPN site of the virtual security system VSYS_customer_A. Mapping information 300 may be input by either root administrator 207 or the authorized VSYS_administrator 209 to resolve either root firewall configuration information or VSYS-specific configuration information to specific MPLS tunnels and next hops where necessary, or the routing component may determine this information dynamically based on the corresponding RIB and FIB utilized for routing and forwarding purposes for each virtual security system. Although shown as a single table, mapping information 300 may be partitioned and separated based on virtual security system and stored in separate data structures and/or memories so as to add an additional degree of separation for the virtual security systems.

[0104] FIG. 12 is a block diagram illustrating an example network environment 400 in which two service provider networks 402A, 402B provide connectivity between customer virtual private network (VPN) sites 406A-406N (collectively, VPN sites 406). In the example of FIG. 12, each service provider network 402 is operated by a different service provider, and PEs 411A, 411B operate at an inter-provider boundary. In this example, autonomous system border routers (ASBRs) 411A, 411B are coupled by a physical link 415 and exchange network traffic for VPN sites 406A, 406B. Similar to FIG. 1, VPN sites 406A, 406B include customer edge (CE) routers 408A-8N connected to provider edge (PE) routers 410A-410N via network links 416A-416N.

[0105] As described with respect to the embodiments of FIGS. 1, service provider networks 402A and 402B supports provider-provisioned VPNs (PPVPNs). For example, administrators associated with service provider networks 402 may configure PE routers 410 and ASBRs 411 so as to provision VPN services for one or more customer VPNs for VPN sites 406. At this time the administrators for the different service provider networks 402 separately define a VPN identifier for each customer VPN (e.g., VPN_CUSTOMER_A) traversing their respective service provider network 402, and PE routers 410 and ASBRs 411 allocate VPN labels, VPN addresses, a router target, a router distinguisher, and all other state information necessary for the VPN.

[0106] As shown in FIG. 12, each of service provider networks 402 may include additional internal label switched routers (LSRs) 414 that provide a Multi-protocol Label Switching (MPLS) MPLS core network within each service provider network 402. PE routers 410 and ASBRs 411 may communicate with LSRs 414 to establish one or more one or more label switch paths (LSPs) for transporting the VPN communications through service provider networks 404. or may be end-to-end LSPs spanning service provider networks 402 so as to originate and terminate at PE routers 412. Traffic flowing along network links 416 to and from VPN sites 406 may take the form of Internet Protocol (IP) packets, and may be secured using Internet Protocol Security (IPSec) protocols, Secure Sockets Layer (SSL) protocols or other protocols that make use of cryptographic technology.

[0107] In one example, PE routers 410 exchange VPN information, exchange VPN routes and agree on inner VPN labels via mpBGP so as to form one or more end-to-end VPN tunnels 418 for transporting communications of customer VPN sites 406 through service provider networks 402. In this embodiment, ASBRs 411 and LSRs 414 might not directly participate in the mpBGP negotiation or VPN label assignment, but may utilize LDP or RSVP to allocate outer MPLS labels to be applied to the VPN communications for traversing service provider networks 402. In this example, PE routers

410 provide ingress and egress for the IP traffic with respect to the MPLS services and VPNs provided within service provider networks 404. That is, PE routers 10 operate as ingress and egress routers for communicating the IP packets of VPN sites 6 as encapsulated VPN packets traversing VPN tunnels 418. For example, PE router 410A may receive IP traffic from VPN site 406A, and may then prepend a VPN label based on the corresponding customer VPN associated with the traffic. The VPN traffic may then be viewed as flowing along a VPN tunnel 418 through service provider networks 402. One or more of these VPN tunnels (i.e., packet flows having VPN labels prepended to each packet) may then further be encapsulated within a label stack of additional MPLS labels allocated by LSRs 414 and ASBRs 411.

[0108] In another example embodiment, ASBRs 411 communicate to form an LSP between the two ASBRs, as opposed to an end-to-end VPN tunnel 418, so as to convey VPN communications between service provider networks. In this example, ASBRs 411 may utilize mpBGP to agree on inner VPN labels and outer MPLS labels to be assigned to the packets.

[0109] In either case, similar to FIG. 1, each of PE routers 410 includes an integrated firewall (FW) 412A-412N (collectively, FWs 412) that is an MPLS-aware firewall that allows service provider networks 402 to apply firewall security policies at the IP-MPLS interface between the service provider networks and the customer VPN sites 406. Further, each of PE routers 411 located at the inter-provider boundary between service provider networks 402 includes an integrated firewall (FW) 413A, 413B that is an MPLS-aware firewall that allows service provider networks 404 to apply firewall security policies at the interface between the service provider networks. In one example, FWs 413 allow firewall security policies to be applied at the point where VPN traffic is communicated between service provider networks on link 415 via VPN tunnels 418. Moreover, by applying the techniques discussed above, administrators may define different firewall zones and different security policies to be applied to VPN traffic for different VPNs even though that VPN traffic is flowing through the same physical link 415. For example, in accordance with the techniques described herein, FWs 413 may be zone-based firewalls that allow firewall zones and security policies to be specified in reference to the customer VPNs provisioned by the service provider network in accordance with either of the examples set forth above. Moreover, FWs 413 allow such techniques to be applied at an MPLS-MPLS interface typically found at an inter-provider boundary. That is, packets exchanged at the inter-provider boundary between service provider networks 4 packets are typically in the form of VPN packets having inner VPN labels and optionally additional outer MPLS labels.

[0110] When defining zone-based security services for the inter-provider boundary, administrators may configure FWs 413 by specifying both input zones and output zones having interface lists that include identifiers for customer VPNs. That is, similar to the techniques described above with respect to FIGS. 1-11, each of PE routers 411 may provide a user interface having a command syntax that allows individual customer VPNs to be defined and recognized by FWs 12 as logical interfaces, and these logical interfaces can be used like other physical interfaces of the PE routers to define zones and corresponding security policies to be applied to those zones. As described above, these identifiers for the customer VPN are mapped to VPN labels to be applied on either side of FWs 413 (i.e., either to traverse link 415 or when internally commuted to the MPLS core of the service provider network). Alternatively or in addition, system administrators may define a single firewall zone with respect to physical link 415 so as to be able to define common security policies to be applied to all traffic traversing the inter-provider boundary.

[0111] As illustrated in FIG. 12, the MPLS-aware FWs 413 may be integrated within routing device (e.g., PE routers 411), thus allowing a single device to be deployed by each service provider network 404 at the inter-provider boundary to provide both routing functionality, including MPLS and VPN support, as well as firewall services. FW 413 may implement any of the functions describes above with respect to FIGS. 1-11 including the user command syntax of the user interface and support for virtual security systems.

[0112] Although described with respect to provider edge routers, the techniques described herein may be applied to other types of routers and network devices generally. For example, the router may be an edge device, peering device, or core device of a Service Provider (SP) network. As additional examples, the router may be an edge router that provides broadband access, such as a Broadband Remote Access Server (BRAS) or a Broadband Network Gateway (BNG) or a Cable Modem Termination System (CMTS). As another example, the router may be an edge router that provides enterprise connectivity to public networks, such a Multi-Service Edge router (MSE). As another example, the router may be an edge router that provides mobile access, such as a Gateway GPRS (General Packet Radio Services) Support Node (GGSN), a Packet Data Serving Node (PDSN), or a Public Data Network Gateway (PDN-GW). As a further example, the router may be a data center device (e.g., and edge router) that provides routing and security functions for packets flowing in or out of a data center. As another example, the router may be a peering router that serves as a point of interconnection between network service providers. As yet another example, the router may be an aggregation router or core router within an IP network core of a service provider, such as a core router positioned between GGSNs or PDSNs or BNGs. In addition, the router may be a device associated with a private enterprise network.

[0113] Further, the techniques may be applied to any network device that implements layer three functionality in the control plane so as to be aware of the MPLS signaling utilized by a network when establishing MPLS VPNs. In this manner, the network device may incorporate any of the functions described herein so as to provide an MPLS-aware firewall, such as a zone-based firewall in which MPLS VPNs and other interfaces of the device may be seamlessly

specified by the administrator when defining zones and zone-based policies for the firewall services provided by the device.

[0114] Various embodiments of the invention have been described. These and other embodiments are within the scope of the following claims.

[0115] Throughout the description and claims of this specification, the words "comprise" and "contain" and variations of them mean "including but not limited to", and they are not intended to (and do not) exclude other moieties, additives, components, integers or steps. Throughout the description and claims of this specification, the singular encompasses the plural unless the context otherwise requires. In particular, where the indefinite article is used, the specification is to be understood as contemplating plurality as well as singularity, unless the context requires otherwise.

[0116] Features, integers, characteristics, compounds, chemical moieties or groups described in conjunction with a particular aspect, embodiment or example of the invention are to be understood to be applicable to any other aspect, embodiment or example described herein unless incompatible therewith. All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive. The invention is not restricted to the details of any foregoing embodiments. The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

[0117] The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

Claims

1. A network router comprising:

a plurality of interfaces configured to send and receive packets;
a firewall integrated within the network router, the firewall configured to apply stateful firewall services to the packets;
a routing engine comprising a control unit that executes a routing protocol to maintain routing information specifying routes through a network, wherein the control unit executes at least one protocol to establish virtual private network (VPN) tunnels for one or more customer VPNs;
a forwarding engine configured by the routing engine to select next hops for the packets in accordance with the routing information, the forwarding engine comprising a switch fabric to forward the packets to the interfaces based on the selected next hops, wherein the forwarding engine includes a flow control module that, upon receiving packets from the network, directs one or more of the packets to the firewall for application of the stateful firewall services; and
a user interface by which a user specifies one or more zones to be recognized by the firewall when applying the stateful firewall services to the packets, each of the zones defined by a list of one or more of the interfaces, wherein the user interface supports a syntax that allows the user to define the zones by specifying the customer VPNs within lists of interfaces associated with the zones.

2. The network router of claim 1, wherein the firewall stores configuration data that specifies the zones defined by the user, at least one of the zones specifying a collection of interfaces that includes identifiers for one or more of the customer VPNs.

3. The network router of claim 1 or 2, wherein the control unit of the routing engine executes a network services protocol that communicates mapping information between the routing engine and the firewall, wherein the mapping information associates multi-protocol label switched (MPLS) VPN labels for the VPNs with the identifiers for the customer VPNs.

4. The network router of claim 3, wherein for VPN tunnels for which the network router operates as an egress label switched router, the mapping information between the routing engine and the firewall associates inner VPN labels affixed to packets received from the LSPs by the interface cards with respective ones of the identifiers for the customer VPNs.

5. The network router of claim 3, wherein for VPN tunnels for which the network router operates as an ingress label

switched router, the mapping information communicated between the routing engine and the firewall associates pairs of a VPN label and a forwarding next hop with respective ones of the identifiers for the customer VPNs, wherein the VPN labels are VPN labels to be subsequently affixed to the packets when output to the network by the forwarding engine.

5

6. The network router of claim 3,
wherein the user interface allows the user to specify one or more policies for the firewall,
wherein, based on the mapping information, the firewall applies the policies to multi-protocol label switched (MPLS) packets received from the forwarding plane, and
wherein, based on the mapping information, the firewall applies the policies to packets received from the forwarding plane that are destined to be forwarded by the routing device to the VPN tunnels as multi-protocol label switched (MPLS) packets.

10

7. The network router of any one of claims 1 to 3,
wherein the firewall determines an input zone and an output zone for each of the packets based on the zones defined by the user,
wherein the firewall applies one or more of the stateful firewall services to each of the packets based on the input zone and output zone determined for the packet, and
wherein at least one of the input zone or output zone is defined by the user by specifying at least one of the customer VPNs within a collection of interfaces associated with the input zone or output zone.

15

20

8. The network router of any one of claims 1 to 3,
wherein, based on the routing information, the routing engine programs the forwarding engine with forwarding information that associates network destinations and MPLS labels with specific next hops and corresponding interface ports of interface cards of the router,
wherein the routing engine programs the firewall with at least a portion of the forwarding information, and
wherein, for each packet received from the forwarding engine, the firewall performs a route lookup for the packet using the portion of the forwarding information to determine an output zone for the packet.

25

30

9. The network router of any preceding claim,
wherein the user interface is a text-based interface that supports a command syntax that allows the user to specify the zones, and
wherein the stateful firewall services include multiple services including, intrusion deep packet inspection, virus scanning of application-layer data carried by the packets, layer seven security services, and
wherein the network router comprises one of a provider edge router, a Broadband Remote Access Server (BRAS), a Broadband Network Gateway (BNG), Cable Modem Termination System (CMTS), a Multi-Service Edge router (MSE), a Gateway GPRS (General Packet Radio Services) Support Node (GGSN), a Packet Data Serving Node (PDSN), or a Public Data Network Gateway (PDN-GW), a data center device that provides routing and security functions for packets flowing in or out of a data center, a peering router that serves as a point of interconnection between network service providers, or an autonomous system border router (ASBR).

35

40

10. The network router of any preceding claim, where the lists of interfaces are lists of logical interfaces, and wherein at least two or more of the VPN tunnels for the customer VPNs flow through a single physical interface of the router.

45

11. A method comprising:

executing, with a routing engine of a router, at least one protocol to establish virtual private network (VPN) tunnels for one or more customer VPNs;

presenting, with the router, a user interface by which a user specifies one or more zones to be recognized by a firewall integrated within the router, wherein the user interface supports a syntax that allows the user to define the zones by specifying one or more the customer VPNs as interfaces associated with the zones;

50

receiving, from a network, packets at a plurality of interfaces of the router;

directing, with a flow control module of a forwarding engine of the router, one or more of the received packets to the firewall for application of stateful firewall services;

55

applying stateful firewall services to the packets with the firewall of the network router based on the zones specified by the user;

after applying stateful firewall services, forwarding at least some of the packets from the firewall to the forwarding engine;

EP 2 154 834 A1

selecting next hops for the packets within the network with the forwarding engine; and
forwarding the packets to the interfaces in accordance with the selected next hops.

5 12. The method of claim 11, where the lists of interfaces are lists of logical interfaces, and wherein at least two or more of the VPN tunnels for the customer VPNs flow through a single physical interface of the router.

10 13. The method of claim 11 or 12, further comprising storing within the router configuration data that specifies the zones defined by the user, at least one of the zones specifying a collection of interfaces that includes identifiers for one or more of the customer VPNs.

15 14. The method of any one of claims 11 to 13, further comprising communicating mapping information from the routing engine to the firewall, wherein the mapping information associates VPN labels for VPN tunnels with the identifiers for the customer VPNs as specified by the user interface,
wherein for VPN tunnels for which the network router operates as an egress label switched router, the mapping information associates inner VPN labels affixed to packets received from the LSPs by the interface cards with
20 respective ones of the identifiers for the customer VPNs,
wherein for VPN tunnels for which the network router operates as an ingress label switched router, the mapping information associates pairs of a VPN label and a forwarding next hop with respective ones of the identifiers for the customer VPNs, wherein the VPN labels are to be subsequently affixed to the packets when output to the network by the forwarding engine.

25 15. The method of claim 14,
wherein the user interface allows the user to specify one or more policies for the firewall,
wherein, based on the mapping information, the firewall applies the policies to multi-protocol label switched (MPLS)
packets received from the forwarding plane that are encapsulated with at least one label, and
wherein, based on the mapping information, the firewall applies the policies to packets received from the forwarding
plane that are destined to be forwarded by the routing device.

30 16. The method of claim 11 or 12, further comprising
storing, within the router, configuration data that specifies the zones defined by the user, at least one of the zones
specifying a collection of interfaces that includes identifiers for one or more customer VPNs;
communicating mapping information from the routing engine to the firewall, wherein the mapping information asso-
ciates VPN labels used within the LSPs with the identifiers for the customer VPNs;
35 determining, for each of the received packets, whether the received packet is an MPLS packet;
when the received packet is an MPLS packet, accessing the mapping information to map an inner VPN label of
received packet to one of the identifiers for customer VPNs to determine an input zone for the received packet;
determining an output zone for the packet; and
applying one or more of the stateful firewall services to each of the packets based on the input zone and output
zone determined for the packet.

40 17. The method of claim 11, further comprising
storing, within the router, configuration data that specifies the zones defined by the user, at least one of the zones
specifying a collection of interfaces that includes identifiers for one or more of the customer VPNs;
communicating mapping information from the routing engine to the firewall, wherein the mapping information asso-
ciates VPN labels used for the VPN tunnels with the identifiers for the customer VPNs as specified by the user
45 interface;
determining, for each of the received packets, an input zone for the received packet;
performing a route lookup with the firewall to determine whether the received packet is to be output on a VPN tunnel
by the forwarding engine;
50 when the received packet is to be output on the VPN tunnel:

(1) determining from the route lookup a next hop for the packet and a VPN label that the forwarding engine will
affix to the packet when forwarding the packet; and

55 (2) accessing the mapping information to map the next hop and the VPN label to be affixed to the packet to one
of the identifiers for customer VPNs to determine an output zone for the received packet when the packet is
subsequently forwarded by the forwarding engine; and

applying one or more of the stateful firewall services to each of the packets based on the input zone and output

zone determined for the packet.

5

10

15

20

25

30

35

40

45

50

55

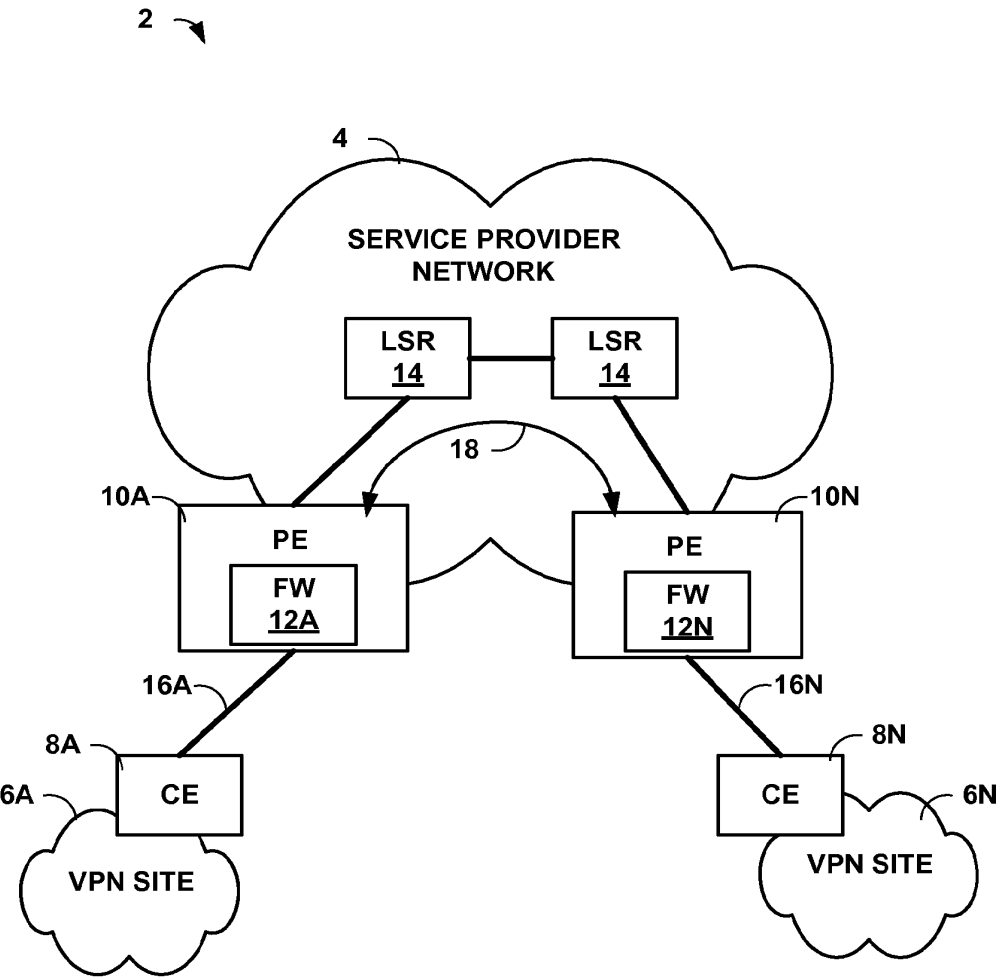


FIG. 1

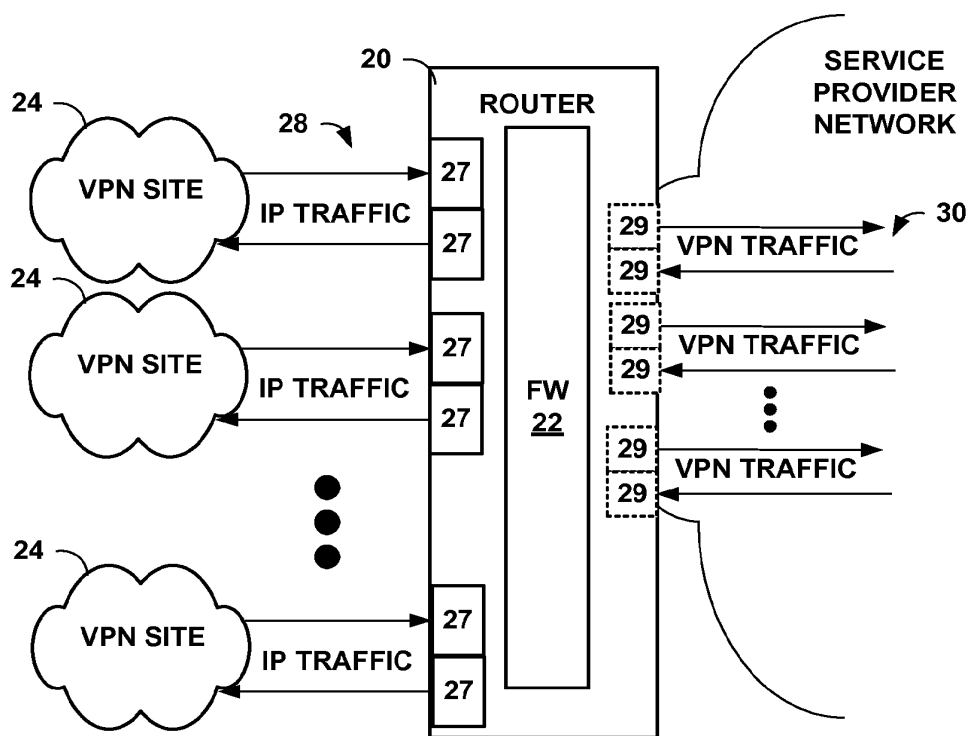


FIG. 2

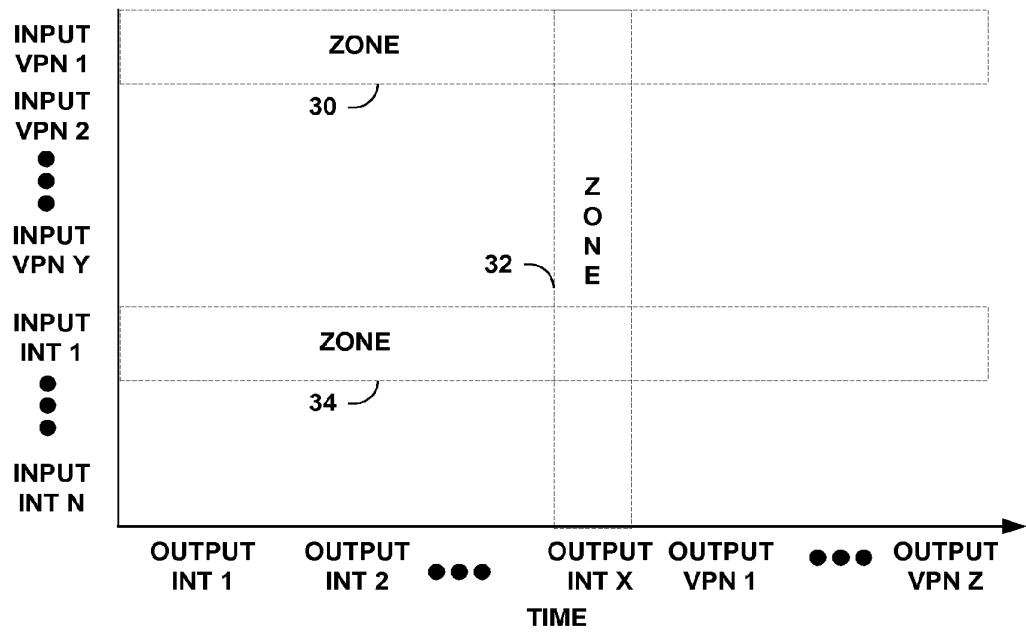


FIG. 3

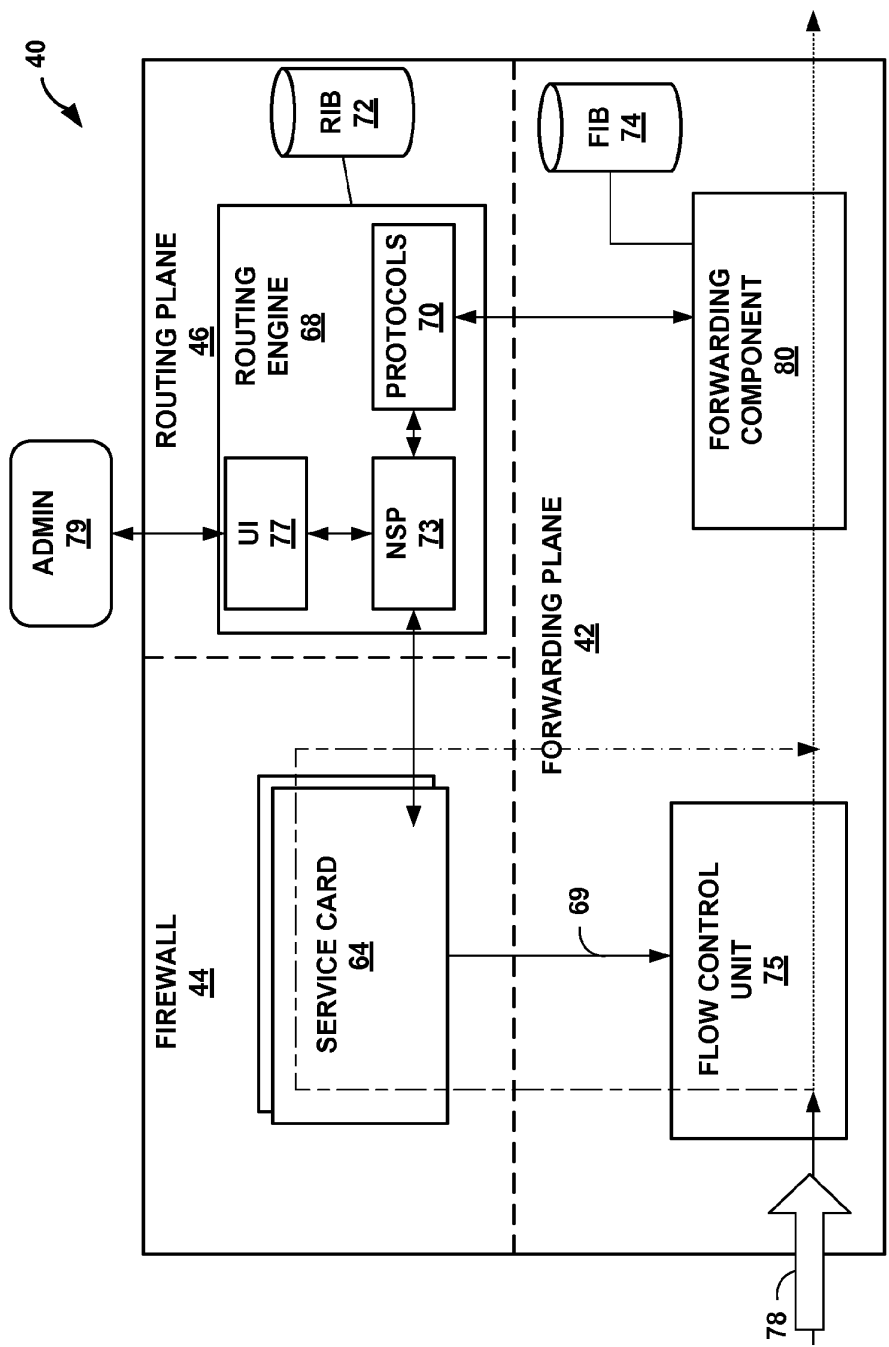
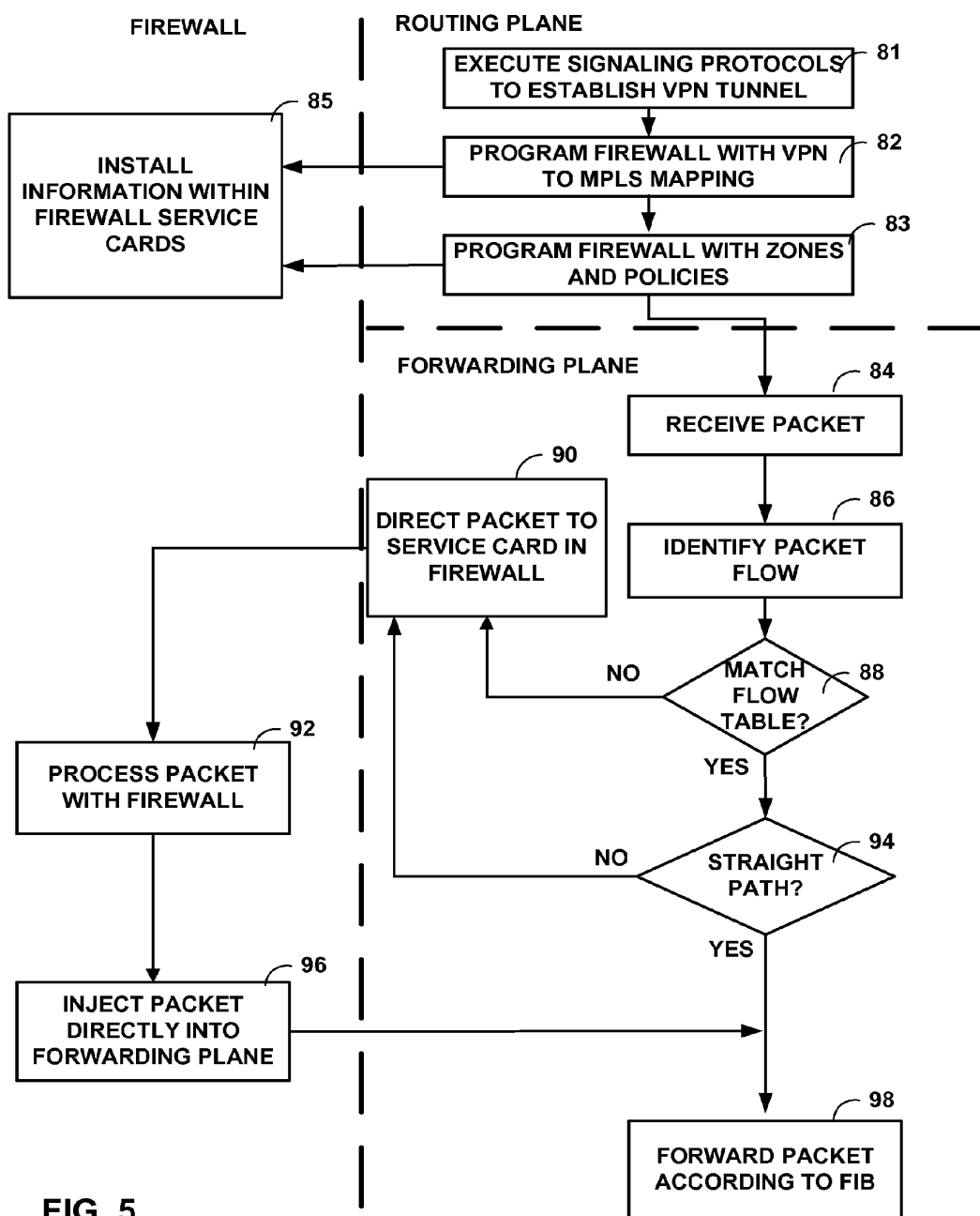


FIG. 4



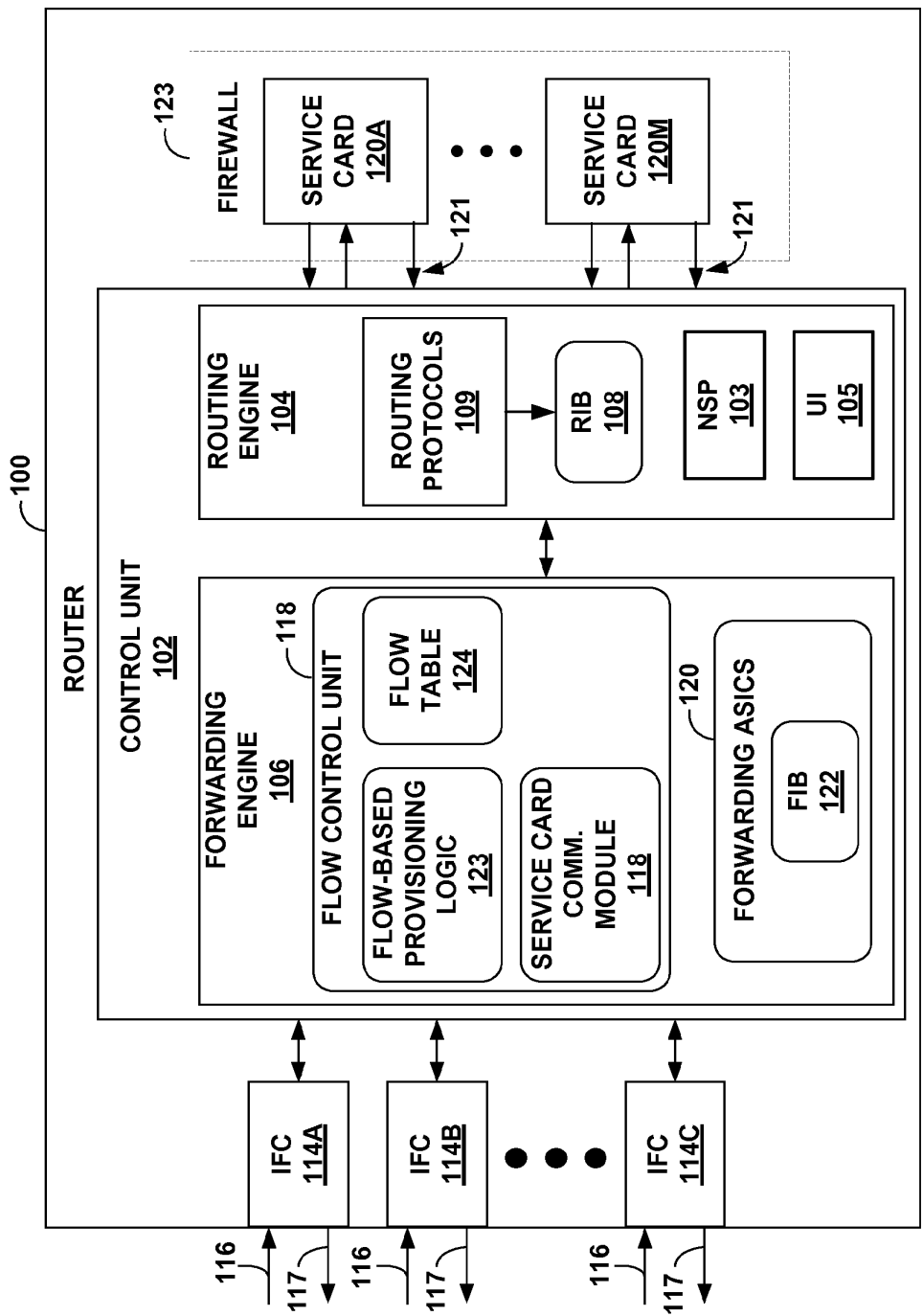


FIG. 6

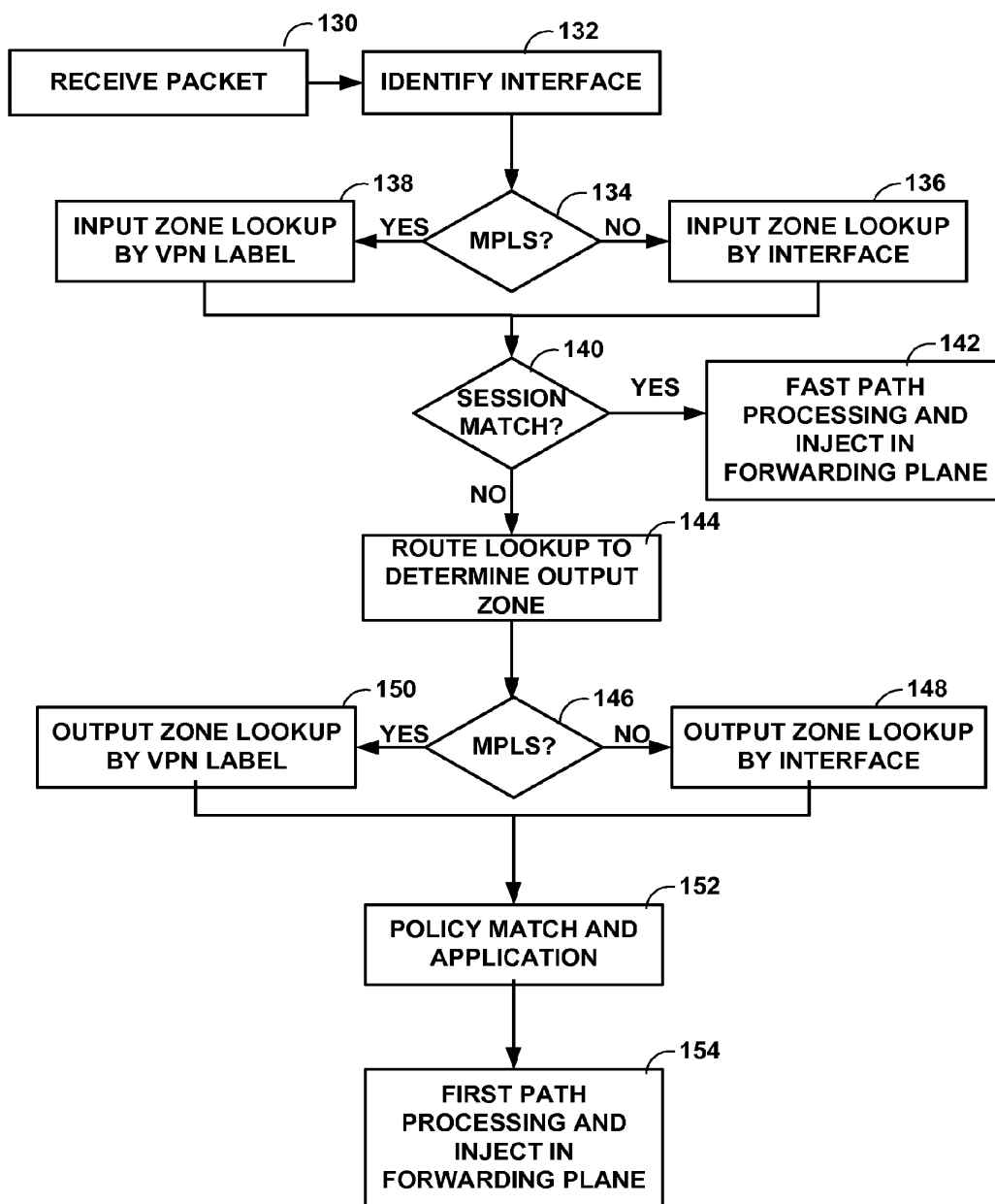


FIG. 7

160

162 VPN Identifier	164 VPN Label	166 Next Hop
VPN_customer_A	100	10.1.1.1
VPN_customer_A	750	
VPN_customer_B	200	10.1.1.2
VPN_customer_B	751	
VPN_customer_C	100	10.1.1.3
VPN_customer_C	752	

FIG. 8

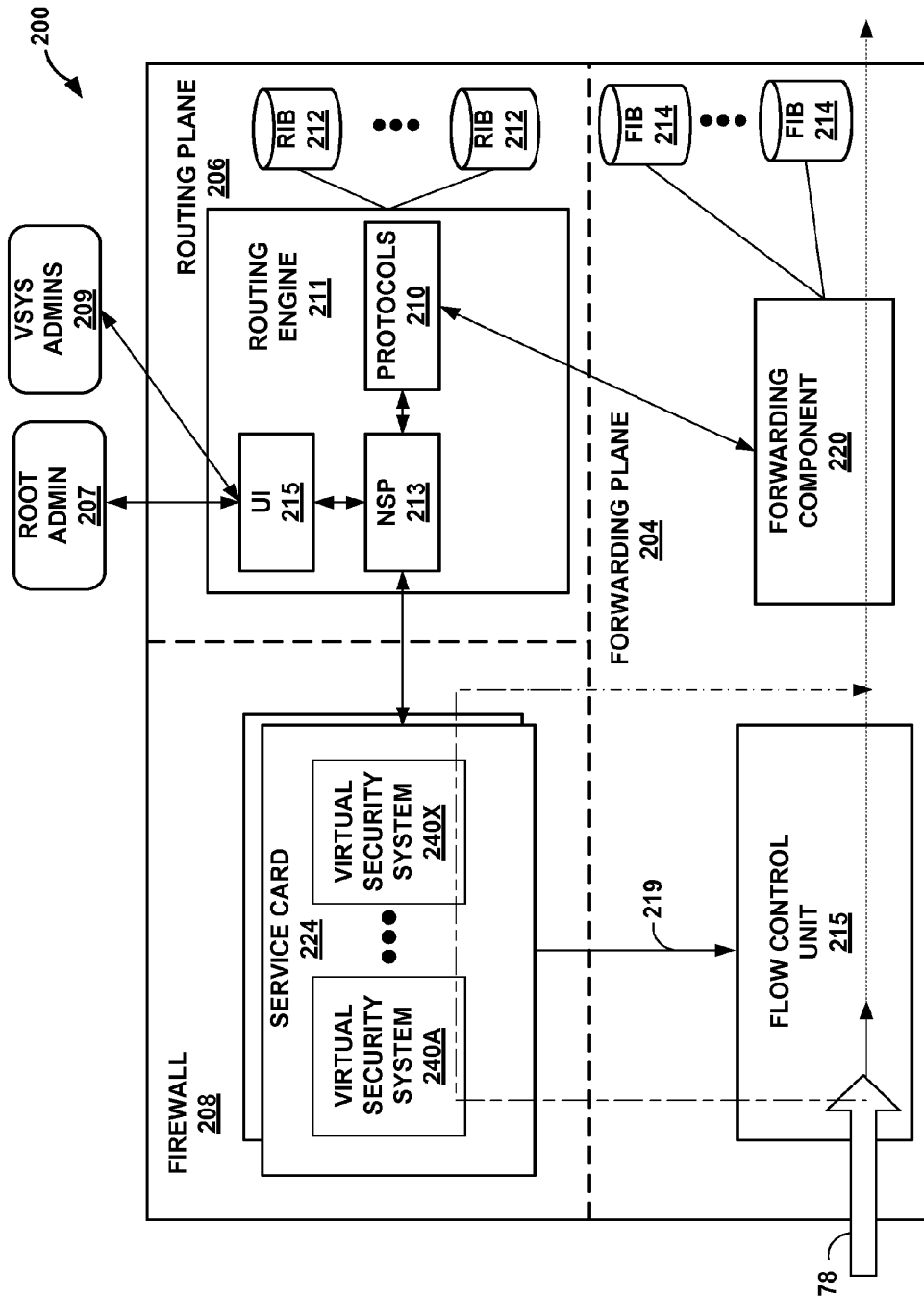


FIG. 9

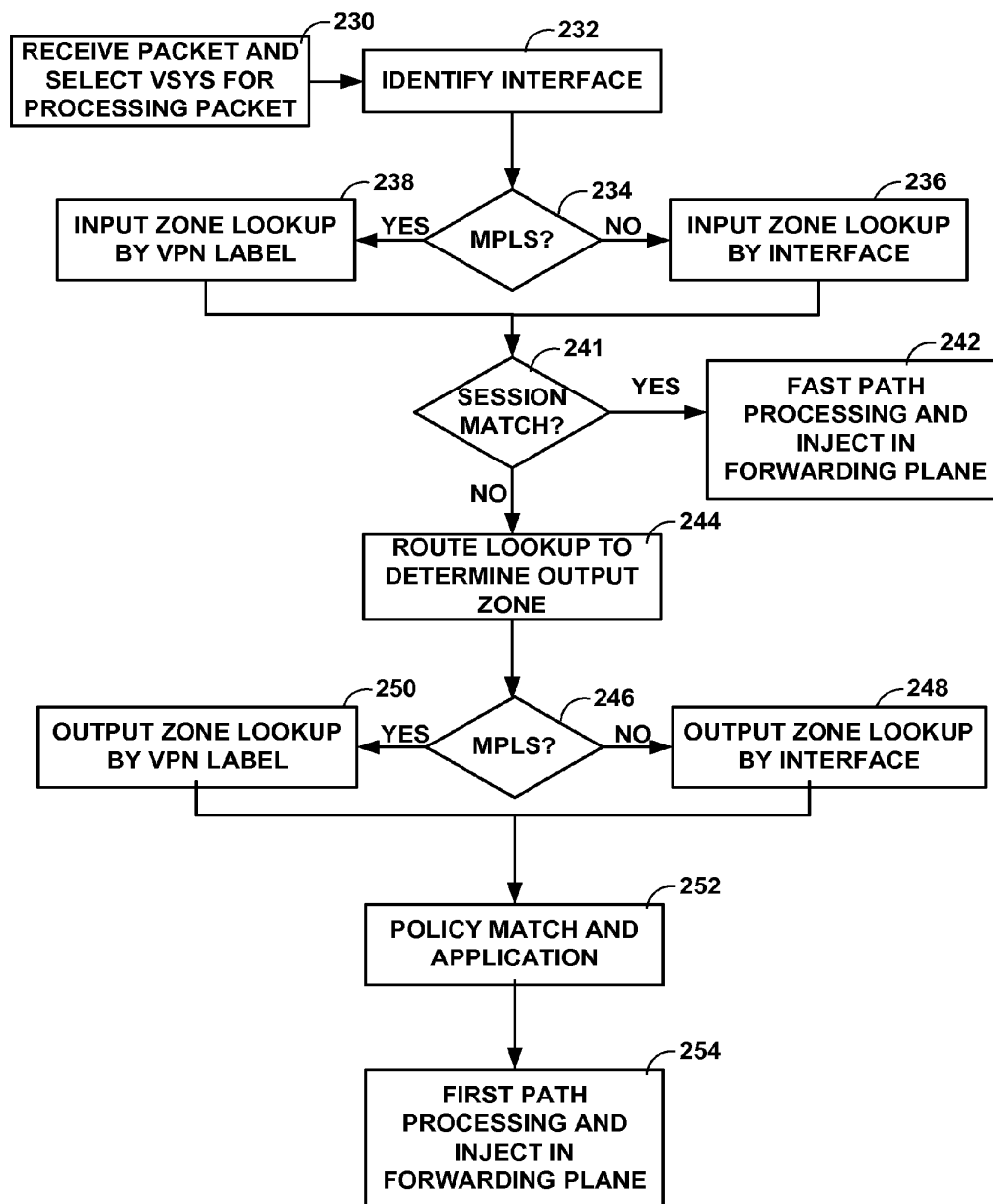
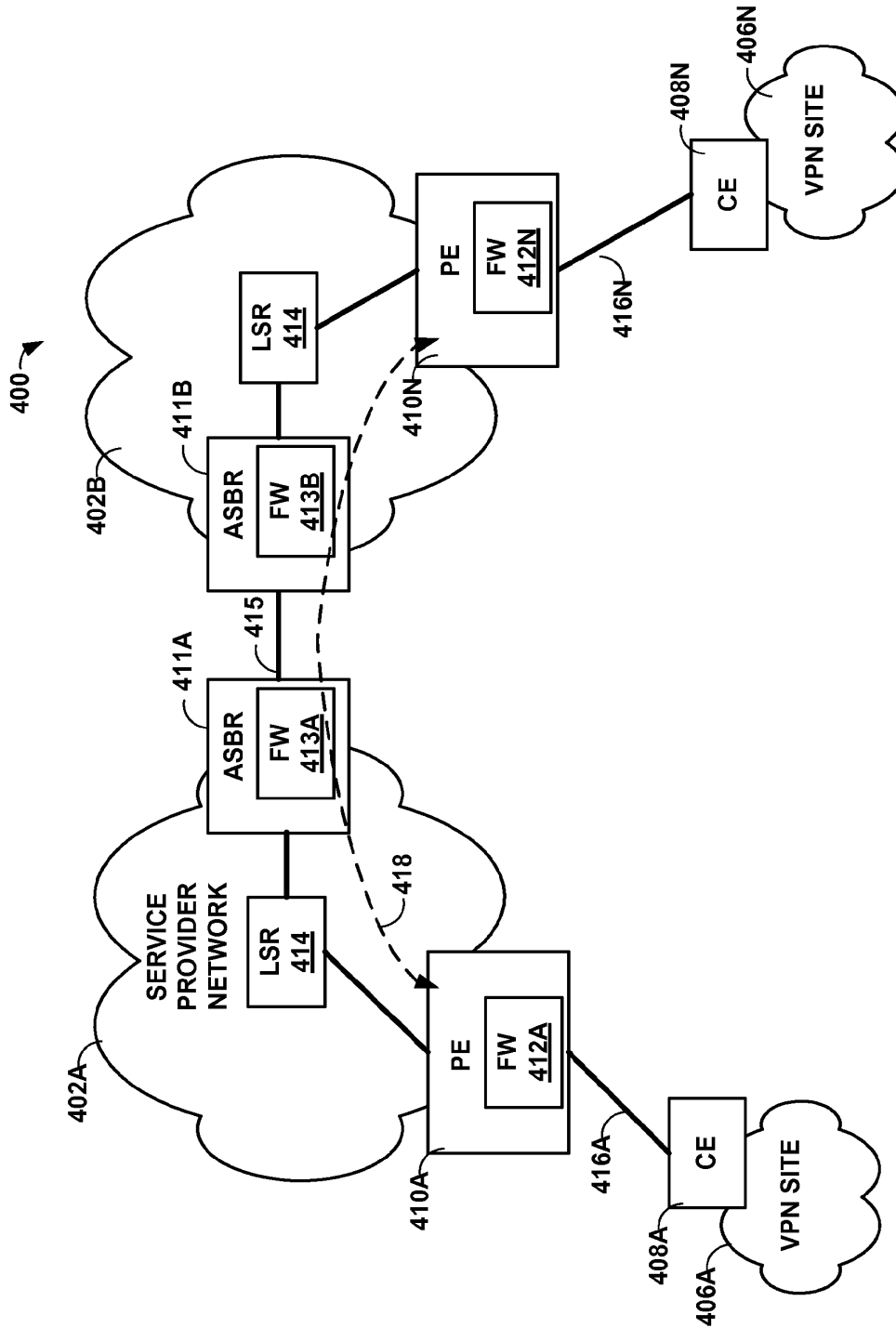


FIG. 10

300

301 VSYS ID	302 VPN ID	304 VPN Label	306 Next Hop
VSYS_customer_A	VPN_OFFICE	100	10.1.1.1
VSYS_customer_A	VPN_OFFICE	750	
VSYS_customer_A	VPN_REMOTE	200	10.1.1.2
VSYS_customer_A	VPN_REMOTE	751	
VSYS_customer_B	VPN_SITE_1	100	10.1.1.3
VSYS_customer_B	VPN_SITE_1	752	

FIG. 11





EUROPEAN SEARCH REPORT

Application Number
EP 09 16 7142

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 2007/209058 A1 (ANANTHARAMIAH PRASANNA [IN] ET AL) 6 September 2007 (2007-09-06) * abstract * * paragraphs [0001] - [0006], [0016] - [0051] * * figures 1-8 *	1-17	INV. H04L12/46 H04L29/06
X	----- "Method and System of MPLS based Firewall/Access Control" IP.COM JOURNAL, IP.COM INC., WEST HENRIETTA, NY, US, 30 May 2008 (2008-05-30), XP013125123 ISSN: 1533-0001 * the whole document * -----	1-17	
			TECHNICAL FIELDS SEARCHED (IPC)
			H04L
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 4 November 2009	Examiner Mariggis, Athanasios
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

1
EPO FORM 1503 (3.82) (P04001)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 09 16 7142

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

04-11-2009

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007209058	A1	06-09-2007	NONE

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

EP 2 154 834 A1

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 20080044181 A [0040]
- US 61054692 A [0041]
- US 7184437 B [0043]

Electronic Patent Application Fee Transmittal				
Application Number:		15546247		
Filing Date:		25-Jul-2017		
Title of Invention:		SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK		
First Named Inventor/Applicant Name:		Joseph E. RUBENSTEIN		
Filer:		Yu Yang/Nirja Shah		
Attorney Docket Number:		2210592.02085US2		
Filed as Small Entity				
Filing Fees for U.S. National Stage under 35 USC 371				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
RCE- 1ST REQUEST	2801	1	650	650
Total in USD (\$)				650

Electronic Acknowledgement Receipt	
EFS ID:	37820870
Application Number:	15546247
International Application Number:	
Confirmation Number:	9030
Title of Invention:	SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK
First Named Inventor/Applicant Name:	Joseph E. RUBENSTEIN
Customer Number:	23483
Filer:	Yu Yang/Nirja Shah
Filer Authorized By:	Yu Yang
Attorney Docket Number:	2210592.02085US2
Receipt Date:	21-NOV-2019
Filing Date:	25-JUL-2017
Time Stamp:	17:19:47
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 650
RAM confirmation Number	E2019AKH20278893
Deposit Account	080219
Authorized User	Nirja Shah
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.19 (Document supply fees)	

37 CFR 1.20 (Post Issuance fees)					
37 CFR 1.21 (Miscellaneous fees and charges)					
37 CFR 1.492 (National application filing, search, and examination fees)					
37 CFR 1.492(a) (Basic national fee only)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	2019-11-21_2085US2_RCE.PDF	1349942	no	3
			262cbe8a7d8cb54d75d0a6e1924f67d18b336685		
Warnings:					
Information:					
2	Transmittal Letter	2019-11-21_2085US2_IDSTrans.pdf	93651	no	2
			b37809beaa25e97bd4491408c75359477e9b6ebf		
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	2019-11-21_2085US2_IDSSB08.pdf	139977	no	2
			f3ee10197c2dfba6272e28057e743536394a8719		
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Foreign Reference	EP1498809A1.PDF	1742061	no	45
			2e154560b9ecaa9be2e7c2920a22e9773fb8c02a		
Warnings:					
Information:					
5	Foreign Reference	EP2154834A1.PDF	1898742	no	35
			c5724cfd228454a13eb23472b2feaf25aab15c9d		
Warnings:					
Information:					
6	Non Patent Literature	OpenRadioEquipmentInterface_Part2.PDF	15471635	no	185
			5ed58a64c58035f2c1ec4968dc1420313d55dc23		
Warnings:					

Information:					
7	Non Patent Literature	RobertRussell_IntrotoRDMAProgramming.PDF	373713	no	76
			680c4c5026b7afc7bf1ab0eee521c04e1436fb5f		
Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	30844	no	2
			37dd21fb267025b659b944d55812a921b79ef06c		
Warnings:					
Information:					
Total Files Size (in bytes):			21100565		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 15/546,247		Filing Date 07/25/2017		☐ To be Mailed		
ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO										
APPLICATION AS FILED - PART I										
		(Column 1)	(Column 2)							
FOR		NUMBER FILED	NUMBER EXTRA	RATE (\$)		FEE (\$)				
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A	N/A						
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))		N/A	N/A	N/A						
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A	N/A						
TOTAL CLAIMS (37 CFR 1.16(j))		20 minus 20 =	* 0	x \$40 =		0				
INDEPENDENT CLAIMS (37 CFR 1.16(h))		3 minus 3 =	* 0	x \$210 =		0				
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).								
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL		0				
APPLICATION AS AMENDED - PART II										
		(Column 1)	(Column 2)	(Column 3)						
AMENDMENT	11/21/2019	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)			
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	x \$50 =		0		
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	x \$230 =		0		
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
					TOTAL ADD'L FEE		0			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)			
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$0 =				
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$0 =				
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
					TOTAL ADD'L FEE					
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.					LIE					
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".					/PEGGY S YARBOROUGH/					
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".										
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

23483 7590 08/21/2019
WILMERHALE/BOSTON
60 STATE STREET
BOSTON, MA 02109

EXAMINER

POLLACK, MELVIN H

ART UNIT

PAPER NUMBER

2445

DATE MAILED: 08/21/2019

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/546,247	07/25/2017	Joseph E. RUBENSTEIN	2210592.02085US2	9030

TITLE OF INVENTION: SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	11/21/2019

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

23483 7590 08/21/2019
WILMERHALE/BOSTON
60 STATE STREET
BOSTON, MA 02109

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/546,247	07/25/2017	Joseph E. RUBENSTEIN	2210592.02085US2	9030

TITLE OF INVENTION: SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	11/21/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
POLLACK, MELVIN H	2445	709-249000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☐ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/546,247	07/25/2017	Joseph E. RUBENSTEIN	2210592.02085US2	9030
23483	7590	08/21/2019	EXAMINER	
WILMERHALE/BOSTON			POLLACK, MELVIN H	
60 STATE STREET			ART UNIT	
BOSTON, MA 02109			PAPER NUMBER	
			2445	
DATE MAILED: 08/21/2019				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 15/546,247	Applicant(s) RUBENSTEIN et al.	
	Examiner MELVIN H POLLACK	Art Unit 2445	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the amendment dated 6/21/19.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 1-20 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
a) ☒ All b) ☐ Some *c) ☐ None of the:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)	5. ☐ Examiner's Amendment/Comment
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.	6. ☐ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.	7. ☐ Other _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.	

/MELVIN H POLLACK/ Primary Examiner, Art Unit 2445	
---	--

<i>Search Notes</i> 	Application/Control No. 15/546,247	Applicant(s)/Patent Under Reexamination RUBENSTEIN et al.
	Examiner MELVIN H POLLACK	Art Unit 2445

CPC - Searched*		
Symbol	Date	Examiner
east	02/15/2019	mhp
update	08/16/2019	mhp

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
709	249	02/15/2019	MHP
	update	08/16/2019	MHP

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
east	02/15/2019	MHP
update	08/16/2019	MHP

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
	EAST	08/16/2019	MHP

/MELVIN H POLLACK/ Primary Examiner, Art Unit 2445	
---	--

<i>Index of Claims</i> 	Application/Control No. 15/546,247	Applicant(s)/Patent Under Reexamination RUBENSTEIN et al.
	Examiner MELVIN H POLLACK	Art Unit 2445

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS										
☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47										
CLAIM		DATE								
Final	Original	02/14/2019	08/16/2019							
1	1	✓	=							
2	2	✓	=							
3	3	✓	=							
4	4	✓	=							
5	5	✓	=							
6	6	✓	=							
7	7	✓	=							
8	8	✓	=							
9	9	✓	=							
10	10	✓	=							
11	11		=							
12	12		=							
13	13		=							
14	14		=							
15	15		=							
16	16		=							
17	17		=							
18	18		=							
19	19		=							
20	20		=							

Issue Classification 	Application/Control No. 15/546,247	Applicant(s)/Patent Under Reexamination RUBENSTEIN et al.
	Examiner MELVIN H POLLACK	Art Unit 2445

CPC						
Symbol					Type	Version
H04L	/	12	/	4633	F	2013-01-01
H04L	/	45	/	64	I	2013-01-01
H04L	/	45	/	12	I	2013-01-01
H04L	/	61	/	1511	I	2013-01-01
H04L	/	63	/	02	I	2013-01-01

CPC Combination Sets				
Symbol	Type	Set	Ranking	Version
/				

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/MELVIN H POLLACK/ Primary Examiner, Art Unit 2445	16 August 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	15

U.S. Patent and Trademark Office

Part of Paper No.: 20190816

Issue Classification 	Application/Control No. 15/546,247	Applicant(s)/Patent Under Reexamination RUBENSTEIN et al.
	Examiner MELVIN H POLLACK	Art Unit 2445

INTERNATIONAL CLASSIFICATION			
CLAIMED			
G06F		15	16
NON-CLAIMED			

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
709	249

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/MELVIN H POLLACK/ Primary Examiner, Art Unit 2445	16 August 2019	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	15

Issue Classification 	Application/Control No. 15/546,247	Applicant(s)/Patent Under Reexamination RUBENSTEIN et al.
	Examiner MELVIN H POLLACK	Art Unit 2445

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47
--

CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	10	10	19	19										
2	2	11	11	20	20										
3	3	12	12												
4	4	13	13												
5	5	14	14												
6	6	15	15												
7	7	16	16												
8	8	17	17												
9	9	18	18												

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 20	
/MELVIN H POLLACK/ Primary Examiner, Art Unit 2445 (Primary Examiner) _____ (Date) 16 August 2019		O.G. Print Claim(s) 1	O.G. Print Figure 15

U.S. Patent and Trademark Office

Part of Paper No.: 20190816

Bibliographic Data

Application No: 15/546,247

Foreign Priority claimed: ☒ Yes ☐ No

35 USC 119 (a-d) conditions met: ☒ Yes ☐ No ☐ Met After Allowance

Verified and Acknowledged: /MELVIN H POLLACK/

Examiner's Signature

Initials

Title: SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
07/25/2017	709	2445	2210592.02085US2
RULE			

APPLICANTS

UMBRA Technologies Ltd., Hong Kong, CHINA

INVENTORS

Joseph E. RUBENSTEIN Beijing, CHINA

Jørn Allan Dose KNUTSEN Oslo, NORWAY

Thibaud Auguste Bernard Jean SAINT-MARTIN Aubignan, FRANCE

Carlos Eduardo ORÉ Saint-Herblain, FRANCE

Fred BROUSSARD Indianapolis, IN, UNITED STATES

CONTINUING DATA

This application is a 371 of PCT/US2016/015278 01/28/2016

PCT/US2016/015278 is a CON of PCT/IB2016/000110 01/05/2016

PCT/US2016/015278 has PRO of 62266060 12/11/2015

PCT/US2016/015278 is a CON of PCT/US2015/064242 12/07/2015

PCT/US2016/015278 has PRO of 62174394 06/11/2015

PCT/US2016/015278 has PRO of 62151174 04/22/2015

PCT/US2016/015278 has PRO of 62144293 04/07/2015

PCT/US2016/015278 has PRO of 62108987 01/28/2015

FOREIGN APPLICATIONS

PCT/IB2016/000110 01/05/2016

IF REQUIRED, FOREIGN LICENSE GRANTED**

09/29/2017

** SMALL ENTITY **

STATE OR COUNTRY

CHINA

ADDRESS

WILMERHALE/BOSTON
60 STATE STREET
BOSTON, MA 02109
UNITED STATES

FILING FEE RECEIVED

\$1,030

EAST Search History**EAST Search History (Prior Art)**

< This search history is empty >

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1773	(access adj point\$1).clm. and tunnel\$4.clm.	US-PGPUB; USPAT	OR	OFF	2019/08/16 20:34
L2	31	L1 and intermediate.clm.	US-PGPUB; USPAT	OR	OFF	2019/08/16 20:34
L3	23	L1 and (server\$1 near2 control).clm.	US-PGPUB; USPAT	OR	OFF	2019/08/16 20:35

8/ 16/ 2019 8:35:44 PM**C:\ Users\ mpollack\ Documents\ EAST\ Workspaces\ 15546247.wsp**

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	145	(RUBENSTEIN near2 Joseph).in. or (KNUTSEN near2 (Jorn or Allan or Dose)).in. or (SAINT\$1MARTIN near2 (Thibaud or Auguste or Bernard or Jean)).in. or (ORE near2 (Carlos or Eduardo)).in. or (BROUSSARD near2 Fred).in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/08/16 16:49
L2	501	umbra.as.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/08/16 16:49
L3	2405	709/249.ccls.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L4	20038	(H04L12/4633 or H04L45/12 or H04L45/64 or H04L61/1511 or H04L63/02).cpc.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L5	22309	L3 or L4	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L6	152167	(virtual near2 network\$4) and (@ad<="20150128" or @rlad<="20150128")	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L7	2939	L6 and endpoint\$1 and tunnel\$4 and (access adj point\$1)	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L8	981	L7 and (server\$1 near2 control\$4)	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L9	2405	709/249.ccls.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L10	20038	(H04L12/4633 or H04L45/12 or H04L45/64 or H04L61/1511 or H04L63/02).cpc.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L11	22309	L9 or L10	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L12	137	L8 and L11	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L13	517	L8 and DNS	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L14	615	L8 and (cache or caching)	US-PGPUB;	OR	OFF	2019/08/16

			USPAT; USOCR			16:49
L15	824	L8 and firewall\$1	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L16	943	L13 or L14 or L15	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L17	359	L13 and L14 and L15	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L18	935	L16 and (route\$4 or routing)	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L19	2	L18 and (smart near2 (route or routing))	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L20	462	L12 or L17 or L19	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L21	668	L18 and ((route or routing) same (bandwidth or latency or hops or (packet adj loss) or realtime or real\$1time or (real adj time) or histor\$6 or statistic\$6))	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L22	250	L21 and (DNS same (lookup or cache or caching))	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L23	464	L20 or L22	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:49
L24	28414	(tunnel\$4 and (access adj point\$1)) and (@ad<="20150128" or @rlad<="20150128")	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:53
L25	1642	L24 and (intermediate near3 (access or point\$1 or server\$1))	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:53
L26	92	L25 and L11	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:54
L27	192	L25 and (tunnel\$4 near4 (end or "end-to-end"))	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:54
L28	66	L25 and (tunnel\$4 near4 select\$4)	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:55
L29	626	L25 and (DNS or "domain name system")	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:56
L30	580	L29 and ((smart adj routing) or firewall\$1 or bandwidth or latency or hop\$1 or loss)	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:58
L31	779	L26 or L27 or L28 or L30	US-PGPUB; USPAT; USOCR	OR	OFF	2019/08/16 16:59

EAST Search History (Interference)

EAST Search History

< This search history is empty >

8/ 16/ 2019 5:03:32 PM

C:\ Users\ mpollack\ Documents\ EAST\ Workspaces\ 15546247.wsp

Docket No.: 2210592.20085US2
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Joseph E. Rubenstein et al. Confirmation No.: 9030
Application No.: 15/546,247 Art Unit: 2445
Filed: July 25, 2017 Examiner: M. H. Pollack
Title: SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION UNDER 37 C.F.R. § 1.111

Dear Commissioner:

INTRODUCTORY COMMENTS

In response to the Office Action dated February 21, 2019, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 6 of this paper.

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Currently amended) A network system ~~for connecting devices via a global virtual network,~~ comprising:
 - a first device ~~in communication with a first endpoint device;~~
 - a second device ~~in communication with a second endpoint device;~~ and
 - a ~~communication path~~ plurality of intermediate access point servers that form a plurality of end-to-end tunnels connecting the first device and the second end-point device; and
 - a control server, wherein the control server receives information from at least one of the plurality of intermediate access point servers, and wherein the control server selects one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information

~~further comprising one or more intermediate tunnels connecting each endpoint device to one or more intermediate access pointer servers and one or more control servers.~~
2. (Currently amended) The network system according to claim 1, wherein at least one of the first ~~end-point~~ device ~~[[and]]~~ or the plurality of intermediate access point servers is configured to perform a domain name system ~~Domain Name System~~ lookup to locate the second device.
3. (Currently amended) The network system according to claim 1, wherein at least one of the ~~[[the]] first end-point device~~ ~~[[and]]~~ or the plurality of intermediate access point servers is configured to perform a domain name system ~~Domain Name System~~ lookup from a cache to locate the second device.
4. (Currently amended) The network system according to claim 1, wherein at least one of the plurality of intermediate access point servers is configured to cache content.

5. (Currently amended) The network system according to claim 1, wherein at least one of the ~~end-point~~ first device[[s]], the second ~~endpoint~~ device, [[and]] or the plurality of intermediate access point servers is configured to perform smart routing.

6. (Currently amended) The network system according to claim 5, wherein the smart routing is based on at least one of best bandwidth, lowest latency, fewest hops, [[and]] or no packet loss.

7. (Currently amended) The network system according to claim 5, wherein the smart routing is based on at least one of real-time statistics [[and]] or historical statistics.

8. (Currently amended) The network system according to claim 1, wherein at least one of the ~~end-point~~ first device[[s]], the second device, or [[and]] the plurality of intermediate access point servers is configured to perform firewall services.

9. (Currently amended) The network system according to claim 8, wherein the first ~~endpoint~~ device provides firewall services between the first device and the plurality of intermediate access point servers.

10. (Currently amended) The network system according to claim 8, wherein [[an]] a first intermediate access point server among the plurality of intermediate access point servers provides firewall services between [[a]] the first ~~endpoint~~ device and other intermediate access point servers among the plurality of intermediate access point servers or the second ~~endpoint~~ device.

11. (New) A method comprising:

establishing, by one or more computer processors, a plurality of end-to-end tunnels between a first device and a second device, the plurality of end-to-end tunnels being configured to carry network traffic via a plurality of intermediate access point servers;

receiving, by the one or more computer processors, information from at least one of the plurality of intermediate access point servers; and

selecting, by the one or more computer processors, one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information.

12. (New) The method according to claim 11, further comprising configuring, by the one or more computer processors, at least one of the first device or the plurality of intermediate access point servers to perform a domain name system lookup to locate the second device.

13. (New) The method according to claim 11, further comprising configuring, by the one or more computer processors, at least one of the first device or the plurality of intermediate access point servers to perform a domain name system lookup from a cache to locate the second device.

14. (New) A system comprising:

a memory storing instructions; and
one or more processors coupled to the memory, the one or more processors being configured to execute the instructions, the instructions causing the one or more processors to perform operations comprising:

establishing a plurality of end-to-end tunnels between a first device and a second device, the plurality of end-to-end tunnels being configured to carry network traffic via a plurality of intermediate access point servers;

receiving information from at least one of the intermediate access point servers; and

selecting one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information.

15. (New) The system according to claim 14, wherein the operations further comprise configuring at least one of the first device, the second device, or the plurality of intermediate access point servers to perform smart routing.

16. (New) The system according to claim 15, wherein the smart routing is based on at least one of best bandwidth, lowest latency, fewest hops, or no packet loss.

17. (New) The system according to claim 15, wherein the smart routing is based on at least one of real-time statistics or historical statistics.

18. (New) The system according to claim 14, wherein the operations further comprise configuring at least one of the first device, the second device, or the plurality of intermediate access point servers is configured to perform firewall services.

19. (New) The system according to claim 18, wherein the first device provides firewall services between the first device and the plurality of intermediate access point servers.

20. (New) The system according to claim 18, wherein a first intermediate access point server among the plurality of intermediate access point servers provides firewall services between the first device and other intermediate access point servers among the plurality of intermediate access point servers or the second device.

REMARKS

I. Status of the Claims

Claims 1-10 are pending in the present application (“Application”). In this response, claims 1-10 have been amended, and new claims 11-20 have been added. Support for the claim amendments can be found throughout the as-filed specification including, for example, paragraphs [0155], [0175], [0228], [0336] and Figures 33-35. No new matter has been added. Upon entry of the amendments, claims 1-20 will be pending. Applicant requests reconsideration and allowance of the Application in view of the following comments.

II. Claim Rejection Under 35 U.S.C § 112

Claims 1-10 stand rejected under 35 U.S.C. § 112(b) as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor regards as the invention. Specifically, the Office Action states that the terms “access pointer” in claim 1, “access point servers” and “end point device” in claims 2 and 3, and “intermediate access” in claim 4 lack antecedent basis. (Office Action, p. 2). The Office Action further identifies the term “global virtual network” in the preamble of claim 1 as being indefinite. (*Id.*, p. 3). Dependent claims 5-10 were rejected based on their dependency from claim 1. (*Id.*, p. 2).

By this Amendment, Applicant amends claims 1-4 to remove the terms “access pointer” and “end point device” and address the antecedent basis issues associated with the term “access point servers” identified in the Office Action. Applicant further amends the preamble of claim 1 to remove the term “global virtual network.” Applicant respectfully submits that these amendments address each of the issues identified in the Office Action.

Thus, claims 1-10, as amended, are not indefinite under 35 U.S.C. § 112(b). Applicant respectfully requests that the Office reconsider and withdraw the rejections.

III. Claim Rejections Under 35 U.S.C § 102

Claims 1-4, 8, and 9 stand rejected under 35 U.S.C. § 102(a)(2) as being anticipated by U.S. Pat. App. Publ. No. 2014/0359704 to Chen (“Chen,” also referred to in the Office Action as

“Kingston Digital”). Applicant respectfully traverses these rejections in view of the following comments.

A. Claim 1

Independent claim 1, as amended, recites “a plurality of intermediate access point servers that form *a plurality of end-to-end tunnels connecting the first device and the second device*” and “a control server, wherein the control server receives information from at least one of the intermediate access point servers, and wherein *the control server selects one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information*.” (Emphases added).

Chen generally discloses techniques for establishing a “private network service [that is] manageable and accessible by the at least one smart device client from anywhere at anytime without utilizing a public cloud based routing server.” (Chen, Abstract). For example, Chen teaches that “a Smart Device Client 101, 107 or 109 can connect to the Private Cloud Server 108.” (*Id.*, ¶ 0053). Chen further teaches that “[a]ll communication between the Smart Device Client 109 and the Private Cloud Server 108 are encapsulated under the VPN protocol.” (*Id.*, ¶ 0059).

The Office Action identifies the Smart Device Clients 101, 107 or 109 of Chen as corresponding to “endpoint devices,” as recited by claim 1. (Office Action, pp. 3-4). The Office Action further identifies the encapsulation of communications between Smart Device Clients 101, 107 or 109 and Private Cloud Server 108 under the VPN protocol as corresponding to an “intermediate tunnel,” as recited by claim 1. (*Id.*, p. 4). Applicant disagrees that Chen teaches these limitations. However, even assuming, *arguendo*, that the Smart Device Clients 101, 107 or 109 constitute “endpoint devices” and that the encapsulation of communications under the VPN protocol constitutes an “intermediate tunnel,” Chen does not teach “a plurality of end-to-end tunnels connecting the first device and the second device,” as recited by amended claim 1. For example, to the extent that Chen teaches the use of the VPN protocol to encapsulate “communication *between the Smart Device Client 109 and the Private Cloud Server 108*,” (Chen, ¶ 0059 (emphasis added)), nowhere does Chen teach the use of the VPN protocol to encapsulate communications *between pairs of Smart Device Clients 101, 107, or 109* (i.e., the purported endpoint devices). Furthermore,

even if a pair of clients among Smart Device Clients 101, 107, or 109 were to communicate with each other via separately established VPN links to Private Cloud Server 108, the separate VPN links would not constitute a “plurality of end-to-end tunnels” between the pair of clients. Specifically, Chen does not teach that the Private Cloud Server 108 joins multiple VPN links to provide end-to-end encapsulation and consequently the VPN links would not form a “plurality of end-to-end tunnels.” Consequently, Chen does not teach a “plurality of end-to-end tunnels” as recited by amended claim 1. For at least this reason, Chen also does not teach a “control server [that] selects one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information,” as recited by amended claim 1. Accordingly, Chen fails to teach “a plurality of intermediate access point servers that form a plurality of end-to-end tunnels connecting the first device and the second device” and “a control server, wherein the control server receives information from at least one of the intermediate access point servers, and wherein the control server selects one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information,” as recited by amended claim 1.

Thus, claim 1 is allowable over Chen. Applicant respectfully requests that the Office reconsider and withdraw the rejection.

B. Claims 2-4, 8 and 9

Each of dependent claims 2-4, 8 and 9 depends, directly or indirectly, from claim 1. Accordingly, each of these dependent claims is also patentable over Chen, at least based on their dependency. Applicant respectfully requests that the Office reconsider and withdraw the rejections.

IV. Claim Rejections Under 35 U.S.C § 103

A. Claims 5-7

Claims 5-7 stand rejected under 35 U.S.C. § 103 as being unpatentable over Chen as applied to claim 1 above, and further in view of U.S. Pat. No. 8,611,355 to Sella *et al.* (“Sella,” also referred to in the Office Action as “TW Telecom”). Applicant respectfully traverses these rejections in view of the following comments.

Each of dependent claims 5-7 depends, directly or indirectly, from claim 1. Accordingly, each of these dependent claims is also patentable over Chen, at least based on their dependency.

Sella fails to cure the above-identified deficiencies of Chen. Sella is directed to techniques for “rout[ing] data streams in an intelligent manner based on global network knowledge without requiring initial packets to be buffered at an edge router.” (Sella, 2:34-36). A virtual router of Sella “gather[s] information related to network operation such as traffic load, link latencies, link jitter, link packet loss, and link failures [and] provide[s] an optimized route for a data stream.” (*Id.*, 2:41-44).

The Office Action relies on Sella for limitations associated with “smart routing.” (Office Action, p. 7). Applicant disagrees that Sella teaches these limitations. However, even assuming, *arguendo*, that Sella teaches “smart routing,” Sella does not further teach or suggest “a plurality of end-to-end tunnels connecting the first device and the second device,” as recited by amended claim 1. In fact, Sella is silent regarding a tunnel. Accordingly, Sella fails to teach or suggest “a plurality of intermediate access point servers that form a plurality of end-to-end tunnels connecting the first device and the second device” and “a control server, wherein the control server receives information from at least one of the intermediate access point servers, and wherein the control server selects one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information,” as recited by amended claim 1.

Thus, claims 5-7 are patentable over the combination of Chen and Sella. Applicant respectfully requests reconsideration and withdrawal of these rejections.

B. Claim 10

Claim 10 stands rejected under 35 U.S.C. § 103 as being unpatentable over Chen as applied to claim 1 above, and further in view of U.S. Pat. App. Publ. No. 2009/0217109 to Sekaran *et al.* (“Sekaran”). Applicant respectfully traverses this rejection in view of the following comments.

Claim 10 depends from claim 1. Accordingly, claim 10 is patentable over Chen, at least based on its dependency.

Sekaran fails to cure the above-identified deficiencies of Chen. Sekaran is directed to techniques for detecting “[e]ndpoint crashes in a real time communication system.” (Sekaran, Abstract). The communication system of Sekaran includes a “[f]irewall 232 [that] provides protection for connections with other networks such as Internet 220, [and an] edge server 234 [that] provides connectivity through the perimeter network.” (*Id.*, 2:41-44).

The Office Action relies on Sekaran for limitations associated with “firewall services.” (Office Action, p. 8). Applicant disagrees that Sekaran teaches these limitations. However, even assuming, *arguendo*, that Sekaran teaches “firewall services,” Sekaran does not further teach or suggest “a plurality of end-to-end tunnels connecting the first device and the second device,” as recited by amended claim 1. In fact, Sekaran is silent regarding a tunnel. Accordingly, Sekaran fails to teach or suggest “a plurality of intermediate access point servers that form a plurality of end-to-end tunnels connecting the first device and the second device” and “a control server, wherein the control server receives information from at least one of the intermediate access point servers, and wherein the control server selects one of the plurality of end-to-end tunnels for communication between the first and second devices based on the information,” as recited by amended claim 1.

Thus, claim 10 is patentable over the combination of Chen and Sekaran. Applicant respectfully requests reconsideration and withdrawal of this rejection.

IV. New Claims

New independent claims 11 and 14 recite features that are substantially similar to those of amended claim 1. Accordingly, claims 11 and 14 are allowable for at least the same reasons as claim 1. Each of new dependent claims 12, 13, and 15-20 depends, directly or indirectly, from claims 11 or 14. Accordingly, each of these dependent claims is also allowable, at least based on their dependency. Applicant respectfully requests allowance of the new claims.

CONCLUSION

In view of the above response, Applicant believes the pending application is in condition for allowance.

Applicant submits a one-month extension fee with this response. Applicant believes no additional fee is due with this response. However, in the event the U.S. Patent and Trademark Office determines that a fee is required, Applicant petitions for any required relief including extensions of time and authorizes the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to Deposit Account No. 08-0219 under Order No. 2210592.20085US2.

Respectfully submitted,

Dated: June 21, 2019

/Yu Yang/
Yu Yang
Registration No.: 68,839
Attorney for Applicant(s)

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000 (telephone)
(617) 526-5000 (facsimile)

Electronic Patent Application Fee Transmittal				
Application Number:		15546247		
Filing Date:		25-Jul-2017		
Title of Invention:		SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK		
First Named Inventor/Applicant Name:		Joseph E. RUBENSTEIN		
Filer:		Brian James Lambson/Arann Capri		
Attorney Docket Number:		2210592.02085US2		
Filed as Small Entity				
Filing Fees for U.S. National Stage under 35 USC 371				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension - 1 month with \$0 paid	2251	1	100	100
Miscellaneous:				
Total in USD (\$)				100

Electronic Acknowledgement Receipt	
EFS ID:	36374694
Application Number:	15546247
International Application Number:	
Confirmation Number:	9030
Title of Invention:	SYSTEM AND METHOD FOR A GLOBAL VIRTUAL NETWORK
First Named Inventor/Applicant Name:	Joseph E. RUBENSTEIN
Customer Number:	23483
Filer:	Brian James Lambson/Arann Capri
Filer Authorized By:	Brian James Lambson
Attorney Docket Number:	2210592.02085US2
Receipt Date:	21-JUN-2019
Filing Date:	25-JUL-2017
Time Stamp:	16:35:43
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$100
RAM confirmation Number	062419INTEFSW16362000
Deposit Account	080219
Authorized User	Arann Capri
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.19 (Document supply fees)	

37 CFR 1.20 (Post Issuance fees)					
37 CFR 1.21 (Miscellaneous fees and charges)					
37 CFR 1.492 (National application filing, search, and examination fees)					
37 CFR 1.492(a) (Basic national fee only)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		2019-06-21_2085_US2_Non-Final_Office_Action_Response.pdf	242412	yes	11
			ada81be1130c73a0f9c6ea245f8ef38e73c8b640		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	5	
	Applicant Arguments/Remarks Made in an Amendment		6	11	
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30904	no	2
			d9dc8678bd5df8bb6c1d85608363e29f798c97be		
Warnings:					
Information:					
Total Files Size (in bytes):			273316		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 15/546,247		Filing Date 07/25/2017		☐ To be Mailed		
ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO										
APPLICATION AS FILED - PART I										
		(Column 1)	(Column 2)							
FOR		NUMBER FILED	NUMBER EXTRA	RATE (\$)		FEE (\$)				
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A	N/A						
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))		N/A	N/A	N/A						
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A	N/A						
TOTAL CLAIMS (37 CFR 1.16(j))		minus 20 =	*	x \$40 =						
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 =	*	x \$210 =						
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).								
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL						
APPLICATION AS AMENDED - PART II										
		(Column 1)	(Column 2)	(Column 3)						
AMENDMENT	06/20/2019	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)			
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	x \$50 =		0		
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	x \$230 =		0		
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE		0		
AMENDMENT		(Column 1)	(Column 2)	(Column 3)						
		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)			
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$0 =				
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$0 =				
	☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
						TOTAL ADD'L FEE				
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.						LIE				
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".						/GAIL D WOOTEN/				
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".										
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/546,247	07/25/2017	Joseph E. RUBENSTEIN	2210592.02085US2	9030
23483	7590	02/21/2019	EXAMINER	
WILMERHALE/BOSTON			POLLACK, MELVIN H	
60 STATE STREET			ART UNIT	
BOSTON, MA 02109			PAPER NUMBER	
			2445	
			NOTIFICATION DATE	
			DELIVERY MODE	
			02/21/2019	
			ELECTRONIC	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

teresa.maia@wilmerhale.com
whipusptopairs@wilmerhale.com

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Claim Rejections - 35 USC § 112

2. The following is a quotation of 35 U.S.C. 112(b):
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-10 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.
4. Claim 1 recites the limitation "access pointer servers". There is insufficient antecedent basis for this limitation in the claim. Claim 1 and accompanying spec does not have antecedent basis for the term "access pointer" as recited. For the purpose of the office action, the term "access pointer" in claim 1 is interpreted as "access point", which provides proper antecedent basis.
5. Claims 2-10 inherit this deficiency while introducing their own deficiencies. Claims 2 and 3 use "access point servers" but they also use "end point device" instead of "endpoint device." Claim 4 uses "[an] intermediate access" as a noun, which may refer to the access point servers. Other typographical errors may populate the other claims.

6. Additionally, claim 1 uses the term “global virtual network” in the preamble. None of the other claim limitations reference any virtual network structure or functionality, nor do they recite problems or operations specific to a virtual rather than physical network, making the term indefinite unless meant to be “intended use.” The claims may be rejected by art in traditional or other forms of networks.

Claim Rejections - 35 USC § 102

7. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

9. Claim(s) 1-4, 8 and 9 is/are rejected under 35 U.S.C. 102(a)(2) as being anticipated by Kingston Digital (2014/0,359,704).

10. Regarding Claim 1, Kingston Digital discloses a network system for connecting devices via a global virtual network (Private Network Service by itself is designed to be managed and accessed on the private network environment, be it wired or wireless, by the Smart Device Client, para. [0041]), comprising:

- a. a first device in communication with a first endpoint device (a Smart Device Client [first endpoint device] 101, 107 or 109 can connect to [...] the public cloud 100

- [first device], para. [0053]; a Smart Device Client 101 [...] Smart Device Clients 109, 110 and 111 [...] Any one of the Smart Device Clients above is interchangeable, para. [0051-52], Fig IB);
- b. a second device in communication with a second endpoint device (a Smart Device Client [second endpoint device] 101, 107 or 109 can connect to [...] the public cloud 100 [second device; a cloud typically comprises multiple devices], para. [0053]; a Smart Device Client 101 [...] Smart Device Clients 109, 110 and 111 [...] Any one of the Smart Device Clients above is interchangeable, para. [0051-52], Fig IB); and a communication path connecting the first and second endpoint device (Behind the LAN 105 [communication path], there are Smart Device Clients 109, 110 and 111 [first and second endpoint device], para. [0073], Fig IB) further comprising
- c. one or more intermediate tunnels connecting each endpoint device to one or more intermediate access point servers and one or more control servers (Smart Device Client 109 [endpoint device] then logs in to the VPN Routing Server 114 [access point server] [...] the VPN Routing Server 114 is a middleman [intermediate] during all communication transactions between the Smart Device Client 109 and the Private Cloud Server 108, para. [0060]; the Smart Device Client 109 and sets up a Virtual Private Network 302 [intermediate tunnel] [...] All communication between the Smart Device Client 109 [endpoint device] and the Private Cloud Server 108 [control server] are encapsulated under the VPN protocol [intermediate tunnel], para. [0059]).
11. Regarding Claim 2, Kingston Digital discloses at least one of the first end point device and the intermediate access point servers is configured to perform a Domain Name System lookup to locate the second device (Smart Device Client 109 [first end point device] then logs in

to the VPN Routing Server 114 [intermediate access point servers] and looks up the virtual IP address of the Private Cloud Server 108 [second device], para. [0055]).

12. Regarding Claim 3, Kingston Digital discloses at least one of the first end point device and the intermediate access point servers is configured to perform a Domain Name System lookup from a cache to locate the second device (Smart Device Client 109 [first end point device] then logs in to the VPN Routing Server 114 [intermediate access point servers] and looks up the virtual IP address of the Private Cloud Server 108 [second device], para. [0055]; the VPN Routing Server 114 is a middleman during all communication transactions [...] It may hold [cache] all user account information, password and their corresponding IP addresses, para. [0061]).

13. Regarding Claim 4, Kingston Digital discloses at least one of the intermediate access is configured to cache content (the VPN Routing Server 114 is a middleman during all communication transactions [...] It may hold [cache] all user account information, password and their corresponding IP addresses, para. [0061]).

14. Regarding Claim 8, Kingston Digital discloses at least one of the end point devices and the intermediate access point servers is configured to perform firewall services (allow a Client [endpoint devices] to be able to access the Private Network Service [...] behind a firewall with fixed or dynamic IP, para. [0050]).

15. Regarding Claim 9, Kingston Digital discloses the first endpoint device provides firewall services between the first device and the intermediate access point servers (Access the Private Cloud Routing Server (PCRS) [access point servers] (...) Access the PCRS behind the firewall, para. [0043-44]; allow a Client [endpoint devices] to be able to access [...] behind a firewall with fixed or dynamic IP, para. [0050]).

Claim Rejections - 35 USC § 103

16. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

17. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

18. Claims 5-7 is/are rejected under 35 U.S.C. 103 as being unpatentable over Kingston Digital as applied to claim 1 above, and further in view of TW Telecom (8,611,355).

19. Regarding Claim 5, Kingston Digital fails to explicitly disclose at least one of the end point devices and the intermediate access point servers is configured to perform smart routing.

20. TW Telecom is in a related field of a network connecting endpoint routers using routing servers (Abstract).

21. TW Telecom teaches at least one of the end point devices and the intermediate access point servers is configured to perform smart routing (To route data, embodiments use a virtual routing server [access point server] [...] the virtual router is in the best position to provide an optimized route [smart routing] for a data stream, Col 2 Ln 37-44)

22. It would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of TW Telecom to incorporate the teachings regarding the intermediate access point servers is configured to perform smart routing in the invention of Kingston Digital.

23. The motivation would have been to allowing routing data in an intelligent manner based on global network knowledge (TW Telecom, Col 2 34-36).

24. Regarding Claim 6, Kingston Digital fails to explicitly disclose the smart routing is based on at least one of best bandwidth, lowest latency, fewest hops, and no packet loss.

25. TW Telecom teaches the smart routing is based on at least one of best bandwidth, lowest latency, fewest hops, and no packet loss (information related to network operation such as traffic load, link latencies, link jitter, link packet loss, and link failures. Using such information, [...] provide an optimized route, Col 2 Ln 41-44).

26. It would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of TW Telecom to incorporate the teachings regarding the smart routing is based on at least one of best bandwidth, lowest latency, fewest hops, and no packet loss in the invention of Kingston Digital. The motivation would have been to allowing routing data in an intelligent manner based on global network knowledge (TW Telecom, Col 2 34-36).

27. Regarding Claim 7, Kingston Digital fails to explicitly disclose smart routing is based on at least one of real-time statistics and historical statistics.

28. TW Telecom teaches smart routing is based on at least one of real-time statistics and historical statistics (To determine the path, the virtual routing server may take into account current or historical bandwidth usage. For example, the virtual routing server may consider network usage during previous weeks, Col 5 Ln 32-37)

29. It would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of TW Telecom to incorporate the teachings regarding smart routing is based on at least one of real-time statistics and historical statistics in the invention of Kingston Digital.

30. The motivation would have been to allowing routing data in an intelligent manner based on global network knowledge (TW Telecom, Col 2 34-36).

31. Claim 10 is/are rejected under 35 U.S.C. 103 as being unpatentable over Kingston Digital as applied to claim 1 above, and further in view of Sekaran (2009/0,217,109).

32. Regarding Claim 10, Kingston Digital fails to explicitly disclose an intermediate access point server provides firewall services between a first endpoint device and other intermediate access point servers or the second endpoint device.

33. Sekaran is in a related field of an access server receiving communications between an endpoint and server (Abstract).

34. Sekaran teaches an intermediate access point server provides firewall services between a first endpoint device and other intermediate access point servers or the second endpoint device (Access server 112 [intermediate access point server] resides in a perimeter network and enables connectivity [...Access server 112 may provide multiple functionalities such as firewall protection, para. [0020] Firewall 232 provides protection for connections with other networks [other intermediate access point servers], para. [0029]).

35. It would have been obvious to one of ordinary skill in the art at the time of the invention to use the teachings of Sekaran to incorporate the teachings regarding an intermediate access point server provides firewall services between a first endpoint device and other intermediate access point servers in the invention of Kingston Digital. The motivation would have been to allowing protection for connections with other networks (Sekaran, para. [0029]).