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 Western District of Texas on the following

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

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
1:22-cv-01324	12/16/2022	Western District of Texas

PLAINTIFF	DEFENDANT
Entangled Media, LLC	Dropbox, Inc.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,296,338	10/23/2012	Entangled Media, LLC
2	8,484,260	7/9/2013	Entangled Media, LLC
3			
4			
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
PHILIP J. DEVLIN		12/19/2022

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.
12/774,231	10/23/2012	8296338	3689.001US1	7527

21186 7590 10/03/2012

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

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 226 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):

Erik Caso, Santa Monica, CA;
Michael Abraham, Boulder, CO;

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.

Dropbox Exhibit 1002 - Page 2
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (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)

21186 7590 09/12/2012
SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

Sasha Reese	(Depositor's name)
/Sasha Reese/	(Signature)
September 18, 2012	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/774,231	05/05/2010	Erik Cano	3689.001US1	7527

TITLE OF INVENTION: METHOD FOR A CLOUD-BASED META-FILE SYSTEM TO VIRTUALLY UNIFY REMOTE AND LOCAL FILES ACROSS A RANGE OF DEVICES' LOCAL FILE SYSTEMS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$300	$0	$1170	12/12/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
HO, BINH VAN	2163	707-827000

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 03-02 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 Schwegman Lundberg
2 & Woessner, P.A.
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 has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Entangled Media Corp.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Huntington Beach, California

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

4a. The following fee(s) are submitted:
- ☒ Issue Fee
- ☒ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies: _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 19-0743 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Thierry Lo/ Date 9/18/2012

Typed or printed name Thierry Lo Registration No. 49,097

This collection of information 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 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, 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.

Dropbox Exhibit 1002 - Page 3
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Erik Caso et al.	Examiner: Binh Ho	
Serial No.:	12/774,231	Group Art Unit: 2163	
Filed:	May 5, 2010	Docket No.: 3689.001US1	
Customer No.:	21186	Confirmation No.: 7527	
Title:	Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems		

COMMUNICATION RE: FEE ADDRESS

Mail Stop Issue Fee
Commissioner for Patents
P.O.Box 1450
Alexandria, VA 22313-1450

In response to the Notice of Allowance and Issue Fee Due, please record the Fee Address under the provisions of 37 CFR 1.363 as the following:

Customer Number 21186

Please direct any inquiries to the undersigned attorney at (949) 354-0200.

Respectfully submitted,

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(949) 354-0200

Date 9/18/2012 By /Thierry Lo/
Thierry Lo
Reg. No. 49,097

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is filed using the USPTO's electronic filing system EFS-Web, and is addressed to: Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 18th day of September, 2012.

Sasha Reese /Sasha Reese/
Name Signature

Electronic Patent Application Fee Transmittal

Application Number:	12774231
Filing Date:	05-May-2010
Title of Invention:	METHOD FOR A CLOUD-BASED META-FILE SYSTEM TO VIRTUALLY UNIFY REMOTE AND LOCAL FILES ACROSS A RANGE OF DEVICES' LOCAL FILE SYSTEMS
First Named Inventor/Applicant Name:	Erik Caso
Filer:	Myunggon Hong/Sasha Reese
Attorney Docket Number:	3689.001US1

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

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	870	870
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1170**

Electronic Acknowledgement Receipt	
EFS ID:	13777835
Application Number:	12774231
International Application Number:	
Confirmation Number:	7527
Title of Invention:	METHOD FOR A CLOUD-BASED META-FILE SYSTEM TO VIRTUALLY UNIFY REMOTE AND LOCAL FILES ACROSS A RANGE OF DEVICES' LOCAL FILE SYSTEMS
First Named Inventor/Applicant Name:	Erik Caso
Customer Number:	21186
Filer:	Myunggon Hong/Sasha Reese
Filer Authorized By:	Myunggon Hong
Attorney Docket Number:	3689.001US1
Receipt Date:	18-SEP-2012
Filing Date:	05-MAY-2010
Time Stamp:	17:01:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1170
RAM confirmation Number	3603
Deposit Account	190743
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		3689001US1_IssueFee.pdf	398670 ac984a24deaf967702df2f65422ec04a6b6a85b5	yes	3

Multipart Description/PDF files in .zip description

Document Description	Start	End
Transmittal Letter	1	1
Issue Fee Payment (PTO-85B)	2	2
Miscellaneous Incoming Letter	3	3

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	32131 d577aae00e08111691306970fa24fa53a912dc95	no	2

Warnings:

Information:

Total Files Size (in bytes):	430801

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Erik Caso et al.

Title: Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems

Docket No.:	3689.001US1	Serial No.:	12/774,231
Filed:	May 5, 2010	Due Date:	December 12, 2012
Examiner:	Binh Ho	Group Art Unit:	2163
Customer No.:	21186	Confirmation No.:	7527

Notice of Allowance Date: September 12, 2012

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

We are transmitting herewith the following:

X Authorization to charge Deposit 19-0743 in the amount of $870.00 to cover the Small Entity Issue Fee Payment.
X Authorization to charge Deposit 19-0743 in the amount of $300.00 to cover the Publication Fee Payment.
X Issue Fee Transmittal (Form PTOL-85).
X Communication Re: Fee Address (1 page).

Please charge any additional required fees or credit overpayment to Deposit Account No. 19-0743.

SCHWEGMAN, LUNDBERG & WOESSNER, P.A. By /Thierry Lo/
Customer No.: 21186
Thierry Lo
Reg. No. 49,097

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to: Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 18th day of September, 2012.

Sasha Reese
Name

/Sasha Reese/
Signature

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

21186 7590 09/12/2012

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER
HO, BINH VAN

ART UNIT	PAPER NUMBER
2163	

DATE MAILED: 09/12/2012

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/774,231	05/05/2010	Erik Caso	3689.001US1	7527

TITLE OF INVENTION: METHOD FOR A CLOUD-BASED META-FILE SYSTEM TO VIRTUALLY UNIFY REMOTE AND LOCAL FILES ACROSS A RANGE OF DEVICES' LOCAL FILE SYSTEMS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$300	$0	$1170	12/12/2012

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 SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

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: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 02/11)

Dropbox Exhibit 1002 - Page 10
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (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)

21186 7590 09/12/2012
SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

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 facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/774,231	05/05/2010	Erik Caso	3689.001US1	7527

TITLE OF INVENTION: METHOD FOR A CLOUD-BASED META-FILE SYSTEM TO VIRTUALLY UNIFY REMOTE AND LOCAL FILES ACROSS A RANGE OF DEVICES' LOCAL FILE SYSTEMS

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$870	$300	$0	$1170	12/12/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
HO, BINH VAN	2163	707-827000

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 03-02 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, 1_____

(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. 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 has been filed for recordation as set forth in 37 CFR 3.11. 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. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

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

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information 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 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, 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.

Dropbox Exhibit 1002 - Page 11
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

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.
12/774,231	05/05/2010	Erik Caso	3689.001US1	7527

21186 7590 09/12/2012

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
HO, BINH VAN	
ART UNIT	PAPER NUMBER
2163	

DATE MAILED: 09/12/2012

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

The Patent Term Adjustment to date is 226 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 226 day(s).

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 Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Dropbox Exhibit 1002 - Page 12
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

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.	Applicant(s)	
	12/774,231	CASO ET AL.	
	Examiner	Art Unit	
	BINH V. HO	2163	

-- 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 *07/10/2012*.
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 *1-4,6,7 and 13-20*.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   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. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ 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).
7. ☐ 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)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/BINH V HO/
Primary Examiner, Art Unit 2163

Dropbox Exhibit 1002 - Page 14
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

DETAILED ACTION

Examiner's Amendment

1. An examiner's amendment to the record appears below. Should the changes and /or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.3.12. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. The following claim has been amended upon agreement by applicant during a telephone conversation with Mr. Thierry Lo on 09/04/2012.

Amendments to claims 1, 6, 13, and 16; and cancelled claim 5:

Claim 1 (Currently Amended):

A process for establishing a singular file system across multiple devices comprising:

receiving user information to open an account for establishing a singular file system across multiple devices via a web-based system that includes at least one server;

installing an individual software client on each of the multiple devices via the web-based system;

accepting registration of multiple devices via the web-based system;

scanning each of the multiple devices by each of the individual software clients to inventory data on each of the multiple devices and create a meta-index of the files for the inventoried data;

providing by the individual software clients via the multiple devices individual meta-indices of the inventoried data for each of the multiple devices to the at least one server;

integrating by the at least one server the individual meta-indices to create a single master meta-index;

providing by the at least one server the single master meta-index and meta-indices for each of the other multiple devices to each of the multiple devices via the individual software clients;

integrating metadata from the meta-indices of each of the other multiple devices into a local file system of each of the multiple devices to generate virtual files stored in the same locations as local files of the local file system, the virtual files indistinguishable from the local files by the local file system at each of the multiple devices; and

continually updating the single master meta-index on the at least one server and each of the multiple devices in response to changes to the data indexed thereon,

wherein the individual software clients facilitate storage of the data within each of the multiple devices in accordance with the single meta-data index by modifying file systems of each of the multiple devices to include virtual files for data from the single meta-data index that is not local to a multiple device.

Claim 5 (Cancelled)

Claim 6 (Currently Amended)

The process according to claim [[5]] 1, wherein the individual software clients facilitate creation of a visual representation of the virtual files on a remote one of each of the multiple devices that is indistinguishable from a visual representation of an actual file that is located on a local one of the multiple devices.

Claim 13 (Currently Amended)

A system for establishing a singular file system across multiple devices comprising:

a web-accessible server;

at least one software client plug-in;

multiple devices for storing and operating on files;

wherein the web-accessible server receives user information to open an account for establishing a singular file system across multiple devices, installs the at least one software plug-in on each of the multiple devices, accepts registration of the multiple devices, wherein the at least one software plug-in varies in accordance with an operating system of each of the multiple devices;

further wherein the at least one software client plug-in scans its respective one of the multiple devices to inventory files thereon, creates a meta-index to files for the inventoried data, provides the meta-index of the inventoried data for its respective one of the multiple devices to the web-accessible server;

further wherein the web-accessible server receives meta-indices from each of the multiple devices and integrates the meta-indices to create a single meta-index, provides the single meta-index and meta-indices for each of the other multiple devices to each of the multiple devices via the individual software clients, integrates at each of the multiple devices metadata from the meta-indices of each of the other multiple devices into a local file system of each of the multiple devices to generate virtual files stored in the same locations as local files of the local file system, the virtual files indistinguishable from the local files by the local file system at each of the multiple devices, and continually updates the single meta-index on each of the multiple devices in response to operations on the files indexed thereon,

wherein the individual software clients facilitate storage of the data within each of the multiple devices in accordance with the single meta-data index by modifying file systems of each of the multiple devices to include virtual files for data from the single meta-data index that is not local to a multiple device.

Claim 16 (Currently Amended)

A non-transitory computer-readable storage medium storing a set of instructions that, when executed by a processor, cause the processor to perform operations, comprising:

registering multiple devices with an account for establishing a singular file system across the multiple devices;

scanning each of the multiple devices to inventory data on each of the multiple devices and create a meta-index of the files for the inventory data;

generating a single master meta-index from meta-indices of files corresponding to inventory data on each of the multiple devices; ~~and~~

providing the single master meta-index and meta-indices for each of the other multiple devices to each of the multiple devices, metadata from the meta-indices of each of the other multiple devices to be integrated into a local file system of each of the multiple devices to generate virtual files stored in the same locations as local files of the local file system, the virtual files indistinguishable from the local files by the local file system at each of the multiple devices; and

facilitating storage of data within each of the multiple devices in accordance with the single master meta-index by modifying file systems of each of the multiple devices to include virtual files for data from the single master meta-data index that is not local to a multiple device.

The Examiner's amendment has been made in order to place the application in a condition for allowance.

Reasons for Allowance

3. The following is an examiner's statement of reason for allowance:

Claims 1, 13, and 16 are considered allowable since the prior made of record and considered pertinent to the applicant's disclosure does not teach or suggest the claimed limitations. Vesper (U.S. 2011/0110568), Or Wills (U.S. 2012/0079117), Floyd (U.S. 2007/0153703), or Ben-Shaul (U.S. 2011/0231844), taken individually or in combination, do not teach the claimed invention having a process for establishing a singular file system across multiple devices comprising: receiving user information to open an account for establishing a singular file system across multiple devices via a web-based system that includes at least one server; accepting registration; scanning each of the multiple devices by each of the individual software clients to inventory data on each of the multiple devices and create a meta-index of the files for the inventoried data; providing by the individual software clients via the multiple devices individual meta-indices of the inventoried data for each of the multiple devices to the at least one server; providing by the at least one server the single master meta-index and meta-indices for each of the other multiple devices; integrating metadata from the meta-indices of each of the other multiple devices into a local file system of each of the multiple devices to generate virtual files stored in the same locations as local files of the local file system, the virtual files indistinguishable from the local files by the local file system at each of the multiple devices; and continually updating the single master meta-index on the at least one server and each of the multiple devices in response to changes to the data indexed thereon, wherein the individual software clients facilitate

storage of the data within each of the multiple devices in accordance with the single meta-data index by modifying file systems of each of the multiple devices to include virtual files for data from the single meta-data index that is not local to a multiple device with a combination of all recitations as defined in claims 1, 13, and 16.

Therefore, claims 1-4, 6-7, and 13-20 *are* presently allowed.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Inquiry

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Binh V. Ho whose telephone number is 571 272 8583. The examiner can normally be reached on M-F from 8:00AM - 4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tony Mahmoudi can be reached on 571 272 4078. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/BINH V HO/
Primary Examiner, Art Unit 2163

Binh V Ho
Examiner
Art Unit 2163

Notice of References Cited	Application/Control No. 12/774,231	Applicant(s)/Patent Under Reexamination CASO ET AL.	
	Examiner BINH V. HO	Art Unit 2163	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2012/0079117	03-2012	Wills et al.	709/226
*	B	US-2011/0110568	05-2011	Vesper et al.	382/128
*	C	US-2008/0189390	08-2008	Heller et al.	709/218
*	D	US-2008/0082490	04-2008	MacLaurin et al.	707/3
*	E	US-2010/0274982	10-2010	Mehr et al.	711/162
*	F	US-2010/0205152	08-2010	Ansari et al.	707/654
*	G	US-2011/0231844	09-2011	Ben-Shaul et al.	718/1
*	H	US-7,805,565	09-2010	Milligan et al.	711/114
*	I	US-2009/0062944	03-2009	Wood et al.	700/94
*	J	US-2011/0093471	04-2011	Brockway et al.	707/747
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Dropbox Exhibit 1002 - Page 23
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12774231	CASO ET AL.
	Examiner	Art Unit
	BINH V HO	2163

SEARCHED			
Class	Subclass	Date	Examiner
707	827	04/18/2012	BH

SEARCH NOTES		
Search Notes	Date	Examiner
707/827;717/168-178 East search (see printout)	04/18/2012	BH
East search (Inventors)	04/18/2012	BH
Interference East search (see printout)	04/18/2012	BH
Google search (see printout)	04/18/2012	BH
East search (U.S. Pub.)	04/18/2012	BH
Update East search (see printout)	09/06/2012	BH

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
717	168	09/06/2012	BH

Dropbox Exhibit 1002 - Page 24
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12774231	CASO ET AL.
	Examiner	Art Unit
	BINH V HO	2163

ORIGINAL		INTERNATIONAL CLASSIFICATION															
CLASS	SUBCLASS	CLAIMED									NON-CLAIMED						
707	827	G	0	6	F	12 / 00 (2006.01.01)											
CROSS REFERENCE(S)		G	0	6	F	17 / 30 (2006.01.01)											
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																
717	168																

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

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

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	14	
/B.V.H./ Primary Examiner.Art Unit 2163	09/06/2012	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	6

Dropbox Exhibit 1002 - Page 25
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

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

BIB DATA SHEET

CONFIRMATION NO. 7527

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
12/774,231	05/05/2010	707	2163	3689.001US1

APPLICANTS

Erik Caso, Santa Monica, CA;
Michael Abraham, Boulder, CO;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/175,489 05/05/2009

**** FOREIGN APPLICATIONS *************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
05/17/2010

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☐ No Verified and Acknowledged /BINH VAN HO/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	6	14 ~~15~~ – –	3

ADDRESS

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402
UNITED STATES

/Binh Van Ho/
09/06/2012

TITLE

Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems

FILING FEE RECEIVED	FEES: Authority has been given in Paper	☐ All Fees
462	No._____ to charge/credit DEPOSIT ACCOUNT	☐ 1.16 Fees (Filing)
	No._____ for following:	☐ 1.17 Fees (Processing Ext. of time)
		☐ 1.18 Fees (Issue)
		☐ Other _____
		☐ Credit

Dropbox Exhibit 1002 - Page 26
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L7	144	(virtual$4 near5 stor$5 near5 device) with metadata	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/06 19:43
L8	5	index$4 with (virtual$4 near5 stor$5 near5 device) with metadata	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/06 19:43
L14	72	(meta-index$4 meta$1index$4 index$4) with (virtual$4 near5 storage near5 device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/06 19:52
L16	5	(meta-index$4 meta$1index$4 index$4 metaindex$4) with (virtual$4 near5 storage near5 device) with metadata	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/06 19:53
L17	336	(scan$4 collect$4) with ((multipl$4 pluralit$4) near2 device) with software	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/06 19:54
L18	3	(scan$4 collect$4) with ((multipl$4 pluralit$4) near2 device) with software with $5index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/09/06 19:55
S1	2	"20100287219"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/23 16:55
S2	266	707/827.ccls.	US-PGPUB;	OR	ON	2011/12/23

Dropbox Exhibit 1002 - Page 27
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			16:59
S3	770	717/176.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/23 17:00
S5	151	michael with abraham	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/23 17:01
S6	53	("20040172449" | "20050114711" | "20050138186" | "20050144195" | "20050144200" | "20050149481" | "20050256909" | "20060206533" | "20060277314" | "20070162510" | "20080104077" | "20090254592" | "6381019" | "6499054" | "6512586" | "6732158" | "6938042" | "7120692" | "7337171" | "7467187" | "7499905" | "7546353" | "7587467" | "7587471" | "7600036").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 19:01
S7	6	("7747999" "20030221190" "7266595").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:14
S8	5	("7747999" "20030221190" "7266595").pn. and (install$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:18
S9	5	erik with caso	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:18
S10	1881	(install$6 same multipl$4 same (device user)).ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:22
S11	14	(install$6 same software same multipl$4 same (device user)).ti.	US-PGPUB; USPAT;	OR	ON	2012/01/31 21:25

Dropbox Exhibit 1002 - Page 28
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S12	7366	717/168-178.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:32
S13	7335	717/168-178.ccls. and (install$6 multipl$4 device user)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:33
S14	5793	717/168-178.ccls. and (install$6 multipl$4 device user) with software	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:33
S15	756	717/168-178.ccls. and (install$6 multipl$4 device user) with software and registrat$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:33
S16	390	717/168-178.ccls. and (install$6 multipl$4 device user) with software and registrat$4 and inventor$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:34
S17	79	717/168-178.ccls. and (install$6 multipl$4 device user) with software and registrat$4 and inventor$4 and index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:36
S18	1	"20100287219" and peer-to-peer	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:59
S22	6	("20060077189" "20080195693" "20090319635").pn. and (monitor device software install$6 inventor$4 plug$1in)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/12 23:10

Dropbox Exhibit 1002 - Page 29
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

S23	0	(("20040172449" | "20050114711" | "20050138186" | "20050144195" | "20050144200" | "20050149481" | "20050256909" | "20060206533" | "20060277314" | "20070162510" | "20080104077" | "20090254592" | "6381019" | "6499054" | "6512586" | "6732158" | "6938042" | "7120692" | "7337171" | "7467187" | "7499905" | "7546353" | "7587467" | "7587471" | "7600036").PN.) and cloud	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/13 18:05
S24	1	(("20040172449" | "20050114711" | "20050138186" | "20050144195" | "20050144200" | "20050149481" | "20050256909" | "20060206533" | "20060277314" | "20070162510" | "20080104077" | "20090254592" | "6381019" | "6499054" | "6512586" | "6732158" | "6938042" | "7120692" | "7337171" | "7467187" | "7499905" | "7546353" | "7587467" | "7587471" | "7600036").PN.) and index	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/13 18:38
S25	31	(michael with abraham) and index	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/13 18:46
S26	25	(michael with abraham) and index and (scan$4 inventor$4 collect$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/13 18:47
S27	4	(cloud$4 same storage same index$4).ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 13:08
S28	31	(cloud$4 same storage same index$4).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 14:34
S29	0	(cloud$4 same storage same index$4 same plug$1in).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 14:34
S30	62	(cloud$4 with storage with index$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2012/04/17 15:19

Dropbox Exhibit 1002 - Page 30
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

			DERWENT; IBM_TDB			
S31	5	(cloud$4 with storage with index$4) and plug$1in	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 15:19
S40	21	("20100257142" "20100257403" "20100199042" "20100274765" "20100191783" "20100229108" "20110110568" "20110093471" "20090164790" "20100274762" "7636764").pn. and (cloud storage index$4 metadata device log$1in registrat$4 categ$7 class$10 group$4 down$1load$4 up$1load$4 creat$4 collect$4 replicas Redundant$4 duplicat$4 replicat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 22:18
S41	1	(scan$4 collect$4) with ((multipl$4 pluralit$4) near2 device) with (creat$4 near5 index$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 22:38
S42	3	(("20040172449" | "20050114711" | "20050138186" | "20050144195" | "20050144200" | "20050149481" | "20050256909" | "20060206533" | "20060277314" | "20070162510" | "20080104077" | "20090254592" | "6381019" | "6499054" | "6512586" | "6732158" | "6938042" | "7120692" | "7337171" | "7467187" | "7499905" | "7546353" | "7587467" | "7587471" | "7600036").PN.) and (index$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 22:40
S44	78	(scan$4 collect$4) with ((multipl$4 pluralit$4) near2 device) with index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 22:42
S45	38	(scan$4 collect$4) near5 ((multipl$4 pluralit$4) near2 device) with index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 22:42
S47	1	singlular near3 (file index$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 14:07
S49	141	((set$1up request$4) near5 account$4) with up$1load$4	US-PGPUB; USPAT; USOCR;	OR	ON	2012/04/18 14:52

Dropbox Exhibit 1002 - Page 31
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S50	6	((set$1up request$4) near5 account$4) with up$1load$4 with (categ$8 class$10 group$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 14:53
S51	0	up$1load$4 with (categ$8 class$10 group$4) with cloud with index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 19:57
S52	13	up$1load$4 with (categ$8 class$10 group$4) with cloud	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 19:57
S53	0	(cloud$4 same up$1load$4 same index$4).ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 20:34
S54	1	(cloud$4 same up$1load$4 same index$4).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 20:34
S55	5	(storag$4 same up$1load$4 same index$4).ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 20:35
S56	57	(storag$4 same up$1load$4 same index$4).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 20:39
S57	20	(storag$4 same up$1load$4 same index$4 same device).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 20:39
S62	1	"20120079117" and (pluralit$4 multipl$4	US-PGPUB;	OR	ON	2012/04/18

Dropbox Exhibit 1002 - Page 32
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

		scan$4 collect$4 class$10 group$4 categ$8 index$4 registrat$4 log$1in device)	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			22:45
S63	3	(BLACKBURN with DAVID with A$1) and (storag$4 same up$1load$4 same index$4 same device) and (class$10 categ$7 group$4 device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 22:46
S67	2	("20110110568" "20120079117") and (pluralit$4 multipl$4 scan$4 collect$4 class$10 group$4 categ$8 index$4 registrat$4 log$1in device account$4 log$1in cloud$4 transfer$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 23:30
S68	160	(set$1up$4 log$1in Account$4) near5 servic$4 near5 (cloud$4 back$1up)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/19 10:44
S69	41	((set$1up$4 log$1in Account$4) near5 servic$4 near5 (cloud$4 back$1up)) and index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/19 10:45
S70	19	((set$1up$4 log$1in Account$4) near5 servic$4 near5 (cloud$4 back$1up)) and index$4 and ((multipl$4 pluralit$4) near3 (unit device))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/19 10:46
S71	19	((set$1up$4 log$1in Account$4) near5 servic$4 near5 (cloud$4 back$1up)) and index$4 and ((multipl$4 pluralit$4) near3 (unit device))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/19 14:21
S72	19	((set$1up$4 log$1in Account$4) near5 servic$4 near5 (cloud$4 back$1up)) and index$4 and ((multipl$4 pluralit$4) near3 (unit device)) and (class$10 categ$7 group$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/19 14:22
S75	6	("20110110568" "20120079117" "20080082490" "20080005168") and (pluralit$4 multipl$4 scan$4 collect$4 class$10 group$4 categ$8 index$4 registrat$4 log$1in device account$4 log$1in cloud$4 transfer$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2012/04/19 17:20

Dropbox Exhibit 1002 - Page 33
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

			IBM_TDB			
S77	6	("20110110568" "20120079117" "20080082490" "20080005168") and (pluralit$4 multipl$4 scan$4 collect$4 class$10 group$4 categ$8 index$4 registrat$4 log$1in device account$4 log$1in cloud$4 transfer$4 updat$4 modif$4 chang$4 individual$4 password)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/19 22:52
S78	5	categor$7 near5 (document and video and (pictur$4 imag$4 photo) and (music))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 10:55
S79	16	categor$7 near5 (document and video and (pictur$4 imag$4 photo) and (music audio))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 10:57
S83	2	creat$4 near3 virtual near4 (represent$6 display$4) near5 data near5 devices with (metadata index$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 12:23
S84	80	light$1weight$4 near5 metadata	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 12:26
S87	22	light$1weight$4 near5 metadata and index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 12:28
S88	45	light$1weight$4 near5 metadata and virtual$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 12:29
S89	13	light$1weight$4 near5 metadata and virtual$4 and index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 12:29
S90	5340	virtual$4 near5 store$3 near5 device	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2012/04/20 13:21

Dropbox Exhibit 1002 - Page 34
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

			EPO; JPO; DERWENT; IBM_TDB			
S91	37	(virtual$4 near5 store$3 near5 device) with metadata	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 13:22

09/06/2012 8:30:24 PM
C:\Users\bho\Documents\EAST\Workspaces\12774231.wsp

Dropbox Exhibit 1002 - Page 35
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12774231	CASO ET AL.
	Examiner	**Art Unit**
	BINH V HO	2163

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

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

CLAIM		DATE								
Final	Original	02/12/2012	04/18/2012	09/06/2012						
1	1	÷	✓	=						
2	2	÷	✓	=						
3	3	÷	✓	=						
4	4	÷	✓	=						
	5	÷	✓	-						
5	6	÷	✓	=						
6	7	÷	✓	=						
	8	÷	N	-						
	9	÷	N	-						
	10	÷	N	-						
	11	÷	N	-						
	12	÷	N	-						
7	13	÷	✓	=						
8	14	÷	✓	=						
9	15	÷	✓	=						
10	16			=						
11	17			=						
12	18			=						
13	19			=						
14	20			=						

Dropbox Exhibit 1002 - Page 36
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

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
12/774,231	05/05/2010	Erik Caso	3689.001US1

CONFIRMATION NO. 7527

21186
SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

POA ACCEPTANCE LETTER

OC000000055983781

Date Mailed: 08/17/2012

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/03/2012.

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.

/tnnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Dropbox Exhibit 1002 - Page 37
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

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
12/774,231	05/05/2010	Erik Caso	ENT0001-US

CONFIRMATION NO. 7527

74877
King and Spalding LLP
1700 Pennsylvania Ave, NW
Suite 200
Washington, DC 20006

POWER OF ATTORNEY NOTICE

OC000000055983731

Date Mailed: 08/17/2012

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/03/2012.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/tnnguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Dropbox Exhibit 1002 - Page 38
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

RECEIVED (2/3) 08/03/2012 03:48:57 PM -0500
CENTRAL FAX CENTER
AUG 0 3 2012

MODIFIED PTO/SB/80 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
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 displays a valid OMB control number.

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(b).

I hereby appoint:

☒ Practitioners associated with the Customer Number: **21186**

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(b).

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

☒ The address associated with Customer Number: **21186**

OR

☐ Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address:
Entangled Media Corp.
606 Lake Street
#18
Huntington Beach, CA 92648
United States of America

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, 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	Eric Caso	Date:	8/1/12
Name	Eric Caso	Telephone:	714-875-3745
Title	CEO		

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.

RECEIVED
CENTRAL FAX CENTER
AUG 0 3 2012

MODIFIED PTO/SB/96 (07-09)
Approved for use through 07/31/2012. 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 displays a valid OMB control number.

STATEMENT UNDER 37 C.F.R. 3.73(b)

Applicant/Patent Owner: Erik Caso et al. Attorney Docket No. 3689.001US1
Application No./Patent No.: 12/774,231 Filed/Issue Date: May 5, 2010
Titled: Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems

Entangled Media Corp., a Corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

States that it is:

1. ☒ the assignee of the entire right, title, and interest in;

2. ☐ an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is _____ %); or

3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

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 _____, Frame _____, or for which a copy therefore is attached.

OR

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

1. From: Erik Caso et al. To: Entangled Media LLC
The document was recorded in the United States Patent and Trademark Office at Reel 024338, Frame 0846 - 0850, or for which a copy thereof is attached.
2. From: Entangled Media LLC To: Entangled Media Corp.
The document was recorded in the United States Patent and Trademark Office at Reel 027246, Frame 0293 - 0298, 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(b)(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.

/Thierry Lo/ 8/3/2012
Signature Date

Thierry Lo USPTO Reg. No. 49,097
Printed or Typed Name Title

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.

Dropbox Exhibit 1002 - Page 40
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

RECEIVED
CENTRAL FAX CENTER
AUG 0 3 2012

SCHWEGMAN ▪ LUNDBERG ▪ WOESSNER
PATENT PROTECTION FOR HIGH TECHNOLOGY

P.O. Box 2938
Minneapolis, MN 55402
Telephone (612) 373-6900 Facsimile (612) 339-3061

Date: August 3, 2012

Time: 3:46 p.m.
(Minneapolis, Minn.)

TO: Commissioner for Patents
Attn: Binh Ho
Patent Examining Corps
Facsimile Center
P.O. Box 1450
Alexandria, VA 22313-1450

FAX NUMBER 571-273-8300

FROM: Thierry Lo

OUR REF: 3689.001US1

*** Please deliver to Examiner Binh Ho in Art Unit 2163. ***

Document(s) Transmitted: **Power of Attorney to Prosecute Applications before the USPTO (PTO/SB/80) (1 pg.), Statement Under 37 C.F.R. 3.73(b) (PTO/SB/96) (1 pg.)**

Total pages of this transmission, including cover letter: 3

If you do NOT receive all of the pages described above, please telephone us at 612-373-6900 or fax us at 612-339-3061.

In re. Patent Application of: Erik Caso et al.
Serial No.: 12/774,231
Filed: May 5, 2010
Title: Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems

Examiner: Binh Ho
Group Art Unit: 2163
Docket No.: 3689.001US1

Please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

By: /Thierry Lo/
Name: Thierry Lo
USPTO Reg. No. 49,097

I hereby certify that this paper is being transmitted by facsimile to the U.S. Patent and Trademark Office on the date shown below.

/Mandy Brown/
Mandy Brown

August 3, 2012
Date of Transmission

Dropbox Exhibit 1002 - Page 41
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Erik Michael Caso et al.	Examiner: Binh Ho
Serial No.:	12/774,231	Group Art Unit: 2163
Filed:	May 5, 2010	Docket No.: 3689.001US1
Customer No.:	21186	Confirmation No.: 7527
Title:	Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems	

AMENDMENT & RESPONSE UNDER 37 C.F.R. § 1.111

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

In response to the Office Action dated April 26, 2012, please amend the application as follows:

IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A process for establishing a singular file system across multiple devices comprising:

receiving user information to open an account for establishing a singular file system across multiple devices via a web-based system that includes at least one server;

installing an individual software client on each of the multiple devices via the web-based system;

accepting registration of multiple devices via the web-based system;

scanning each of the multiple devices by each of the individual software clients to inventory data on each of the multiple devices and create a meta-index of the files for the inventoried data;

providing by the individual software clients via the multiple devices individual meta-indices of the inventoried data for each of the multiple devices to the at least one server;

integrating by the at least one server the individual meta-indices to create a single master meta-index;

providing by the at least one server the single master meta-index and meta-indices for each of the other multiple devices to each of the multiple devices via the individual software clients;

integrating metadata from the meta-indices of each of the other multiple devices into a local file system of each of the multiple devices to generate virtual files stored in the same locations as local files of the local file system, the virtual files indistinguishable from the local files by the local file system at each of the multiple devices; and

continually updating the single master meta-index on the at least one server and each of the multiple devices in response to changes to the data indexed thereon.

2. (Original) The process according to claim 1 wherein the individual software clients vary according to the individual operating systems of each of the multiple devices.

3. (Original) The process according to claim 1 wherein registration of the multiple devices includes selection of categories of data for each of the multiple devices to be inventoried.

4. (Original) The process according to claim 3 wherein categories of data include documents, videos, pictures and music.

5. (Original) The process according to claim 1, wherein the individual software clients facilitate storage of the data within each of the multiple devices in accordance with the meta-data by modifying file systems of each of the multiple devices to include virtual files for data from the single meta-data index that is not local to a multiple device.

6. (Original) The process according to claim 5, wherein the individual software clients facilitate creation of a visual representation of the virtual files on a remote one of each of the multiple devices that is indistinguishable from a visual representation of an actual file that is located on a local one of the multiple devices.

7. (Currently Amended) The process according to claim 1, wherein the meta-data includes at least information regarding file name, file type, file size, local path the file is stored in, date created, and date modified.

8. (Withdrawn) A process for operating on files located on multiple devices using a singular file system comprising:

accepting a request to operate on a file at a first device, wherein the file is selected from the singular file system on the first device;

intercepting the request by a software client on the first device;

determining by the software client if the file is physically located on the first device or a second device, wherein a visual representation of the singular file system on the first device is identical to a visual representation of the singular file system on the second device;

if the file is physically located on a second device, requesting by the software client on the first device that a peer-to-peer connection be brokered by a server-based web service between the first device and the second device;

if the peer-to-peer connection is brokered, transferring the physical file from the second device to the first device; and

performing the operation on the file at the first device.

9. (Withdrawn) The process according to claim 8, wherein if the peer-to-peer connection cannot be brokered between the first device and the second device, an alternative connection is established by the server-based web service.

10. (Withdrawn) The process according to claim 9, wherein the alternative connection is an HTTP relay.

11. (Withdrawn) The process according to claim 8, wherein the software client determines if the file is physically located on the first device or a second device by reviewing file metadata.

12. (Withdrawn) The process according to claim 8, further comprising updating metadata of the singular file system on the first device and the second device to reflect a change in physical location of the file from the second device to the second device.

13. (Currently Amended) A system for establishing a singular file system across multiple devices comprising:

a web-accessible server;

at least one software client plug-in;

multiple devices for storing and operating on files;

wherein the web-accessible server receives user information to open an account for establishing a singular file system across multiple devices, installs the at least one software plug-in on each of the multiple devices, accepts registration of the multiple devices, wherein the at least one software plug-in varies in accordance with an operating system of each of the multiple devices;

further wherein the at least one software client plug-in scans its respective one of the multiple devices to inventory files thereon, creates a meta-index to files for the inventoried data, provides the meta-index of the inventoried data for its respective one of the multiple devices to the web-accessible server;

further wherein the web-accessible server receives meta-indices from each of the multiple devices and integrates the meta-indices to create a single meta-index, provides the single meta-index and meta-indices for each of the other multiple devices to each of the multiple devices via the individual software clients, integrates at each of the multiple devices metadata from the meta-indices of each of the other multiple devices into a local file system of each of the multiple devices to generate virtual files stored in the same locations as local files of the local file system, the virtual files indistinguishable from the local files by the local file system at each of the multiple devices, and continually updates the single meta-index on each of the multiple devices in response to operations on the files indexed thereon.

14. (Original) The system according to claim 13, wherein the at least one software client plug-in facilitates storage of the files within its respective one of the multiple devices in accordance with the meta-data by modifying a file system of its respective one of the multiple devices to include virtual files for files from the single meta-index that are not local to the multiple device.

15. (Original) The process according to claim 14, wherein the at least one software client plug-in facilitates creation of a visual representation of the virtual files on its respective one of the multiple devices that is indistinguishable from a visual representation of an actual file that is physically located on a another of the multiple devices.

16. (New) A non-transitory computer-readable storage medium storing a set of instructions that, when executed by a processor, cause the processor to perform operations, comprising:

registering multiple devices with an account for establishing a singular file system across the multiple devices;

generating a single master meta-index from meta-indices of files corresponding to inventory data on each of the multiple devices; and

providing the single master meta-index and meta-indices for each of the other multiple devices to each of the multiple devices, metadata from the meta-indices of each of the other multiple devices to be integrated into a local file system of each of the multiple devices to generate virtual files stored in the same locations as local files of the local file system, the virtual files indistinguishable from the local files by the local file system at each of the multiple devices.

17. (New) The non-transitory computer-readable storage medium of claim 16, further comprising:

continually updating the single master meta-index on each of the multiple devices in response to changes to the data indexed thereon.

18. (New) The non-transitory computer-readable storage medium of claim 16, further comprising:

updating the single master meta-index on each of the multiple devices in response to changes to meta-indices of a local file of one of the multiple devices.

19. (New) The non-transitory computer-readable storage medium of claim 16, further comprising:

updating the single master meta-index on each of the multiple devices in response to changes to a local file of a first device, the local file corresponding to a virtual file of a second device, the local file system of the second device retrieving the local file from the first device.

20. (New) The non-transitory computer-readable storage medium of claim 19, wherein the the virtual files and the local files in the first device are indistinguishable by the local file system of the first device.

REMARKS

This responds to the Office Action dated April 26, 2012.

Claims 1, 7, and 13 are amended, and claims 16-20 are added; as a result, claims 1-7, and 13-20 are now pending in this application. The amendments are supported by the originally filed specification, for example, at Paragraph [0028], and FIGS. 1 and 2.

New Claims

Claims 16-20 are new. Support for the new claims may be found in the specification, such as at Paragraph [0028], and FIGS. 1 and 2. Applicants believe that no new matter has been introduced in the added claims. Additionally, Applicants respectfully submit that the new claims are patentably distinct over the references currently cited as a basis of rejection, such as by virtue of the feature "providing the single master meta-index and meta-indices for each of the other multiple devices to each of the multiple devices, metadata from the meta-indices of each of the other multiple devices to be integrated into a local file system of each of the multiple devices to generate virtual files stored in the same locations as local files of the local file system, the virtual files indistinguishable from the local files by the local file system at each of the multiple devices."

Accordingly, Applicants respectfully request that the Examiner consider and allow the newly added claims.

Claim Objections

Claim 7 is objected to because of the following informalities: In claim 7, "modified" should be changed to - modified. --. Accordingly, claim 7 has been amended and Applicants respectfully request that the present objection be withdrawn.

The Rejection of Claims Under § 103

Claims 1-3, 7, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vesper (U.S. 2011/0110568) in view of Wills (U.S. 2012/0079117).

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vesper (U.S. 2011/0110568) in view of Wills (U.S. 2012/0079117) and further in view of Floyd (U.S. 2007/0153703).

Claims 5-6, 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vesper (U.S. 2011/0110568) in view of Wills (U.S. 2012/0079117) and further in view of Ben-Shaul (U.S. 2011/0231844).

As pointed by the Office Action, Vesper and Wills fail to describe "the individual software clients facilitate storage of the data within each of the multiple devices in accordance with the meta-data by modifying file systems of each of the multiple devices to include virtual files for data from the single meta-data index that is not local to a multiple device" as recited in claim 6. Instead, the Office Action relies the teachings of Ben-Shaul.

Ben-Shaul describes a desktop delivery system where multiple computing devices are connected to a single data center 102 that includes a separate virtual disk 112a, 112b, 112n for each computing device 130a, 130b, 130n. In particular, "each virtual personal disk is a set of images that collectively represents data that is stored at a particular computing device." Paragraph [0035]. As such, all virtual personal disks 112a, 112b, 112n are stored in a single data center 102 to help IT manage a large number of enterprise desktop computers from a central location (Admin Management Client 120). There is no suggestion in Ben-Shaul to have the virtual personal disk of computing devices stored in other computing devices because it would fragment further the IT management of the enterprise desktops. Thus, Ben-Shaul describes storing the virtual personal disk of Computing Device 130a in a central data center 102 and not in other Computing Devices such as 130b or 130n.

In contrast, claim 1 and similarly claims 13, and 16 recite in part "providing by the at least one server the single master meta-index and meta-indices *for each of the other multiple devices to each of the multiple devices* via the individual software clients; at *each of the multiple*

devices, integrating metadata from the meta-indices of each of the other multiple devices into a local file system of each of the multiple devices to generate virtual files stored in the same locations as local files of the local file system, the virtual files indistinguishable from the local files by the local file system at each of the multiple devices." (emphasis added).

Therefore, Applicants respectfully submit that the proposed combined teachings of Vesper, Wills, and Ben-Shaul fail to suggest the recited limitation of "providing by the at least one server the single master meta-index and meta-indices *for each of the other multiple devices to each of the multiple devices* via the individual software clients; at *each of the multiple devices, integrating metadata from the meta-indices of each of the other multiple devices into a local file system of each of the multiple devices to generate virtual files stored in the same locations as local files of the local file system, the virtual files indistinguishable from the local files by the local file system at each of the multiple devices*." (emphasis added) as recited in claim 1, and similarly in claims 13 and 16.

Thus, Applicants respectfully request that the present rejection be withdrawn for at least the reasons previously set forth.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's representative at (949) 354-0200 to facilitate prosecution of this application.

If necessary, please charge any additional fees or deficiencies, or credit any overpayments to Deposit Account No. 19-0743.

Respectfully submitted,

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. Box 2938
Minneapolis, MN 55402--0938
(949) 354-0200

Date 7/20/2012

By /Thierry Lo/
Thierry Lo
Reg. No. 49,097

Electronic Acknowledgement Receipt	
EFS ID:	13307124
Application Number:	12774231
International Application Number:	
Confirmation Number:	7527
Title of Invention:	Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems
First Named Inventor/Applicant Name:	Erik Caso
Customer Number:	74877
Filer:	Gregory M. Stark/John Gustav-Wrathall
Filer Authorized By:	Gregory M. Stark
Attorney Docket Number:	ENT0001-US
Receipt Date:	20-JUL-2012
Filing Date:	05-MAY-2010
Time Stamp:	18:29:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		3689001US1_resp_072012.pdf	132057 62b6798debfdbb2c964c9d4ed3e02376616531f3	yes	13

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Miscellaneous Incoming Letter	1	1
	Miscellaneous Incoming Letter	2	2
	Amendment/Req. Reconsideration-After Non-Final Reject	3	3
	Claims	4	9
	Applicant Arguments/Remarks Made in an Amendment	10	13
Warnings:			
Information:			
	Total Files Size (in bytes):	132057	

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Erik Michael Caso et al.

Title: Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems

Docket No.:	3689.001US1	Serial No.:	12/774,231
Filed:	May 5, 2010	Due Date:	July 26, 2012
Examiner:	Binh Ho	Group Art Unit:	2163
Customer No.:	21186	Confirmation No.:	7527

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

We are transmitting herewith the following attached items (as indicated with an "X"):

X Amendment and Response under 37 C.F.R. § 1.111 (11 pgs.)
X Communication Concerning Prior and Copending Applications (1 pg.)

If not provided for in a separate paper filed herewith, please consider this a PETITION FOR EXTENSION OF TIME for sufficient number of months to enter these papers and please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
Customer No.: 21186

By: /Thierry Lo/
Thierry Lo
Reg. No. 49,097

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Erik Michael Caso et al.	Examiner:	Binh Ho
Serial No.:	12/774,231	Group Art Unit:	2163
Filed:	May 5, 2010	Docket:	3689.001US1
Customer No.:	21186	Confirmation No.:	7527
Title:	Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems		

COMMUNICATION CONCERNING PRIOR OR COPENDING APPLICATION(S)

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

Pursuant to the guidance of MPEP §§ 2001.06(b) and 2004(9), Applicants would like to bring the following additional application(s) to the Examiner's attention. The identification of these applications is not intended to suggest that the subject matter claimed in any listed application is, or has been, substantially similar to any claim or claims in the present application.

Serial No./ Patent No.	Filing Date	Attorney Docket	Title
13/424,366	March 19, 2012	3689.001US2	Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems

Respectfully submitted,

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(949) 354-0200

Date 7/20/2012 By /Thierry Lo/

Thierry Lo
Reg. No. 49,097

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
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 displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
12/774,231	05/05/2010	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
FOR	NUMBER FILED	NUMBER EXTRA					
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 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			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 07/20/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $30 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $125 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** 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.

Legal Instrument Examiner:
/ERIC DANTZLER/

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.
12/774,231	05/05/2010	Erik Caso	ENT0001-US	7527

74877 7590 04/26/2012

King and Spalding LLP
1700 Pennsylvania Ave, NW
Suite 200
Washington, DC 20006

EXAMINER	
HO, BINH VAN	
ART UNIT	PAPER NUMBER
2163	

NOTIFICATION DATE	DELIVERY MODE
04/26/2012	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):

dbey@KSLaw.com
jpaolella-bald@kslaw.com

Dropbox Exhibit 1002 - Page 58
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Office Action Summary	Application No.	Applicant(s)	
	12/774,231	CASO ET AL.	
	Examiner	Art Unit	
	BINH V. HO	2163	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 May 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ 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.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-15* is/are pending in the application.

5a) Of the above claim(s) *8-12* is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-7 and 13-15* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *05/05/2010* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

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)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05/05/2010*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Dropbox Exhibit 1002 - Page 59
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

DETAILED ACTION

Claim Objections

1. Claim 7 is objected to because of the following informalities:

In claim 7, **"**modified**"** should be changed to – modified**. --**.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3, 7, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vesper (U.S. 2011/0110568) in view of Wills (U.S. 2012/0079117).

(Claim 1)

Vesper discloses substantially all of the elements, a process for establishing a singular file system across multiple devices comprising:

receiving user information to open an account *(102 of Fig. 14A)* for establishing a singular file system across multiple devices via a web-based system *(12 of Fig. 1A)* that includes at least one server *(14 of Fig. 1A)*;

installing an individual software client on each of the multiple devices via the web-based system *("the physician in block 116 is permitted to download the*

Client Application, also called the Viewing Application, software", paragraph [0155]; fig. 14A; "client viewer or viewing application 40", paragraph [0143]);

accepting registration of multiple devices via the web-based system *("In block 118, the physician receives a registration key and node ID", paragraph [0155]; Fig. 14A; paragraph [0104])*;

integrating by the at least one server the individual meta-indices to create a single master meta-index *("a PHI directory, also called a Central Index, that maintains pointers to the distributed locations of all copies of all PHIs in the system", paragraph [0073]; "Central Server 14 also includes database server 36. Database server 36 may run any suitable software, for example SQ L2000 or SQL2005. Database server 36 comprises the Central Index 38 and thus is the main repository for patient information (PHI) and the location of related records on the system", paragraph [0108])*;

providing by the at least one server the single master meta-index to each of the multiple devices via the individual software clients *("each node and the Central Index through the node component", paragraph [0142])*; and

continually updating the single master meta-index on the at least one server and each of the multiple devices in response to changes to the data indexed thereon *("The central index 3702 can use the DICOM header information to determine if the image is new or it is an update to an existing image. The central index 3702 can return either a new grid identifier or the grid identifier to update", paragraph [0303]);* except scanning each of the multiple devices by each of the individual software clients to inventory data on each of the multiple devices and create a

meta-index of the files for the inventoried data; providing by the individual software clients via the multiple devices individual meta-indices of the inventoried data for each of the multiple devices to the at least one server;.

Wills teaches scan and index data stored in a single device or a plurality of different devices (paragraph [0012]; Claim 19, 22).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to scan and index data stored in a plurality of different devices as shown by Wills in Vesper. The skilled artisan would have been motivated to improve, Vesper per the above in order to create an index of the files for the inventory data.

(Claim 2)

The combination of Vesper and Wills discloses substantially all of the elements of claim 1, and Vesper further discloses wherein the individual software clients vary according to the individual operating systems of each of the multiple devices *("The P2P network server 34 can run any suitable operating system and software", paragraph [0110]).*

(Claim 3)

The combination of Vesper and Wills discloses substantially all of the elements of claim 1, and Vesper further discloses wherein registration of the multiple devices includes selection of categories of data for each of the multiple

devices to be inventoried *("Users are also classified into groups based on their responsibilities and requirements", paragraph [0221])*.

(Claim 7)

The combination of Vesper and Wills discloses substantially all of the elements of claim 1, and Vesper further discloses wherein the meta-data includes at least information regarding file name, file type *("the system will transfer various types of data over its network in different functional scenarios", paragraph [0094]; [0243])*, file size, local path the file is stored in, date created, and date modified

(Claim 13)

Vesper discloses substantially all of the elements, a system for establishing a singular file system across multiple devices comprising:

a web-accessible server *("the Central Network 14 are accessed through the Internet or World Wide Web, in some instances as a web site", paragraph [0090]; Fig. 1B; paragraph [0101])*;

at least one software client plug-in *("The user application or viewer application 40 is the component record consumers use to view the current records available to that record consumer. Viewer application 40 allows multiple records to be loaded simultaneously in the application to allow side by side and other types of comparisons", paragraph [0160])*;

multiple devices for storing and operating on files *(Fig. 1A-B)*;

wherein the web-accessible server receives user information to open an account *(102 of Fig. 14A)* for establishing a singular file system across multiple devices, installs the at least one software plug-in on each of the multiple devices *("the physician in block 116 is permitted to download the Client Application, also called the Viewing Application, software", paragraph [0155]; fig. 14A; "client viewer or viewing application 40", paragraph [0143])*, accepts registration of the multiple devices, wherein the at least one software plug-in varies in accordance with an operating system of each of the multiple devices *("In block 118, the physician receives a registration key and node ID", paragraph [0155]; Fig. 14A; paragraph [0104])*;

further wherein the web-accessible server receives meta-indices from each of the multiple devices and integrates the meta-indices to create a single meta-index *("a PHI directory, also called a Central Index, that maintains pointers to the distributed locations of all copies of all PHIs in the system", paragraph [0073]; "Central Server 14 also includes database server 36. Database server 36 may run any suitable software, for example SQ L2000 or SQL2005. Database server 36 comprises the Central Index 38 and thus is the main repository for patient information (PHI) and the location of related records on the system", paragraph [0108])*, provides the single meta-index to each of the multiple devices via the individual software clients *("each node and the Central Index through the node component", paragraph [0142])*, and continually updates the single meta-index on each of the multiple devices in response to operations on the files indexed thereon *("The central index 3702 can use the DICOM header information to determine if the image is new or it is an update to*

an existing image. The central index 3702 can return either a new grid identifier or the grid identifier to update", paragraph [0303]); except further wherein the at least one software client plug-in scans its respective one of the multiple devices to inventory files thereon, creates a meta-index to files for the inventoried data, provides the meta-index of the inventoried data for its respective one of the multiple devices to the web-accessible server;.

Wills teaches scan and index data stored in a single device or a plurality of different devices (paragraph [0012]; Claim 19, 22).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to scan and index data stored in a plurality of different devices as shown by Wills in Vesper. The skilled artisan would have been motivated to improve, Vesper per the above in order to create an index of the files for the inventory data.

4. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vesper (U.S. 2011/0110568) in view of Wills (U.S. 2012/0079117) and further in view of Floyd (U.S. 2007/0153703).

(Claim 4)

The combination of Vesper and Wills discloses substantially all of the elements of claim 3, except wherein categories of data include documents, videos, pictures and music.

Floyd teaches a media category (e.g., audio, video, image, document, software, other or any) determining the category under which the advertisement will be presented (paragraph [0123]).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to have a media category include audio, video, image and document as shown by Floyd in Vesper and Wills. The skilled artisan would have been motivated to improve, Vesper and Wills per the above in order to provide to the user a category include audio, video, image and document.

5. Claims 5-6, 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vesper (U.S. 2011/0110568) in view of Wills (U.S. 2012/0079117) and further in view of Ben-Shaul (U.S. 2011/0231844).

(Claim 5)

The combination of Vesper and Wills discloses substantially all of the elements of claim 1, except wherein the individual software clients facilitate storage of the data within each of the multiple devices in accordance with the meta-data by modifying file systems of each of the multiple devices to include virtual files for data from the single meta-data index that is not local to a multiple device.

Ben-Shaul teaches the metadata information for a particular virtual disk may include: a virtual disk identifier that uniquely identifies that particular virtual disk; a device identifier that uniquely identifies a particular computing device that stores the disk

content of that particular virtual disk; and any other data associated with the particular virtual disk and/or the particular computing device, (paragraph [0047]).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to use a device identifier that uniquely identifies a particular computing device that stores the disk content of that particular virtual disk; and any other data associated with the particular virtual disk and/or the particular computing device as shown by Ben-Shaul in Vesper and Wills. The skilled artisan would have been motivated to improve, Vesper and Wills per the above in order to determine which virtual disk needs to be updated when disk content changes are received from a particular computing device, and to determine to which computing device to send images from a particular virtual disk.

(Claim 6)

The combination of Vesper and Wills discloses substantially all of the elements of claim 6, except wherein the individual software clients facilitate creation of a visual representation of the virtual files on a remote one of each of the multiple devices that is indistinguishable from a visual representation of an actual file that is located on a local one of the multiple devices.

Ben-Shaul teaches a set of images that collectively represents data that is stored at a particular computing device. For example, virtual disk 112a stores a set of images that store the data from computing device 130a, virtual disk 112b stores a set of images

that store the data from computing device 130b, and similarly virtual disk 112n stores a set of images that store the data from computing device 130n, paragraph [0045])

(Claim 14)

The combination of Vesper and Wills discloses substantially all of the elements of claim 13, except wherein the at least one software client plug-in facilitates storage of the files within its respective one of the multiple devices in accordance with the meta-data by modifying a file system of its respective one of the multiple devices to include virtual files for files from the single meta-index that are not local to the multiple device.

Ben-Shaul teaches the metadata information for a particular virtual disk may include: a virtual disk identifier that uniquely identifies that particular virtual disk; a device identifier that uniquely identifies a particular computing device that stores the disk content of that particular virtual disk; and any other data associated with the particular virtual disk and/or the particular computing device, (paragraph [0047]).

It would have been obvious to one having ordinary skill in the art at the time the invention was made to use a device identifier that uniquely identifies a particular computing device that stores the disk content of that particular virtual disk; and any other data associated with the particular virtual disk and/or the particular computing device as shown by Ben-Shaul in Vesper and Wills. The skilled artisan would have been motivated to improve, Vesper and Wills per the above in order to determine which virtual disk needs to be updated when disk content changes are received from a particular computing device, and to

determine to which computing device to send images from a particular virtual disk.

(Claim 15)

The combination of Vesper and Wills discloses substantially all of the elements of claim 14, except wherein the at least one software client plug-in facilitates creation of a visual representation of the virtual files on its respective one of the multiple devices that is indistinguishable from a visual representation of an actual file that is physically located on a another of the multiple devices.

Ben-Shaul teaches a set of images that collectively represents data that is stored at a particular computing device. For example, virtual disk 112a stores a set of images that store the data from computing device 130a, virtual disk 112b stores a set of images that store the data from computing device 130b, and similarly virtual disk 112n stores a set of images that store the data from computing device 130n, paragraph [0045])

Inquiry

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Binh V. Ho whose telephone number is 571 272 8583. The examiner can normally be reached on M-F from 8:00AM - 4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tony Mahmoudi can be reached on 571 272 4078. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/BINH V HO/
Examiner, Art Unit 2163

Binh V Ho
Examiner
Art Unit 2163

Notice of References Cited	Application/Control No. 12/774,231	Applicant(s)/Patent Under Reexamination CASO ET AL.	
	Examiner BINH V. HO	Art Unit 2163	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2012/0079117 A1	03-2012	Wills et al.	709/226
*	B	US-2011/0110568 A1	05-2011	Vesper et al.	382/128
*	C	US-2008/0189390 A1	08-2008	Heller et al.	709/218
*	D	US-2008/0082490 A1	04-2008	MacLaurin et al.	707/3
*	E	US-2010/0274982 A1	10-2010	Mehr et al.	711/162
*	F	US-2010/0205152 A1	08-2010	Ansari et al.	707/654
*	G	US-2011/0231844 A1	09-2011	Ben-Shaul et al.	718/1
*	H	US-7,805,565 B1	09-2010	Milligan et al.	711/114
*	I	US-2009/0062944 A1	03-2009	Wood et al.	700/94
*	J	US-2011/0093471 A1	04-2011	Brockway et al.	707/747
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Dropbox Exhibit 1002 - Page 71
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	"20100287219"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/23 16:55
S2	266	707/827.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/23 16:59
S3	770	717/176.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/23 17:00
S5	151	michael with abraham	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2011/12/23 17:01
S6	53	("20040172449" | "20050114711" | "20050138186" | "20050144195" | "20050144200" | "20050149481" | "20050256909" | "20060206533" | "20060277314" | "20070162510" | "20080104077" | "20090254592" | "6381019" | "6499054" | "6512586" | "6732158" | "6938042" | "7120692" | "7337171" | "7467187" | "7499905" | "7546353" | "7587467" | "7587471" | "7600036").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 19:01
S7	6	("7747999" "20030221190" "7266595").pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:14
S8	5	("7747999" "20030221190" "7266595").pn. and (install$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	ON	2012/01/31 21:18

Dropbox Exhibit 1002 - Page 72
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

			DERWENT; IBM_TDB			
S9	5	erik with caso	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:18
S10	1881	(install$6 same multipl$4 same (device user)).ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:22
S11	14	(install$6 same software same multipl$4 same (device user)).ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:25
S12	7366	717/168-178.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:32
S13	7335	717/168-178.ccls. and (install$6 multipl$4 device user)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:33
S14	5793	717/168-178.ccls. and (install$6 multipl$4 device user) with software	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:33
S15	756	717/168-178.ccls. and (install$6 multipl$4 device user) with software and registrat$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:33
S16	390	717/168-178.ccls. and (install$6 multipl$4 device user) with software and registrat$4 and inventor$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:34
S17	79	717/168-178.ccls. and (install$6 multipl$4 device user) with software and registrat$4 and inventor$4 and index$4	US-PGPUB; USPAT; USOCR;	OR	ON	2012/01/31 21:36

Dropbox Exhibit 1002 - Page 73
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
S18	1	"20100287219" and peer-to-peer	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/01/31 21:59
S22	6	("20060077189" "20080195693" "20090319635").pn. and (monitor device software install$6 inventor$4 plug$1in)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/12 23:10
S23	0	(("20040172449" | "20050114711" | "20050138186" | "20050144195" | "20050144200" | "20050149481" | "20050256909" | "20060206533" | "20060277314" | "20070162510" | "20080104077" | "20090254592" | "6381019" | "6499054" | "6512586" | "6732158" | "6938042" | "7120692" | "7337171" | "7467187" | "7499905" | "7546353" | "7587467" | "7587471" | "7600036").PN.) and cloud	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/13 18:05
S24	1	(("20040172449" | "20050114711" | "20050138186" | "20050144195" | "20050144200" | "20050149481" | "20050256909" | "20060206533" | "20060277314" | "20070162510" | "20080104077" | "20090254592" | "6381019" | "6499054" | "6512586" | "6732158" | "6938042" | "7120692" | "7337171" | "7467187" | "7499905" | "7546353" | "7587467" | "7587471" | "7600036").PN.) and index	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/13 18:38
S25	31	(michael with abraham) and index	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/13 18:46
S26	25	(michael with abraham) and index and (scan$4 inventor$4 collect$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/13 18:47
S27	4	(cloud$4 same storage same index$4).ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 13:08

Dropbox Exhibit 1002 - Page 74
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

S28	31	(cloud$4 same storage same index$4).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 14:34
S29	0	(cloud$4 same storage same index$4 same plug$1in).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 14:34
S30	62	(cloud$4 with storage with index$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 15:19
S31	5	(cloud$4 with storage with index$4) and plug$1in	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 15:19
S40	21	("20100257142" "20100257403" "20100199042" "20100274765" "20100191783" "20100229108" "20110110568" "20110093471" "20090164790" "20100274762" "7636764").pn. and (cloud storage index$4 metadata device log$1in registrat$4 categ$7 class$10 group$4 down$1load$4 up$1load$4 creat$4 collect$4 replicas Redundant$4 duplicat$4 replicat$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 22:18
S41	1	(scan$4 collect$4) with ((multipl$4 pluralit$4) near2 device) with (creat$4 near5 index$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 22:38
S42	3	(("20040172449" | "20050114711" | "20050138186" | "20050144195" | "20050144200" | "20050149481" | "20050256909" | "20060206533" | "20060277314" | "20070162510" | "20080104077" | "20090254592" | "6381019" | "6499054" | "6512586" | "6732158" | "6938042" | "7120692" | "7337171" | "7467187" | "7499905" | "7546353" | "7587467" | "7587471" | "7600036").PN.) and (index$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 22:40
S44	78	(scan$4 collect$4) with ((multipl$4 pluralit$4) near2 device) with index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2012/04/17 22:42

Dropbox Exhibit 1002 - Page 75
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

			IBM_TDB			
S45	38	(scan$4 collect$4) near5 ((multipl$4 pluralit$4) near2 device) with index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/17 22:42
S47	1	singlular near3 (file index$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 14:07
S49	141	((set$1up request$4) near5 account$4) with up$1load$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 14:52
S50	6	((set$1up request$4) near5 account$4) with up$1load$4 with (categ$8 class$10 group$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 14:53
S51	0	up$1load$4 with (categ$8 class$10 group$4) with cloud with index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 19:57
S52	13	up$1load$4 with (categ$8 class$10 group$4) with cloud	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 19:57
S53	0	(cloud$4 same up$1load$4 same index$4).ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 20:34
S54	1	(cloud$4 same up$1load$4 same index$4).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 20:34
S55	5	(storag$4 same up$1load$4 same index$4).ti.	US-PGPUB; USPAT; USOCR; FPRS;	OR	ON	2012/04/18 20:35

Dropbox Exhibit 1002 - Page 76
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

			EPO; JPO; DERWENT; IBM_TDB			
S56	57	(storag$4 same up$1load$4 same index$4).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 20:39
S57	20	(storag$4 same up$1load$4 same index$4 same device).ab.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 20:39
S62	1	"20120079117" and (pluralit$4 multipl$4 scan$4 collect$4 class$10 group$4 categ$8 index$4 registrat$4 log$1in device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 22:45
S63	3	(BLACKBURN with DAVID with A$1) and (storag$4 same up$1load$4 same index$4 same device) and (class$10 categ$7 group$4 device)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 22:46
S67	2	("20110110568" "20120079117") and (pluralit$4 multipl$4 scan$4 collect$4 class$10 group$4 categ$8 index$4 registrat$4 log$1in device account$4 log$1in cloud$4 transfer$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/18 23:30
S68	160	(set$1up$4 log$1in Account$4) near5 servic$4 near5 (cloud$4 back$1up)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/19 10:44
S69	41	((set$1up$4 log$1in Account$4) near5 servic$4 near5 (cloud$4 back$1up)) and index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/19 10:45
S70	19	((set$1up$4 log$1in Account$4) near5 servic$4 near5 (cloud$4 back$1up)) and index$4 and ((multipl$4 pluralit$4) near3 (unit device))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/19 10:46
S71	19	((set$1up$4 log$1in Account$4) near5 servic$4 near5 (cloud$4 back$1up)) and	US-PGPUB; USPAT;	OR	ON	2012/04/19 14:21

Dropbox Exhibit 1002 - Page 77
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

		index$4 and ((multipl$4 pluralit$4) near3 (unit device))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
S72	19	((set$1up$4 log$1in Account$4) near5 servic$4 near5 (cloud$4 back$1up)) and index$4 and ((multipl$4 pluralit$4) near3 (unit device)) and (class$10 categ$7 group$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/19 14:22
S75	6	("20110110568" "20120079117" "20080082490" "20080005168") and (pluralit$4 multipl$4 scan$4 collect$4 class$10 group$4 categ$8 index$4 registrat$4 log$1in device account$4 log$1in cloud$4 transfer$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/19 17:20
S77	6	("20110110568" "20120079117" "20080082490" "20080005168") and (pluralit$4 multipl$4 scan$4 collect$4 class$10 group$4 categ$8 index$4 registrat$4 log$1in device account$4 log$1in cloud$4 transfer$4 updat$4 modif$4 chang$4 individual$4 password)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/19 22:52
S78	5	categor$7 near5 (document and video and (pictur$4 imag$4 photo) and (music))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 10:55
S79	16	categor$7 near5 (document and video and (pictur$4 imag$4 photo) and (music audio))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 10:57
S83	2	creat$4 near3 virtual near4 (represent$6 display$4) near5 data near5 devices with (metadata index$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 12:23
S84	80	light$1weight$4 near5 metadata	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 12:26
S87	22	light$1weight$4 near5 metadata and index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 12:28

Dropbox Exhibit 1002 - Page 78
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

S88	45	light$1weight$4 near5 metadata and virtual$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 12:29
S89	13	light$1weight$4 near5 metadata and virtual$4 and index$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 12:29
S90	5340	virtual$4 near5 store$3 near5 device	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 13:21
S91	37	(virtual$4 near5 store$3 near5 device) with metadata	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2012/04/20 13:22

04/20/2012 6:48:19 PM
C:\Users\bho\Documents\EAST\Workspaces\12774231.wsp

Dropbox Exhibit 1002 - Page 79
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Form PTO-1449 (Rev. 2-32) U.S. Department of Commerce Patent & Trademark Office INFORMATION DISCLOSURE STATEMENT *(Use several sheets if necessary)*	Atty. Docket No. **ENT0001-US**	Serial No. **To Be Assigned**
	Applicant **Erik CASO, et al.**	
	Filing Date **Herewith**	Group **To Be Assigned**

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date (if appropriate)
		2009/0254592	10/8/09	Marinov, et al.	1	1	11/11/08
		7,600,036	10/6/09	Hesselink, et al.	709	234	6/2/05
		7,587,471	9/8/09	Yasuda, et al.	709	220	3/14/03
		7,587,467	9/8/09	Hesselink, et al.	709	214	11/13/04
		7,546,353	6/9/09	Hesselink, et al.	709	216	11/13/04
		7,499,905	3/3/09	Jaschek, et al.	1	1	10/17/05
		7,467,187	12/16/08	Hesselink, et al.	709	205	10/9/02
		2008/0104077	5/1/08	Gimpl, et al.	1	1	1/6/08
		7,337,171	2/26/08	Gimpl, et al.	1	1	5/12/05
		2007/0162510	7/12/07	Lenzmeier, et al.	707	200	12/30/05
		2006/0277314	12/7/06	Hesselink, et al.	709	229	8/16/06
		7,120,692	10/10/06	Hesselink, et al.	709	225	11/19/02
		2006/0206533	9/14/06	MacLaurin, et al.	707	200	3/14/05
		2005/0256909	11/17/05	Aboulhosn, et al.	1	1	12/15/04
		6,938,042	8/30/05	Aboulhosn, et al.	1	1	10/8/02
		2005/0149481	7/7/05	Hesselink, et al.	1	1	11/13/04
		2005/0144195	6/30/05	Hesselink, et al.	1	1	11/13/04
		2005/0144200	6/30/05	Hesselink, et al.	1	1	11/13/04

EXAMINER /Binh Ho/	DATE CONSIDERED 01/31/2012

EXAMINER: Initial if citation 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.

WDC_IMANAGE-1052702 v1-14682.105472

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /B.H./

Serial No. To Be Assigned (Docket No. ENT0001-US)
Information Disclosure Statement

U.S. PATENT DOCUMENTS CONT'D.							
		2005/0138186	6/23/05	Hesselink, et al.	709	229	11/13/04
		2005/0114711	5/26/05	Hesselink, et al.	726	4	11/13/04
		2004/0172449	9/2/04	Hesselink, et al.	709	204	3/5/04
		6,732,158	5/4/04	Hesselink, et al.	709	208	6/29/00
		6,512,586	1/28/03	Maris	356	432	11/13/01
		6,499,054	12/24/02	Hesselink, et al.	709	204	12/2/99
		6,381,019	4/30/02	Maris	356	432	6/30/00
FOREIGN PATENT DOCUMENTS							
		WO 04/046852	6/3/04	Senvid, Inc., et al.	G06F	15/16	11/6/03
		JP 2004-046661	2/12/04	Hitachi Ltd.	G06F	12/00	7/15/02
		WO 03/085559	10/16/03	Synerdrive, Inc.	G06F	17/30	4/3/03
		WO 02/003046	1/10/02	Brown University Research Foundation	G01N	21/00	6/26/01
		WO 01/040887	6/7/01	Senvid, Inc.	H04L	12/28	12/1/00
		WO 01/014634	3/1/01	AstenJohnson, Inc., et al.	D21F	1/00	8/18/00
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)							

EXAMINER	/Binh Ho/	DATE CONSIDERED	01/31/2012

EXAMINER: Initial if citation 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.

17676/105001
Doc. No. 1490629

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /B.H./

WDC_IMANAGE-1052702 v1-14682.105472

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12774231	CASO ET AL.
	Examiner	Art Unit
	BINH V HO	2163

SEARCHED			
Class	Subclass	Date	Examiner
707	827	04/18/2012	BH

SEARCH NOTES		
Search Notes	Date	Examiner
707/827;717/168-178 East search (see printout)	04/18/2012	BH
East search (Inventors)	04/18/2012	BH
Interference East search (see printout)	04/18/2012	BH
Google search (see printout)	04/18/2012	BH
East search (U.S. Pub.)	04/18/2012	BH

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12774231	CASO ET AL.
	Examiner	**Art Unit**
	BINH V HO	2163

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

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

CLAIM		DATE								
Final	Original	02/12/2012	04/18/2012							
	1	÷	✓							
	2	÷	✓							
	3	÷	✓							
	4	÷	✓							
	5	÷	✓							
	6	÷	✓							
	7	÷	✓							
	8	÷	N							
	9	÷	N							
	10	÷	N							
	11	÷	N							
	12	÷	N							
	13	÷	✓							
	14	÷	✓							
	15	÷	✓							

Dropbox Exhibit 1002 - Page 83
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Erik CASO, et al.		Art Unit:	**2163**
Serial No.:	**12/774,231**	Examiner:	**Binh Van Ho**
Filed:	**May 5, 2010**		

For: **METHOD FOR A CLOUD-BASED META-FILE SYSTEM TO VIRTUALLY UNIFY REMOTE AND LOCAL FILES ACROSS A RANGE OF DEVICES' LOCAL FILE SYSTEMS**

FILED ELECTRONICALLY

U.S. Patent and Trademark Office
Customer Service Window, Mail Stop Amendment
Randolph Building
401 Dulany Street
Alexandria, VA 22314

RESPONSE TO RESTRICTION REQUIREMENT

Sir:

In response to the Restriction Requirement mailed February 17, 2012, the undersigned elects Species/Group I, claims 1-7 and 13-15, without traverse.

Dropbox Exhibit 1002 - Page 84
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

REMARKS

In the Office Action mailed February 16, 2012, the Examiner imposed a restriction requirement pursuant to 35 U.S.C. §121, alleging that the instant application presented the following patentably distinct inventions:

I. Species I, a process for a process for establishing a singular file system across multiple devices comprising integrating by the at least one server the individual meta-indices to create a single master meta-index; providing by the at least one server the single master meta-index to each of the multiple devices via the individual software clients; and continually updating the single master meta-index on the at least one server and each of the multiple devices in response to changes to the data indexed thereon define by claims 1-7, 13-15, as illustrated in Fig. 2.

II. Species II, a process for operating on files located on multiple devices using a singular file system comprising if the peer-to-peer connection is brokered, transferring the physical file from the second device to the first device; and performing the operation on the file at the first device define by claim 8-12, as illustrated in Fig. 4.

The undersigned representative hereby elects Species/Group I: Claims 1-7 and 13-15, without traverse, for examination. The undersigned representative reserves the right to file a divisional application(s) covering the subject matter of the non-elected claims.

Dropbox Exhibit 1002 - Page 85
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

CONCLUSION

The undersigned representative respectfully submits that this election is responsive to the outstanding requirement. If the Examiner believes that the prosecution might be advanced by discussing the application with the undersigned representative, in person or over the telephone, we welcome the opportunity to do so. In addition, if any additional fees are required in connection with the filing of this response, the Commissioner is hereby authorized to charge the same to Deposit Account No. 50-4402.

Respectfully submitted,

Date: March 2, 2012
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4706
(202) 626-8978

By: */Dawn-Marie Bey - 44,442/*
Dawn-Marie Bey
Registration No. 44,442

17676/105001
Doc. No. 18332816

Dropbox Exhibit 1002 - Page 86
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Electronic Acknowledgement Receipt	
EFS ID:	12240712
Application Number:	12774231
International Application Number:	
Confirmation Number:	7527
Title of Invention:	Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems
First Named Inventor/Applicant Name:	Erik Caso
Customer Number:	74877
Filer:	Dawn-Marie Bey./Jeanne Paolella-Bald
Filer Authorized By:	Dawn-Marie Bey.
Attorney Docket Number:	ENT0001-US
Receipt Date:	06-MAR-2012
Filing Date:	05-MAY-2010
Time Stamp:	23:46:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response to Election / Restriction Filed	ent0001_resprr.pdf	136606 1059284f4ac249a4b22778468e252c61ceffb96b	no	3

Warnings:
Information:

Total Files Size (in bytes):	136606

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.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
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 displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
12/774,231	05/05/2010	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 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			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 03/06/2012	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 15	Minus	** 20	= 0	X $30 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $125 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** 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.

Legal Instrument Examiner:
/MARY HOLMES/

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.
12/774,231	05/05/2010	Erik Caso	ENT0001-US	7527

74877 7590 02/16/2012

King and Spalding LLP
1700 Pennsylvania Ave, NW
Suite 200
Washington, DC 20006

EXAMINER	
HO, BINH VAN	
ART UNIT	PAPER NUMBER
2163	

NOTIFICATION DATE	DELIVERY MODE
02/16/2012	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):

dbey@KSLaw.com
mblasik@kslaw.com
jpaolella-bald@kslaw.com

Dropbox Exhibit 1002 - Page 90
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Office Action Summary	Application No.	Applicant(s)	
	12/774,231	CASO ET AL.	
	Examiner	Art Unit	
	BINH V. HO	2163	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *1* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 May 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ 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.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-15* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☐ Claim(s) _____ is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☒ Claim(s) *1-15* are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *05/05/2010* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

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)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Dropbox Exhibit 1002 - Page 91
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

DETAILED ACTION

Election/Restrictions

1. This application contains claims directed to the following patentably distinct species of the claimed invention:

I. Species I, a process for a process for establishing a singular file system across multiple devices comprising integrating by the at least one server the individual meta-indices to create a single master meta-index; providing by the at least one server the single master meta-index to each of the multiple devices via the individual software clients; and continually updating the single master meta-index on the at least one server and each of the multiple devices in response to changes to the data indexed thereon define by claims 1-7, 13-15, as illustrated in Fig. 2.

II. Species II, a process for operating on files located on multiple devices using a singular file system comprising if the peer-to-peer connection is brokered, transferring the physical file from the second device to the first device; and performing the operation on the file at the first device define by claim 8-12, as illustrated in Fig. 4.

2. Applicant is required under 35 U.S.C. 121 to elect a single disclosed species for prosecution on the merits to which the claims shall be restricted if no generic claim is finally held to be allowable. Currently, no claim is generic.

Applicant is advised that a reply to this requirement must include an identification of the species that is elected consonant with this requirement, and a listing of all claims

readable thereon, including any claims subsequently added. An argument that a claim is allowable or that all claims are generic is considered nonresponsive unless accompanied by an election.

Upon the allowance of a generic claim, applicant will be entitled to consideration of claims to additional species which are written in dependent form or otherwise include all the limitations of an allowed generic claim as provided by 37 CFR 1.141. If claims are added after the election, applicant must indicate which are readable upon the elected species. MPEP § 809.02(a).

Should applicant traverse on the ground that the species are not patentably distinct, applicant should submit evidence or identify such evidence now of record showing the species to be obvious variants or clearly admit on the record that this is the case. In either instance, if the examiner finds one of the inventions unpatentable over the prior art, the evidence or admission may be used in a rejection under 35 U.S.C. 103(a) of the other invention.

3. A telephone call was made to Applicant's representative on 02/10/2012 to request an oral election to the above restriction requirement, but did not result in an election being made.

4. Applicant is advised that the reply to this requirement to be complete must include an election of the invention to be examined even though the requirement is traversed (37 CFR 1.143).

Inquiry

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BINH V. HO whose telephone number is (571)272-8583. The examiner can normally be reached on M-F from 8:00AM - 4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Don K. Wong can be reached on 571 272 1834. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BINH V HO/
Primary Examiner, Art Unit 2163

Binh V Ho
Examiner
Art Unit 2163

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	12774231	CASO ET AL.
	Examiner	**Art Unit**
	BINH V HO	2163

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

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

CLAIM		DATE								
Final	Original	02/12/2012								
	1	÷								
	2	÷								
	3	÷								
	4	÷								
	5	÷								
	6	÷								
	7	÷								
	8	÷								
	9	÷								
	10	÷								
	11	÷								
	12	÷								
	13	÷								
	14	÷								
	15	÷								

Dropbox Exhibit 1002 - Page 95
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

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
12/774,231	05/05/2010	Erik Caso	ENT0001-US

CONFIRMATION NO. 7527

74877
King and Spalding LLP
1700 Pennsylvania Ave, NW
Suite 200
Washington, DC 20006

PUBLICATION NOTICE

OC000000044460258

Title: Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems

Publication No.US-2010-0287219-A1
Publication Date:11/11/2010

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Dropbox Exhibit 1002 - Page 96
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

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
12/774,231	05/05/2010	Erik Caso	ENT0001-US

CONFIRMATION NO. 7527

74877
King and Spalding LLP
1700 Pennsylvania Ave, NW
Suite 200
Washington, DC 20006

NOTICE

OC000000041652831

Date Mailed: 05/20/2010

NOTICE OF INFORMAL APPLICATION

This application is considered to be informal since it does not comply with the regulations for the reason(s) indicated below. The period within to correct the informalities noted below and avoid abandonment is set in the accompanying Office action.

Items Required To Avoid Processing Delays:

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

A new oath or declaration, identifying this application number, or, if appropriate, an application data sheet (37 CFR 1.76), is required. The oath or declaration does not comply with 37 CFR 1.63 in that it:

- does not identify the complete mailing or post office address of each inventor.

Dropbox Exhibit 1002 - Page 97
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

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	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
12/774,231	05/05/2010		462	ENT0001-US	15	3

CONFIRMATION NO. 7527

74877
King and Spalding LLP
1700 Pennsylvania Ave, NW
Suite 200
Washington, DC 20006

FILING RECEIPT

OC000000041652830

Date Mailed: 05/20/2010

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Erik Caso, Santa Monica, CA;
Michael Abraham, Boulder, CO;

Assignment For Published Patent Application

Entangled Media LLC

Power of Attorney: The patent practitioners associated with Customer Number 74877

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/175,489 05/05/2009

Foreign Applications

If Required, Foreign Filing License Granted: 05/17/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 12/774,231**

Projected Publication Date: 11/11/2010

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **

Dropbox Exhibit 1002 - Page 98
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Title

Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems

Preliminary Class

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

Dropbox Exhibit 1002 - Page 99
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

Dropbox Exhibit 1002 - Page 100
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

PTO/SB/05 (08-08)
Approved for use through 06/30/2010. OMB 0651-0032
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 displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. 1.53(b))

Attorney Docket No.	ENT0001-US
First Inventor	Erik CASO, et al.
Title	Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☐ **Fee Transmittal Form (e.g., PTO/SB/17)**
   (Submit an original and a duplicate for fee processing)
2. ☒ **Applicant claims small entity status.**
   See 37 CFR 1.27.
3. ☒ **Specification** [*Total Pages* 20]
   Both the claims and abstract must start on a new page
   (For information on the preferred arrangement, see MPEP 608.01(a))
4. ☒ **Drawing(s)** (*35 U.S.C.113*) [*Total Sheets* 6]
5. **Oath or Declaration** [*Total Sheets* 3]
   a. ☒ Newly executed (original or copy)
   b. ☐ A copy from a prior application (37 CFR 1.63 (d))
   (for a continuation/divisional with Box 18 completed)
   i. ☐ DELETION OF INVENTOR(S)
   Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☐ **Application Data Sheet.** See 37 CFR 1.76
7. ☐ **CD-ROM or CD-R** in duplicate, large table or Computer Program *(Appendix)*
   ☐ Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
   (if applicable, items a.-c. are required)
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
   i. ☐ CD-ROM or CD-R (2 copies); or
   ii. ☐ Paper
   c. ☐ Statements verifying identity of above copies

ADDRESS TO: **Commissioner for Patents**
P.O. Box 1450
Alexandria VA 22313-1450

ACCOMPANYING APPLICATIONS PARTS

9. ☒ **Assignment Papers** (cover sheet & document(s))
   Name of Assignee Entangled Media LLC
10. ☐ **37 C.F.R. 3.73(b) Statement** ☐ **Power of Attorney**
    (when there is an assignee)
11. ☐ **English Translation Document** *(if applicable)*
12. ☒ **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    ☒ Copies of citations attached
13. ☐ **Preliminary Amendment**
14. ☐ **Return Receipt Postcard** (MPEP 503)
    (Should be specifically itemized)
15. ☐ **Certified Copy of Priority Document(s)**
    (if foreign priority is claimed)
16. ☐ **Nonpublication Request** under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
17. ☒ Other: Filed Electronically

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____ / _____

Prior application information: *Examiner* _____ *Art Unit:* _____

19. CORRESPONDENCE ADDRESS

☒ The address associated with Customer Number 74877 *OR* ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	/Dawn-Marie Bey - 44,442/		Date	May 5, 2010	
Name (Print/Type)	Dawn-Marie Bey			Registration No. (Attorney/Agent)	44,442

This collection of information is required by 37 CFR 1.53(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: Mail Stop Patent Application, 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.

METHOD FOR A CLOUD-BASED META-FILE SYSTEM TO VIRTUALLY UNIFY REMOTE AND LOCAL FILES ACROSS A RANGE OF DEVICES' LOCAL FILE SYSTEMS

Cross-Reference to Related Applications

[0001] The present application claims the benefit of and incorporate by reference herein in its entirety United States provisional patent application serial no. 61/175,489, filed May 5, 2009 entitled Method For Virtual Synchronization Of Data Across Heterogeneous Devices And Performing On-Demand Transfer Of Remote Data Between Devices.

Background of the Invention

Field of the Invention:

[0002] The present invention relates generally to the field of data virtualization and more specifically to a system and method for using data virtualization coupled with a cloud-based file system that is shared among devices and integrated into the device operating system so as to unify the representation of files across devices for availability of and access to data across multiple devices a user might own.

Description of the Related Art:

[0003] Competitive data synchronization products generally fall into one of two types:

locally installed software for file replication across devices and online backup/storage based file replication across devices. The local install file replication software is installed on computers and makes sure that all devices with the same software have the same data physically replicated on each device. Once configured by the user, it is able to identify updates to files on one device and update the corresponding files on other devices. These products or services essentially duplicate all designated data between the devices being synchronized. Each file stored on N devices results in N duplicates of the same file. The online backup/storage based file replication software is a blend of software that installed on local devices along with online storage. The process requires that ALL designated data is stored online and is then in turn replicated across all devices that are connected to the online storage server. These services duplicate all designated

Dropbox Exhibit 1002 - Page 102
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

data between devices being synchronized, AND store an additional copy on their servers. Each file stored on N devices results in N+ 1 duplicates of the same file.

Summary of the Invention

[0004] The most obvious shortcoming of the data synchronization implementations described above is the amount of storage space that is required. For individual users with multiple devices, each with varying storage capacity, synchronization across all devices for all content on all devices is limited or even prohibited by space restrictions. Additionally, present solutions to the storage problem can be expensive, requiring payment for third party on-line storage or device storage upgrades. It is also important to note that with other solutions the data on separate devices is kept separated when synchronized- local data is stored in a set of locations within the operating system's native file system (e.g. "My Documents", "My Pictures", etc.), while remote data on other devices or other online services is kept in a new location such as a new directory/folder or secondary location (e.g., removable hard drive) mounted on the device. Finally, present solutions generally require a high-degree of user involvement for their operation – users must designate certain files and/or directories for synchronization or backup, and must consciously store content to be synced or backed-up in those locations. Accordingly, there is a need in the art for a system and process that facilitates access to content that physically resides on any one of multiple user devices, e.g., laptop, desktop, personal digital assistant (PDA), cell phone or the like, from any one of the multiple user devices without the need to physically store all content on every device, and without complex configuration or continual interaction from the user and without the data from multiple devices being treated as separate and, thus, segregated within the file system as such.

[0005] As described in detail herein, the present solution creates a unified representation of all data on all registered devices – it ensures that all a user's devices appear to share one single native file system containing all the user's files across all devices, and that this file system is that of the device operating system, instead of any third party solution or secondary representation. Unlike the existing solutions, the implementations described herein do not require physical data replication across multiple devices. Instead, the present solution creates a virtual representation of data on all of the devices using metadata indexing. This virtual representation of data means

Dropbox Exhibit 1002 - Page 103
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

that the files are not actually stored on all devices and thus, with the exception of a single physical location, they take up limited space (i.e. storage) on any additional device's hard drive. This allows for otherwise impossible amounts of data to be virtually stored on each device, even if there is no physical storage room available for the data on each device. Furthermore, the present solution does not require data to be stored on a provider server, but instead stores only lightweight metadata (small fraction of information about the files) online. The solution establishes the ability for user devices to be aware of one another and communicate directly when data is requested. In addition to user devices, the solution described herein can also incorporate files stored in an online service account, such as a photo account or video account (exemplary- YouTube.com or Picasa.com). Finally, beyond initial installation, the present solution requires no configuration or interaction with the user to virtualize any and all data across all devices. Rather than act as software that is interacted with by the user, the present solution is designed to integrate with the operating system on a device and thus modify said operating system to not only account for files that are stored locally on the device (e.g. on the hard drive), but also account files on all other devices the user may own. This is done without adding additional storage locations, such as a networked storage location or a sync folder; it is done without the user having to continually designate files for inclusion or exclusion. Moreover, it does not present the user with a new or additional user interface, but rather relies entirely on the device operating system for such user interaction.

[0006] The solution described herein unifies the representation of and access to files and data across all of a user's devices, as well as online service accounts.

[0007] In a first exemplary embodiment of the present invention a process for establishing a singular file system across multiple devices is described. The process includes: receiving user information to open an account for establishing a singular file system across multiple devices via a web-based system that includes at least one server; installing an individual software client on each of the multiple devices via the web-based system; accepting registration of multiple devices via the web-based system; scanning each of the multiple devices by each of the individual software clients to inventory data on each of the multiple devices and create a meta-index of the files for the inventoried data; providing by the individual software clients via the multiple devices individual meta-indices of the inventoried data for each of the multiple devices to the at least one server; integrating by the at least one server the individual meta-

Dropbox Exhibit 1002 - Page 104
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

indices to create a single master meta-index; providing by the at least one server the single master meta-index to each of the multiple devices via the individual software clients; and continually updating the single master meta-index on the at least one server and each of the multiple devices in response to changes to the data indexed thereon.

[0008] In a second exemplary embodiment of the present invention a process for operating on files located on multiple devices using a singular file system is described. The process includes: accepting a request to operate on a file at a first device, wherein the file is selected from the singular file system on the first device; intercepting the request by a software client on the first device; determining by the software client if the file is physically located on the first device or a second device, wherein a visual representation of the singular file system on the first device is identical to a visual representation of the singular file system on the second device; if the file is physically located on a second device, requesting by the software client on the first device that a peer-to-peer connection be brokered by a server-based web service between the first device and the second device; if the peer-to-peer connection is brokered, transferring the physical file from the second device to the first device; and performing the operation on the file at the first device.

[0009] In a third exemplary embodiment, a system for establishing a singular file system across multiple devices is described. The system includes: a web-accessible server; at least one software client plug-in; multiple devices for storing and operating on files; wherein the web-accessible server receives user information to open an account for establishing a singular file system across multiple devices, installs the at least one software plug-in on each of the multiple devices, accepts registration of the multiple devices, wherein the at least one software plug-in varies in accordance with an operating system of each of the multiple devices; further wherein the at least one software client plug-in scans its respective one of the multiple devices to inventory files thereon, creates a meta-index to files for the inventoried data, provides the meta-index of the inventoried data for its respective one of the multiple devices to the web-accessible server; further wherein the web-accessible server receives meta-indices from each of the multiple devices and integrates by the meta-indices to create a single master meta-index, provides the single master meta-index to each of the multiple devices via the individual software clients, and continually updates the single master meta-index on each of the multiple devices in response to operations on the files indexed thereon.

Dropbox Exhibit 1002 - Page 105
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Brief Description of the Figures

[0010] The following Figures are intended to be considered in conjunction with the descriptions provided herein and represent exemplary systems and processes of the present invention.

[0011] **Figure 1** is a schematic showing an exemplary configuration of the components of the invention;

[0012] **Figure 2** is a device registration and data virtualization process flow in accordance with an exemplary embodiment of the present invention;

[0013] **Figure 3** is a device registration and data virtualization process flow in accordance with an exemplary embodiment of the present invention;

[0014] **Figure 4** is a file retrieval process flow in accordance with an exemplary embodiment of the present invention;

[0015] **Figure 5** is a schematic showing the exemplary configuration of **Figure 1** with communication paths therebetween; and

[0016] **Figure 6** illustrates an exemplary unified file structure scenario.

Detailed Description of the Invention

[0017] The following words and phrases are used throughout this document and are attributed the definitions provided below for the purposes of describing the invention. One skilled in the art recognizes that there are obvious extensions to certain of these definitions and these are intended to fall within the scope of the listed definition, even if not explicitly reference therein.

[0018] Devices - Internet-enabled devices that may be used for a variety of communications and data purposes, including document creation, media players, Internet browsing, etc. These devices include desktop computers, laptop computers, netbooks, mobile Internet Devices (MIDs), smartphone mobile handsets, "nettop" computers, gaming consoles, cable set-top boxes, televisions and other computing devices and telecommunications devices that are able to communicate using any form of data communications protocols such as TCP/IP, 30, CDMA, GSM, OSM, WiFi, WiMax, etc.

Dropbox Exhibit 1002 - Page 106
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0019] File System – is the component within an operating system responsible for managing all manner of files, as well as presenting them within a graphical user interface. The native file system of any given operating system has a set of standard file storage options, such as "My Documents" for documents, "My Music" for music, "My Pictures" for pictures, and so on. Local file systems allow for secondary file systems to be "mounted" and even accommodate the tracking of such file, but in all cases are managed separately. An example of this would be a USB thumb drive, which, when plugged into a computer, is mounted as a secondary storage location.

[0020] Local Device - is a device that a user (person) is currently using (i.e. they are in front of the device and actively using it).

[0021] Remote Device - is a device that the user (person) is not using; this device is in another location and is only accessible via an Internet connection.

[0022] Software Client (or the Client) - is a piece of software that is installed and runs continuously on the device.

[0023] Web Service - is a part of the system that operates on the Internet and is made up of several types of web technologies including web servers, databases, peer-to-peer services (e.g., jingle, BitTorrent, Skype, JXTA), an HTTP Relay and other systems that interact with the clients. The web service acts as an information manager that coordinates information, communication and activities with the clients. It also coordinates the transfer of files between devices by establishing a transfer protocol, such as peer-to-peer or HTTP relay, or other such method, depending on the type of connection that is available for a given network or Internet connection.

[0024] Referring to **Figure 1** an exemplary system includes of a server **10** which hosts a web service and various user devices such as PDA **12**, laptop computer **14** and desktop computer **16** with a particular software client installed thereon, to facilitate the virtual unification of data, including documents and media files, across all devices **12, 14** and **16**. The system facilitates transfer of data (e.g. files) on-demand between devices when requested. The devices **12, 14** and **16** are merely exemplary and can vary in their number, type, use and operating system/platform, ranging from mobile phones to desktop computers to gaming consoles or cable set-top boxes, each running a different operating system that uses a proprietary and different file system. In

Dropbox Exhibit 1002 - Page 107
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

addition to user devices, the solution described herein can also incorporate files stored in an online service account, such as a photo account or video account (exemplary- YouTube.com or Picasa.com). Additionally, though a single server is shown for illustration purposes, multiple servers, databases, processors may be used to implement the invention.

[0025] The system's method of data unification does not rely on file replication or cloning, but instead creates "virtual" file unification using a proprietary technique of differentiating local, physically stored data files versus remote data files and creating a unified, virtual representation of remote data on a local device. The system uses an operating-system extension, in conjunction with an intelligent web service, to determine the varying types of data that exist on each device that is a part of the system. The system will differentiate data on a Local Device from data on a Remote Device. The system then communicates to each client what data is remote so that each client can create the virtual representation of the remote data within its local device file system. The client creates the virtual representation of all remote files using the same "path" or storage location on the remote device, resulting in a common, single view of all data across all devices that is consistent with the formatting and structure of the local file system.

[0026] Critical to the unique nature of this system is that it is totally transparent, not requiring the user to interact with software, nor distinguish files in local vs. remote locations. All file metadata is integrated into the local device so that the view of data is common across all devices as if the files were actually stored locally across all devices, even though they are not. In essence, each device file system then acts as if it is a shared file system; enabling the local operating system to manage remote and local file as if they are all stored in the same location. For example, moving a file on one device results in the file moving on all other devices, even if it was moved on a device where that file is virtual.

[0027] Referring to **Figure 2**, a detailed overview of a first exemplary process from user sign-up to virtual file access across devices is shown. In **S10**, access to the system is accomplished via creation of a user account with the provider of the service. Registration information includes user name, e-mail address and other required personal information as well as creation of user name and password to facilitate establishing and securing a user account. Once an account has been created, the user can install the required software client on each of

Dropbox Exhibit 1002 - Page 108
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

their individual devices and initiate the process of registering each device with the service provider **S12**. As part of the registration process, for each individual user device, the user names the device, e.g., laptop, desktop, smartphone (e.g., Blackberry, Droid), and selects the type or category of data, e.g., documents (exemplary: text), pictures (exemplary: .jpg, .img), audio (exemplary: MP3), video (exemplary: .dvi, files .mov files) available on the device that the user wishes to virtually unify across multiple devices. In a preferred embodiment, all categories are automatically selected. Alternatively, this selection may be accomplished by a drop down menu listing file types, categories, extensions, etc. For online service accounts, the user registers these accounts and provides appropriate log-in information, e.g., username and password. As described below, once this selection is made, the installed software client then scans and inventories the selected data into a meta-index of the file system and reports back to the web service on that selected data **S14** in order to create a singular file system based on said metadata that is shared among all devices in the user's account. Alternatively, once the software client is installed on the user device, it could automatically scan and inventory all the data available on the user device and report back to the service provider. The web service can then create a listing of the inventory and prompt the user to select which data the user wishes to virtually synchronize.

[0028] The software client provides user device data in the form of a meta-index. For each identified data file, the meta-index includes metadata such as file name, file type, file size, local path the file is stored in, date created, date modified, etc. Once all of the user's devices and on-line service accounts are registered and meta-indexed by the software client **S16** (or the service provider in the case of the on-line service accounts by interacting through the respective application programming interfaces (APIs) of the on-line services to obtain data information), the web service integrates all of the individual meta-indices for all of the user's registered devices into a database **S18**. This master index of metadata thus becomes the singular file system that all devices use; integrated locally into a device's operating system via the software client. The web service then sends the meta-indices for each of the registered devices to each of the other individual registered user devices **S20**. At each registered local device, the software client integrates metadata from the remote device indices into the local device's file system **S22.** The metadata instructs the software client where to store the data files, ensuring that a common view and storage location is maintained across all devices. At this point, the local operating

Dropbox Exhibit 1002 - Page 109
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

system's file system has been modified to include remote files in the same locations of the local device (such as the "My Documents" folder) as opposed to a separate and segregated location for such remote data (such as a synchronization folder or an additional hard drive "mounted" on the device.) Further, the software client facilitates the creation of a visual representation of the remote or virtual files on the local device, as if the files were indeed local, allowing the user to operate on them as if they were local to the device. The virtual files appear in essentially all ways the same as a local file, making them indistinguishable unless such a distinction is enabled as a separate option. Lastly, if a unique folder or directory exists on one device (e.g. within the My Documents folder) and has several files within it, that folder/directory is created on all other devices so that its files may be put within said folder/directory, ultimately representing the same path to all corresponding files.

[0029] Using their local device, the user attempts to operate on a file **S24**. If the file is a local file, physically located on the local device, the operation is performed on the local file and the software client notifies the web service to update the meta-index to reflect any changes to the attributes of the file, e.g., substantive, location or existence thereof **S26, S28**. If the user attempts an operation on a virtual file that is physically stored on a remote device, the software client intercepts the operation request and, if the file is to being opened or executed, the software client brokers a connection between the remote device containing the physical file and the local device requesting the file **S30**. The file is then transferred from the remote device to the local device and the operation is performed on the file at the local device. As in **S28**, details regarding the location, status, and existence of the file are provided to the web service by the local software client which allows all other devices being unified to be continuously made aware of the changes in the location or existence of the file **S30**. Once the file has been transferred from the remote device to the local device, it can be viewed, edited, or modified in any way by the user. Upon completion of any modification to the file, all changes are propagated back to the remote device and the local file is restored to its 'virtual' state. At this point the local device removes the aforementioned file from memory, so that it is stored only in the single location/device on which it was originally kept. Additionally, the aforementioned file's metadata is updated (such as "date last modified") and propagated to all other devices. The method of file transfer may vary, initially attempted via peer-to-peer methodology. Under certain circumstances, a peer-to-peer connection might be prohibited from occurring, at which point the web service will itself manage

Dropbox Exhibit 1002 - Page 110
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

the connection (via HTTP Relay) between devices to ensure communication can always occur. Alternatively, for virtual files located with an on-line service provider, when the user attempts to operate thereon from a local device file system, a browser window is opened within the on-line service to facilitate operation.

[0030] **Figure 3** illustrates an alternative exemplary process flow. In this flow, which is substantially similar to the process flow from **Figure 2**, this flow illustrates the process flow wherein there is only a single registered user device and devices are added sequentially. After creating an account **S50**, the user registers a device **S52** and the downloaded software client creates a meta-index for the device data and stores in the web service database **S54**. If the user has no other registered devices ("NO" to **S56)**, when the user performs operations on device files **S64**, the answer to the question "Is the file a virtual file?" **S66**, will always be "NO" and the software client will report local file changes to the web service **S68**.

[0031] If the user does have other registered devices ("YES" to **S56**), the process **S58-S70** follows the same flow as steps **S20-S30** in **Figure 2**.

[0032] Accordingly, if a user has a desktop computer and laptop computer and a smartphone, the processes described herein essentially unify the data across those devices once they are registered them with the web service. The user can add and remove devices associated with their customer account at their convenience. The data that is unified across the devices correlates specifically to what devices the user adds to their customer account.

[0033] The embodiments described herein create a single unified file system that is shared across multiple devices a user might own. The software client provided by the web service to facilitate this unification is downloaded to a user's individual devices as described above. The software client is provided in the form of an operating system extension, or 'plug-in' that is unique to the type of device/operating system which is established at the time of registration. The plug-in modifies the natural behavior of the operating systems of the individual registered devices in a way that, as it pertains to remote files, prevents the operating system from doing what it normally does. This is akin to rewriting the behavior of the operating system itself and how it treats files and, thus, runs in a mode that *is* the operating system. This is different from software that runs in a mode that is secondary to the operating system's operations. The software client is responsible for at least: indexing the device data in a meta-index in accordance

Dropbox Exhibit 1002 - Page 111
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

with user selection of data types; providing the meta-index for its device to the web service; receiving meta-index information for all other registered devices on the user's account; creating virtual files in the file system of its device in the file system format of its device; updating the file system of its device to reflect changes to all virtual (remote) files in accordance with meta-index changes provided by the web service; informing the web service of changes to local files; facilitating communications between its device and other registered devices to retrieve remote files for operation on the local device.

[0034] The virtual files appear to the user exactly as local files. For example, each virtual file includes a thumb nail with an icon, it would have the file name, the file size, the file type, the date it was created, the date it was modified, all that the physical file has except that it doesn't take any space on the local device with the exception of the space required for meta-data storage (less than 1 kilobyte per file). The virtual files act as mock files and mock the properties of the physical file. By way of example, if the physical file of File.DOC_{PHY} is located on the hard drive of Device A, a virtual file of File.DOC_{VIR} will be located in the same corresponding file directory of the hard drive on registered Device B and Device C. When the user moves File.DOC_{PHY} from its stored directory (e.g. …/My Documents/Proposals) on the hard drive of Device A to the desktop directory of Device A, this move will be indexed by the software client of Device A, provided to the web service, the user meta-index database at the web service will be updated to reflect the move, the software clients of Devices B and C will be notified of the move and the software clients of Devices B and C will updated Devices B and C, respectively, to show File.DOC_{VIR} on the desktops (or equivalent locations) thereof. Conversely, if the same actions were performed on a virtual file, instead of the physical file, the same corresponding routines and results would occur, thus ensuring that regardless of a user interacting with the physical or virtual version of a file, they are treated as if they were the same.

[0035] The software client described herein acts as an operating system plug-in to intercept calls made to files and programs in the file system of the respective user devices. An exemplary description of software client functionality responsive to calls to the file system is described below and illustrated in **Figure 4**. When the user attempts to open a file on their local Device A **S100**, the application associated with the file, for example, Adobe Reader in the case of a .pdf file, talks to the file system and requests that the selected .pdf file be opened for read access **S105**. The software client intercepts this request from the operating system **S110** and

Dropbox Exhibit 1002 - Page 112
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

checks its metadata to determine whether the selected file is a local file or a virtual file (remote file) **S115**.

[0036] In the case of a local file, there is no action required by the software client and the file system returns the command to the operating system to open the file **S120**. In the case of a virtual file, the software client on Device A determines from the file's metadata the remote device on which it is stored (Device B) and asks the web service to broker a connection between Device A and Device B **S125**. The web service determines what type of connection is possible between Device A and Device B and instructs both devices of the communication protocol and parameters to be used for the transfer. Initially, the web service determines if a peer-to-peer connection is available **S135**. If that peer to peer (p-to-p) connection is possible, Device B sends the physical file directly to Device A for operation on Device A **S140**. In instances where a p-to-p connection is not possible, e.g., due to firewall restrictions, the web service acts as an HTTP relay server **S145**. During the time that the request to Device B for the file transfer to Device A is happening, the operating system, and in turn the requesting application (Adobe Reader) has no idea that the requested file is not local to Device A and is simply waiting for that command to return the number of bytes that it requested so that it can display them. The software clients, in combination with the web service, transparently perform numerous commands to request, locate and retrieve a physical copy of the virtual file without the knowledge of the requesting application or operating system. Further, the entirety of the physical file need not be downloaded in order to be responsive to most actions, so, just as with streaming video, the underlying transfer continues while the user action is taking place with the initial buffer of required bytes (e.g., approximately 32 kilobytes per read operation in the case Adobe Reader running on Mac OS X, version 10.6) **S150**.

[0037] **Figure 5** is a schematic exemplifying various devices as described with respect to **Figure 1** and connections between the devices constituting a user's closed data virtualization system in accordance with the descriptions herein.

[0038] In the exemplary embodiments described herein, the software clients recognize and account for differences in file structures and nomenclature. So, for example, documents stored in the "Documents" folder of a user's registered Mac would show up in the "My Documents" folder of a Windows system registered to the same user. The software client and

Dropbox Exhibit 1002 - Page 113
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

web service perform a logical mapping between available desktop platforms, e.g., Windows, Mac, Linux. Figure **6** illustrates an exemplary unified file structure $\mathbf{20}_{\mathbf{UFS}}$ created from the individual device file structures $\mathbf{12}_{\mathbf{UFS}}$, $\mathbf{14}_{\mathbf{UFS}}$ and $\mathbf{16}_{\mathbf{UFS}}$ and on-line service file structure $\mathbf{18}_{\mathbf{UFS}}$ in accordance with the methods described herein. This unified file structure $\mathbf{20}_{\mathbf{UFS}}$ will replace file structures $\mathbf{12}_{\mathbf{UFS}}$, $\mathbf{14}_{\mathbf{UFS}}$ and $\mathbf{16}_{\mathbf{UFS}}$ in devices **12**, **14** and **16**. The file structure of on-line service **18** is not be unified.

[0039] Other than mapping between the 'canonical' elements of the file system, the software does not interfere with the user's choice of file locations. For example, if a registered user chooses to store music files in their Windows 'Desktop' folder, rather than under their 'My Music' folder, as is the convention, the software will respect their choice and make those files appear under the 'Desktop' folder of their other registered devices. Furthermore, the system is able to create unique directories on the device in order to maintain the appropriate path for a given file (in the case where a user manages their file system to have a naming system for how they store their files). In the specific cases where two devices each have a different file but with the same path, the system will employ a process for resolution. For example, the system may use a naming convention to resolve the collision and show both files on each device. For example, if there are 2 registered devices called 'Mac' and 'Windows', and a file called 'resume.doc' under 'Desktop' in both devices, the system creates 2 separate files on each device. On 'Mac', a local file called 'resume.doc' and a remote file called 'resume (Windows).doc' which is a virtual file on the local 'resume.doc' located on the 'Windows' device. On 'Windows', a local file called 'resume.doc' and a remote file called 'resume (Mac).doc which is a virtual file on the local 'resume.doc' located on the 'Mac' device. This resolution method is but one non-limiting example. One skilled in the art recognizes that other methodologies may be employed to resolve collisions in a transparent and completely automatic manner.

[0040] For certain devices, the logical mapping is not as readily accomplished as it is with established operating systems such as Mac, Windows, and Linux. For example, while numerous mobile devices, gaming consoles, cable set top boxes, televisions and other computing devices and telecommunications devices can certainly store documents, pictures, video, music and the like, the operating systems, file structures and interfaces vary significantly from one another and from the established personal computer systems. Accordingly, when a user registers mobile devices such as the iPhone, Droid or other smart phones, the listing of virtual files in an

Dropbox Exhibit 1002 - Page 114
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

established file directory may not be feasible. Accordingly, such devices may store all virtual files in an application that is downloaded as part of the software client. When a user wishes to access content that is physically stored on a different device, the user would search for the file in the dedicated software client application.

[0041] The software embodiments may include but are not limited to firmware, resident software, microcode, etc. Furthermore, the invention can take the form of a computer program product accessible from a computer-usable or computer-readable medium providing program code for use by or in connection with a computer or any instruction execution system. For the purposes of this description, a computer-usable or computer readable medium can be any tangible apparatus that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device. The medium can utilize electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device) or a propagation medium (though propagation mediums in and of themselves as signal carriers are not included in the definition of physical computer-readable medium). Examples of a physical computer-readable medium include a semiconductor or solid state memory, magnetic tape, a removable computer diskette, a random access memory (RAM), a read-only memory (ROM), a rigid magnetic disk, and an optical disk. Current examples of optical disks include compact disk – read only memory (CD-ROM), compact disk – read/write (CD-R/W) and DVD.

[0042] A data processing system suitable for storing and/or executing program code includes at least one processor coupled directly or indirectly to memory elements through a system bus. The memory elements can include local memory employed during actual execution of the program code, bulk storage, and cache memories that provide temporary storage of at least some program code in order to reduce the number of times code must be retrieved from bulk storage during execution. Input/output or I/O devices (including but not limited to keyboards, displays, pointing devices, etc.) can be coupled to the system either directly or through intervening I/O controllers. Network adapters may also be coupled to the system to enable the data processing system to become coupled to other data processing systems or remote printers or storage devices through intervening private or public networks, including various client-server configurations. Modems, cable modem, and Ethernet cards are just a few of the currently available types of network adapters.

Dropbox Exhibit 1002 - Page 115
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0043] Moreover, the disclosed processes may be readily implemented in software, e.g., as a computer program product having one or more modules each adapted for one or more functions of the software, executed on a programmed general purpose computer, cellular telephone, PDA, a special purpose computer, a microprocessor, or the like. In these instances, the systems and methods of this invention can be implemented as a program embedded on a personal computer such as a JAVA, CGI or Perl script, as a resource residing on a server or graphics workstation, as a routine embedded in a dedicated image system, or the like. The systems and methods of this invention can also be implemented by physically incorporating this system and method into a software and/or hardware system, such as the hardware and software systems of a computer. Such computer program products and systems can be distributed and employ a client-server architecture, a peer-to-peer network or a combination thereof.

[0044] It is to be appreciated that the various components of the technology can be located at distant portions of a distributed network and/or the Internet, or within a dedicated secure, unsecured and/or encrypted system. Thus, it should be appreciated that the components of the system can be combined into one or more devices or co-located on a particular node of a distributed network, such as a telecommunications network. As will be appreciated from the description, and for reasons of computational efficiency, the components of the system can be arranged at any location within a distributed network without affecting the operation of the system. Moreover, the components could be embedded in a dedicated machine.

[0045] Furthermore, it should be appreciated that the various links connecting the elements can be wired or wireless links, or any combination thereof, or any other known or later developed element(s) that is capable of supplying and/or communicating data to and from the connected elements. The terms software client and web service as used herein can refer to any known or later developed hardware, software, firmware, or combination thereof that is capable of performing the functionality associated with that element.

[0046] While embodiments of this disclosure have been depicted, described, and are defined by reference to example embodiments of the disclosure, such references do not imply a limitation on the disclosure, and no such limitation is to be inferred. The subject matter disclosed is capable of considerable modification, alteration, and equivalents in form and function, as will occur to those ordinarily skilled in the pertinent art and having the benefit of this

Dropbox Exhibit 1002 - Page 116
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

disclosure. The depicted and described embodiments of this disclosure are examples only, and are not exhaustive of the scope of the disclosure.

Dropbox Exhibit 1002 - Page 117
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Claims:

1. A process for establishing a singular file system across multiple devices comprising:

receiving user information to open an account for establishing a singular file system across multiple devices via a web-based system that includes at least one server;

installing an individual software client on each of the multiple devices via the web-based system;

accepting registration of multiple devices via the web-based system;

scanning each of the multiple devices by each of the individual software clients to inventory data on each of the multiple devices and create a meta-index of the files for the inventoried data;

providing by the individual software clients via the multiple devices individual meta-indices of the inventoried data for each of the multiple devices to the at least one server;

integrating by the at least one server the individual meta-indices to create a single master meta-index;

providing by the at least one server the single master meta-index to each of the multiple devices via the individual software clients; and

continually updating the single master meta-index on the at least one server and each of the multiple devices in response to changes to the data indexed thereon.

2. The process according to claim 1 wherein the individual software clients vary according to the individual operating systems of each of the multiple devices.

3. The process according to claim 1 wherein registration of the multiple devices includes selection of categories of data for each of the multiple devices to be inventoried.

4. The process according to claim 3 wherein categories of data include documents, videos, pictures and music.

5. The process according to claim 1, wherein the individual software clients facilitate storage of the data within each of the multiple devices in accordance with the meta-data by modifying file systems of each of the multiple devices to include virtual files for data from the single meta-data index that is not local to a multiple device.

6. The process according to claim 5, wherein the individual software clients facilitate creation of a visual representation of the virtual files on a remote one of each of the multiple

Dropbox Exhibit 1002 - Page 118
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

devices that is indistinguishable from a visual representation of an actual file that is located on a local one of the multiple devices.

7. The process according to claim 1, wherein the meta-data includes at least information regarding file name, file type, file size, local path the file is stored in, date created, and date modified

8. A process for operating on files located on multiple devices using a singular file system comprising:

accepting a request to operate on a file at a first device, wherein the file is selected from the singular file system on the first device;

intercepting the request by a software client on the first device;

determining by the software client if the file is physically located on the first device or a second device, wherein a visual representation of the singular file system on the first device is identical to a visual representation of the singular file system on the second device;

if the file is physically located on a second device, requesting by the software client on the first device that a peer-to-peer connection be brokered by a server-based web service between the first device and the second device;

if the peer-to-peer connection is brokered, transferring the physical file from the second device to the first device; and

performing the operation on the file at the first device.

9. The process according to claim 8, wherein if the peer-to-peer connection cannot be brokered between the first device and the second device, an alternative connection is established by the server-based web service.

10. The process according to claim 9, wherein the alternative connection is an HTTP relay.

11. The process according to claim 8, wherein the software client determines if the file is physically located on the first device or a second device by reviewing file metadata.

12. The process according to claim 8, further comprising updating metadata of the singular file system on the first device and the second device to reflect a change in physical location of the file from the second device to the second device.

13. A system for establishing a singular file system across multiple devices comprising:

a web-accessible server;

at least one software client plug-in;

Dropbox Exhibit 1002 - Page 119
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

multiple devices for storing and operating on files;

wherein the web-accessible server receives user information to open an account for establishing a singular file system across multiple devices, installs the at least one software plug-in on each of the multiple devices, accepts registration of the multiple devices, wherein the at least one software plug-in varies in accordance with an operating system of each of the multiple devices;

further wherein the at least one software client plug-in scans its respective one of the multiple devices to inventory files thereon, creates a meta-index to files for the inventoried data, provides the meta-index of the inventoried data for its respective one of the multiple devices to the web-accessible server;

further wherein the web-accessible server receives meta-indices from each of the multiple devices and integrates the meta-indices to create a single meta-index, provides the single meta-index to each of the multiple devices via the individual software clients, and continually updates the single meta-index on each of the multiple devices in response to operations on the files indexed thereon.

14. The system according to claim 13, wherein the at least one software client plug-in facilitates storage of the files within its respective one of the multiple devices in accordance with the meta-data by modifying a file system of its respective one of the multiple devices to include virtual files for files from the single meta-index that are not local to the multiple device.

15. The process according to claim 14, wherein the at least one software client plug-in facilitates creation of a visual representation of the virtual files on its respective one of the multiple devices that is indistinguishable from a visual representation of an actual file that is physically located on a another of the multiple devices.

Dropbox Exhibit 1002 - Page 120
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

ABSTRACT

A system and process that establish a singular shared file system among devices in order to create a virtual representation of data on all of the devices via metadata indexing. This virtual representation of data means that the files are not actually stored on all devices and thus, with the exception of a single physical location, they do not need to take up any space (i.e. storage) on any additional device's hard drive. This allows for significant amounts of data to be virtually stored on each device, even if there is no physical storage room available for the data on each device. The system and process do not require data to be stored on a provider server, but instead stores only lightweight metadata, i.e., a small fraction of information about the files, online.

Dropbox Exhibit 1002 - Page 121
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

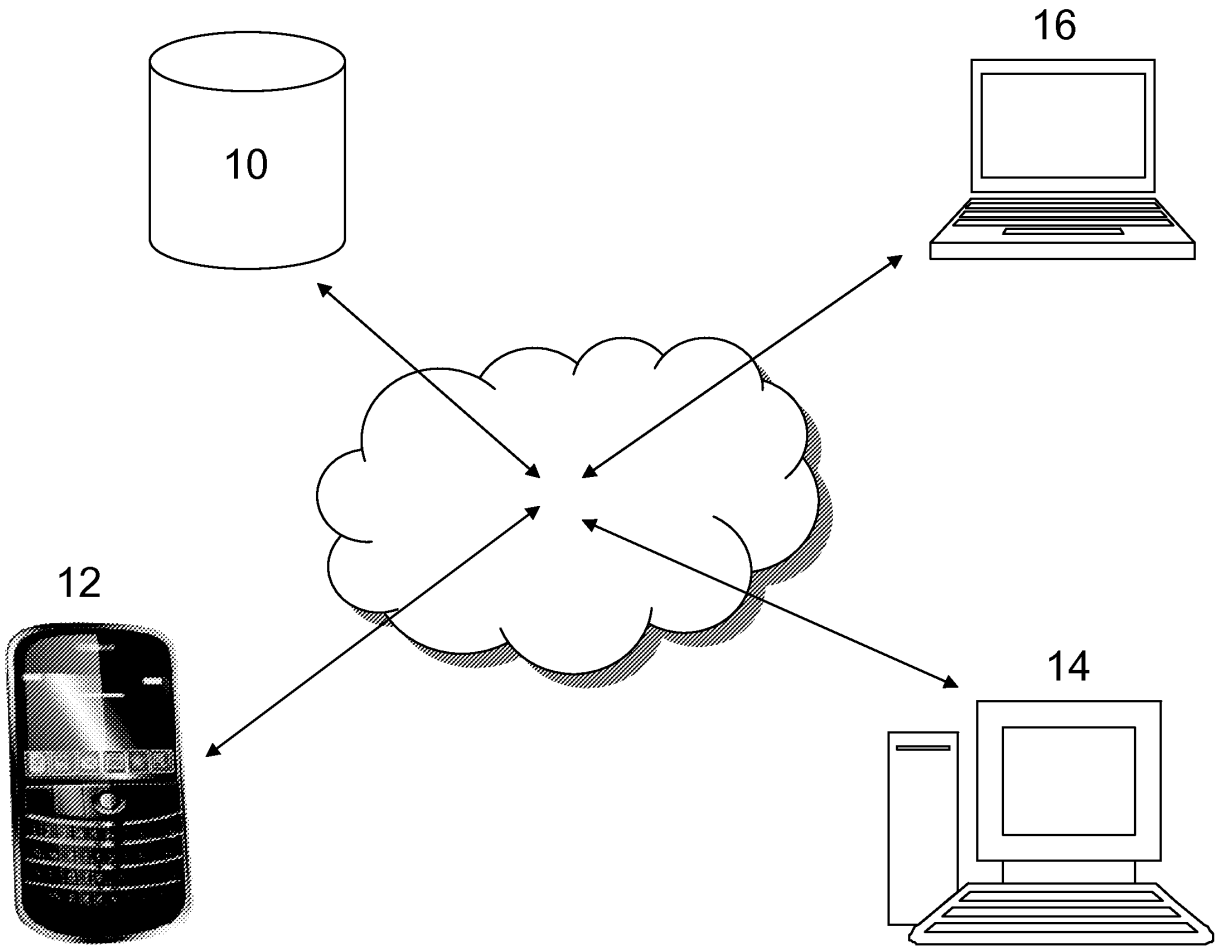


Figure 1

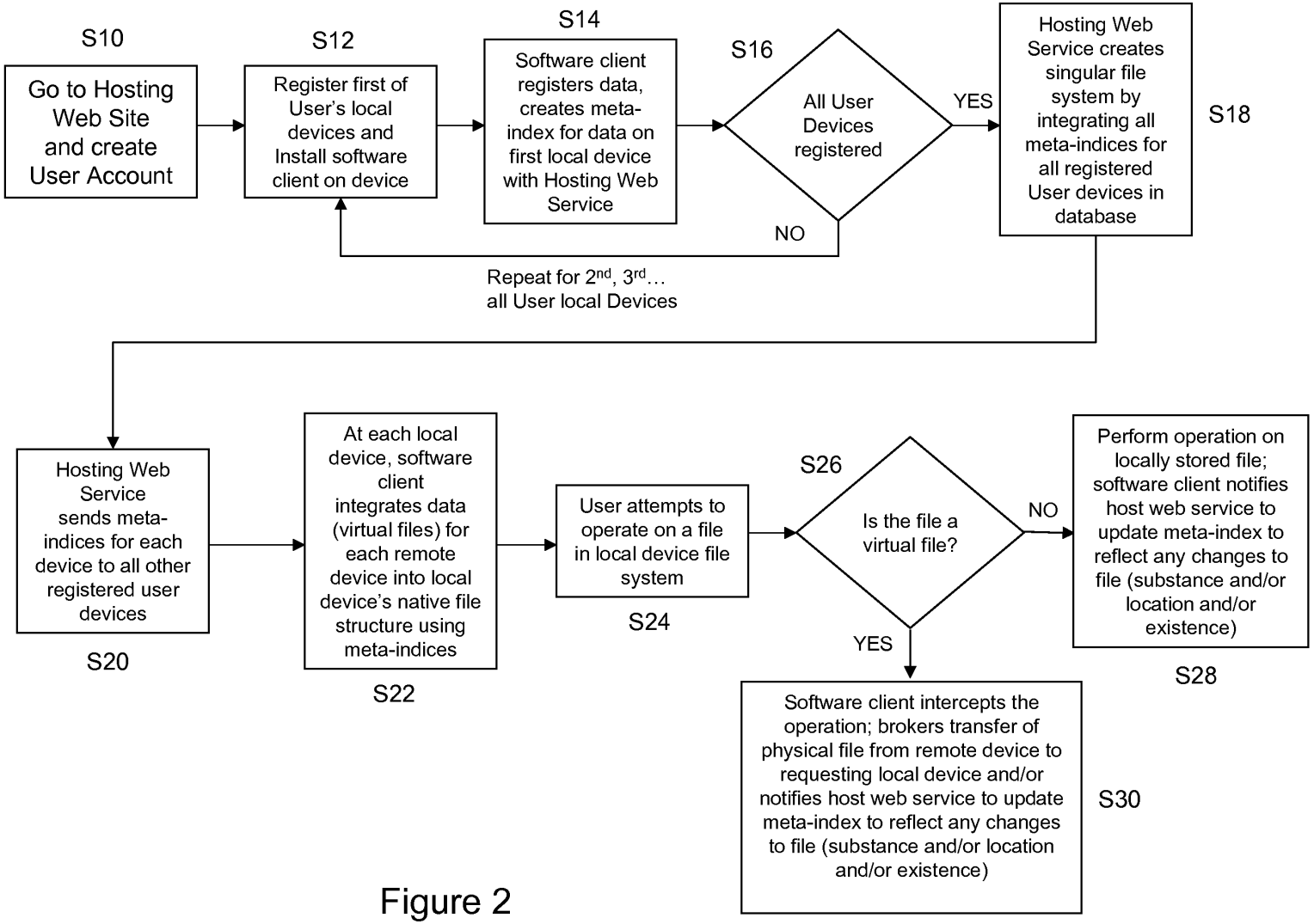

S10
Go to Hosting Web Site and create User Account
S12
Register first of User's local devices and Install software client on device
S14
Software client registers data, creates meta-index for data on first local device with Hosting Web Service
S16
All User Devices registered
YES
NO
Repeat for 2nd, 3rd… all User local Devices
Hosting Web Service creates singular file system by integrating all meta-indices for all registered User devices in database
S18
Hosting Web Service sends meta-indices for each device to all other registered user devices
S20
At each local device, software client integrates data (virtual files) for each remote device into local device's native file structure using meta-indices
S22
User attempts to operate on a file in local device file system
S24
S26
Is the file a virtual file?
NO
YES
Perform operation on locally stored file; software client notifies host web service to update meta-index to reflect any changes to file (substance and/or location and/or existence)
S28
Software client intercepts the operation; brokers transfer of physical file from remote device to requesting local device and/or notifies host web service to update meta-index to reflect any changes to file (substance and/or location and/or existence)
S30

Figure 2

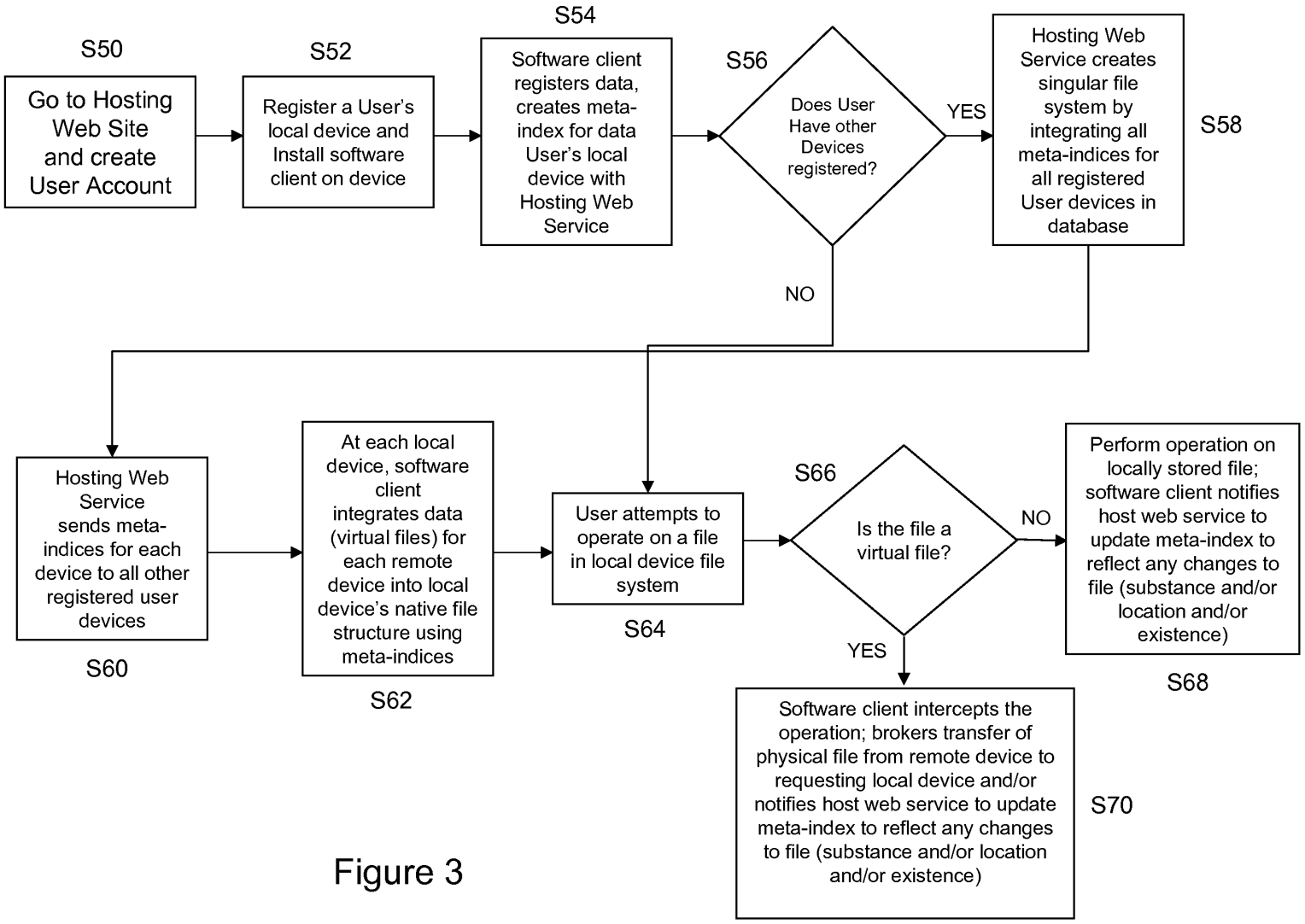

S50
Go to Hosting Web Site and create User Account
S52
Register a User's local device and Install software client on device
S54
Software client registers data, creates meta-index for data User's local device with Hosting Web Service
S56
Does User Have other Devices registered?
YES
Hosting Web Service creates singular file system by integrating all meta-indices for all registered User devices in database
S58
NO
Hosting Web Service sends meta-indices for each device to all other registered user devices
S60
At each local device, software client integrates data (virtual files) for each remote device into local device's native file structure using meta-indices
S62
User attempts to operate on a file in local device file system
S64
S66
Is the file a virtual file?
NO
Perform operation on locally stored file; software client notifies host web service to update meta-index to reflect any changes to file (substance and/or location and/or existence)
S68
YES
Software client intercepts the operation; brokers transfer of physical file from remote device to requesting local device and/or notifies host web service to update meta-index to reflect any changes to file (substance and/or location and/or existence)
S70

Figure 3

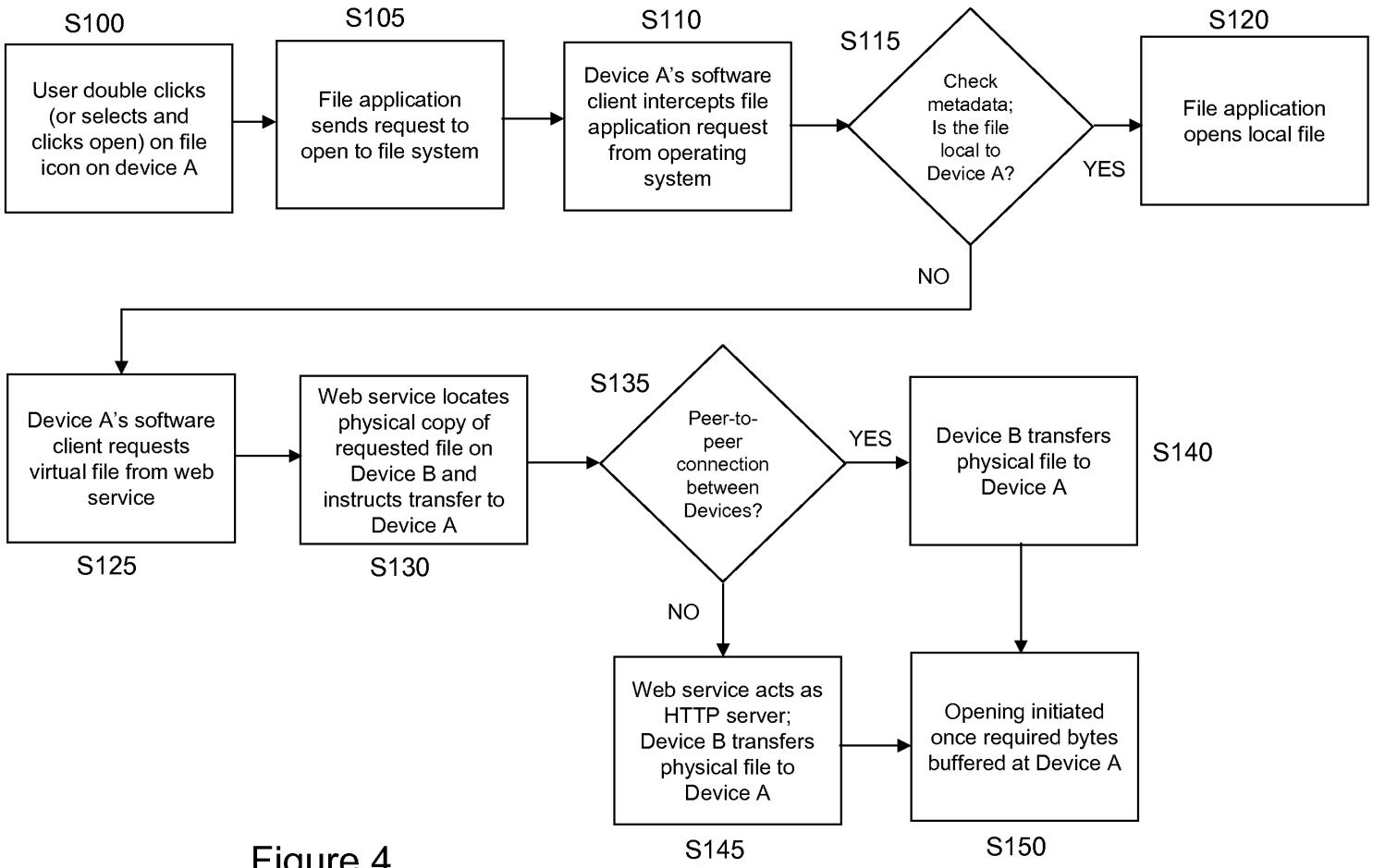

S100
User double clicks (or selects and clicks open) on file icon on device A
S105
File application sends request to open to file system
S110
Device A's software client intercepts file application request from operating system
S115
Check metadata; Is the file local to Device A?
YES
S120
File application opens local file
NO
Device A's software client requests virtual file from web service
S125
Web service locates physical copy of requested file on Device B and instructs transfer to Device A
S130
S135
Peer-to-peer connection between Devices?
YES
Device B transfers physical file to Device A
S140
NO
Web service acts as HTTP server; Device B transfers physical file to Device A
S145
Opening initiated once required bytes buffered at Device A
S150

Figure 4

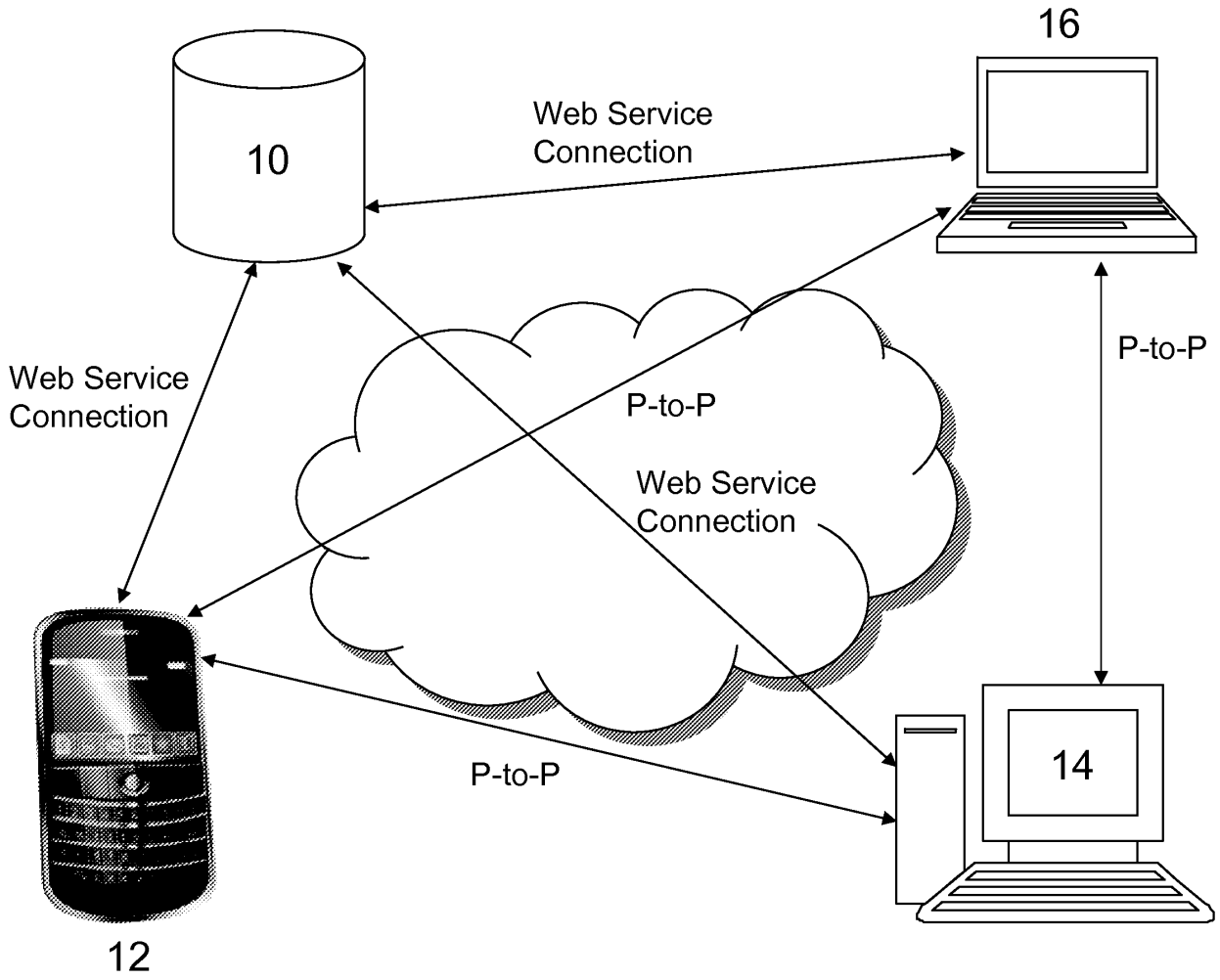

16
10
Web Service
Connection
Web Service
Connection
P-to-P
P-to-P
Web Service
Connection
P-to-P
14
12

Figure 5

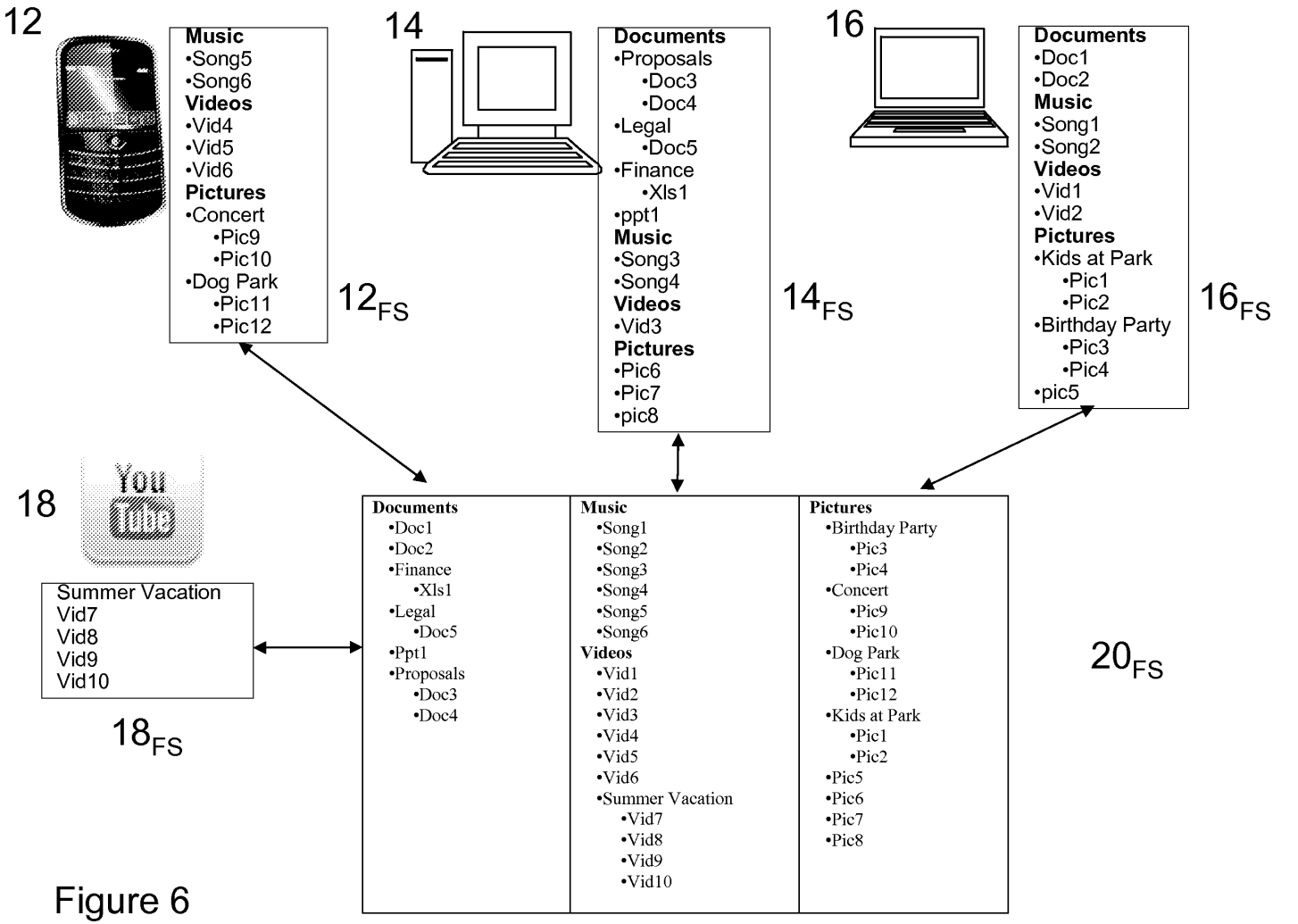

12
Music
•Song5
•Song6
Videos
•Vid4
•Vid5
•Vid6
Pictures
•Concert
•Pic9
•Pic10
•Dog Park
•Pic11
•Pic12
12FS
14
Documents
•Proposals
•Doc3
•Doc4
•Legal
•Doc5
•Finance
•Xls1
•ppt1
Music
•Song3
•Song4
Videos
•Vid3
Pictures
•Pic6
•Pic7
•pic8
14FS
16
Documents
•Doc1
•Doc2
Music
•Song1
•Song2
Videos
•Vid1
•Vid2
Pictures
•Kids at Park
•Pic1
•Pic2
•Birthday Party
•Pic3
•Pic4
•pic5
16FS
18
You Tube
Summer Vacation
Vid7
Vid8
Vid9
Vid10
18FS
Documents
•Doc1
•Doc2
•Finance
•Xls1
•Legal
•Doc5
•Ppt1
•Proposals
•Doc3
•Doc4
Music
•Song1
•Song2
•Song3
•Song4
•Song5
•Song6
Videos
•Vid1
•Vid2
•Vid3
•Vid4
•Vid5
•Vid6
•Summer Vacation
•Vid7
•Vid8
•Vid9
•Vid10
Pictures
•Birthday Party
•Pic3
•Pic4
•Concert
•Pic9
•Pic10
•Dog Park
•Pic11
•Pic12
•Kids at Park
•Pic1
•Pic2
•Pic5
•Pic6
•Pic7
•Pic8
20FS

Figure 6

COMBINED DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

☒ Original ☐ Supplemental ☐ Substitute ☐ PCT

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below), or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD FOR A CLOUD-BASED META-FILE SYSTEM TO VIRTUALLY UNIFY REMOTE AND LOCAL FILES ACROSS A RANGE OF DEVICES' LOCAL FILE SYSTEMS

(Title of the Invention)

the specification of which (check one)

☒ is attached hereto

☐ was filed on _____, as U.S. Application Serial Number _____ or PCT International Application Number _____ and was amended _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 (a) - (d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified, by checking the box below, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Applications			Priority Claimed		Copy Attached	
Application Number	Country	Foreign Filing Date (MM/DD/YYYY)	YES	NO	YES	NO

I authorize the U.S. attorneys or agents associated with the customer number provided below to accept and follow instructions from my employer (if I am an employee and this application has been or will be assigned to my employer) or the entity with which I have contracted (if I am an independent contractor and this application has been or will be assigned to such entity), as to any action to be taken in the United States Patent and Trademark Office regarding this application

Dropbox Exhibit 1002 - Page 128
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

without direct communication between the U.S. attorney or agent and the undersigned. In the event of a change in the persons from whom instructions may be taken, the U.S. attorneys or agents associated with the customer number provided below will be so notified by the undersigned.

As a named inventor, I hereby revoke all prior powers and appoint the practitioners associated with **Customer Number 74877** prosecute this application and transact all business in the United States Patent and Trademark Office connected therewith.

I acknowledge that the attorneys and agents associated with the aforementioned customer number are with King & Spalding LLP and represent my employer (if I am an employee and this application has been or will be assigned to my employer) or the entity with which I have contracted (if I am an independent contractor and this application has been or will be assigned to such entity) and in such cases do not represent me individually. I further acknowledge I have not established, nor will I seek to establish, any personal attorney/client relationship with King & Spalding LLP in connection with this application and understand that, should I require legal representation, I will obtain such, at my expense, other than through King & Spalding LLP.

Please recognize or change the correspondence address for the above-identified application to the address associated with the above-mentioned Customer Number 74877.

Direct telephone calls to: Dawn-Marie Bey (202) 737-0500

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of 1st inventor Erik CASO

Inventor's signature _____ Date 5/4/2010
Residence 1258 Berkeley Street, Santa Monica, CA 90404
Citizenship United States

Full name of 2nd inventor Michael ABRAHAM

Inventor's signature _____ Date _____
Residence 3580 Catalpa Way, Boulder, CO 80304
Citizenship United States

Dropbox Exhibit 1002 - Page 129
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

without direct communication between the U.S. attorney or agent and the undersigned. In the event of a change in the persons from whom instructions may be taken, the U.S. attorneys or agents associated with the customer number provided below will be so notified by the undersigned.

As a named inventor, I hereby revoke all prior powers and appoint the practitioners associated with **Customer Number 74877** prosecute this application and transact all business in the United States Patent and Trademark Office connected therewith.

I acknowledge that the attorneys and agents associated with the aforementioned customer number are with King & Spalding LLP and represent my employer (if I am an employee and this application has been or will be assigned to my employer) or the entity with which I have contracted (if I am an independent contractor and this application has been or will be assigned to such entity) and in such cases do not represent me individually. I further acknowledge I have not established, nor will I seek to establish, any personal attorney/client relationship with King & Spalding LLP in connection with this application and understand that, should I require legal representation, I will obtain such, at my expense, other than through King & Spalding LLP.

Please recognize or change the correspondence address for the above-identified application to the address associated with the above-mentioned Customer Number 74877.

Direct telephone calls to: Dawn-Marie Bey (202) 737-0500

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of 1st inventor **Erik CASO**

Inventor's signature _____ Date _____
Residence 1258 Berkeley Street, Santa Monica, CA 90404
Citizenship United States

Full name of 2nd inventor **Michael ABRAHAM**

Inventor's signature _____ Date 5/4/2010
Residence 3580 Catalpa Way, Boulder, CO 80304
Citizenship United States

Dropbox Exhibit 1002 - Page 130
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Docket No. ENT0001-US **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Erik CASO, et al.

Serial No.:	**To Be Assigned**	Group Art Unit:	**To Be Assigned**
Filed:	**Herewith**	Examiner:	**To Be Assigned**

For: **METHOD FOR A CLOUD-BASED META-FILE SYSTEM TO VIRTUALLY UNIFY REMOTE AND LOCAL FILES ACROSS A RANGE OF DEVICES' LOCAL FILE SYSTEMS**

INFORMATION DISCLOSURE STATEMENT
UNDER 37 C.F.R. §§ 1.97 AND 1.98

U.S. Patent and Trademark Office
Customer Window, Mail Stop Amendment
Randolph Building
401 Dulany Street
Alexandria , VA 22314

Sir:

In accordance with the requirements of 37 C.F.R. §§ 1.56, 1.97-1.98 and MPEP § 609, the references noted on the attached Form PTO-1449 are hereby brought to the attention of the Examiner.

No fees are believed to be necessary since the references cited in this statement are being submitted before the First Office Action. However, the Commissioner is hereby authorized to charge any additional fees which may be required, or to credit any overpayment, to Deposit Account No. 50-4402.

The above information is presented so that the United States Patent and Trademark Office may, in the first instance, determine any materiality thereof to the claimed invention. See

37 C.F.R. §§ 1.104(a) conferring the PTO duty to consider and use any such information. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

Respectfully submitted,

Date: May 5, 2010

By: */Dawn-Marie Bey-44,442/*
Dawn-Marie Bey
Registration No. 44,442

KING & SPALDING LLP
1700 Pennsylvania Avenue, N.W.
Suite 200
Washington, DC 20006
(202) 737-0500

17676/105001
Doc. No. 1490628

Form PTO-1449 (Rev. 2-32) U.S. Department of Commerce Patent & Trademark Office INFORMATION DISCLOSURE STATEMENT *(Use several sheets if necessary)*	Atty. Docket No. **ENT0001-US**	Serial No. **To Be Assigned**
	Applicant **Erik CASO, et al.**	
	Filing Date **Herewith**	Group **To Be Assigned**

U.S. PATENT DOCUMENTS

Examiner Initial		Document Number	Date	Name	Class	Sub-Class	Filing Date (if appropriate)
		2009/0254592	10/8/09	Marinov, et al.	1	1	11/11/08
		7,600,036	10/6/09	Hesselink, et al.	709	234	6/2/05
		7,587,471	9/8/09	Yasuda, et al.	709	220	3/14/03
		7,587,467	9/8/09	Hesselink, et al.	709	214	11/13/04
		7,546,353	6/9/09	Hesselink, et al.	709	216	11/13/04
		7,499,905	3/3/09	Jaschek, et al.	1	1	10/17/05
		7,467,187	12/16/08	Hesselink, et al.	709	205	10/9/02
		2008/0104077	5/1/08	Gimpl, et al.	1	1	1/6/08
		7,337,171	2/26/08	Gimpl, et al.	1	1	5/12/05
		2007/0162510	7/12/07	Lenzmeier, et al.	707	200	12/30/05
		2006/0277314	12/7/06	Hesselink, et al.	709	229	8/16/06
		7,120,692	10/10/06	Hesselink, et al.	709	225	11/19/02
		2006/0206533	9/14/06	MacLaurin, et al.	707	200	3/14/05
		2005/0256909	11/17/05	Aboulhosn, et al.	1	1	12/15/04
		6,938,042	8/30/05	Aboulhosn, et al.	1	1	10/8/02
		2005/0149481	7/7/05	Hesselink, et al.	1	1	11/13/04
		2005/0144195	6/30/05	Hesselink, et al.	1	1	11/13/04
		2005/0144200	6/30/05	Hesselink, et al.	1	1	11/13/04

EXAMINER	DATE CONSIDERED

EXAMINER: Initial if citation 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.

WDC_IMANAGE-1052702 v1-14682.105472

U.S. PATENT DOCUMENTS CONT'D.							
		2005/0138186	6/23/05	Hesselink, et al.	709	229	11/13/04
		2005/0114711	5/26/05	Hesselink, et al.	726	4	11/13/04
		2004/0172449	9/2/04	Hesselink, et al.	709	204	3/5/04
		6,732,158	5/4/04	Hesselink, et al.	709	208	6/29/00
		6,512,586	1/28/03	Maris	356	432	11/13/01
		6,499,054	12/24/02	Hesselink, et al.	709	204	12/2/99
		6,381,019	4/30/02	Maris	356	432	6/30/00
FOREIGN PATENT DOCUMENTS							
		WO 04/046852	6/3/04	Senvid, Inc., et al.	G06F	15/16	11/6/03
		JP 2004-046661	2/12/04	Hitachi Ltd.	G06F	12/00	7/15/02
		WO 03/085559	10/16/03	Synerdrive, Inc.	G06F	17/30	4/3/03
		WO 02/003046	1/10/02	Brown University Research Foundation	G01N	21/00	6/26/01
		WO 01/040887	6/7/01	Senvid, Inc.	H04L	12/28	12/1/00
		WO 01/014634	3/1/01	AstenJohnson, Inc., et al.	D21F	1/00	8/18/00
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)							

EXAMINER	DATE CONSIDERED

EXAMINER: Initial if citation 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.

17676/105001
Doc. No. 1490629

WDC_IMANAGE-1052702 v1-14682.105472

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 March 2001 (01.03.2001)

PCT

(10) International Publication Number
WO 01/14634 A1

(51) International Patent Classification[7]: D21F 1/00

(21) International Application Number: PCT/US00/22723

(22) International Filing Date: 18 August 2000 (18.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/150,068 20 August 1999 (20.08.1999) US

(71) Applicant *(for all designated States except US)*: **ASTEN-JOHNSON, INC.** [US/US]; 4399 Corporate Road, P.O. Box 118001, Charleston, SC 29423-8001 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **JOHNSON, C., Barry** [US/US]; 1186 Waterfront Drive, Mt. Pleasant, SC 29464 (US).

(74) Agents: **VOLPE, Anthony, S.** et al.; Volpe and Koenig, P.C., Suite 400, One Penn Center, 1617 John F. Kennedy Boulevard, Philadelphia, PA 19103 (US).

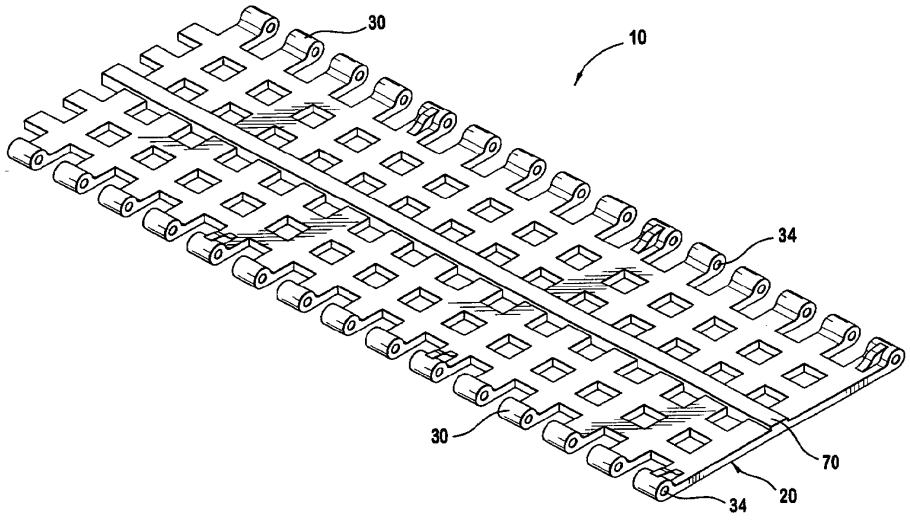
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: MOLDED MODULAR LINK AND A FABRIC MADE FROM A PLURALITY THEREOF



(57) Abstract: A link for making a modular papermaking fabric by interconnecting with other links is made through molding techniques to have predetermined characteristics such as open area, permeability, surface finish, etc. A papermaking fabric is constructed from a plurality of interconnected links and has predetermined permeability established by the combination of open and contact areas on each link.

WO 01/14634 A1

Dropbox Exhibit 1002 - Page 135
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

MOLDED MODULAR LINK AND A FABRIC MADE FROM A PLURALITY THEREOF

BACKGROUND

The present invention relates to papermaking fabrics, especially dryer fabrics. More specifically it relates to fabrics made from interconnected modular subassemblies. Most specifically it relates to pre-molded subassembly links used to make a modular fabric.

A papermaking fabric is used in the form of an endless belt which is supported by and advanced through the papermaking machine by various machine rolls. The process and the various sections of the machine, forming, press and dryer, will be known to those skilled in the art.

Traditionally fabrics have been made either through endless or flat weaving techniques. More recently, spiral fabrics have been made by connecting spiral coils with pintles to create a fabric. The spiral fabrics have allowed for greater flexibility in making fabrics of various dimensions, unlike flat or endless woven fabrics whose dimensions must be known ahead of time and are limited by loom design. The spiral fabric, however, lacks adaptability with regard to desired changes in drainage, permeability and surface characteristics.

Papermaking fabrics, especially dryer fabrics, commonly comprise woven monofilament yarns. The monofilaments have traditionally been extruded from materials such as nylon, polyester, etc. Unfortunately, the extrusion process renders many plastics unsuitable for use in the harsh environment of the paper machine's dryer section.

Dropbox Exhibit 1002 - Page 136
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Therefore, the choice of materials suitable for use in forming the monofilament has been limited. Many more plastics would become available if a dryer fabric could be made with molding techniques. To date, few practical mechanisms exist for constructing fabrics from molded parts.

Present dryer fabrics form endless belts passing around rollers having diameters from 18 to 60 in. (45.7 to 152.4 cm). While flexibility is an important requirement, fabrics also must be strong enough to support the paper web along its path under a variety of conditions and temperatures. Suggested load capacities have been fifteen pounds per linear inch (PLI) (267.9 kg/m). The fabric must also withstand traveling at greater than 4,000 feet per minute (1219.2 m/min).

Damage and dirt accumulation are also major factors which typically limit the maximum useful life of the fabric to about one year. Fabric edges are particularly vulnerable because of a tendency of the yarns to unravel and shift. Once damaged, the entire fabric must be replaced. Although traditional woven fabrics have been limited in size by loom construction, they have still reached as much as thirty feet wide by three hundred feet long. Damage to even a small area of the fabric necessitates costly replacement of the entire fabric.

Even minor marring of the surface may deteriorate fabric quality because the paper contact surface characteristics greatly affect the final paper product. Traditional fabrics adjust these characteristics through choice of materials and the type of weave used. Often, a compromise between the best material or the best weave and final product quality must be made. Batting or other material has been affixed to the paper support

Dropbox Exhibit 1002 - Page 137
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

surface to gain benefits not available from standard materials and weaves. A molded fabric offers greater flexibility in this regard, as surface characteristics may be incorporated directly into the mold and repeated consistently throughout the fabric.

The use of molded fabrics will benefit the art in many ways. A more direct process, avoiding additional storage and coiling requirements of monofilament yarns, as well as reducing trimming time and eliminating sealing will be enjoyed by using molded fabrics. More choices of less expensive material will become available, including lower molecular weight materials and gels having less stringent filtration requirements. The molding process also allows the use of composite materials to achieve more beneficial physical properties while maintaining cost effectiveness. A molded fabric allows greater flexibility and efficiency in design when creating fabric patterns (i.e., weave patterns and fabric dimensions). A fabric assembled from pre-molded subassemblies is strong, dimensionally stable, thermally stable, easy to join, distortion free, and has tough finished edges. Furthermore, use of a molded fabric limits fabric stretch, reduces costs, facilitates repair and generally benefits the papermakers art.

SUMMARY

The present invention is a pre-molded plastic subassembly for making papermaking fabrics. A plurality of the subassemblies are interconnected to create an endless fabric. The completed fabric also forms a part of the present invention.

Dropbox Exhibit 1002 - Page 138
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a bottom perspective view of a link of the present invention.

Figure 2 is a plan view of a link of the present invention.

Figure 3 is an end view of a link of the present invention as seen along line 3-3 of Figure 2.

Figure 4 is a plan view of a plurality of interconnected links of the present invention.

Figure 5 is a perspective view of an alternative link of the present invention.

Figure 6 is a perspective view of a pintle system for interconnecting the subassembly links of the present invention.

Figure 7 is a perspective view of a pin lock system for interconnecting the subassembly links of the present invention.

Figure 8 is a side elevational view of a D-link system for interconnecting the subassembly links of the present invention.

Figure 9 is a perspective view of a snap support system for interconnecting the subassembly links of the present invention.

Figure 10 is a perspective view of a finger lock system for interconnecting the subassembly links of the present invention.

Figure 11 is a perspective view of a grip linkage system for interconnecting the subassembly links of the present invention.

Figure 12 is a perspective view of a lock-fit system for interconnecting the subassembly links of the present invention.

Dropbox Exhibit 1002 - Page 139
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Figure 13 is a perspective view of a I-bar lock system for interconnecting the subassembly links of the present invention.

Figure 14 is a perspective view of a alternative link base with a sliding system for interconnecting the subassembly links of the present invention.

Figure 15 is a plan view of an alternative bi-component link of the present invention.

Figure 16 is a plan view of an alternative bi-component link of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Throughout the figures of the various embodiments of the present invention, like elements are identified with the same numerals.

The invention may be described generically as comprising a pliable, modular link 10, as shown in Figures 1-4. The link 10 is molded from appropriate plastics by molding techniques as are well known in the art. The link 10 has a planar upper support surface 20 for supporting and carrying the paper web and is molded to have a predetermined open area or permeability, based upon fabric needs and product demands. Finally, the link 10 is provided with means for interconnecting with other links to form an endless papermaking fabric. The completed fabric will be made of a plurality of interconnected links 10.

Materials and dimensions are chosen for a combination of reasons taking into account fabric demands and tooling concerns. Nylon 6/6 material, available from Dupont

Dropbox Exhibit 1002 - Page 140
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

under the trademark Zytel®, is useful because of its desirable properties of strength, flexibility, impact resistance, heat performance and good mold processability. Other materials and specialized higher heat grades of resin may be used.

Along with choice of material, the actual link dimensions, interconnection means, and "weave pattern" must be determined according to fabric and tooling demands. The link dimensions have been found to be most limited by practical tooling and molding considerations rather than fabric considerations. Interconnection means, such as those illustrated in Figures 6-16, include a pintle system, integrated pin locks, D-link and finger locks, snap supports, grip linkages, and lock-fit mechanisms. The "weave pattern" must be chosen with fabric considerations in mind, but is limited only by mold construction and paper marking considerations. It may take a variety of patterns such as the gingham-type pattern shown in Figs. 1-4 or the alternative structures shown in Figs. 14-16. The latter figures show a flexible matt-like structure and adjustable X-weave patterns which slide atop each other for adjusting permeability in the finished fabric.

The link 10 described below was developed for use in a corrugated paper process. In the process, the completed fabric wraps around rollers having 18 inch (45.72cm) and 60 inch (152.4 cm) diameters. A maximum temperature of 300° F (148.9° C) is estimated at the fabric as it travels over steam cans having estimated temperatures up to 400° F (204.4° C). The temperature differential is due to a layer of pulp that separates the fabric from the steam cans. Typically, woven fabrics used in this process have a thickness of 0.140 inch (3.56 mm) and weigh approximately 5.9 oz./ft.^{2} (1.8kg/m^2). Normal running tension load on the fabric ranges from 8-15 PLI (142.9 - 267.9 kg/m),

Dropbox Exhibit 1002 - Page 141
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

however, higher loads may be caused when a pulp wad passes through the rollers. Fabric thickness of the new modular fabric should approximate existing fabric thickness and, ideally, reduce weight. Since current seam strengths in woven fabrics presently range between 200-300 PLI (3572-5358 kg/m), 500 PLI (8930 kg/m) was the goal for the present example.

Keeping those requirements in mind, the link 10 was constructed generally as shown in Figures 1-4. As seen in Figure 1, link 10 was molded in a generally rectangular shape having a major axis and a minor axis. The major axis relates generally to the cross-machine direction in the papermaking machine while the minor axis relates to the machine direction. A pintle system similar to that shown in Figure 6 was chosen as the interconnection means due to its inherent strength. A plurality of individual pintle links 30 project from the two sides of the link 10 parallel to the major axis, each defining a bearing area 32 and pintle hole 34. Each pintle hole 34 is aligned with the next to form part of a pintle channel running parallel to the major axis along the length of each side. A pintle inserted through a completed pintle channel formed by interdigitating individual pintle links 30 of adjacent links 10 is used to interconnect a plurality of the links 10 to make a complete fabric. Each link 10 has an upper surface 20 which defines a planar support surface for contacting and carrying the paper web through the paper machine.

The link 10 was molded with a 6 inch (15.2 cm) major axis and a 2 inch (5.1 cm) minor axis. The three-to-one ratio of major axis to minor axis is believed to aid mold processability. Open area was established on the link 10 by a gingham-like pattern defining rectangular or squared openings. As shown in Figures 2 and 3, the link 10

Dropbox Exhibit 1002 - Page 142
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

thickness t was established at 0.060 in. (1.5mm) with a 0.090 in. (2.3mm) runner 70 centrally located parallel to the major axis, to help flow during molding. A maximum thickness M of 0.143 in. (3.6mm) is found at each side parallel to the major axis due to the bearing thickness h, 0.040 in. (1.0mm), surrounding the pintle hole diameter d, 0.063 in. (1.6mm). A minimum pintle hole diameter was calculated based on an individual pintle link width w of 0.200 inch (5.1mm). A minimum 0.044 inch (1.1mm) diameter was calculated for a stainless steel pintle because a nylon pintle yielding the desired load capacity exceeded thickness requirements. The specific diameter, 0.063 in. (1.6mm), was chosen for tooling reasons; it is sized to receive a 0.0625 inch (1.59mm) diameter pintle.

The resultant weight was calculated from measured volume of the link, 0.56 $in.^3$ (9.18 cm^3), and known specific gravity of nylon 6/6 (1.14) to be 0.023 pounds (10.4 gm) per link. Each link has an area of 6 in. (15.2 cm) x 2 in. (5.1 cm) or 12 $in.^2$ (77.5 cm^2) resulting in a weight per area of 0.0019 pounds per square inch (1.34 kg/m^2), as compared to existing fabric weight of 0.0025 pounds per square inch (5.9 $oz./ft.^2$) (1.8 kg/m^2). Thus, the goal of maintaining fabric thickness while reducing weight was achieved.

A molded fabric establishes open area and permeability just as the weave of a traditional fabric, but without the concerns over shifting yarns and fabric stability. Although the link 10, shown in Figs. 1-4 has a gingham-like "weave pattern" with rectangular or squared openings, circular, oval, or other shaped openings and patterns may also be employed. Because of the molded nature, even three dimensional shapes may be made in the links for desired results, such as permeability, flow control, etc. In

Dropbox Exhibit 1002 - Page 143
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

fact, link 10 may be made using material only in the machine direction as seen in Figure 5. Fabric stability and paper marking must be considered when designing a link and a modular papermaking fabric just as in traditional fabric design.

In making a complete fabric, a plurality of the subassembly links 10 are interconnected to form an endless belt. Fabrics constructed from the modular links are not limited in dimension by loom size as in traditional fabrics. A fabric of any size can be made by interconnecting the appropriate number of subassembly links. Preferably, a brick layered pattern as shown in Figure 4 will be used to increase the fabric strength. In such an arrangement, each link 10 is staggered so that their individual pintle links 30 intermesh with the pintle links 30 of two other links 10. Accordingly, some sizing may be necessary at the fabric edges and final seam. This, however, can be accomplished at the edges through simple straight cuts. Alternatively, because of the modular design, special links may be molded to complete the edge without cutting. Similarly, smaller links can be molded to fill a variety of sizes that may be needed to complete the final fabric seam. Preferably, however, the overall fabric length needed will be considered when establishing link dimensions, so that special links of fractional dimensions will not be required to close the final seam.

Calendar finishing may be used on each link 10, much as in traditional fabrics. For the most uniform treatment, an assembled fabric will be subjected to the finishing treatment. For a more unique fabric, individual links can be given different surface finishes prior to assembly.

Dropbox Exhibit 1002 - Page 144
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

The modular design of the fabric allows for easy replacement of individual sections of the fabric. When one section of the fabric becomes damaged, worn, or dirty, it may be replaced without having to remove and replace the entire fabric. This feature alone will result in a significant cost savings over traditional papermaking fabrics. Additionally, modular papermaking fabrics are strong, stable, versatile, light-weight, easy to install, and easy to repair or replace.

* * *

Dropbox Exhibit 1002 - Page 145
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

What is claimed is:

1. A link for producing a fabric from the interconnection of a plurality of links, said link comprising:

a molded, pliable body defining a planar paper support surface having a predetermined amount of open area; and

means for interconnecting with another link.

2. A modular papermaking fabric comprising a plurality of interlinked molded links as recited in claim 1 wherein each of said plurality of links is connected to adjacent links to create an endless fabric of predetermined dimensions and having predetermined contact and open areas.

3. The fabric of claim 2 wherein the interlinked links are connected by a pintle engaging respective interconnecting means.

4. The fabric of claim 3 wherein the pintle is manufactured from stainless steel.

5. The fabric of claim 2 wherein each link body has a generally rectangular configuration with a major axis extending between first and second substantially parallel sides and a minor axis extending between third and fourth substantially parallel sides and the links are generally interconnected such that the third and fourth sides of each link do

Dropbox Exhibit 1002 - Page 146
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

not align with the respective third and fourth sides of links adjacent their first or second side.

6. The fabric of claim 2 comprising a plurality of interconnected links defining a first layer and a plurality of interconnected links defining a second layer with the first and second layers interconnected to define a multi-layer fabric.

7. The link of claim 1 wherein the link body has a generally rectangular configuration with a major axis extending between first and second substantially parallel sides and a minor axis extending between third and fourth substantially parallel sides.

8. The link of claim 7 wherein the major and minor axes have a length ration of 3 to 1.

9. The link of claim 7 wherein the interconnecting means are provided along at least the first and second sides.

10. The link of claim 9 wherein a pintle receiving hole is defined along each of the first and second sides.

11. The link of claim 7 wherein the interconnecting means are provided along at least the third and fourth sides.

Dropbox Exhibit 1002 - Page 147
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

12. The link of claim 11 wherein at least one pintle receiving hole is defined along each of the third and fourth sides.

13. The link of claim 11 wherein at least two spaced pintle receiving holes are defined along each of the third and fourth sides.

14. The link of claim 1 wherein the open area is defined by a plurality of apertures defined through the paper support surface.

15. The link of claim 14 wherein the apertures define a gingham-like pattern.

16. The link of claim 1 wherein the body is defined by an X-weave pattern.

17. The link of claim 1 wherein the interconnecting means is chosen from the group consisting of a pintle system, an integrated pin lock system, a D-link and finger lock system, snap supports, grip linkages, and lock-fit mechanisms.

Dropbox Exhibit 1002 - Page 148
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

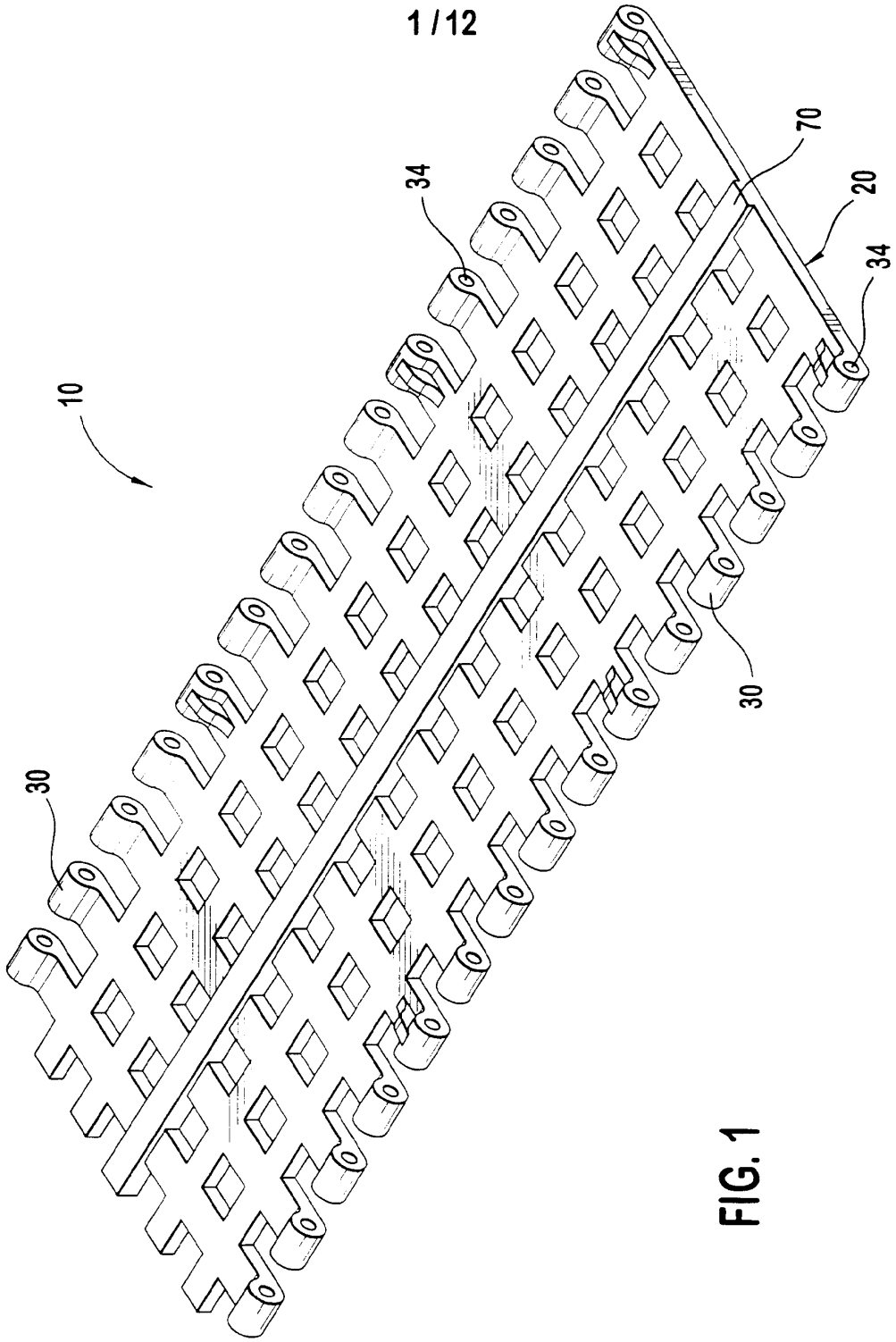


FIG. 1

Dropbox Exhibit 1002 - Page 149
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

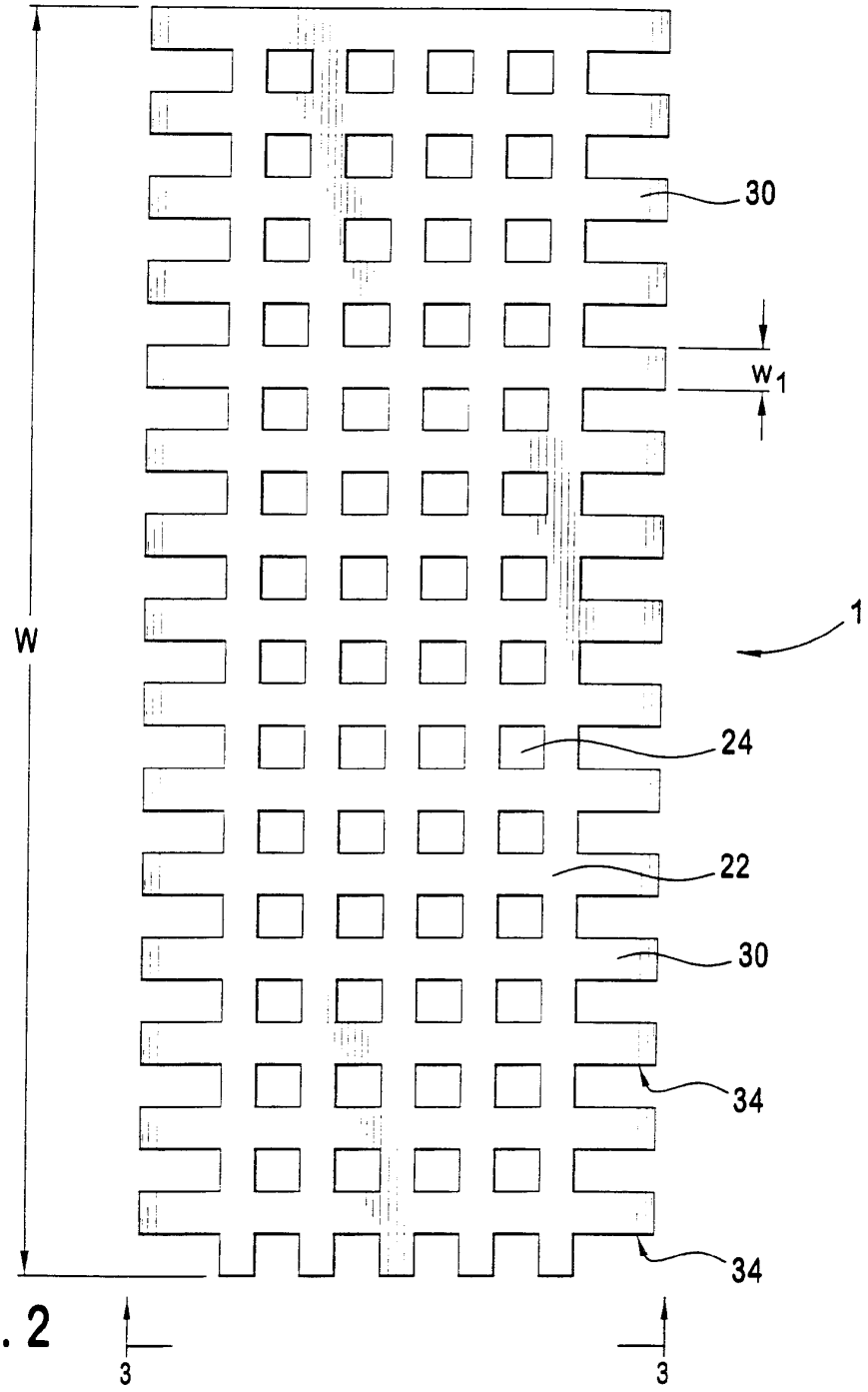


FIG. 2

Dropbox Exhibit 1002 - Page 150
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

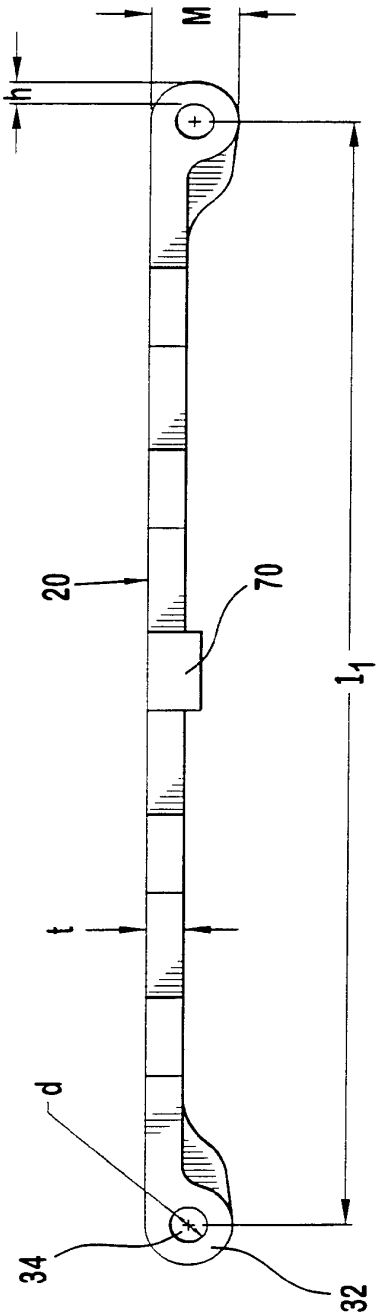


FIG. 3

Dropbox Exhibit 1002 - Page 151
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

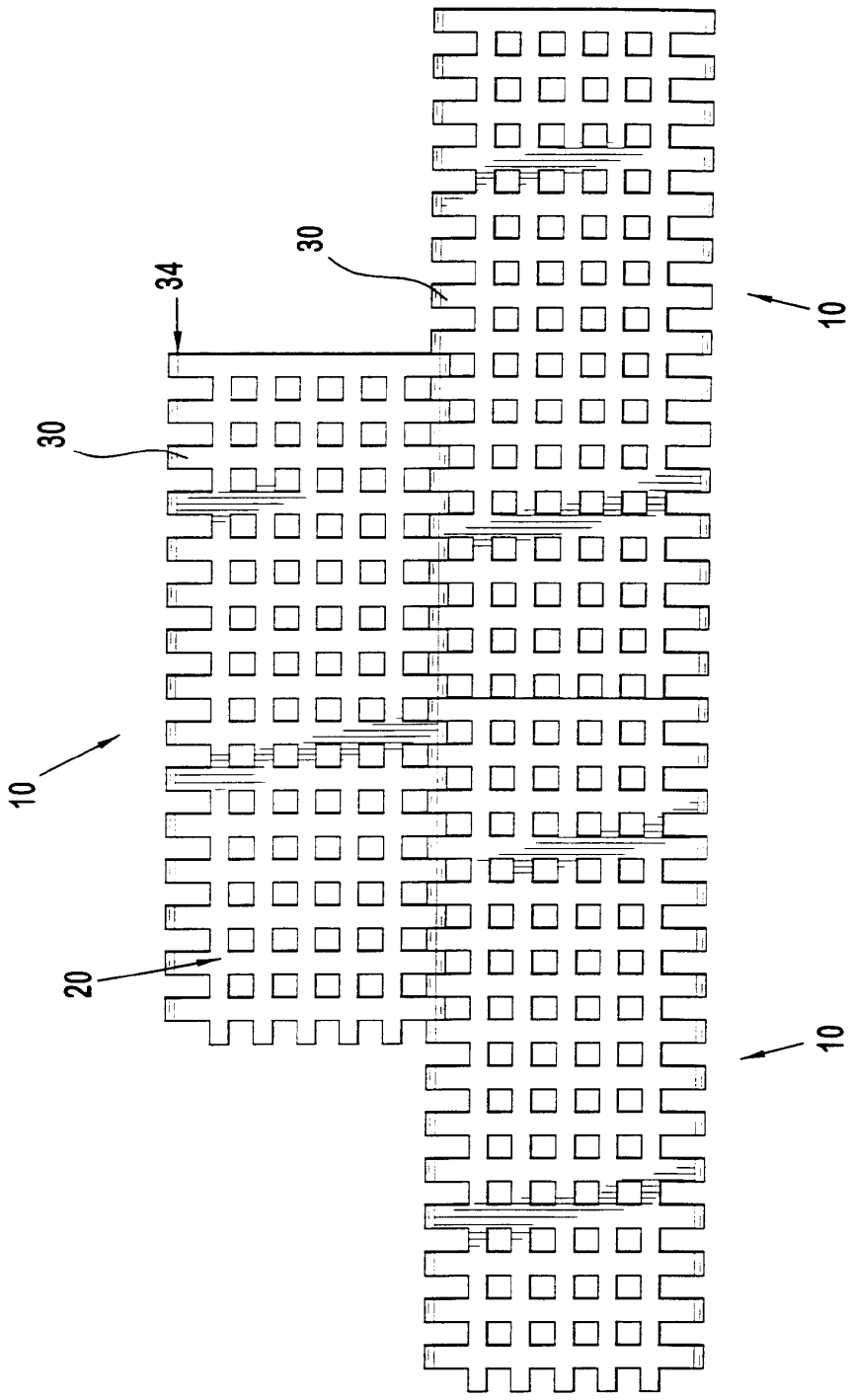


FIG. 4

Dropbox Exhibit 1002 - Page 152
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

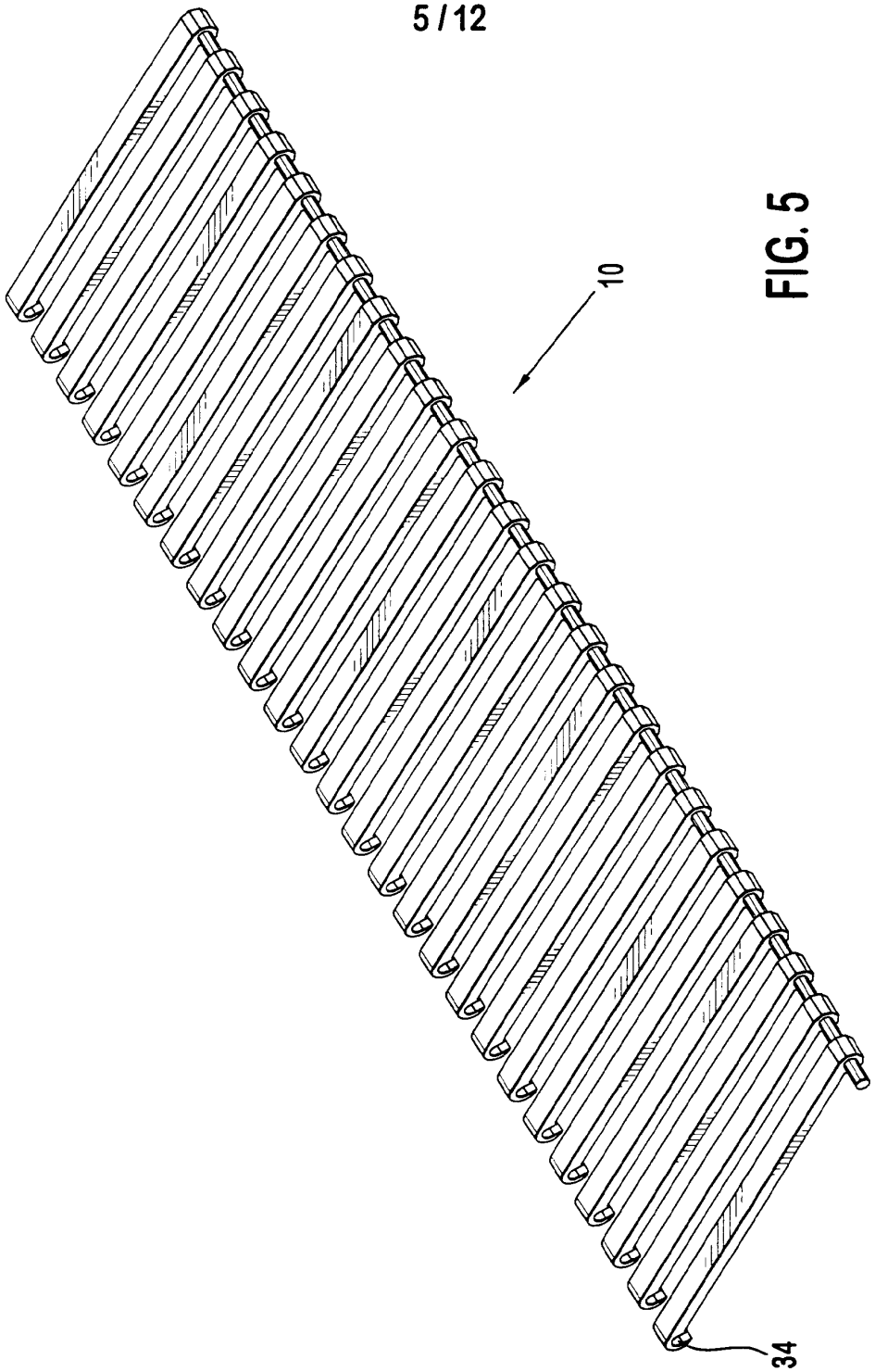
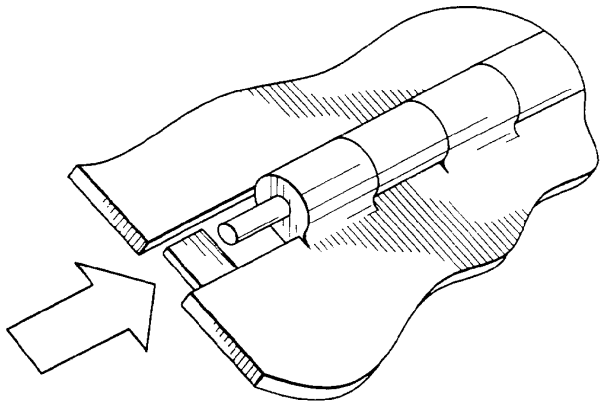


FIG. 5

Dropbox Exhibit 1002 - Page 153
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

FIG. 6



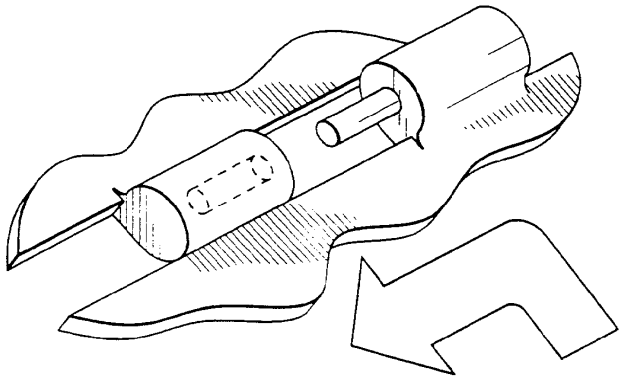
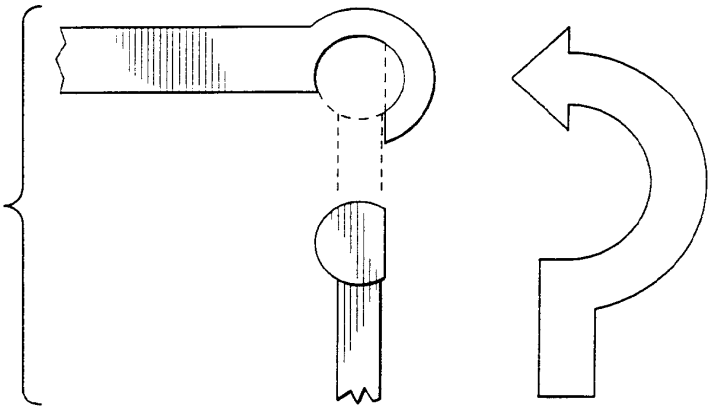


FIG. 7

FIG. 8



Dropbox Exhibit 1002 - Page 154
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

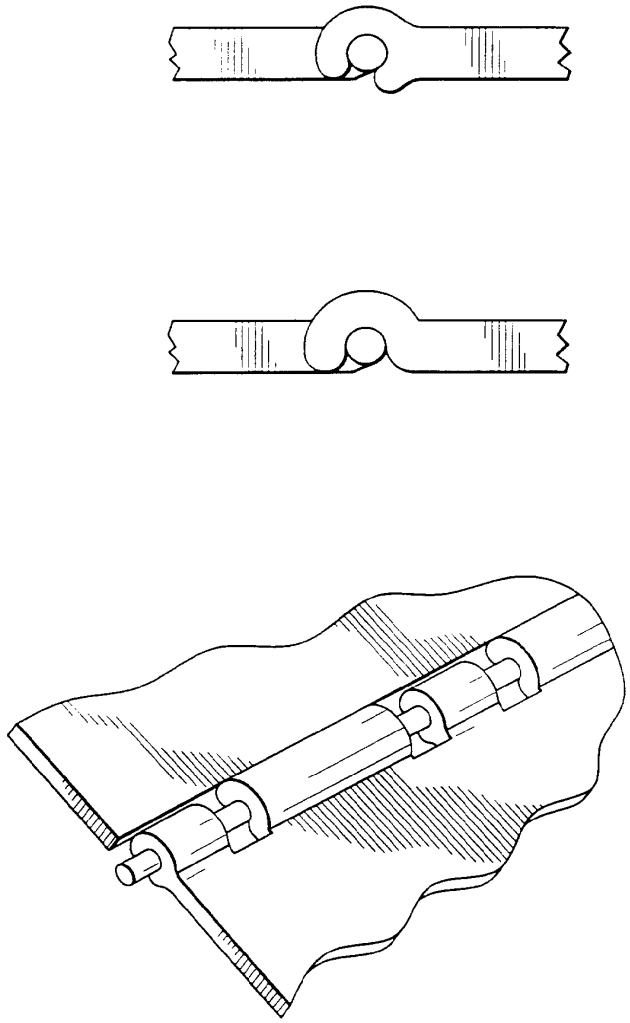


FIG. 9

Dropbox Exhibit 1002 - Page 155
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

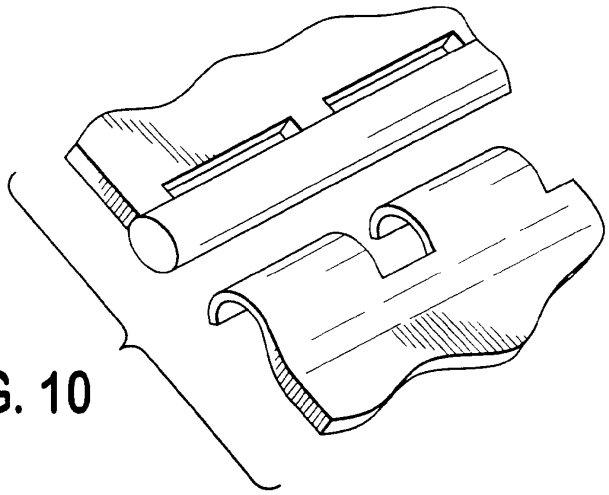


FIG. 10

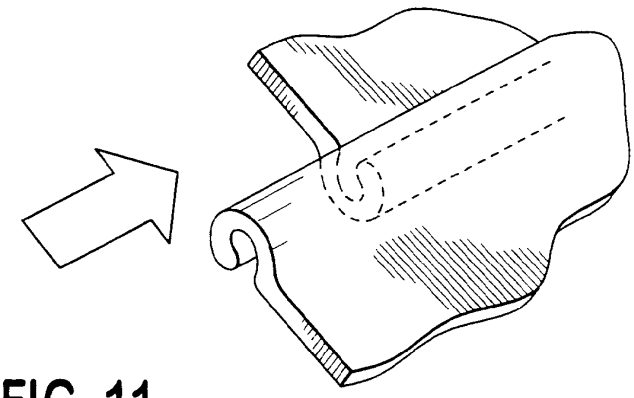


FIG. 11

Dropbox Exhibit 1002 - Page 156
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

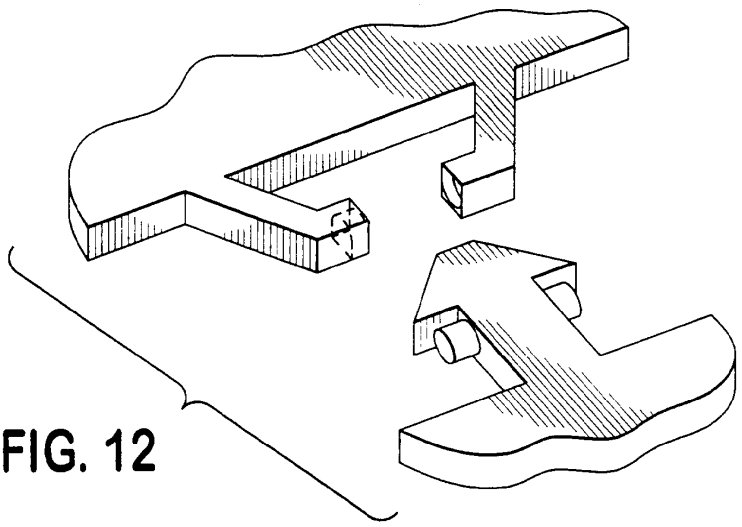


FIG. 12

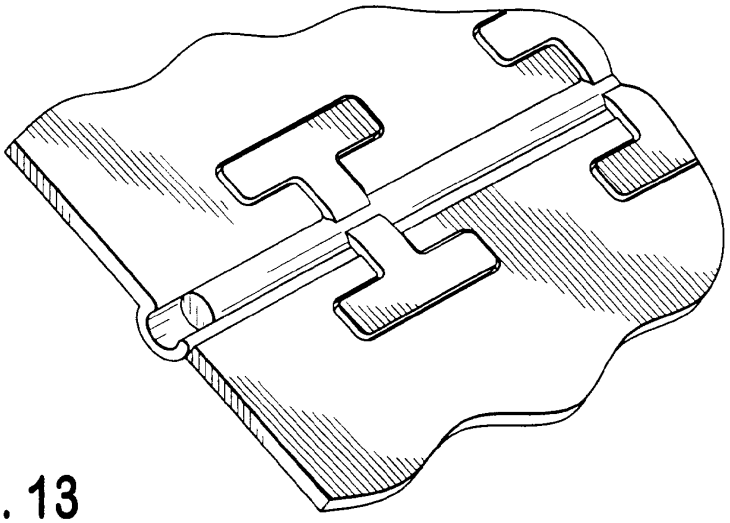


FIG. 13

Dropbox Exhibit 1002 - Page 157
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

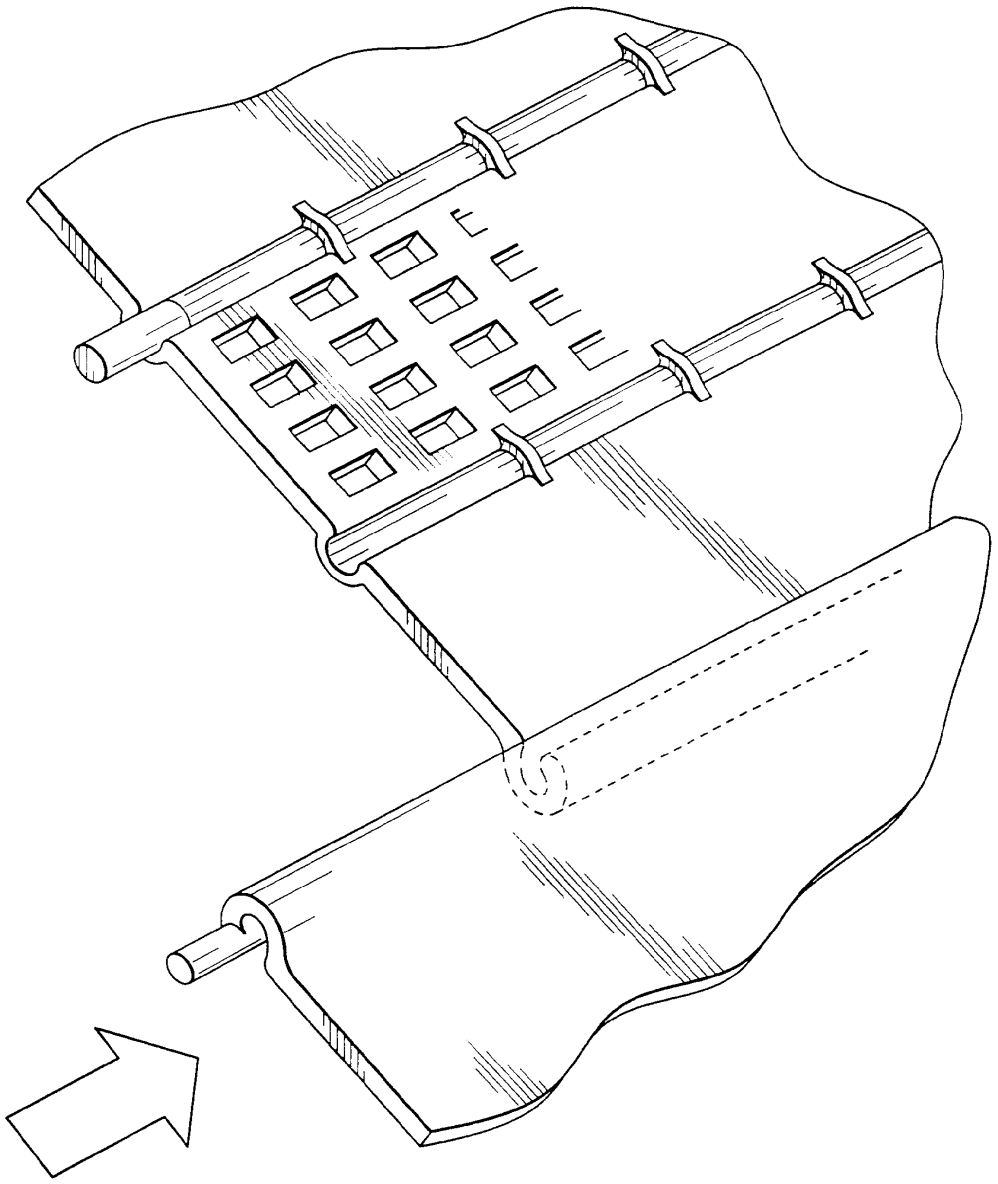
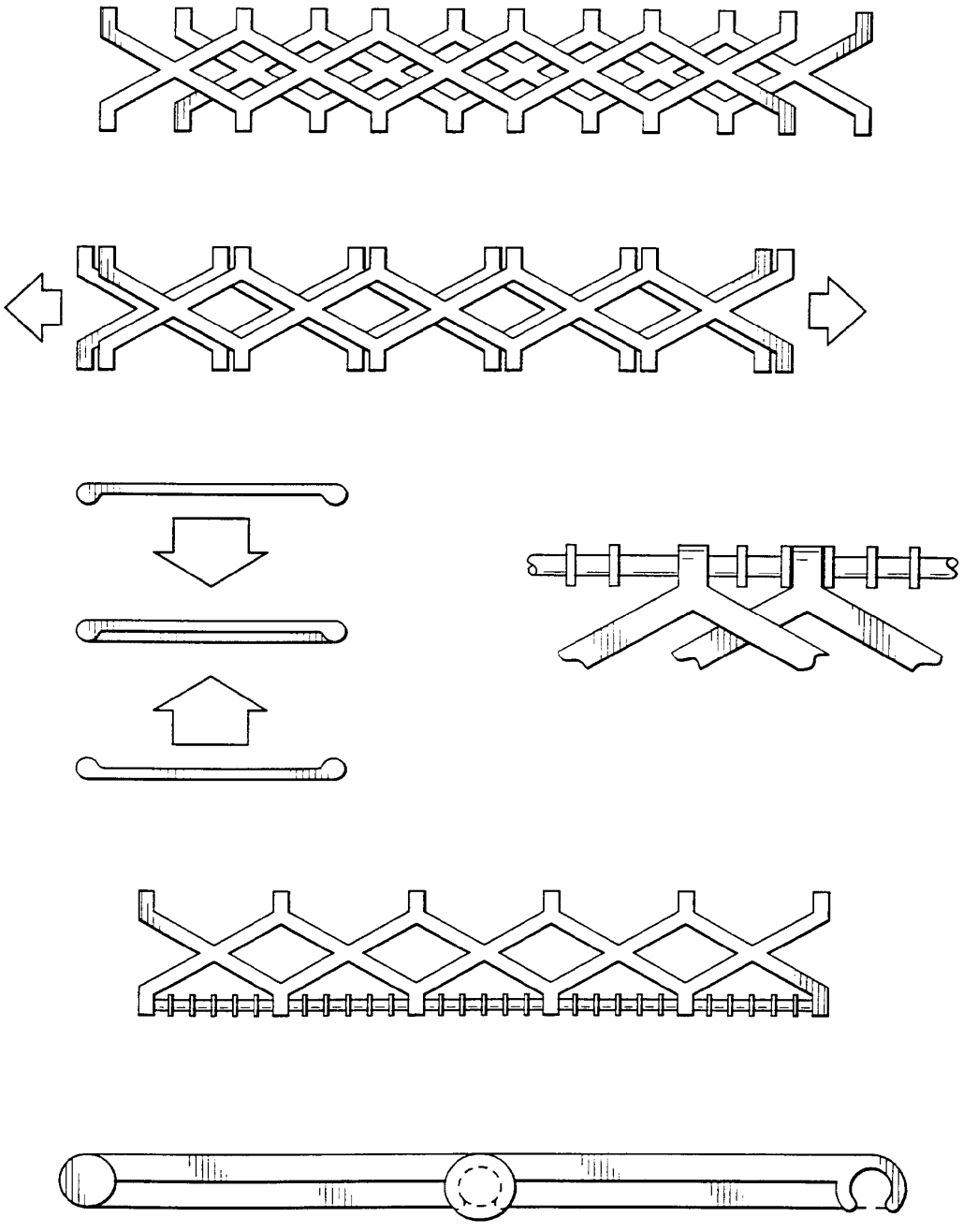


FIG. 14

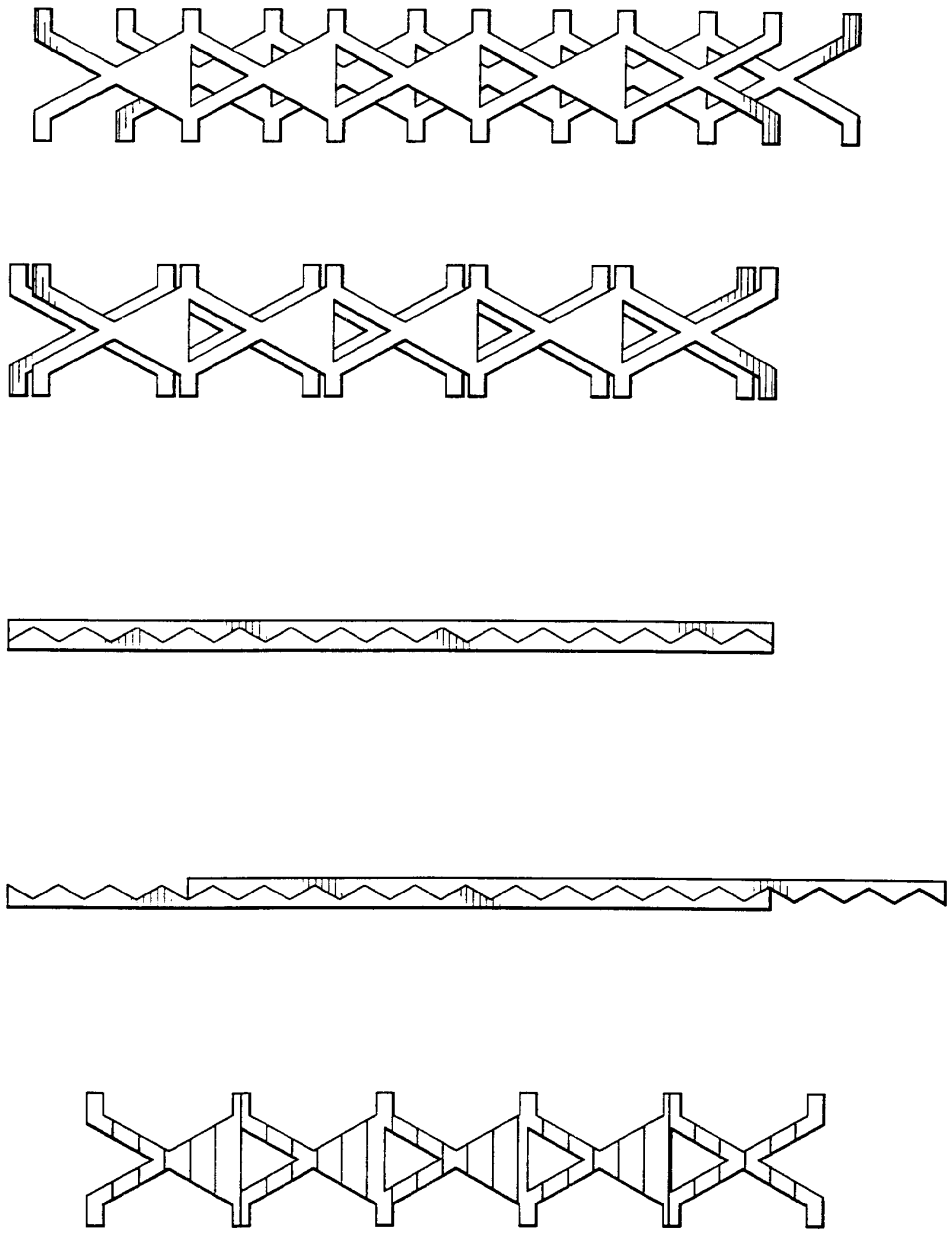
Dropbox Exhibit 1002 - Page 158
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

FIG. 15



Dropbox Exhibit 1002 - Page 159
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

FIG. 16



Dropbox Exhibit 1002 - Page 160
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/US 00/22723

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 D21F1/00

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)
IPC 7 D21F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 37 35 709 A (HEIMBACH GMBH THOMAS JOSEF) 3 May 1989 (1989-05-03) column 1, line 60 -column 2, line 5 column 5, line 24 -column 7, line 52; figures ---	1-4,7, 9-12,14, 17
X A	US 4 842 905 A (STECH WILLIAM J) 27 June 1989 (1989-06-27) the whole document ---	1-4,7, 9-12,14, 17 5,15,16
X	US 4 537 658 A (ALBERT HANS) 27 August 1985 (1985-08-27) abstract; figures column 3, line 52 -column 5, line 35 --- -/--	1-4,7, 9-12,14, 17

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

[X] Patent family members are listed in 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	Date of mailing of the international search report
7 November 2000	16/11/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Helpiö, T.

1

Form PCT/ISA/210 (second sheet) (July 1992)

Dropbox Exhibit 1002 - Page 161
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/US 00/22723

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 802 280 A (JWI LTD) 22 October 1997 (1997-10-22) abstract; figures	6

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

Dropbox Exhibit 1002 - Page 162
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/US 00/22723

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 3735709 A	03-05-1989	NONE	
US 4842905 A	27-06-1989	CA 1317142 A	04-05-1993
US 4537658 A	27-08-1985	CA 1240188 A	09-08-1988
EP 0802280 A	22-10-1997	AU 1789397 A	23-10-1997
		BR 9701853 A	15-12-1998
		CA 2202817 A	18-10-1997
		US 6124015 A	26-09-2000

Form PCT/ISA/210 (patent family annex) (July 1992)

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 June 2004 (03.06.2004)

PCT

(10) International Publication Number
WO 2004/046852 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2003/035271

(22) International Filing Date:
6 November 2003 (06.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/300,500 19 November 2002 (19.11.2002) US

(71) Applicant *(for all designated States except US)*: **SENVID, INC.** [US/US]; 20300 Stevens Creek Blvd., Suite 250, Cupertino, CA 95014-2240 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **HESSELINK, Lambertus** [NL/US]; 101 Green Oaks Drive, Atherton, CA 94027 (US). **RIZAL, Dharmarus** [ID/US]; 100 N. Whisman Road, #821, Mountain View, CA 94043 (US). **BJORNSON, Eric, S.** [US/US]; 550 Dawn Drive, Sunnyvale, CA 94087 (US).

(74) Agent: **CANNON, Alan, W.**; Law Office of Alan W. Cannon, 834 South Wolfe Road, Sunnyvale, CA 94086 (US).

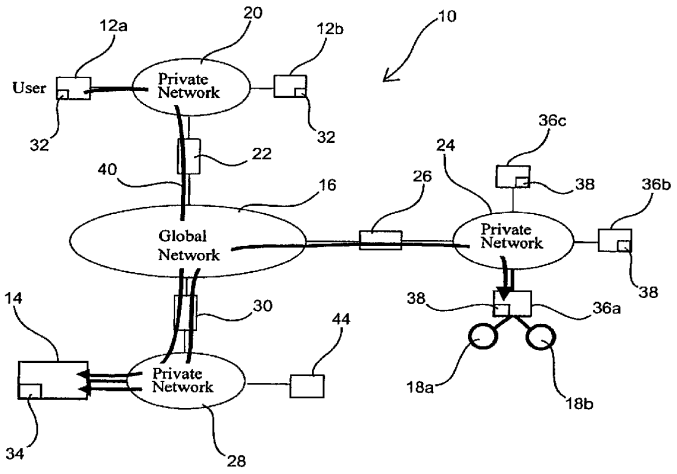
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ACCESS AND CONTROL SYSTEM FOR NETWORK-ENABLED DEVICES



(57) Abstract: Systems and methods for remote access of network-enabled devices that provide seamless, firewall-compliant connectivity between multiple users and multiple devices, that allow collaborative operations by multiple users of remotes devices, that allow point to multipoint control of multiple devices and which allow rapid, secure transmission of data between remote users and devices. In general terms, the system includes at least one connection server, and at least two computers operatively coupled to the connection server via the public or global network. In an example where at least one client computer is operatively connected to at least one network-enabled device through a connection server via the public or global network, the connection server is configured to route control instructions from the client to the network-enable device, and route data from the network-enabled device to the client.

WO 2004/046852 A2

ACCESS AND CONTROL SYSTEM FOR NETWORK-ENABLED DEVICES

RELATED APPLICATION DATA

[0001] The present application is a Continuation-In-Part of co-pending U.S. Application Serial No. 09/608,685, filed June 29, 2000, which is a Continuation-In-Part of U.S. Application Serial No. 09/454,178, filed December 2, 1999. The present application also claims priority to U.S. Provisional Patent Application Serial No. 60/331,642 Filed on November 20, 2001. Each of the afore-mentioned applications are hereby incorporated, in their entireties, be reference thereto.

BACKGROUND OF THE INVENTION

[0002] The Internet has made large amounts of information available to computer users around the world. A tremendous amount of information is exchanged between individual users via public computer networks, e.g., the Internet, and the volume of such information will continue to increase. A particularly attractive aspect of the Internet and networked computers generally is the potential for users to remotely access network-enabled devices to perform functions with the devices while not being physically present. Such remotely accessed devices may include, for example, surveillance cameras, manufacturing equipment, or like devices. An important class of Internet users that employ remotely accessed devices via a computer network are private individuals and professional users that are interconnected via a private network, such as a corporate intranet or local area network (LAN).

[0003] Remote access of devices through the Internet has presented many problems. Providing access to remote devices has typically required setup of a dedicated private network or dedicated virtual private network (VPN) for remote device access. A dedicated server within the private network provides for communication with the Internet, and a dedicated telephone line, digital subscriber line (DSL) or like communication interface is used to connect the device to the dedicated server. Such a

Dropbox Exhibit 1002 - Page 165
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

system involves costly and difficult installation and maintenance. Connection to the remote access device is typically through a modem connection, and data transfer between the device and remote user is slow. Even where DSL or other broadband capability is available for connection to the remote device, real time data transfer of video streams and data intensive operations cannot be effectively carried out. Remote device access systems have also been deficient in that only a single user can access a remote device at a time. This problem is particularly acute in situations when a customer and a support person at different locations both simultaneously wish to access a remote device at a third location.

[0004] Remote access of devices via the Internet in many cases involves a user located within one private local area network, and a device located within another, different private network. Information exchange between private computer networks via the Internet has created various security issues associated with protection of information on the private computer networks. Connection of a personal computer in a private network to the Internet can expose confidential data to unauthorized access or hostile attack from virtually anywhere in the world. Some of the sophisticated types of security threats posed by "hackers" include "logic bomb", "trapdoor", "Trojan horse", "virus" and "worm" programs. Such software programs can work independently or via an invoked host program to breach security, disrupt activity and cause damage by destruction of electronic files, alteration of databases, or introduction of computer viruses which affect the operability of the private computer network, computer hardware connected to the private network, and network-accessible devices within the private network.

[0005] One approach to private network security has been the use of "firewalls" embodied in hardware and/or software to protect private local area networks from hostile intrusion from the Internet. A firewall is located generally at the junction point or gateway between a private network and a public network such as the Internet and allows a network administrator to selectively offer access to specific types of Internet services to specific LAN users by filtering inbound and outbound traffic. Nearly every private network now has some form of firewall in place to protect internal data from outside intrusion.

Dropbox Exhibit 1002 - Page 166
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0006] Firewalls may operate by inspection of binary data at different layers of the TCP/IP (Transport Control Protocol/Internet Protocol) hierarchy in order to use different criteria for restriction of traffic. Binary data from the highest protocol layer, i.e., the Application Layer, is encapsulated within lower-level protocols all the way to the physical layer for transmission in network media such as twisted pair wire, fiber optic, or wireless channels. Packet filtering firewalls may be carried out at the Internet Protocol or Network layer. Circuit level gateway firewalls work at the TCP or Session Layer, and monitor TCP "handshaking" between packets to determine whether a requested session is legitimate. Application level gateway firewalls or "proxies" are application specific and can filter application specific commands such as http:post and get, which cannot be accomplished by packet filtering or circuit level firewalls. State-full multilayer inspection firewalls can combine the aspects of the above types of firewalls to provide a high level of security.

[0007] While firewalls have been largely beneficial for the security of private networks, the implementation of firewalls brings some important drawbacks. Particularly, there is an increasing use of applications that involve data transfer between different, heterogeneous private networks via the Internet. Users increasingly need to make connections from various locations across local-area-networks or wide-area-networks to perform remote diagnostics, calibration, controlling, monitoring or other functions associated with remote network-enabled devices. For example, a scientist or engineer operating within one firewall-protected private network may require access to a network-enabled device in a second firewall-protected private network in order to obtain data, make adjustments to the device remotely, or perform other operations remotely. The firewalls involved will typically be different due to the different security needs and corporate environments involved in the different private networks, and the firewall systems can impose serious limitations to data transfer between the heterogeneous networks.

[0008] In one common scenario of this type, a customer in one private corporate network may have a network-enabled instrument or device that needs to be calibrated by

Dropbox Exhibit 1002 - Page 167
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

expert personnel operating within the instrument manufacturer's private corporate network. In this case, the instrument is connected to the public network behind the customer's corporate firewall, which keeps the network address of the instrument anonymous to the outside public network. The expert personnel will typically be connected to the public network behind the manufacturer's firewall systems, which will prevent the expert personnel from establishing a network connection to the outside public network. The network-enabled device is thus not accessible via the public network by the service personnel. This problem is not easily remedied, as the firewall systems will frequently be different commercial software and/or hardware products, which are not amenable to modification in a manner that will allow the desired connection and communication.

[0009] One approach to allowing secured connection between local area networks is to employ virtual private network (VPN) systems. However, such VPN systems require expensive and complex installation of additional hardware and/or software at network access locations. The use of VPN systems also require that network administrators for participating networks implement some kind of joint network security policy, which is difficult or impossible in many situations. Furthermore, VPN systems are still an "emerging" technology, and interoperability among different VPN systems imposes limitations to connection of multiple private networks.

[0010] There is accordingly a need for a system that allows quick and easy communication between users and remote, network-enabled devices, that allows collaborative use of remote devices by multiple users, that is simple and inexpensive to install and maintain, that provides secure communication between firewall-protected private networks, and which is generally compatible with emerging, increasingly important applications such as remote diagnostics, calibration, controlling and monitoring functions for remote devices. The present invention satisfies these needs, as well as others, and generally overcomes the deficiencies found in the background art.

SUMMARY OF THE INVENTION

Dropbox Exhibit 1002 - Page 168
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0011] The invention provides systems and methods for remote access of network-enabled devices that provide seamless, firewall-compliant connectivity between multiple users and multiple devices, that allow collaborative operations by multiple users of remote devices, and which allow rapid, secure transmission of data between remote users and devices. In general terms, the system of the invention comprises at least one connection server, at least one client operatively coupled to the connection server via a public or global network, and at least one network-enabled device operatively coupled to the connection server via the public or global network. The connection server is configured to route control instructions from the client to the network-enabled device, and route data from the network-enabled device to the client.

[0012] By way of example, and not of limitation, the system may comprise one or a plurality of clients operatively coupled to one or more connection servers via a public network such as the Internet, as well as one or a plurality of network-enabled devices operatively coupled to the one or more connection servers via the Internet. The clients may comprise personal computers or other data processors within one or more private network that are operatively coupled to the Internet via one or more servers internal to the private networks. The clients may exist within private networks. The clients may in some embodiments comprise wireless data processor devices that are part of a mobile network. The network-enabled devices may comprise any equipment or components capable of receiving instructions and transmitting data via computer network, and may also be located within one or more private networks. The network-enabled devices may comprise equipment with internal data processing capability or may be used together with an external data processor(s) such as a personal computer. Such devices may comprise, for example, scientific instruments, chemical reactors, video security devices, surgical devices, power meters, power generators, home security systems, office security systems or like devices that are configured to be controlled, monitored or otherwise operated remotely via a network connection.

[0013] The connection servers may comprise a plurality of server modules, arranged in an extensible, scalable framework, that is configured to provide a distributed control infrastructure for collaborative interaction of multiple users with multiple network-

Dropbox Exhibit 1002 - Page 169
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

enabled devices. The distributed control infrastructure may comprise one or more databases operatively coupled to the connection servers, that store data which provides for maintenance of user data, data associated with device control, user security information, and other data used in monitoring and managing the distributed control infrastructure. The distributed control infrastructure may additionally comprise a security server and security database for providing user authentication. A load balancing system may be employed, in certain embodiments that assigns users to server modules at the time of authentication. The load balancing may be based on user and/or session types to facilitate collaborative, multi-user interaction with remote network-enabled devices.

[0014] Each connection server includes a plurality of connection handlers configured to maintain a plurality of network connections between a plurality of clients and one or more remote devices or one client with a plurality of remote devices, and of course can also maintain network connections between a single user and a single remote device. In this manner, the connection servers provide a connection mechanism that can route control instructions from a plurality of clients to a plurality of network-enabled devices, and route data from the network-enabled devices to the clients, in a collaborative fashion, such that multiple clients may simultaneously communicate with one or more remote devices via the connection server.

[0015] The system and methods of the invention are firewall compliant, and allow access and control of devices that are behind firewall and/or proxy systems in different private networks without modification of existing firewall or proxy systems. Once users are authenticated, connections between users and remote devices are established and maintained without further encryption key exchange, which greatly reduces computer overhead associated with data transfer, via the connection server, between remote devices and users. In contrast, prior art systems require encryption key exchange with each new command or communication, which significantly slows the communication processes in addition to requiring a much greater amount of computing power and time. A system according to the present invention may comprise at least one connection server, at least one client within a first, firewall-protected private network or single,

Dropbox Exhibit 1002 - Page 170
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

point of use, connection address, that is operatively coupled to the connection server via a public or global network, and at least one network-enabled device within a second, firewall protected private network or single, point of use, connection address operatively coupled to the connection server via the public or global network, or by a direct telephone line. The connection server is configured to establish connections between the user and the network-enabled device in each of the private networks via a common protocol that complies with the firewall system of each private network.

[0016] The invention also provides methods for establishing secured communication links between users and network-enabled devices in private, firewall-protected networks that comply with private network firewall systems. The methods of the invention comprise, in general terms, authenticating a user in a first, firewall protected private network or private address, and creating a communication channel between the user and a network-enabled device in a second, firewall protected private network or firewall protected private address, via a connection server associated with a public network. The communication channel is created using a protocol common to or acceptable to the firewall systems of each of the private networks/private addresses. Thus, to provide network connectivity across private and public networks, both network-enabled devices and users in the different private networks establish firewall-permissible network connections as clients to a central connection server. The methods may further comprise transmitting commands from the user, by the connection server, to the network-enabled device, and transmitting data from the network-enabled device, by the connection server. The methods may additionally comprise storing data from the network-enabled device for subsequent use by the user and others.

[0017] The connection servers are configured to accept, verify and route information received via connection with network-enabled devices in the private corporate networks, and monitor and maintain reliable network connections and data transmission modes via connection handlers and connection monitors. The connection servers act as a bridging medium wherein data can be moved between network-enabled devices and users in the different corporate networks, i.e., from device(s) to user(s) and vice versa, from user(s) to user(s) from device(s) to device(s), etc. The connection servers can be implemented

Dropbox Exhibit 1002 - Page 171
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

using standard server computers equipped with network interface units and other means to access the data network. The connection servers also provide server service to process client requests, in HTTP or other acceptable format.

[0018] The private-to-public-to-private communication tunnel nature of the systems and methods according to the present invention are advantageous in several respects. Since the users and devices within the different private networks do not actually connect directly to each other during data transmission, the network addresses of each user and each device can be kept confidential. Attacks by hackers from the public network would typically end up being directed to the connection servers, while sensitive data within the private networks remains secure behind the firewalls. Since individual users only need to know the network address of the connection server(s) accessed, and not the addresses of any of the devices accessed or addresses of other users they may be collaborating with, the users can access remote devices (and/or other users) even when location of the remote device(s) and/or user(s) has changed, as long as the remote device(s)/users(s) can achieve connection to the connection server(s). The connection servers thus provide multi-point data routing platforms wherein users can send command data to multiple remote devices of the same type, as well as send collaborative data to other users. These and other objects and advantages of the invention will be apparent from the detailed description below.

BRIEF DESCRIPTIONS OF THE DRAWINGS

[0019] The invention will be more fully understood by reference to the following drawings, which are for illustrative purposes only.

[0020] FIG. 1 is a functional block diagram of an access and control system for network-enabled devices in accordance with the invention.

[0021] FIG. 2 is a functional block diagram of an access and control system in accordance with the invention with distributed control infrastructure that includes a plurality of connection servers.

Dropbox Exhibit 1002 - Page 172
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0022] FIG. 3 is a functional block diagram of an alternative embodiment access and control system in accordance with the present invention wherein a security server is used in a connection server system.

[0023] FIG. 4 is a flow chart illustrating user authentication and connection aspects of the methods of the invention.

[0024] FIG. 5 is a flow chart illustrating authorization and security aspects of the methods of the invention

[0025] FIG. 6 is a flow chart illustrating load balancing aspects of server selection in the methods of the invention.

[0026] FIG. 7 is a flow chart illustrating operation of a client process and device control computer process in accordance with the invention.

[0027] FIG. 8 is a flow chart illustrating operation of a connection server process in accordance with the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0028] Disclosed herein are remote access and control systems and methods for remote, network-enabled devices that provide seamless, firewall-compliant connectivity between multiple users and multiple devices, and which allow collaborative operations by multiple users of remote devices. Before the subject invention is described further, it should be understood that the invention is not limited to the particular embodiments described below, as variations of the particular embodiments may be made and still fall within the scope of the appended claims. It is also to be understood that the terminology employed is for the purpose of describing particular embodiments, and is not intended to be limiting. Instead, the scope of the present invention will be established by the appended claims.

Dropbox Exhibit 1002 - Page 173
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0029] Any definitions herein are provided for reasons of clarity, and should not be considered as limiting. The technical and scientific terms used herein are intended to have the same meaning as commonly understood by one of ordinary skill in the art to which the invention pertains.

[0030] Any publications discussed herein are provided solely for their disclosure prior to the filing date of the present application. Nothing herein is to be construed as an admission that the present invention is not entitled to antedate such publication by virtue of prior invention. The dates of publication provided may be different from the actual publication dates, which may need to be independently confirmed. All publications mentioned herein are incorporated herein by reference to disclose and describe the methods, systems or other subject matter in connection with which the publications are cited.

[0031] Referring more specifically to the drawings, for illustrative purposes the present invention is embodied in the apparatus and flow charts shown in FIG. 1 through FIG. 8. It will be appreciated that apparatus disclosed herein may vary as to configuration and as to details of the parts, and that methods may vary as to details and the order of the acts, without departing from the basic concepts as disclosed herein. It should also be understood that the terminology used herein is for the purpose of describing particular embodiments only, and is not intended to be limiting, since the scope of the present invention will be limited only by the appended claims. The invention may be embodied in networked computer systems in a variety of configurations other than the exemplary configurations shown herein. The invention is described primarily in terms of use with HTTP (Hypertext Transfer Protocol), but may be used with other data transfer protocols. It should also be apparent to those skilled in the art that various functional components of the invention as described herein may share the same logic and be implemented within the same circuit, or in different circuit configurations.

[0032] Referring now to FIG. 1, an access and control system 10 for network-enabled devices is shown in accordance with the invention. The system 10 includes one or more

Dropbox Exhibit 1002 - Page 174
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

client or user computers 12a, 12b that are operatively coupled to a connection server 14 via a public or global network 16 such as the Internet. Also included in system 10 are one or more network-enabled devices 18a, 18b that are also operatively coupled to connection server 14 via global network 16. As shown, client computers 12a, 12b are part of a first private network 20 that is operatively coupled to the global network 16 through a firewall element 22. Network-enabled devices 18a, 18b are located within a second private network 24 that is operatively coupled to global network 16 via firewall element 26. In the embodiment of FIG. 1, connection server 14 is located within a private network 28 that is operatively coupled to global network 16 via firewall element 30.

[0033] User or client computers 12a, 12b may comprise any standard computer such as a minicomputer, a microcomputer, a UNIX® machine, mainframe machine, personal computer (PC) such as INTEL®, APPLE®, or SUN® based processing computer or clone thereof, or other appropriate computer. Client computers 12a, 12b may also include typical computer components (not shown), such as a motherboard, central processing unit (CPU), memory in the form of random access memory (RAM), hard disk drive, display adapter, other storage media such as diskette drive, CD-ROM, DVD-ROM, CD-RW, DVD-RW, flash-ROM, tape drive, PCMCIA cards and/or other removable media, a monitor, keyboard, mouse and/or other user interface, a modem, network interface card (NIC), and/or other conventional input/output devices. In many embodiments, client computers 12a, 12b comprise conventional desktop or "tower" machines, but can alternatively comprise portable or "laptop" computers, notebook computers, handheld personal digital assistants (PDAs) or "palm-top" computers, tablet computers, cellular phones capable of browsing Web pages, "dumb terminals" capable of browsing Web pages, internet terminals capable of browsing Web pages such as WEBTV®, or other Web browsing or network-enabled devices.

[0034] Each user or client computer 12a, 12b may comprise, loaded in its memory, an operating system (not shown) such as UNIX®, WINDOWS® 98, WINDOWS® ME, WINDOWS® 2000, LINUX®, System X®, Apple OS® or the like, or a proprietary operating system. Each client computer 12a, 12b may further have loaded in memory a

Dropbox Exhibit 1002 - Page 175
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Web Browser program (not shown) such as NETSCAPE NAVIGATOR®, INTERNET EXPLORER®, AOL®, or like browsing software for client computers. In accordance with the invention, client computers 12a, 12b may each comprise programming 32 stored in memory that allow client computers 12a, 12b to send instructions to network-enabled devices 18a, 18b as requests through connection server 14, and receive data from network-enabled devices 18a, 18b via responses through connection server 14, as described further below. Programming 32 may be the form of electronically, optically, or magnetically stored code or other form of computer readable stored code, that is loaded in the RAM or other memory of client computers 12a, 12b.

[0035] Connection server 14 may be any standard data processing device or computer, including a minicomputer, a microcomputer, a UNIX® machine, a mainframe machine, a personal computer (PC) such as an INTEL® based processing computer or clone thereof, an APPLE® computer or clone thereof or, a SUN® workstation, or other appropriate computer. Connection server 14 may include conventional components (not shown) such as a motherboard, central processing unit (CPU), random access memory (RAM), hard disk drive, display adapter, other storage media such as diskette drive, CD-ROM, DVD-ROM, CD-RW, DVD-RW, flash-ROM, tape drive, PCMCIA cards and/or other removable media, a monitor, keyboard, mouse and/or other user interface means, a modem, network interface card (NIC), and/or other conventional input/output devices. Multiple connection servers 14 may be used, as described further below.

[0036] Connection server 14 has stored in its memory a server operating system (not shown) such as UNIX®, WINDOWS® NT, NOVELL®, SOLARIS®, LINUX® or other server operating system, or a proprietary sever operating system (e.g., NEC or other proprietary system). Connection server 14 also has loaded in its memory web server software (also not shown) such as NETSCAPE®, INTERNET INFORMATION SERVER™ (IIS), or other appropriate web server software loaded for handling HTTP (hypertext transfer protocol) or Web page requests from client computers 12. Connection server 14 may also comprise a connection handler array 34 configured to establish and maintain a plurality of network connections between a plurality of clients 12 and one or more network-enabled devices 18. Each connection handler in array 34

Dropbox Exhibit 1002 - Page 176
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

handles connections between a client computer 12 and a network-enabled device 18 by reading requests and sending responses to and from clients 12 and network-enabled devices 18. The requests and responses may be in HTTP or other suitable protocol as described further below. A connection server usable with the invention is also described in U.S. Patent Application Ser. No. 09/454,178, which was incorporated herein by reference above.

[0037] Within private network 24, network-enabled devices 18a, 18b each are operatively coupled to a device control computer 36, which in turn is operatively coupled to global network 16. Multiple device control computers 36 may be present within network 24, with each device control computer 36a, 36b, 36c configured to support one or more network-enabled devices 18a, 18b. Device control computers 26 may comprise a standard computer such as those noted above, including minicomputers, microcomputers, UNIX® machines, LINUX® machines, mainframe machines, personal computers (PC) such as an INTEL®, APPLE®, or SUN® based processing computer or clone thereof. Each device control computer 36a, 36b, 36c includes typical computer components such as a motherboard, central processing unit (CPU), memory in the form of random access memory (RAM), hard disk drive, display adapter, other storage media such as diskette drive, CD-ROM, DVD-ROM, CD-RW, DVD-RW, flash-ROM, tape drive, PCMCIA cards and/or other removable media, a monitor, keyboard, mouse and/or other user interface, a modem, network interface card (NIC). Device control computers 18a, 18b each generally include an operating system such as UNIX®, WINDOWS® 98, WINDOWS® ME, WINDOWS® 2000, LINUX®, or the like, or proprietary operating system, as well as a browser such as NETSCAPE NAVIGATOR®, INTERNET EXPLORER®, AOL®, or the like. Device control computers 36a, 36b, 36c also include stored programming 38 that allows device control computers 36a, 36b, 36c to receive instructions from clients 12a, 12b via connection server 14 and to send responsive data to clients 12a, 12b via connection server 14.

[0038] Network-enabled devices 18a, 18b may comprise any equipment or components capable of receiving instructions and transmitting data via a computer network. Such devices may comprise, in specific embodiments, scientific instruments, chemical

Dropbox Exhibit 1002 - Page 177
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

reactors, video security devices, surgical devices, power meters, power generators, home appliances, manufacturing equipment, office equipment, or like devices, or electronic control modules for virtually any remotely controllable equipment, that are configured to be controlled, monitored or otherwise operated remotely. More than one network-enabled device 18a, 18b may be used in association with each device control computer 36a, 36b, 36c. Network-enabled devices 18a, 18b may be configured for "plug-and-play" operation wherein the devices 18a, 18b may be coupled to device control computer 36a, 36b, 36c without interruption of operation of device control computer 36 or other network-enabled devices 18a, 18b coupled to the device control computer 36a, 36b, 36c via USB, IEEE 1394, "FIREWIRE®", RS-232, Parallel, PCI or like interface.

[0039] Private networks 20, 24, 28 may comprise corporate local area networks (LANs), wide area networks (WANs), metropolitan area networks (MANs) or other forms of private or non-global networks. Private network 20 may include one or more internal servers (not shown) that manage communication of client computers 12a, 12b with the global network 16 through firewall 22. Client computers 12a, 12b may be arranged in a star topology, bus topology, "token ring" or other configuration within private network 20. Connection to global network 16 may be via DSL (digital subscriber line), telephone connection with a modem and telephone line via an Internet service provider (ISP), wireless connection, satellite connection, infrared connection, or other means for establishing a connection to the Internet 16. Private network 24 similarly may include internal server machines (not shown), with device control computers 36a, 36b, 36c suitably connected to the private network server or servers, and with connection to global network 16 made via DSL (digital subscriber line), telephone connection with a modem and telephone line via an internet service provider (ISP), wireless connection, satellite connection, infrared connection, or the like.

[0040] Firewall elements 22, 26, 30 may comprise any security element or elements, embodied in software and/or hardware, that are used to filter, restrict, or otherwise control network communication to and from private networks 20, 24, 28. Firewall elements may comprise, for example, packet filtering firewalls, circuit level gateways, "proxy" applications that filter specific commands, state-full multilayer inspection

Dropbox Exhibit 1002 - Page 178
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

firewalls, network address translator (NAT) elements that allow use of multiple duplicate IP addresses within a private network while unique IP addresses are required from outside the private network, and/or other elements or systems that restrict traffic and enhance security.

[0041] The system 10 as shown in FIG. 1 represents only one of many possible networked computer systems that is usable with the invention. Only two client computers 12a, 12b are shown within private network 20, and two network-enabled devices 18a, 18b and three device control computers 36a, 36b, 36c are shown within private network 24, for reason of clarity. Additional private networks, client computers, device control computers and network-enabled devices may be present in the system 10. Further, both user or client computers and network-enabled devices may be present within each private network. Numerous variations will suggest themselves to those skilled in the art.

[0042] In the operation of system 10, a user of a client machine 12 establishes a connection 40 with connection server 14 via global network 16. The connection server 14 then establishes a connection 42 to a device control computer 36 and network-enabled device 18 via global network 16. The client process 32 and device control computer process 38 can then send firewall compliant HTTP requests to each other, and receive HTTP responses from each other, via the connection server 14. User instructions for network-enabled devices 18a, 18b, and data from network-enabled devices, may be embedded within the HTTP requests and responses, which are handled by process 34 on connection server 14. Since connections to the network-enabled devices 18a, 18b are made through connection server 14, the IP (internet protocol) addresses for the devices need not be disclosed to the users of client computers 12a, 12b, nor are the IP addresses of the client computers 12a, 12b disclosed to the network-enabled devices 18a, 18b or to each other. Further, since most firewall and proxy systems accept HTTP requests, the connection between client computer 12a, 12b and network-enabled device 18a, 18b is seamless and firewall compliant.

Dropbox Exhibit 1002 - Page 179
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0043] Connection between client computers 12a, 12b and connection server 14 may be made subject to authorization of the user to provide a secure connection as described further below. Connection between network-enabled devices 18a, 18b may also be subject to authorization or authentication for security. Once a secure connection is established between client computer 12a, 12b and connection server 14, and between connection server 14 and network-enabled device 18a, 18b, subsequent data and instructions embedded within HTTP requests and responses need not be encrypted. This greatly reduces the computer overhead for data transmission between client computer 12a, 12b and network-enabled device 18a, 18b, because security is established only once, at the time that the connections between client computer 12a, 12b and network-enabled device 18a, 18b are made, and subsequent data embedded within HTTP requests and response may then be sent with or without encryption over the established secure connections. Even when encrypted data is sent, a new security key is not required to be sent with each transmission or communication. This allows rapid, secure data transfer over the Internet between clients 12a, 12b and remote devices 18a, 18b for uses such as real-time video data streams for monitoring security cameras, patient health, power generation and supply, manufacturing processes, remote manufacturing, smart house control, remote control of office machines, and other uses that require rapid data transfer. In contrast, prior art systems generally require the generation of a new security key for each command/data transmission to be sent in encrypted form, which greatly increases the computer overhead and processing time needed to authenticate and decrypt each individual transmission, which greatly reduces the efficiency of secure transfer of real-time streaming data transmission.

[0044] In the specific embodiments described herein, HTTP is used as a mechanism or protocol to send and receive binary data to and from client computers 12a, 12b and network-enabled devices 18a, 18b because HTTP is widely implemented and is managed by most firewall and proxy systems. It should be understood, however, that other protocols can also be used as long as the firewall/proxy systems 22, 26, 28 are configured to allow data traffic to be transported using such protocol. A data transfer protocol other than HTTP that may be used with the invention in certain embodiments is also described in U.S. Patent Application Ser. No. 09/454,178, noted above.

Dropbox Exhibit 1002 - Page 180
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0045] Multiple client computers 12a, 12b within private network 20 and/or in other private networks (not shown) may simultaneously establish connections to the same device 18a or 18b, or to a plurality of the same devices 18a, 18b, for simultaneous, collaborative use thereof. Support personnel 44 within private network 28 may also arrange for connection, via connection server 14, to the same remote device(s) 18a, 18b accessed by client computers 12a, 12b. The users of client computers 12a, 12b may comprise, for example, persons that are in a customer-vendor relationship, such that both the seller and purchaser of a network-enabled device 18a, 18b may simultaneously, securely, and collaboratively access the same device remotely through connection server 14 via global network 16.

[0046] Referring now to FIG. 2, there is shown another embodiment of an access and control system 46 in accordance with the invention, with like reference numbers used to denote like parts. The system 46 includes a distributed control infrastructure 48 comprising a plurality of connection servers 14a, 14b, 14c, 14d, 14e, 14f, 14g, 14h, 14n. Connection servers 14a-14n each include the same components and software described above for the connection server 14 of FIG. 1. As shown, connection server 14a is configured to operate as a primary connection server, with each of servers 14b-14n operatively coupled to connection server 14a.

[0047] Connection server 14a is operatively coupled to client computers 12a, 12b, 12c, 12n and network-enabled devices 18a, 18b, 18c, 18d, 18e, 18f, 18g, 18n via the Internet or other global network as described above. Client computers 12a-12n each include the stored client process or program 32 (FIG. 1), and device control computers 36a-36n each include the device control process or program 38 (FIG. 1) described above. Connection server 14a during operation is contacted by client computers 12a-12n, and assigns each client user to one of the additional connection servers 14b-14n according to a load balancing algorithm that operates according to load balancing programming 50. Load balancing with regard to servers 14b-14n may be carried out at the time that users are authorized. Each of client computers 12a-12n may be in a different private network (not shown) that is protected by a different firewall (not shown) as described above in

Dropbox Exhibit 1002 - Page 181
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

reference to FIG. 1. Similarly, each device control computer 36a-36n and the corresponding network-enabled devices 18a-18n may be located in multiple different private networks with different firewall systems.

[0048] The distributed control infrastructure 48 is scalable or extensible, and is flexible or re-configurable according to the number and nature of client computers 12a-12n, device control computers 36a-36n and network-enabled devices 18a-18n that are present in the system 46, and the levels of traffic between clients 12a-12n and network-enabled devices 18a-18n. Connection servers 14a-14n thus are modular in nature, and additional connection servers (not shown) may be added to infrastructure 48 as required by the increase in the number of participating client computers 12a-12n and network-enabled devices 18a-18n.

[0049] The distributed control infrastructure also includes a plurality of databases 52a, 52b, 52n, each of which may be operatively coupled to each of connection servers 14a-14n. Connection servers 14a-14n, in this regard, may include stored database management programming (not shown) such as SQL®, DB2® or like programming capable of retrieving and storing information in association with databases 52a-52n. Connection servers 14a-14n alternatively may be operatively coupled to databases 52a-52n through one or more database servers (not shown) that are capable of accessing information from databases 52a-52n.

[0050] Databases 52a-52n may include stored data related to users of client machines 12a-12n and data regarding the operation of remote devices 18a-18n, as well as data regarding the operation of the connection servers 14a-14n. Data associated with the operation of the various remote devices 18a-18n can be stored in databases 52a-52n during one or more sessions. The stored data can then be accessed by users of client computers 12a-12n in subsequent sessions. This database capability allows integration of data from devices 18a-18n with enterprise software solutions. As noted above, the users of clients 12a-12n in many instances may be in a customer-vendor or other business relationship with regard to the use of network-enabled devices 18a-18n, and stored data from devices 18a-18n may be used with software systems enterprise resource

Dropbox Exhibit 1002 - Page 182
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

management, customer relationship management, opportunity management, and other business-related software systems. The users or owners of client computers 12a-12n and/or devices 18a-18n may be involved in the system 46 on a subscription basis wherein each user or owner pays periodic fees or a one-time subscription fee for use of the distributed control infrastructure 48 for secure access to remote devices 18a-18n, as well as use of data in databases 52a-52n.

[0051] Referring next to FIG. 3, another access and control system 54 in accordance with the invention is shown, with like reference numbers used to denote like parts. The system 54 has a distributed control infrastructure 56 with a security server 58. A plurality of connection servers 14a, 14b, 14c, 14d, 14e, 14f, 14g, 14h, 14n are operatively coupled to security server 58, and to a plurality of databases 52a, 52b, 52n. Security server 58 is operatively coupled to a plurality of client computers 12a, 12, 12c, 12n, and to a plurality of device control computers 36a, 36b, 36c, 36d and network-enabled devices 18a, 18b, 18c, 18d, 18e, 18f, 18g, 18n via the Internet or other global network in the manner described above. Client computers 12a-12n each include the stored client process or program 32, and device control computers 36a-36n, each including device control process or program 38. The distributed control infrastructure 56 is scalable and reconfigurable according to the number of client computers, device control computers and network-enabled devices that are present in the system 54. Additional security servers 58 may be included in infrastructure 56 as well, if needed.

[0052] Security server 58, during operation of system 54, is contacted by users of client computers 12a-12n that seek to gain access to network-enabled devices 18a-18n via the Internet. Security server 58 includes security or authentication programming 60 that is used to authenticate the users of client computers 12a-12n prior to establishing a connection between a client computer and network-enabled device 18a-18n. Security server 58 also includes load balancing programming 50 that is used to assign client computers 12a-12n and network-enabled devices 18a-18n to individual ones of connection servers 14a-14n according to load balancing criteria.

Dropbox Exhibit 1002 - Page 183
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0053] The system of the invention as shown in FIG. 1 through FIG. 3 may be embodied in a variety of other networked computer configurations which will suggest themselves to those skilled in the art. The software aspects of the invention are highly distributed in nature, and need not be located on the particular computers shown in FIG. 1 through FIG. 3. Thus, certain of the operations carried out by client application 32 and device control application 36 may be embodied in software that is located on connections servers 14a-14n, security server 58, or other server (not shown) that is accessed by client computers 12a-12n and/or network-enabled devices 18a-18n via the Internet.

[0054] The operation of the access and control system 54 will be more fully understood by reference to the flow chart of FIG. 4, as well as to FIG. 3. The events of FIG. 4, it should be understood, apply to both client computers 12a-12n as well as device control computer computers (DCC) 36a-36n. The events shown in FIG. 4 and in the other flow charts described herein indicate where appropriate that "client/DCC" (i.e., a client machine 12a-12n or device control computer 36a-36n) may carry out or otherwise be involved in the event. For reason of clarity, however, the events of FIG. 4 are described primarily in terms of use with client computers 12a-12n. It should be understood, however, that the same events may be carried out by device control computers 36a-36n as well. It should also be understood that multiple client computers 12a-12n may simultaneously be connected with multiple device control computers 36a-36n and network-enabled devices 18a-18n through multiple connection servers 14a-14n, and in the following description, client computers 12a-12n, connection servers 14a-14n, device control computers 36a-36n, and network-enabled devices 18a-18n are referred to collectively.

[0055] In event 400, the user of a client computer 12a-12n contacts security server 58 of distributed control infrastructure 56. This contact may be carried out in a conventional manner by establishing a TCP socket connection between a client computer 12a-12n and the security server 58.

[0056] At event 410, a determination is made by security server 58 as to whether or not the user of client computer 12a-12n that made contact in event 400 is authorized. The

Dropbox Exhibit 1002 - Page 184
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

user authorization event 410 may comprise submission by the user of an HTTP request, by client application 32 on client computer 12a-12n, with embedded user authentication data. The authentication data embedded in the request may be encrypted. The authentication data may include username and password information, as well as identification information for particular network-enabled devices 18a-18n to which the user wishes to establish a connection. The authentication application 60 on security server 58 checks to see whether or not the authentication data in the request has been altered during transmission from client computer 12a-12n, and whether or not the authentication data verifies the user of client computer 12a-12n. If authorization is denied, event 400 may be repeated. An HTTP response may be sent by the security server to the client computer 12a-12n advising the user of a security error, and that access to any network-enabled devices 18a-18n is denied. If the user of client computer 12a-12n is authorized in event 410, encryption keys may be prepared and verified for the user. Following user authorization, event 420 is then carried out. The authorization process and security aspects of the system 54 are discussed in greater detail below with reference to the flow chart of FIG. 5.

[0057] At event 420, security server 58 assigns one of the connection servers 14a-14n to the user of client computer 12a-12n that was authorized in event 410. Connection server assignment is carried out by load balancing application 50 on security server 58. Assignment of a connection server 14a-14n to a particular user may be based on the type of user, the type of session that the user wishes to establish, and the status and availability of particular connection servers that are configured to accommodate the user type and session type, as well as the relative current workloads of such connection servers. The load balancing aspects of the invention are discussed in more detail below with reference to the flow chart of FIG. 6.

[0058] In event 430, a connection is made between the connection server 14a-14n assigned in event 420, and the network-enabled device 18a-18n selected by the user authorized in event 410. This connection may be in the form of a TCP socket connection between the security server 58 and the network-enabled device 18a, 18n selected by the user.

Dropbox Exhibit 1002 - Page 185
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0059] In event 440, client computer 12a-12n transmits instructions or commands to a network-enabled device 18a-18n, and in event 450, network-enabled device 18a-18n transmits data to client computer 12a-12n. These events may occur concurrently, as full duplex connections are established. Client process 32 on client computers 12a-12n periodically sends HTTP requests to connection server 14a-14n that include embedded command data. Device control process 38 on device control computer 36a-36n also sends periodic HTTP requests to connection server 14a-14n with embedded data from network-enabled device 18a-18n. These requests are handled by process 34 on connection server 14a-14n. Process 34 sends HTTP responses to device control computer 36a-36n that include embedded command data from the client computer 12a-12n. The command data is retrieved from the HTTP responses by process 38 on device control computer 36a-36n and communicated to device 18a-18n. Similarly, process 34 sends HTTP responses to client computer 12a-12n that contain embedded data from device 18a-18n, which is retrieved by client process 32. The operation of client process 32, device control process 38, and connection server process 34 in events 440 and 450 are described in more detail below with reference to the flow charts of FIG. 7 and FIG. 8.

[0060] At event 460, data from network-enabled device 18a-18n (or client computer 12a-12n) is stored in database 52a-52n. This data may be used by other authorized users in the same session or in subsequent sessions.

[0061] As noted above, the events of FIG. 4 as described above may be bi-directional, i.e., a device control computer 36a-36n may first contact security server 58, obtain authorization, be assigned to a connection server 14a-14n, and then connected with one or more a selected client computer(s) 12a-12n, and/or one or more other device control computers 36a-36n. Additionally, the events of Fig. 4 may be carried out by a first client computer 12a-12n to establish a connection with one or more other client computers 12a-12n with or without connection with one or more device control computers 36a-36n. In certain embodiments, the security server 58 may be omitted, and load balancing and authorization applications may be run on one or more connection servers 14a-14n

Dropbox Exhibit 1002 - Page 186
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

instead. In still other embodiments such as that shown in FIG. 1, only a single connection server may be used, with authentication application 60 and load balancing application 50 located on the single connection server, where load balancing application 50 may be used to determine current loads of the single server and whether or not additional applications can be handled by the single server at any given time. In still other embodiments, the load balancing and authentication operations may be omitted. Numerous variations of the events, and variations in the relative order of the events described above are possible and will suggest themselves to those skilled in the art, and such variations are also considered to be within the scope of this disclosure.

[0062] The systems and methods of the invention provide for secure, rapid transfer of data between remote users and devices via the internet without requiring complex encryption of data embedded in each HTTP response and request, thereby providing unprecedented ability to securely transmit data streams in real time. Also provided is the ability to remotely control network-enabled devices by secure communications without requiring compatible security protocols at the sending and receiving ends of the communications. Cryptography plays a significant role in securing data communication. In modern key–based cryptography, data is scrambled into an unreadable form using computational cryptographic algorithms and binary encryption keys. The scrambled data can be decrypted using the corresponding decryption key that is associated with the encryption key. In modern key–based cryptography, the encryption and decryption algorithms may be well known, but the decryption key, and sometimes the encryption key as well, may be well guarded. Hence, the strength of such cryptography system is determined by the size of its key-space that is typically measured in terms of number of bits in the key. For example 40-bit key-space has 240 (i.e., 1,099,511,627,776) possible keys.

[0063] There are two main types of key based cryptography used for Internet-transmitted data: secret-key (symmetric) cryptography and public-key (asymmetric) cryptography. In secret-key cryptography, both the encryption and decryption process use the same symmetric key, which means that the shared key must be kept secret by both sender and receiver. Such system requires coordination of both sender and receiver

Dropbox Exhibit 1002 - Page 187
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

in using their secret keys. The Data Encryption Standard (DES) is an example of a secret-key cryptography algorithm that has been adopted by National Institute of Standards and Technology (NIST). DES uses the same 56-bit key for both encryption and decryption. A variation of this system known as Triple DES or DESede has subsequently been developed. Triple DES encrypts and decrypts data with three iterations of the DES algorithm using three separate keys. As a result, Triple DES is a much stronger algorithm that has an effective key-space of 168 bits.

[0064] Public-key (asymmetric) cryptography employs an algorithm that uses a pair of keys; a public key, and a private key for encryption and decryption processes, respectively. In public-key cryptography algorithms, the private key cannot feasibly be obtained from the public key, and the public key can be published on the Internet without affecting the security of the encryption algorithm. One famous public-key cryptography algorithm, known as RSA algorithm, depends on the difficulty of factoring large numbers. Another well-known public key cryptography is the ElGamal algorithm, which is based on the difficulty of calculating a discrete logarithm in a finite field. In the present invention, either the RSA or ElGamal algorithm can be used to secure data communication between client computers 12a-12n and network-enabled devices 18a-18n.

[0065] Both the secret-key and public-key algorithms above protect data privacy by computationally scrambling the data. However, these algorithms do not protect data integrity to ensure the authenticity of the data. A message digest is a special algorithm known as a one-way (hash) function that is difficult to reverse. A message digest function can be used to calculate a message digest value from a message that provides the signature of that message.

[0066] A good message digest function ensures that it is computationally infeasible to derive a message that can produce the same message digest value under the message digest function. It is also computationally infeasible to produce the same message digest values from two messages using the same message digest function. There is nothing secret about a message digest function, as it is publicly available and uses no keys. If a

Dropbox Exhibit 1002 - Page 188
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

message is altered or tampered with during transport, the message digest value of that message will very likely be altered as well, and comparison of transmitted message digest value with calculated message digest value indicates whether or not alteration has occurred. Possible message digest algorithms that can be used in the present invention include the Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1). NIST developed the SHA-1 algorithm to operate on a message up to 2 to 64 bits in length and produce 160 bits message digest value. Other message digest algorithms may also be used with the invention.

[0067] The main disadvantage of public-key cryptography is that it is computationally more intensive than secret-key algorithms. For example, the ElGamal algorithm can only use a subset of all possible values for a key of a given length, due to the nature of the mathematical problem it is based on. Secret-key algorithms, however, may use all the possible values for a key of a given length. As a result, to be considered cryptographically strong, the ElGamal algorithm may need a key of at least 512 bits, while the same level of security might be provided by the DES algorithm with a 64-bit key. Although the secret-key algorithms are computationally more efficient for large data transfers, they require constant management of key exchanges to ensure the secrecy of the shared key. In the embodiment described below, the invention employs public-key cryptography such as the ElGamal algorithm with a 512-bit key, to both authenticate connection and encrypt key exchange between senders and receivers, i.e., client computers 12a-12n and network-enabled devices 18a-18n. Subsequently, full-duplex data communications may be unencrypted, or may be encrypted using secret-key algorithm such as Triple DES with a 168-bit key.

[0068] With the above in mind, reference is now made to FIG. 5, as well as FIG. 3, wherein user authentication and encryption aspects of the invention are illustrated. The events of FIG. 5 are again described in terms of use with client computers 12a-12n. It should be understood, however, that the same events may be carried out in association with device control computers (DCC) 36a-36n. The events shown in FIG. 5 may occur concurrently with event 410 of FIG. 4, and illustrate in more detail one embodiment of an authentication system that may be used with the invention.

Dropbox Exhibit 1002 - Page 189
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0069] In event 500, process 32 on client computer 12a-12n prepares authentication data that is to be sent to security server 58, and calculates a message digest value for the authentication data. The authentication data may comprise, for example, username and password information for a user of client computer 12a-12n, as well as password or other information related to one or more network-enabled devices 18a-18n, and/or other client computer 12a-12n, that the user of computer 12a-12n wishes to contact and use communicate with.

[0070] At event 502, process 32 on client computer 12a-12n encrypts the authentication data, together with the message digest value calculated in event 100, using the public key for security server 58. The public key 58 may be published on the Internet, or sent to specific users of client computers 12a-12n and device control computer(s) 36a-36n.

[0071] At event 504, process 32 on client computer 12a-12n sends an HTTP request to security server 58 that includes, embedded therein, the encrypted authentication data and message digest value.

[0072] At event 506, security server 58 receives the HTTP request from client computer 12a-12n, and authentication process 60 on security server 58 decrypts the embedded authentication data and corresponding message digest value from the HTTP request using its private key. The authentication process 50 separates the authentication data from the message digest value received in the request.

[0073] At event 508, authentication process 60 computes or calculates a message digest value from the decrypted authentication data and compares the computed message digest value to the received message digest value of event 506.

[0074] At event 510, authentication process 60 determines whether the computed message digest value and the received message digest value match. If the computed message digest value and received message digest value are not identical, the authentication data from client computer 12a-12n has been altered or corrupted while en

Dropbox Exhibit 1002 - Page 190
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

route to security server 58, and event 512 is carried out. If the computed message digest value and received message digest value match or are identical, event 514 occurs.

[0075] At event 512, an HTTP response with a security error message may be sent to client computer 12a-12n by security server 58. The message may advise the user of client computer 12a-12n that authentication data could not be validated, and invite the user of client computer 12a-12n to re-submit the authentication data. After a selected number of failed authentication attempts by client computer 12a, 12n by repeating events 500-10, a message may be sent to client computer 12a-12n to advise the user thereof that the desired network connection is not available due to authentication failure.

[0076] If the computed message digest value and received message digest value match in event 510, the received authentication data has not been altered or corrupted, and event 514 is carried out. Authentication process 60 on security server 58, in event 514, verifies the authentication data recovered in event 506 by comparing the username and password received from client 12a-12n to security information stored in database 52a. This security information includes known usernames and passwords for valid or permitted users of client computers 12a-12n.

[0077] At event 516, authentication process 60 makes a decision as to whether the username and password information data represents an authorized user. If the user is authorized, event 518 occurs. If the user is not authorized, event 512 may be carried out. Event 512 may involve an HTTP response to client computer 12a-12n with a security error message as noted above.

[0078] At event 518, security server 58 sends an HTTP response to client computer 12a-12n with a message indicating that the user of client computer 12a-12n is authorized to proceed and that network communication to the desired network-enabled device 18a-18n and/or other authorized client computer(s) 12a-12n may be established.

[0079] At event 520, client process 32 generates a secret key for encryption of data to be transmitted from client computer 12a-12n to the network-enabled device 18a-18n and/or

Dropbox Exhibit 1002 - Page 191
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

other authorized client computer(s) 12a-12n of interest. Secret key generation may comprise generation of a random secret key using a pseudo-random number generator or PRNG element (not shown) in client computer 12a-12n. The secret key may be symmetric such that the same key is used for encryption of data sent from client computer 12a-12n to network-enabled device 18a-18n, and from network-enabled device 18a-18 to client computer 12a-12n. Alternatively, device control computer 36a-36n may generate its own secret key for transmission of data from network-enabled device 18a-18n to client computer 12a-12n.

[0080] In event 522, process 32 on client computer 12a-12n generates or computes a message digest value for the secret key generated in event 520.

[0081] In event 524, client process 32 encrypts the secret key generated in event 520, and the message digest value for the key that was generated in event 522, using the public key for security server 58.

[0082] In event 526, process 32 on client computer 12a-12n sends an HTTP request to security server 58 that includes the encrypted secret key and corresponding message digest value embedded within the request.

[0083] At event 528, security server 58 receives the HTTP request from client computer 12a-12n that was sent in event 526, and authentication process 60 on security server 58 decrypts the embedded secret key data and corresponding message digest value from the HTTP request using its private key. The authentication process 50 separates the secret key data from the message digest value for the secret key that was received in the request.

[0084] At event 530, authentication process 60 calculates or computes a message digest value for the decrypted secret key, and compares the computed message digest value to the received message digest value for the secret key from event 528.

Dropbox Exhibit 1002 - Page 192
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0085] At event 532, authentication process 60 determines whether the computed message digest value and the received message digest value for the secret key are matched. If the computed message digest value and received message digest value do not match, the secret key transmitted from client computer 12a-12n in event 526 has been altered or corrupted during transmission to security server 58, and event 534 occurs. If the computed message digest value and received message digest value match or are identical, event 536 is carried out.

[0086] At event 534, security server 58 may send an HTTP response to client computer 12a-12n with a security error message. The message may advise the user of client computer 12a-12n that the received secret key could not be verified, and may invite the user to repeat events 522-526. After a selected number of failed attempts by client computer 12a-12n to send a verifiable secret key, a message may be sent to client computer 12a-12n to advise the user that the desired network connection cannot be made.

[0087] At event 536, an HTTP response may be sent by security server 58 to client computer 12a-12n advising the user thereof that the secret key has been received and authenticated. At this point, the security server 58 has successfully authenticated the client computer 12a-12n and has securely received the secret key for encryption of data from the client computer 12a-12n.

[0088] At event 538, a connection may be established between the authenticated client computer 12a-12n and network-enabled device(s) 18a-18n and or other client computer(s) 12a-12n. This event may be carried out by a selected one of connection servers 14a-14n according to the load balancing algorithm shown in FIG. 6 and described below.

[0089] Subsequent to establishing this connection, data transmitted to and from client computer 12a-12n and network-enabled device(s) 18a-18n/client computer(s) 12a-12n may be encrypted using the secret key (assuming symmetric key encryption) and embedded in HTTP requests and responses that are handled by connection server 14a-

Dropbox Exhibit 1002 - Page 193
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

14n as described below. Alternatively, device control computer 36a-36n/other client computer 12a-12n may carry out the events described above to generate its own secret key for asymmetric data encryption wherein data from client computer 12a-12n is encrypted with a first secret key, and data from network-enabled device(s) 18a-18n and device control computer(s) 36a-36n and/or other client computer(s) 12a-12n is encrypted with a second, secret key. Each client computer 12a-12n and device control computer 36a-26n may generate its own secret key. The use of secret key (i.e., non-public key) encryption such as Triple-DES cryptography described above, for data transmissions between client computers 12a-12n and network-enabled devices 18a-18n, provides an efficient way for rapidly sending secure data back and forth via the Internet using connection servers 14a-14n, with relatively little computational overhead required for data encryption and decryption. Once the secret keys from client computer 12a-12n and device control computer 36a-36n have been securely coordinated by security server 58 and shared between client computer(s) 12a-12n and device control computer(s) 36a-36n, the secret-key encryption layer can be easily be implemented by connection servers 14a-14n.

[0090] Numerous variations on the events, and variations in the order of events of FIG. 5 are possible, as will be clear to those skilled in the art. In certain embodiments of the invention, events 520-536 may be omitted, with no secret key generated for subsequent data communication. That is, non-encrypted data may be sent between client computer 12a-12n and network-enabled device 18a-18n following user authorization in event 516. Multiple security servers 58 each including authentication application 60 may be utilized as is required by traffic levels between clients 12a-12n and network-enabled devices 18a-18n. Although the authentication and key generation process is described herein in terms of being carried out by client computer 12a-12n, it is again noted that the various events of FIG. 5 that involve client computer 12a-12n and client process 32 are, in many embodiments, also carried out by device control computer 36a-36n and device control process 38.

[0091] The invention allows the server demands of many client computers 12a-12n and devices 18a-18n that collaborate to be distributed over multiple connection servers 14a-

Dropbox Exhibit 1002 - Page 194
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

14n as noted above. By enabling secure transmission without the need to generate and transmit a new security key for each encrypted transmission following the user authorization in event 516, the present invention permits much more rapid and real-time control and collaboration than has ever before been possible. This is made possible by the central functions of the distributed control infrastructure 48, which ensures secure connections between any users of the system (i.e., communications between any of the various combinations of client computer 12a-12n; device control computer 36a-36n; and client computers 12a-12n and device control computers 36a-36n) prior to sending or communicating encrypted or unencrypted data. By properly balancing the demand of client computers 12a-12n and devices 18a-18n among the available connection servers 14a-14n, greater reliability and efficiency are achieved. This balancing is done by implementing a load balancing algorithm that selects a connection server for which each session is assigned when the session is scheduled.

[0092] When a session is to be created between one or more client computers 12a-12n, between one or more network-enabled devices 18a-18n, or between one or more client computers 12a-12n and one or more network-enabled devices 18a-18n, a connection server 14a-14n to which the session will be assigned must be selected. Scheduling of a session can be done ahead of time, or can be done in real-time at the moment that such a session is needed. Each connection between a client computer 12a-12n and a network-enabled device 18a-18n, or between client computers 12a-12n or between network-enabled devices 18a-18n, that is part of a session will connect through an assigned connection server 14a-14n when the session begins.

[0093] Referring again to FIG. 3, database 52b holds information that allows load balancing in accordance with the invention to be implemented. Data tables (not shown) within database 52b include information about, inter alia, different types of users, different types of sessions which users may wish to establish, and different types of connection servers that may be used for such users and sessions, as well as current statistics regarding the status, availability and power usage of the connection servers.

Dropbox Exhibit 1002 - Page 195
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0094] There may be several different types of users of client computers 12a-12n and/or or devices 18a-18n that may take part as members of a session wherein data is transmitted between client computer(s) 12a-12n and device(s) 18a-18n, between client computers 12a-12n or between devices 18a-18n. A User Type identifies a type of user and each User Type refers to a Session Type, described below, in which such types of users may take part. By differentiating the unique characteristics of each type of user or device that takes part in a session, a more accurate load balancing may be implemented. User Types may be based on the types of device 18a-18n involved, the nature of business that the users are involved in, or other factors. For example, within a single session, there may be one type of device 18a-18n that is expected to send video data (i.e., video monitoring), while another type of user does not send video data. Other users may be interested in monitoring of power generation and distribution, monitoring of remote patients via diagnostic devices, monitoring of robotic manufacturing equipment, or other consideration. By distinguishing between the different demands of each User Type, an effective balancing strategy has been implemented. The term User Type refers to users at both ends of a connection through a connection server 14a-14n, i.e., users of client computers 12a-12n as well as users of device control computers (DCC) 36a-36n.

[0095] A session may include a group of users who want to collaborate in the operation or monitoring of one or more network-enabled devices 18a-18n. Each session must be assigned to a connection server that manages the communication between the users and devices. Sessions may have a designated time at which they start and are expected to end. Each Session can be assigned a Session Type. Session Type may be based on the types of users or devices involved, scheduling considerations, business interactions, or other factors or characteristics. For example, Session Types may be based on customer-vendor interaction involving a shared remote device such as a robotic assembly device, a printer, a photocopier, or other device. Session types may be based on patient-physician interaction involving diagnostic devices, multiple technician monitoring of a chemical reactor, on the basis of particular timing or scheduling considerations, or other basis. Various other bases for defining Session Types will suggest themselves to those skilled in the art.

Dropbox Exhibit 1002 - Page 196
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0096] The connection servers 14a-14n may also comprise different Server Types. For example, selected ones of connection servers 14a-14n may be configured, and may have handler applications 34 configured, for managing different User Types and Session Types. For example, commercial clients may wish to have one or more of connection servers 14a-14n configured for dedicated work with a particular type of business or data communication. Thus, individual connection servers 14a-14n may be configured to specifically handle data transmission associated with video monitoring, while other connection servers 14a-14n are configured specifically to handle transmission of power generation data, patient monitoring data, manufacturing equipment, home appliances and/or security devices, office machines and/or security devices, or other specific types of data associated with specific types of devices 18a-18n. Still other connection servers 14a-14n may be specifically configured to handle large numbers of users that simultaneously collaborate in the operation of a particular device or devices 18a-18n. Various other bases for specific Server Types are also possible, and will suggest themselves to those skilled in the art.

[0097] An important concept in load balancing is that there is a limited load that an individual server can support. This load may be limited by bandwidth, processing power, speed of data access, or other factor. A parameter has been defined that serves as a single metric that indicates a server's ability to support connections. This parameter is hereinafter referred to as "Power", and each connection server 14a-14n has a parameter specifying the maximum Power that it can provide at any given time.

[0098] When a session is to be assigned to a particular connection server 14a, a known parameter of that session is the Session Type, discussed above. From the Session Type, each User Type that may take part in such a Session Type can be determined by querying the data in the previously listed tables (not shown in database 52b. Each User Type may have characteristics that are used in calculating connection server Power requirements, such as the average Power used by each connection between a client computer 12a-12n and a network-enabled device 18a-18n, the minimum number of any reserved connections for the session, the average number of connections for a session, or other considerations.

Dropbox Exhibit 1002 - Page 197
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[0099] Thus, for a single Session Type, the minimum Power can be computed by summing the product of the average Power and the minimum number of reserved connections over each User Type that may take part in such a Session Type. By summing this minimum Power over all scheduled sessions at any point in time on a single connection server 14a-14n, the expected Power usage at that point in time can be calculated for the connection server 14a-14n. This minimum Power value may then be used in restricting the selection of available connection servers 14a-14n to only those that meet the Power requirement during the period of the session to be scheduled. This restriction in connection server selection allows additional reliability to be realized, and guarantees that any selected connection server 14a-14n has not exceeded its Power limitation when a minimum number of reserved connections are being utilized.

[00100] With the above in mind, reference is now made to the load balancing flow diagram of FIG. 6, as well as FIG. 3. At event 600, load balancing application 50 on security server 58 determines the User Type or User Types that will be involved in a session. This determination may be made on the basis of identification information presented to the security server 58 in the form of embedded user identification data in HTTP requests for a connection from client computer 12a-12n and/or device control computer 36a-36n, together with User Type data present in database 52b. The identification information recovered from the HTTP requests by security server 58 may be compared to stored User Type data in database 52b to make the User Type determination for the session.

[00101] At event 610, load balancing process 50 determines the Session Type for the connection to be created. This determination may, as noted, be based on identification data embedded in HTTP requests from client computer 12a-12n and/or device control computer 36a-36n, which may be compared to Session Type information in database 52b.

[00102] Once User Type and Session Type have been determined, server selection is carried out by load balancing process 50 in event 620. Server selection may be based on

Dropbox Exhibit 1002 - Page 198
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

a comparison of User Type and Session Type information determined in events 600, 610, to Server Type information in database 52b. From this information, a particular connection server 14a-14n is selected to handle the session between the client computer 12a-12n and device control computer 36a-36n and network-enabled device 18a-18n.

[00103] At event 630, load balancing process 50 determines whether or not the connection server 14a-14n selected in event 620 is active. The selected server may, for example, be powered down for maintenance or upgrade work, may be malfunctioning, or may be inactive for other reason. If the selected server has active status, event 640 occurs. If the selected server is not active, event 620 is repeated and a different connection server 14a-14n is selected. Selection of servers 14a-14n may occur according to a predefined selection order, so that any particular server will not be selected twice by the process before each server has been selected and analyzed for purposes of load balancing.

[00104] At event 640, load balancing process 50 determines whether or not the connection server 14a-14n selected in event 620 supports the particular User Type determined in event 600. As noted above, certain of connection servers 14a-14n may be configured to handle particular User Types. If the selected connection server 14a-14n is not configured to support the User Type determined in event 600, event 620 is repeated and another, different connection server is selected. If the selected connection server does support the User Type, event 650 occurs.

[00105] At event 650, load balancing process 50 determines whether or not the connection server 14a-14n selected in event 620 supports the particular Session Type determined in event 610. If the selected connection server 14a-14n is not configured to support the Session Type determined in event 610, event 620 is repeated and a different connection server is selected, and events 630-650 are repeated. If the selected connection server does support the User Type, event 660 is carried out.

Dropbox Exhibit 1002 - Page 199
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[00106] At event 660, load balancing process 50 determines whether or not the connection server 14a-14n selected in event 620 has adequate Power to support the connections that will be involved in the session to be established. This query is made to ensure that the selected connection server 14a-14n will have the Power needed to meet the minimum requirements of all sessions that are assigned to it. If the selected connection server 14a-14n has insufficient Power to handle the connections that will be involved in the session to be established, event 620 is repeated and a different connection server 14a-14n is selected. If the selected connection server 14a-14n does have sufficient Power, event 670 is carried out, wherein the designation for that selected server is temporarily stored to be used in a comparison of potentially available servers to determine which is best for load balancing purposes. At event 680 it is determined whether all of the servers have been selected and analyzed at this stage for load balancing purposes. If the last server has not yet been selected, processing returns to event 620 where the next server is selected. If the last server has been selected already, processing goes to event 690.

[00107] At this point, there may still be multiple connection servers 14a-14n available that will meet the requirements of the session to be established. In event 690, a determination is made is to which of the selected connection servers 14a-14n stored at event 670 has the best available power level for the contemplated session. If only one server was stored at event 670, then this server is determined to have the best available server power by default. This event in selecting a connection server 14a-14n implements efficient utilization of the connection servers 14a-14n. Since each connection server 14a-14n can support many simultaneous connections, this calculation takes advantage of the statistically calculated average Power usage that is expected for each connection. Such an average Power usage for one User Type can be calculated by multiplying the Power used for each connection with the average number of connections. An average Power usage for one session can be calculated by summing the previous result over all User Types that refer to the Session Type of the session to be established. By summing this Power usage over all scheduled sessions at any point in time on a single connection server 14a-14n, the expected Power usage at that point in time can be calculated for a particular connection server 14a-14n. The ratio of this expected power

Dropbox Exhibit 1002 - Page 200
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

usage to a connection server's maximum Power usage allows a Utilization Ratio to be determined for each connection server 14a-14n. For each connection server 14a-14n, the maximum value of the Utilization Ratio during the period of the session to be scheduled is calculated. Considering the set of connection servers which were stored in event 670, the connection server with the minimum utilization ratio relative to the others in the set is then selected as the server to which this Session is assigned.

[00108] After determining the server with the best available server power in event 690, the server determined as such is assigned to the current session/client/DCC. At event 695, having determined the best connection server 14a-14n for the upcoming session, the connection server 14a-14n is assigned to the client computer(s) 12a-12n and device control computer(s) 36a-36n and device(s) 18a-18n that will be involved in that session.

[00109] The above load balancing process insures that sessions are statistically distributed among the available connection servers 14a-14n, while also guaranteeing that the minimum number of connections that are expected are always available to users.

[00110] Having now described the authentication, encryption, and load balancing aspects of the subject invention, the actual process of data transfer between client computer(s) 12a-12n and device control computer(s) 36a-36n and their coupled network-enabled devices can be addressed. As noted throughout the specification, processes of data transfer which are described are also applied to transfers between client computers 12a-12n, as well as transfers between device control computers 36a-36n. Data transfers are carried out by client process 32 and device control process 38 in the manner shown in the flow chart of FIG. 7, and by the connection server process 34 as shown in the flow chart of FIG. 8. The process of communicating data from client computer 12a-12n to device control computer 36a-36n, and from device control computer 36a-36n to client computer 12a-12n is the same and, accordingly, the description of FIG. 7 and FIG. 8 provided below is primarily in terms of use with client computer 12a-12n. It should be understood, however, that the same operations of client process 32 on client computer 12a-12n described below for data transmission are also carried out by device control process 38 on device control computer 36a-36n.

Dropbox Exhibit 1002 - Page 201
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[00111] Referring now more particularly to FIG. 7, data transmission using client process 32 and device control process 38 is shown. In event 700, the data transmission events start. Event 700 may occur, for example, after the authentication and secret key generation and verification events of FIG. 5, and the load balancing connection server selection events of FIG. 6 have been completed.

[00112] At event 710, client process 32 determines whether or not client computer 12a-12n has any data to send to network-enabled device 18a-18n. Such data may comprise, for example, command instructions for the operation of network-enabled device 18a-18n. This event is carried out by checking a sending buffer (not shown) in the memory of client computer 12a-12n wherein are stored data that is to be sent to network-enabled device 18a-18n. If no data is present in the sending buffer, events 720 and 730 occur. If data for network-enabled device 18a-18n is present in the sending buffer, event 740 is carried out.

[00113] Client process 32 maintains communication with connection server 14a-14n by periodically sending HTTP requests to connection server 14a-14n. If no data was found in the client computer sending buffer in event 710, client process 32 waits for a selected period of time, i.e., n milliseconds, in event 720. This waiting process allows the processor of client computer to perform other tasks in a multitasking environment. In this way, client process 32 adaptively varies the timing between sending successive HTTP requests to the connection server 14a-14n. That is, if data is found in the sending buffer, the request is sent immediately. Likewise, if data is not initially found in the sending buffer, but is found after a wait of n milliseconds, the data is sent in a request at that time. This waiting and checking loop continues until a maximum preset time is reached, at which time an HTTP request is sent to the connection server 14a-14n, regardless of whether any data is in the sending buffer. By this approach, data is transmitted efficiently around the time that it appears in the sending buffer, so that requests may be sent very rapidly if data continues to be inputted to the sending buffer. On the other hand, the system is persistent, in that HTTP requests are sent at maximum

Dropbox Exhibit 1002 - Page 202
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

predefined intervals regardless of whether any data is sent from the sending buffer along with the request.

[00114] As noted, client process 32 determines, in event 730, whether or not it is time to send a periodic HTTP request to connection server 14a-14n to check for any data that may be sent by network-enabled device 18a-18n for client computer 12a-12n. The time-out parameter of event 730 can be initialized by client process 32 before entering the waiting iteration of event 720. If, in event 730, it is time to send an HTTP request to connection server 14a-14n, event 740 is carried out. If not, event 710 is repeated.

[00115] At event 740, client process prepares and sends an HTTP request to connection server 14a-14n. If data for network-enabled device 18a-18n was present in the sending buffer in event 710, this event may additionally comprise embedding that data in the HTTP request. The data may be encrypted using a secret key prepared in the manner described above. The data embedding may, for example, be carried out using the HTTP POST method.

[00116] At event 750, client process 32 reads an HTTP response from connection server 14a-14n.

[00117] At event 760, client process 32 determines whether or not there is any embedded data from network-enabled device 18a-18n for client computer 12a-12n within the HTTP response of event 750. If there is embedded data in the HTTP response, event 760 occurs. If there is no embedded data in the response, event 780 occurs.

[00118] At event 770, data embedded in the HTTP response of event 750 is read and is buffered in the memory of client computer 12a-12n for use, and client computer 12a-12n is notified that data from network-enabled device 18a-18n has been received. If the data from network-enabled device 18a-18n is encrypted, this event may additionally comprise decryption of the data.

Dropbox Exhibit 1002 - Page 203
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[00119] At event 780, client process determines whether or not the operation of data transfer is to be continued. This determination may be made according to instructions received from the user of client computer 12a-12n, or according to an HTTP response from connection server 14a-14n that includes a notification that the connection to network-enabled device 18a-18n has been broken. If the operation is to be continued, events 710-780 are repeated. If the operation will not be continued, the operation is terminated at event 780.

[00120] The connection server 14a-14n serves as bridging medium between client computer(s) 12a-12n and network-enabled device(s) 18a-18n (via device control computer(s) 36a-36n), between client computer(s) 12a-12n and client computer(s) 12a-12n, and between device control computer(s) 36a-36n and device control computer(s) 36a-36n. Data from the device(s) 18a-18n that are destined for client computer(s) 12a-12n are posted to the connection server 14a-14n using an HTTP request as previously described. Receiving the HTTP request, the connection server 14a-14n then temporarily stores or buffers any data from the request in its memory (i.e., the sending buffer). The next time an HTTP request comes from client computer 12a-12n (in this example, but as noted above, a request could also be from another device control computer 36a-36n), the connection server 14a-14n retrieves the data from the sending buffer and sends the data to client computer 12a-12n (or other device control computer 36a-36n), along with the response for the HTTP request. Like the request sending procedure described above, the response sending procedure is also efficiently adaptive for sending data substantially as quickly as it has been received, with persistent polling also being provided by the HTTP requests which occur at least within a maximum defined interval, regardless of whether any data is being sent along with the HTTP request.

[00121] Referring next to FIG. 8, the operation of connection server process 34 during data transfer is illustrated. At event 800, the data transfer process is initiated. This event may occur, for example, once at least two users (e.g., at least two client computers 12a-12n, at least two device control computers 36a-36n, or, as in this example, at least one client computer 12a-12n and one device control computer 36a-36n) have been authorized and connections to the at least two users have been opened. In this example,

Dropbox Exhibit 1002 - Page 204
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

the at least two users are referred to as a client computer 12a-12n and a device control computer 36a-36n, although it is again emphasized that the present invention is not limited to such communications.

[00122] At event 810, connection server process 34 determines whether or not any HTTP request has been received from client computer 12a-12n (or device control computer 36a-36n). If no HTTP request has been received, event 820 is carried out wherein process 34 waits for a selected period of time, and then repeats the query of event 810. If an HTTP request, has been received, event 830 occurs.

[00123] At event 830, connection server process 34 reads the HTTP request received in event 810.

[00124] At event 840, connection server process 34 determines whether or not any data to or from client computer 12a-12n is embedded within the HTTP request. If there is data embedded in the request, event 850 is carried out. If there is no data with the HTTP request, event 860 occurs.

[00125] At event 850, any data present in the HTTP request is buffered in the sending buffer (not shown) of connection server 14a-14n. This data may be encrypted, as noted above, but need not be decrypted by connection server 14a-14n.

[00126] At event 860, connection server process 34 determines if there is any data present for client computer 12a-12n from network-enabled device 18a-18n. If no data is present in the sending buffer, connection server process 34 waits for n milliseconds in event 870. Connection server process 34 maintains communication with client computer 12a-12n by periodically sending HTTP responses to client computer 12a-12n, which are responsive to the periodic HTTP requests from client computer 12a-12n described above. In event 880, connection server process 34 determines if the time period for sending a periodic HTTP response to client computer 12a-12n has expired. If the time period has expired, event 890 is carried out. If the time period has not expired, event 860 is repeated. Like the request sending procedure described above, the response

Dropbox Exhibit 1002 - Page 205
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

sending procedure is also efficiently adaptive for sending data substantially as quickly as it has been received, with persistent polling also being provided by the HTTP requests which occur at least within a maximum defined interval, regardless of whether any data is being sent along with the HTTP request. Since data in the sending buffer can be sent with the HTTP response at a time which is any multiple of "n milliseconds" upon until the maximum time interval at which an HTTP response must be sent, this acts as an "adaptive polling" of the sending buffer. That is, if data appears in the sending buffer at 30 milliseconds where "n" is 10 milliseconds, then the data will be sent in an HTTP response at the 30 milliseconds time. Alternatively, if data does not appear in the sending buffer until 70 milliseconds, the HTTP response is not sent until the 70 millisecond mark, when the data is sent along with the response.

[00127] It should be further noted here, that HTTP requests are processed in parallel, and that the client process 32 sending the HTTP requests always has a predefined number of HTTP requests (which perform the polling process) at any time (generally, the predefined number is two or more). When an HTTP response is sent in response to an HTTP request (with or without data), this completes that poll and the client process 32 sends out a new HTTP request to replace the previous one. Since the rate of sending HTTP requests and responses are variable depending upon the rate of data that is being communicated in each direction, respectively, the process adapts the rate of polling, in each direction, according to the rate of data which is being communicated. The polling process is persistent, even when no data is being transmitted, because HTTP requests and response are issued when a maximum time interval has elapsed even when no data is being transmitted with the request or response.

[00128] In event 890, an HTTP response is sent to client computer 12a-12n by connection server 14a-14n. If any data was present in the connection server sending buffer for client computer 12a-12n, this data is embedded within the HTTP response.

[00129] Following event 890, events 810-880 are repeated. If a connection to client computer 12a-12n has been terminated, the events of FIG. 8 may be terminated. Once again, it must be understood that the events of FIG. 8 as described above are also carried

Dropbox Exhibit 1002 - Page 206
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

out in association with device control computer 36a-36n, as well as client computer 12a-12n, to provide data communication therebetween.

[00130] The events of FIG. 7 and FIG. 8 are performed iteratively to provide persistence and full-duplex data communication streams between client computers 12a-12n and device control computers 36a-36n and the network-enabled devices 18a-18n associated therewith. Such persistence and continuous communication streams also overcomes any limitations associated with the stateless feature of HTTP protocol.

[00131] The data communication method of the invention allows creation of a continuous data stream from private-to-public-to-private networks using standard HTTP protocol. The invention thus provides a communication "tunnel" across private and public networks to facilitate the flow of data from client computers 12a-12n to network-enabled devices 18a-18n. For many applications, the security and privacy of such data communication are extremely important, to ensure only authorized users can gain access to the device. Security and privacy are established by the security and authentication procedures for establishing a connection with the connection server(s), and these procedures apply to both client computers 12a-12n and device control computers 36a-26n, as described above. Once secured connections have been established, communications can be rapidly delivered without the need for further generation and transmission of a new security key for each communication transmission, which greatly enhances the speed and reduces the costs of performing such communications, compared to prior art techniques. As also noted, communicated data may optionally be encrypted with shared secret keys as described above and shown in FIG. 5.

[00132] In certain embodiments, each HTTP request with embedded, encrypted data may include a message digest value for that data. The client computer 12a-12n or device control computer 36a-36n receiving the embedded encrypted data, can compare the received message digest value to a computed message digest value as described above, to determine authenticity of each data communication. Where a non-match in message digest values occurs, a security error exists, and appropriate HTTP response messages may be sent.

Dropbox Exhibit 1002 - Page 207
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[00133] As can be seen from the above, the invention provides for secure transportation of data to and from users and network-enabled devices that are located behind firewall or proxy systems in different private networks via a connection server. Since a connection server is used to connect the remote users and devices, the network addresses of the users and devices may be kept secret from each other, and attacks from the public network would can still be deflected by the existing firewall or proxy systems that are in place to protect the users and devices. In embodiments where the connection server or servers are located within a public network, attacks directed toward the connection servers would not compromise security of the users and devices behind the firewall or proxy systems.

[00134] The invention also allows multi-point routing of data which enables collaborative communications among users; collaborative control of one or more devices, collaborative monitoring of one or more devices, and other forms of collaborative communication, including learning or teaching sessions. The use of authentication data as described above may include device type information. Typical device and instrumentation commands for control and monitoring can be classified based on its device types. In many instances, users may wish to send commands to devices of the same type. By having devices connected to a connection server, users can instruct the connection server via HTTP request to retransmit command data to all devices of particular type. Thus, the use of a connection server in accordance with the invention can provide a multi-point data routing platform.

[00135] Since users only connect directly to a connection server, users only need to know the network address of the connection server (i.e., only a single network address is needed). Therefore, no matter from where devices are connected to users across the network, the users are able to discover and access the devices, as long as the devices can successfully connect to the connection server. This device location ability can significantly help users to manage connections with distributed devices across the network.

Dropbox Exhibit 1002 - Page 208
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

[00136] While the present invention has been described with reference to the specific embodiments thereof, it should be understood by those skilled in the art that various changes may be made and equivalents may be substituted without departing from the true spirit and scope of the invention. In addition, many modifications may be made to adapt a particular situation, material, composition of matter, process, process step or steps, to the objective, spirit and scope of the present invention. All such modifications are intended to be within the scope of the claims appended hereto.

Dropbox Exhibit 1002 - Page 209
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

CLAIMS

That which is claimed is:

1. A system for remote communications between private users through a public network while providing seamless, firewall-compliant connectivity, said system comprising:

a first computer connectable to the public network over a first secure channel through a first firewall element, said first firewall element adapted to protect said first computer from hostile intrusion from the public network;

a second computer connectable to the public network over a second secure channel through a second firewall element, said second firewall element adapted to protect said second computer from hostile intrusion from the public network; and

a connection server operatively coupled to the public network , said connection server including means for forming a first, secure, firewall compliant connection with said first computer, and means for forming a second, secure, firewall compliant connection with said second computer, means for sending communications received from said first computer to said second computer while maintaining second firewall compliance, and means for sending communications received from said second computer to said first computer while maintaining first firewall compliance.

2. The system of claim 1, wherein said first and second firewall elements use different criteria for restriction of communications traffic therethrough.

3. The system of claim 1, wherein said first computer comprises a client computer and said second computer comprises a device control computer, said system further comprising at least one network-enabled device privately networked to said device control computer behind said second firewall element.

4. The system of claim 1, wherein said first computer comprises a first client computer and said second computer comprises a second client computer.

5. The system of claim 1, wherein said first computer comprises a first device control computer and said second computer comprises a second device control computer, said system

Dropbox Exhibit 1002 - Page 210
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

further comprising at least one first network-enabled device privately networked to said first device control computer behind said first firewall element, and at least one second network-enabled device privately networked to said second device control computer behind said second firewall element.

6. The system of claim 1, wherein said first computer is connected to a first private network behind said first firewall element, and said second computer is connected to a second private network behind said second firewall element.

7. The system of claim 1, wherein said connection server is located within a private network that is operatively coupled to the public network via a third firewall element.

8. The system of claim 2, further comprising at least a second client computer, wherein at least two said client computers may simultaneously establish connection to said at least one network-enabled device through said connection server and said device control computer for simultaneous, collaborative use of said at least one network-enabled device.

9. The system of claim 1, further comprising at least a third computer connectable to the public network through a third firewall element, said third firewall element adapted to protect said third computer from hostile intrusion from the public network, wherein at least three of said computers may simultaneously establish secure connections with each other through said connection server for simultaneous, collaborative communications therebetween, wherein communications sent and received by said first computer are first firewall compliant, communications sent and received by said second computer are second firewall compliant, and communications sent and received by said third computer are third firewall compliant.

10. The system of claim 9, wherein at least two of said first, second and third firewall elements use different criteria for restriction of communications traffic therethrough.

11. The system of claim 1, wherein said connection server comprises means for authorizing a secure connection with said first computer, wherein said means for authorizing a secure connection with said first computer is adapted to receive authentication data from said

Dropbox Exhibit 1002 - Page 211
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

first computer and to determine whether said authentication data verifies a user of said first computer, and wherein said second, secure, firewall compliant connection with said second computer is made according to instructions received from said first computer, only after said first firewall compliant connection with said first computer is made and said first computer user has been verified.

12. The system of claim 11, wherein said authentication data is encrypted, and said connection server further comprises means for decrypting said authentication data.

13. The system of claim 11, wherein said connection server further comprises means for determining whether or not said authentication data has been altered during transmission from said first computer to said connection server.

14. The system of claim 11, wherein said connection server further comprises means for preparing and verifying encryption keys for the user of the first computer when said first computer user has been verified.

15. The system of claim 1, wherein said connection server comprises means for authorizing a connection with said second computer, wherein said means for authorizing a connection with said second computer is adapted to receive authentication data from said second computer and to determine whether said authentication data verifies a user of said second computer, and wherein said first firewall compliant connection with said first computer is made according to instructions received from said second computer, only after said second firewall compliant connection with said second computer is made and said second computer user has been verified.

16. The system of claim 15, wherein said authentication data is encrypted, and said connection server further comprises means for decrypting said authentication data.

17. The system of claim 15, wherein said connection server further comprises means for determining whether or not said authentication data has been altered during transmission from said second computer to said connection server.

Dropbox Exhibit 1002 - Page 212
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

18. The system of claim 15, wherein said connection server further comprises means for preparing and verifying encryption keys for the user of the second computer when said second computer user has been verified.

19. The system of claim 1, wherein said connection server establishes a full duplex connection between said first and second computers.

20. The system of claim 8, wherein said connection server establishes full duplex connections between at least said client computers and said device control computer.

21. The system of claim 9, wherein said connection server establishes full duplex connection among said at least three computers.

22. The system of claim 1, further comprising a distributed control infrastructure coupled to the private network, wherein said connection server operates as a primary connection server, said distributed control infrastructure further comprising at least one secondary connection server operatively coupled to said primary connection server.

23. The system of claim 22, wherein said primary connection server comprises a load balancing algorithm adapted to assign communications, initiated by said first or second computer, to one of said at least one secondary connection servers.

24. The system of claim 22, wherein said distributed control infrastructure is scalable such that connection servers may be added or taken away from said distributed control infrastructure based upon a number of computers to be connected and characteristics of communications to be directed between said computers.

25. The system of claim 22, wherein said distributed control infrastructure further comprises at least one database operatively coupled to each of said connection servers.

Dropbox Exhibit 1002 - Page 213
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

26. The system of claim 25, wherein said distributed control infrastructure comprises a plurality of said databases, wherein said connection servers are adapted to store data related to users of said computers in said databases and to store data relating to the operation of remote devices which are operably coupled to at least one of said computers.

27. The system of claim 26, wherein said stored data may be accessed by users through said computers.

28. A system for remote communications between private users through a public network while providing seamless, firewall-compliant connectivity, said system comprising:

a client computer securely connectable to the public network through a first firewall element, said first firewall element adapted to protect said client computer from hostile intrusion from the public network;

a device control computer securely connectable to the public network through a second firewall element, and at least one network-enabled device privately networked to said device control computer, said second firewall element adapted to protect said device control computer and said at least one network-enabled device from hostile intrusion from the public network; and

at least one connection server operatively coupled to the public network, said at least one connection server including means for forming a secure, first firewall compliant connection with said client computer, and means for forming a secure, second firewall compliant connection with said device control computer and said at least one network-enabled device, means for sending communications from said client computer to said at least one network-enabled device via said device control computer while maintaining second firewall compliance, and means for sending communications from said at least one network-enabled device, received from said device control computer, to said client computer while maintaining first firewall compliance.

29. The system of claim 28, wherein said first and second firewall elements use different criteria for restriction of communications traffic therethrough.

30. The system of claim 28, wherein said communications from said client computer comprise user instructions for said at least one network-enabled device.

Dropbox Exhibit 1002 - Page 214
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

31. The system of claim 28, wherein said communications from said at least one network-enabled device comprise data characterizing an operating state of said at least one network-enabled device.

32.The system of claim 28, wherein a full duplex connection is established between said client computer and each said at least one network-enabled device.

33. The system of claim 28, wherein said client computer is connected to a first private network behind said first firewall element, and said device control computer is connected to a second private network behind said second firewall element.

34. The system of claim 33, further comprising at least one additional client computer connected to said first private network, wherein said at least one connection server is capable of establishing full duplex communications between a plurality of said client computers and said at least one network-enabled device via said device control computer.

35. The system of claim 33, further comprising at least one additional client computer connected to a third private network behind a third firewall element, wherein said at least one connection server further comprises means for forming a secure, third firewall compliant connection with said at least one additional client computer, means for sending communications from said client computer to said at least one network-enabled device via said device control computer while maintaining second firewall compliance and to said at least one additional client computer while maintaining third firewall compliance, means for sending communications from said at least one network-enabled device, received from said device control computer, to said client computer while maintaining first firewall compliance and to said at least one additional client computer while maintaining third firewall compliance, and means for sending communications from said at least one additional client computer to said at least one network-enabled device, via said device control computer, while maintaining second firewall compliance and to said client computer while maintaining first firewall compliance.

Dropbox Exhibit 1002 - Page 215
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

36. The system of claim 35, wherein at least two of said first, second and third firewall elements use different criteria for restriction of communications traffic therethrough.

37. The system of claim 33, further comprising at least one additional device control computer connected to said second private network, and at least one additional network-enabled device connected to said at least one additional device control computer wherein said at least one connection server is capable of establishing full duplex communications between said client computer, said device control computer and said at least one additional device control computer, enabling simultaneous point-to-multipoint instructions to be provided by said client computer to said network-enabled devices.

38. The system of claim 33, further comprising at least one additional device control computer connected to a third private network and at least one additional network-enabled device connected to said at least one additional device control computer behind a third firewall element, wherein said at least one connection server further comprises means for forming a secure, third firewall compliant connection with said at least one additional device control computer, means for sending communications from said client computer to said at least one network-enabled device via said device control computer while maintaining second firewall compliance and to said at least one additional device control computer while maintaining third firewall compliance, means for sending communications from said at least one network-enabled device, received from said device control computer, to said client computer while maintaining first firewall compliance and to said at least one additional device control computer while maintaining third firewall compliance, and means for sending communications from said at least one additional device control computer to said at least one network-enabled device, via said device control computer, while maintaining second firewall compliance and to said client computer while maintaining first firewall compliance.

39. The system of claim 38, wherein at least two of said first, second and third firewall elements use different criteria for restriction of communications traffic therethrough.

40. The system of claim 38, wherein said at least one connection server is capable of establishing full duplex communications between said client computer, said device control

Dropbox Exhibit 1002 - Page 216
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

computer and said at least one additional device control computer, enabling simultaneous point-to-multipoint instructions to be provided by said client computer to said network-enabled devices.

41. The system of claim 40, further comprising at least one additional client computer in a fourth private network protected by a fourth firewall, wherein said at least one connection server is capable of establishing full duplex communications between said client computers and said device control computers, while maintaining all firewall compliances, enabling real-time collaborative control of said network-enabled devices by users of said client computers.

42. The system of claim 28, wherein said at least one connection server is located within a private network that is operatively coupled to the public network via a third firewall element.

43. The system of claim 28, wherein said at least one connection server comprises a plurality of said connection servers networked within a distributed control infrastructure, wherein a first of said connection servers operates as a primary connection server, and the remainder of said plurality of connection servers operate secondarily to said primary connection server.

44. The system of claim 43, wherein said primary connection server comprises a load balancing algorithm adapted to assign communications, initiated by said client control computer or said device control computer, to a secondary connection server.

45. The system of claim 43, wherein said distributed control infrastructure is scalable such that connection servers may be added or taken away from said distributed control infrastructure based upon a number of computers to be connected and characteristics of communications to be directed between said computers.

46. The system of claim 43, wherein said distributed control infrastructure further comprises at least one database operatively coupled to each of said connection servers.

Dropbox Exhibit 1002 - Page 217
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

47. The system of claim 46, wherein said distributed control infrastructure comprises a plurality of said databases, wherein said connection servers are adapted to store data related to users of said computers in said databases and to store data relating to the operation of said network-enabled devices which are operably coupled to said device control computer.

48. The system of claim 47, wherein said stored data may be accessed by users through said computers.

49. The system of claim 28, wherein said at least one connection server comprises a plurality of said connection servers networked within a distributed control infrastructure, said distributed control infrastructure further including a security server operatively coupled to said plurality of connection servers, and wherein a plurality of said client computers are operably connectable to said security server and said device control computer is operably connectable to said security server.

50. The system of claim 49, further comprising a plurality of said device control computers, each having at least one network-enabled device connected thereto, each said device control computer being operably connectable to said security server.

51. The system of claim 28, wherein said at least one connection server comprises a plurality of said connection servers networked within a distributed control infrastructure, said distributed control infrastructure further including a security server operatively coupled to said plurality of connection servers, and wherein a plurality of said device control computers, each having at least one network-enabled device connected thereto, are operably connectable to said security server and said client computer is operably connectable to said security server.

52. The system of claim 50, wherein said security server comprises means for authorizing a connection with any of one said client and device control computers upon receiving contact from said client computer or device control computer, wherein said means for authorizing a connection with said client computer or device control computer is adapted to receive authentication data from said client computer or device control computer and to

Dropbox Exhibit 1002 - Page 218
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

determine whether said authentication data verifies a user of said client computer or device control computer.

53. The system of claim 52, wherein said contact from said client computer or device control computer comprises an HTTP request.

54. The system of claim 53, wherein said HTTP request contains embedded user authentication data.

55. The system of claim 54, wherein said embedded user authentication data is encrypted, and said security server further comprises means for decrypting said encrypted authentication data.

56. The system of claim 52, wherein said security server further comprises means for determining whether or not said authentication data has been altered during transmission from said client computer or device control computer to said connection server.

57. The system of claim 52, wherein said security server further comprises means for preparing and verifying encryption keys for the user of the computer from which the authentication data was received, when said computer user has been verified.

58. The system of claim 52, wherein said security server further comprises means for assigning a said client computer or device control computer to one of said connection servers when said computer user has been verified.

59. The system of claim 52, wherein said security server comprises a load balancing algorithm adapted to assign communications, initiated by said client control computer or said device control computer, to one of said connection servers when said client control computer or said device control computer has been verified.

Dropbox Exhibit 1002 - Page 219
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

60. The system of claim 59, wherein said load balancing algorithm assigns the communications based on at least one of user type, session type, availability of said connection servers and relative current workload of said connection servers.

61. The system of claim 59, wherein said load balancing algorithm assigns the communications based on user type, session type, availability of said connection servers and relative current workload of said connection servers.

62. The system of claim 59, wherein said security server further comprises means for establishing a connection with at least another of said client computers and device control computers, after said assignment of communications to one of said connection servers.

63. The system of claim 62, wherein said security server establishes connections with at least one other of said client computers and device control computers as requested by the verified computer.

64. The system of claim 62, wherein said distributed control infrastructure establishes full duplex connections between said verified computer and said at least one other of said client computer and device control computers.

65. The system of claim 49, wherein said distributed control infrastructure further comprises a plurality of databases operatively coupled to each of said connection servers.

66. The system of claim 62, wherein said distributed control infrastructure further comprises at least one database operatively coupled to the assigned connection server, and wherein communications between said verified computer and said at least one other of said client computers and device control computers are stored in said at least one database, to provide access to other authorized users or the verified computer user at a later time.

67. A distributed control structure providing for secure transmission of communications over a public network between two or more computers protected by two or more firewall

Dropbox Exhibit 1002 - Page 220
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

elements using different criteria for restriction of communications traffic therethrough, said distributed control structure comprising:

at least one connection server operatively coupled to the public network, said at least one connection server including means for forming a first firewall compliant connection with a first of the computers, means for forming a second firewall compliant connection with a second of the computers, means for sending communications from the first computer to the second computer while maintaining second firewall compliance, and means for sending communications from the second computer to the first computer while maintaining first firewall compliance.

68. The distributed control structure of claim 67, wherein a full duplex connection is established between the first and second computers.

69. The distributed control structure of claim 67, wherein said at least one connection server is located within a private network that is operatively coupled to the public network via a connection server firewall element.

70. The distributed control structure of claim 67, wherein said at least one connection server is configured to operatively connect with a plurality of client computers as well as a plurality of device control computers, each having at least one network-enabled device connected thereto.

71. The distributed control structure of claim 67, wherein said at least one connection server comprises a plurality of said connection servers networked within said distributed control structure, wherein a first of said connection servers operates as a primary connection server, and the remainder of said plurality of connection servers operate secondarily to said primary connection server.

72. The distributed control structure of claim 71, wherein said distributed control structure is configured to operatively connect with a plurality of client computers as well as a plurality of device control computers, each having at least one network-enabled device connected thereto.

Dropbox Exhibit 1002 - Page 221
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

73. The distributed control structure of claim 71, wherein said primary connection server comprises a load balancing algorithm adapted to assign communications, initiated by one of the computers, to a secondary connection server.

74. The distributed control structure of claim 71, further comprising at least one database operatively coupled to each of said connection servers.

75. The distributed control structure of claim 71, further comprising a plurality of databases operatively coupled to each of said connection servers, wherein said connection servers are adapted to store data related to users of the computers and to the computers in said databases and to network-enabled devices connected to the computers.

76. The distributed control structure of claim 67, wherein said at least one connection server comprises a plurality of said connection servers networked within said distributed control structure, and a security server operatively coupled to said plurality of connection servers, and wherein said distributed control structure is configured to operatively connect with a plurality of client computers as well as a plurality of device control computers, each having at least one network-enabled device connected thereto.

77. The distributed control structure of claim 76, wherein said security server comprises means for authorizing a connection with any of one the client and device control computers upon receiving contact from the client computer or device control computer, wherein said means for authorizing a connection with the client computer or device control computer is adapted to receive authentication data from the client computer or device control computer and to determine whether the authentication data verifies a user of the client computer or device control computer.

78. The distributed control structure of claim 77, wherein said security server is adapted to receive contact from the client computer or device control computer in the form of an HTTP request.

Dropbox Exhibit 1002 - Page 222
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

79. The distributed control structure of claim 78, wherein said security server is adapted to separate authentication data embedded in an HTTP request received from the client computer or device control computer.

80. The distributed control structure of claim 77, wherein said security server further comprises means for decrypting encrypted authentication data.

81. The distributed control structure of claim 77, wherein said security server further comprises means for determining whether or not authentication data received has been altered during transmission from the client computer or device control computer to said security server.

82. The distributed control structure of claim 77, wherein said security server further comprises means for preparing and verifying encryption keys for the user of the computer from which the authentication data was received, when the computer user has been verified.

83. The distributed control structure of claim 77, wherein said security server further comprises means for assigning the client computer or device control computer to one of said connection servers when the computer user has been verified.

84. The distributed control structure of claim 77, wherein said security server comprises a load balancing algorithm adapted to assign communications, initiated by the client control computer or the device control computer, to one of said connection servers when the client control computer or the device control computer has been verified.

85. The distributed control structure of claim 84, wherein said load balancing algorithm assigns the communications based on at least one of user type, session type, availability of said connection servers and relative current workload of said connection servers.

86. The distributed control structure of claim 84, wherein said load balancing algorithm assigns the communications based on user type, session type, availability of said connection servers and relative current workload of said connection servers.

Dropbox Exhibit 1002 - Page 223
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

87. The distributed control structure of claim 84, wherein said security server further comprises means for establishing a connection with at least another of the client computers and device control computers, after said assignment of communications to one of said connection servers.

88. The distributed control structure of claim 87, wherein said security server establishes connections with at least one other of the client computers and device control computers as requested by the verified computer.

89. The distributed control structure of claim 88, wherein full duplex connections are established between the verified computer and the at least one other of the client computers and device control computers.

90. The distributed control structure of claim 76, further comprising a plurality of databases operatively coupled to each of said connection servers.

91. A method of establishing a private-to-public-to-private communications tunnel, wherein at least the private addresses of the communications tunnel are firewall protected, said method comprising:

authenticating a first computer having a first, firewall protected private address;

creating a first firewall compliant connection between a publicly addressed connection server and said first computer upon authentication of said first computer;

establishing a second firewall compliant connection between said publicly addressed connection server and a second computer having a second firewall protected private address; and

establishing the private-to-public-to-private communications tunnel, wherein said connection server routes communications from said first computer through said first firewall compliant connection and said second firewall compliant connection to said second computer, and from said second computer through said second firewall compliant connection and said first firewall compliant connection to said first computer.

Dropbox Exhibit 1002 - Page 224
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

92. The method of claim 91, wherein said first computer is a client computer and said second computer is a device control computer, said device control computer being operably connected to at least one network-enabled device, wherein said communications from said first computer to said second computer include control instructions for operating said at least one network-enable device, and wherein said communications from said second computer to said first computer include data received by said second computer from said at least one network-enabled device.

93. The method of claim 91, wherein said communications comprises HTTP requests and responses, said HTTP requests and responses being compliant with said first or second firewall associated with said first or second computer to which the communications are directed.

94. The method of claim 91, wherein said authenticating comprises receiving a request from said first computer, said request including user authentication data; and verifying whether or not the authentication data matches authentication data of said first computer as stored in association with said connection server.

95. The method of claim 94, wherein said user authentication data is embedded in said request, and wherein said authenticating further comprises determining whether or not the authentication data has been altered during transmission from said first computer to said connection server.

96. The method of claim 94, wherein said authentication data is encrypted, and wherein said authenticating further comprises decrypting said encrypted authentication data prior to said verifying.

97. The method of claim 96, further comprising preparing and verifying encryption keys for a user of the first computer after said authenticating step.

98. The method of claim 91, wherein said connection server comprises a plurality of connection servers networked as a publicly addressable distributed control infrastructure, said method further comprising assigning on of said plurality of connection servers to create said

Dropbox Exhibit 1002 - Page 225
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

first and second firewall compliant connections, wherein said assigning is based on at least one of: a type of user using said first computer, a type of session requested to be established by the first computer; configuration of connection servers for a particular type or types of sessions; availability of connection servers; statuses of connection servers; and relative work loads of connection servers at time that session is to occur.

99. The method of claim 91, further comprising storing at least a portion of said communications in at least one database associated with said connection server, wherein the stored communications may be accessed by the first computer, second computer or other computers that are authorized access to said connection computer and the stored data.

100. The method of claim 99, wherein said access is allowed contemporaneously during the communications and in subsequent sessions.

101. A method for establishing a secure connection for rapid transfer of data between privately addressed, firewall protected locations over a public network, said method comprising:

preparing authentication data on a first computer having a first, firewall protected private address;

encrypting the authentication data using a public security key;

sending a request over the public network to a publicly addressed server, wherein the request includes the encrypted authentication data;

decrypting the encrypted authentication data at the location of the publicly addressed server using a private security key;

verifying the decrypted authentication data to determine whether the authentication data represents an authorized user;

authorizing the first computer to proceed if the authentication data represents an authorized user;

generating a secret security key on the first computer for encryption of data to be sent over the secure connection;

encrypting the secret key using the public security key and sending the encrypted secret security key to the publicly addressed server;

Dropbox Exhibit 1002 - Page 226
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

decrypting the encrypted secret security key at the location of the publicly addressed server using the private security key; and

establishing a second firewall compliant connection between said publicly addressed server and a second computer having a second firewall protected private address; and

establishing a private-to-public-to-private communications tunnel connecting said first computer, said publicly addressed server and said second computer.

102. The method of claim 101, further comprising transmitting data from said first computer to said second computer via said publicly addressed server.

103. The method of claim 102, further comprising transmitting data from said second computer to said first computer via said publicly addressed server.

104. The method of claim 103, wherein said private-to-public-to-private communications tunnel comprises full duplex connections between said first computer and said publicly addressed server and between said publicly addressed server and said second computer.

105. The method of claim 103, wherein the data transmitted subsequent to establishing the private-to-public-to-private communications tunnel is encrypted using the secret key.

106. The method of claim 103, wherein the data transmitted from the first computer is encrypted using the secret key, and the data transmitted from the second computer encrypted using a second secret key generated by the second computer.

107. The method of claim 103, wherein the data transmitted subsequent to establishing the private-to-public-to-private communications tunnel is unencrypted.

108. The method of claim 102, wherein the data transmitted subsequent to establishing the private-to-public-to-private communications tunnel is encrypted using the secret key.

109. The method of claim 102, wherein the data transmitted subsequent to establishing the private-to-public-to-private communications tunnel is unencrypted.

Dropbox Exhibit 1002 - Page 227
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

110. The method of claim 101, wherein the encrypted authentication data is embedded in the request.

111. The method of claim 110, wherein the request is an HTTP request.

112. The method of claim 101, further comprising:

calculating a message digest value on the first computer for the authentication data;

encrypting the calculated message digest value together with said encrypting the authentication data; and

embedding the encrypted authentication data and message digest value in the request;

wherein said decrypting the encrypted authentication data further comprises decrypting the message digest value;

said method further comprising computing a message digest value for the decrypted authentication data, and comparing the computed message digest value with the decrypted message digest value to determine whether the authentication data has been altered or corrupted; and

allowing said verifying to proceed only if the computed message digest value and the decrypted digest value are the same.

113. The method of claim 101, further comprising:

generating a message digest value for the secret security key;

encrypting said message digest value with said encrypting the secret key, and sending the encrypted message digest value with the encrypted secret key to the publicly addressed server;

wherein said decrypting the encrypted security key further comprises decrypting the message digest value;

said method further comprising computing a message digest value for the decrypted secret key, and comparing the computed message digest value with the decrypted message digest value to determine whether the secret key has been altered or corrupted; and

allowing said establishing a second firewall compliant connection to proceed only if the computed message digest value and the decrypted digest value are the same.

Dropbox Exhibit 1002 - Page 228
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

114. A method of load balancing communications among a plurality of connection servers networked in a publicly addressable distributed control infrastructure which multiple computers within multiple private networks may access for establishing communications over a public network, said method comprising:

determining a user type of each computer to be connected by communications through said publicly addressable distributed control infrastructure in a particular session;

determining a session type of the particular session to be established;

comparing user type and session type determinations with server type information stored in at least one database connected to said distributed control infrastructure;

selecting a connection server characterized by server type information that indicates the connection server is capable of handling the determined user types and session type;

determining if the selected server is active;

determining whether or not the selected server, if active, has adequate Power to handle the connections that will be required to establish the communications for the session; and

if the selected server is active and has adequate Power, determining whether the selected server has the best available Power level for carrying out the session, based upon a calculated average Power expected for the session and Utilization Ratios of each capable, active connection server which has adequate Power.

115. The method of claim 114, further comprising assigning the selected server determined to active and to have the best available Power level to establish connections between the computers to be included in the session.

116. A method of persistent, secure transfer of data between at least two computers over a public network, wherein the computers have separate privately addressed, firewall protected locations, said method comprising:

accessing a connection server operably connected to the public network by addressing a request from a first of the computers to a public address of the connection server;

establishing a secure connection between the first computer and the connection server, after which, the connection server establishes a secure connection between the connection server

Dropbox Exhibit 1002 - Page 229
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

and at least a second of the computers, according to instructions received from the first computer as to which computers the first computer desires to communicate with;

wherein secure, full-duplex, persistent communications are established through the connection server without the need for any of the computers to know or address a private address of any of the other computers between which the communications take place.

117. The method of claim 116, wherein the first computer includes a first data control process, the second computer includes a second data control process and the connection server includes a third data control process; and

wherein, after establishment of a secure communication channel between the first and second computers via the connection server, the first data control process adaptively polls a first sending buffer to determine whether any data to be communicated is contained in the first sending buffer, and sends the data, along with a request to the connections server when data is contained in the first sending buffer.

118. The method of claim 117, wherein the third data control process adaptively polls the first computer to determine whether a request has been sent; and

upon receiving a request, the third data process reads the request and buffers any data that is included with the request, in a connection server sending buffer associated with the third data process;

the third data control process additionally adaptively polls the connection server sending buffer to determine whether any data to be sent to the first computer is contained in the connection server sending buffer; and

when data to be sent to the first computer is present, the third data control process sends the data along with a response to the request.

119. The method of claim 118, wherein the first data control process reads the response, buffers any data that is contained with the response, and notifies the first computer that data has been received.

120. The method of claim 119, wherein the process steps are iteratively repeated to maintain persistent communications.

Dropbox Exhibit 1002 - Page 230
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

121. The method of claim 117, wherein the third data control process adaptively polls the connection server sending buffer to determine whether any data to be sent to the second computer is contained in the connection server sending buffer; and

when data to be sent to the second computer is present, the third data control process sends the data along with a response to the second computer.

122. The method of claim 117, wherein the third data control process adaptively polls the second computer to determine whether a request has been sent; and

upon receiving a request, the third data process reads the request and buffers any data that is included with the request, in the connection server sending buffer;

the third data control process additionally adaptively polls the connection server sending buffer to determine whether any data to be sent to the second computer is contained in the connection server sending buffer; and

when data to be sent to the second computer is present, the third data control process sends the data along with a response to the request.

123. The method of claim 122, wherein the second data control process reads the response, buffers any data that is contained with the response, and notifies the second computer that data has been received.

124. The method of claim 122, wherein the process steps are iteratively repeated to maintain persistent communications.

125. A process for remotely controlling one or more network-enabled devices by one or more client computers over a public network, wherein the one or more network-enabled devices are operatively connected within one or more different private networks and the one or more client computers are operatively connected within one or more other different private networks, at least one of the private networks being protected by a firewall element, said process comprising:

accessing at least one connection server by at least one of the client computers, said at least one connection server being operably connected to the public network;

Dropbox Exhibit 1002 - Page 231
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

establishing a secure connection between each of the at least one client computers and the at least one connection server, after which, the at least one connection server establishes a secure connection between the at least one connection server and each of the network-enabled devices requested to be connected with the at least one client computer, through at least one device control computer connected with said network-enabled devices, wherein secure, full-duplex, persistent communications are established through the connection server without the need for any of the computers to know or address a private address of any of the other computers between which the communications take place;

sending control instructions from said at least one client computer to at least one of the connected network-enabled devices, via the at least one connection server; and

receiving data at said at least one client computer received from said at least one connected network-enabled device via said at least one connection server.

126. The process of claim 125, wherein a plurality of the client computers send control instructions to collaboratively control at least one of said network-enabled devices.

127. The process of claim 125, wherein one or more of said client computers send control instructions for point to multipoint delivery of said instructions to a plurality of said network-enabled devices.

Dropbox Exhibit 1002 - Page 232
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

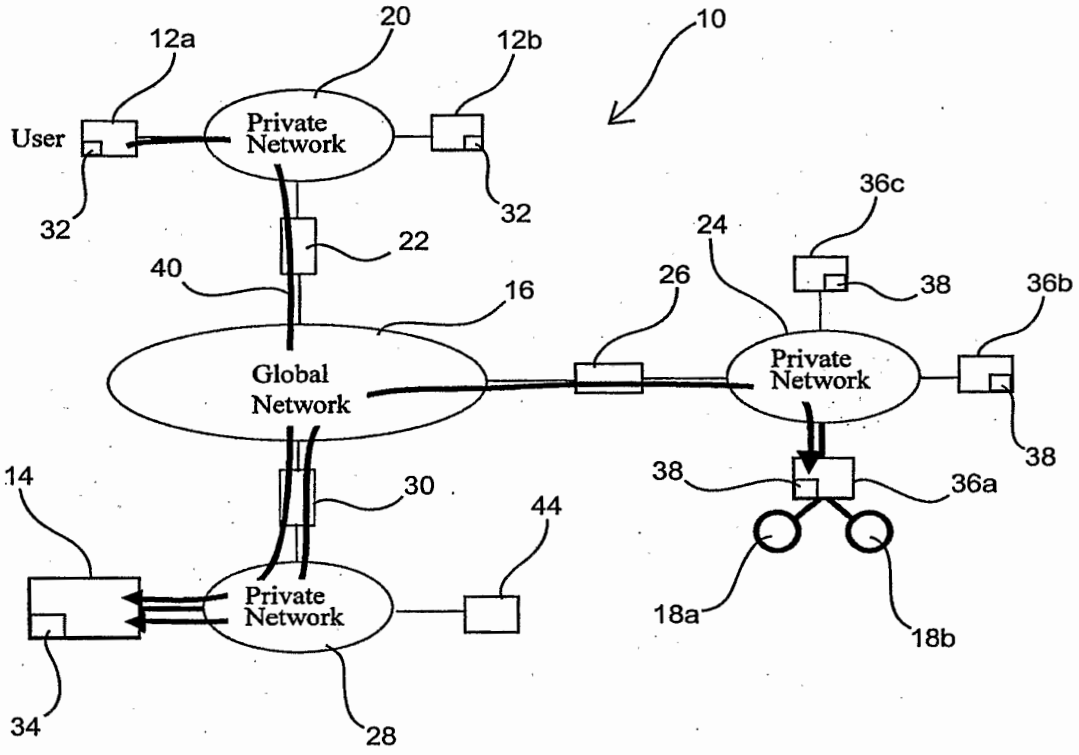


FIG. 1

Dropbox Exhibit 1002 - Page 233
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

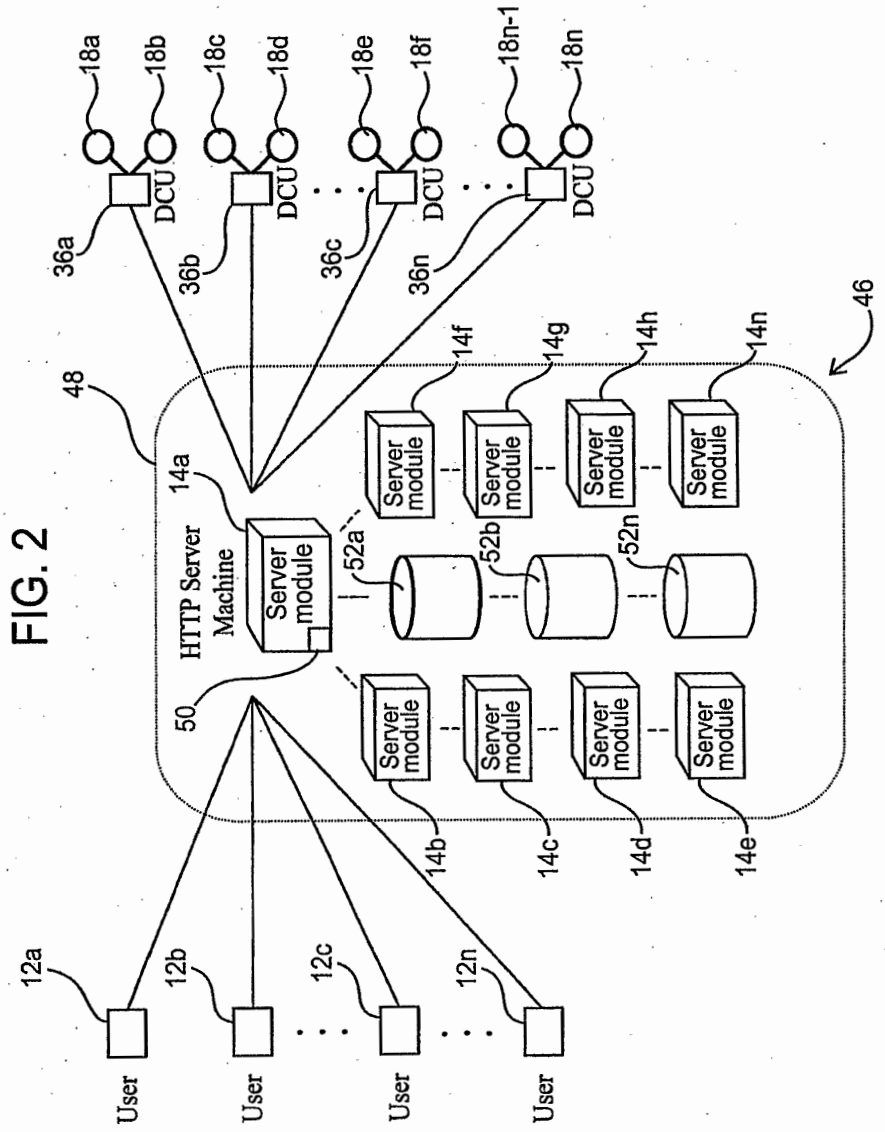


FIG. 2

Dropbox Exhibit 1002 - Page 234
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Dropbox Exhibit 1002 - Page 235
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

FIG. 3

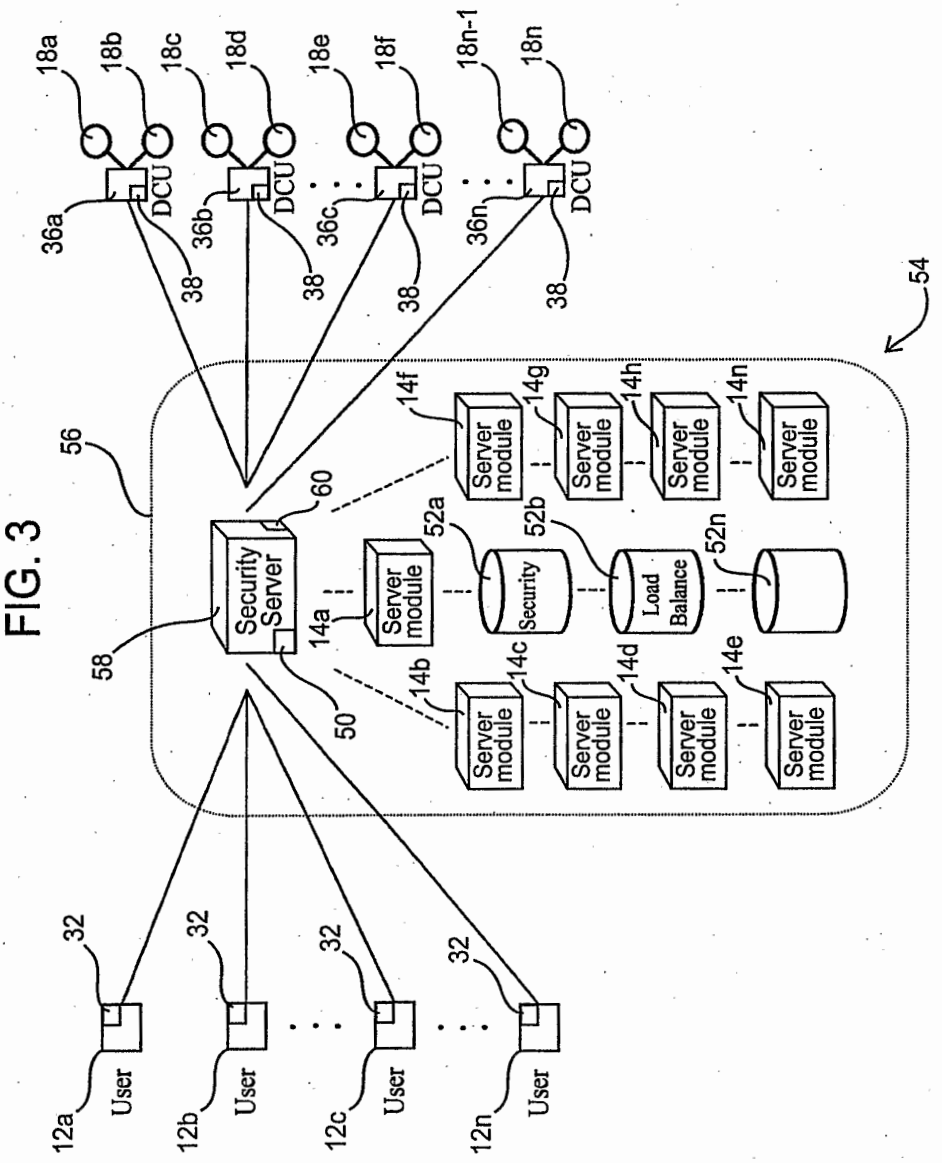
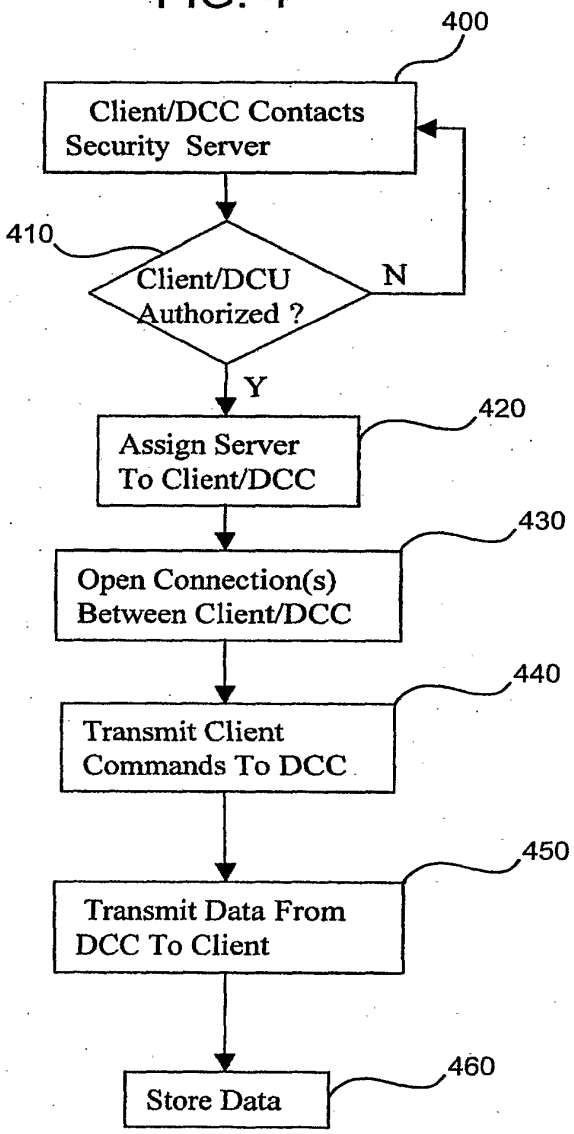


FIG. 4



Dropbox Exhibit 1002 - Page 236
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

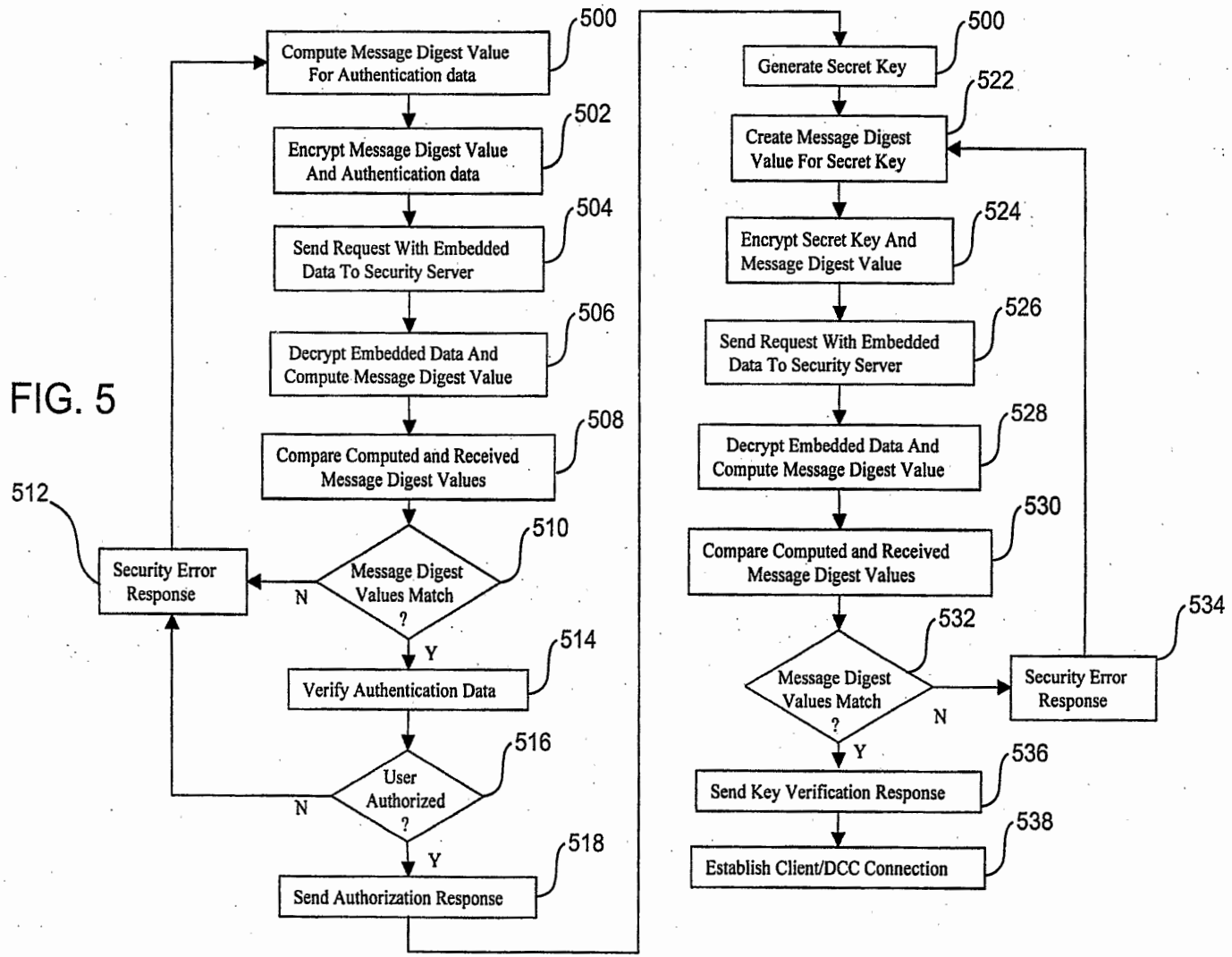
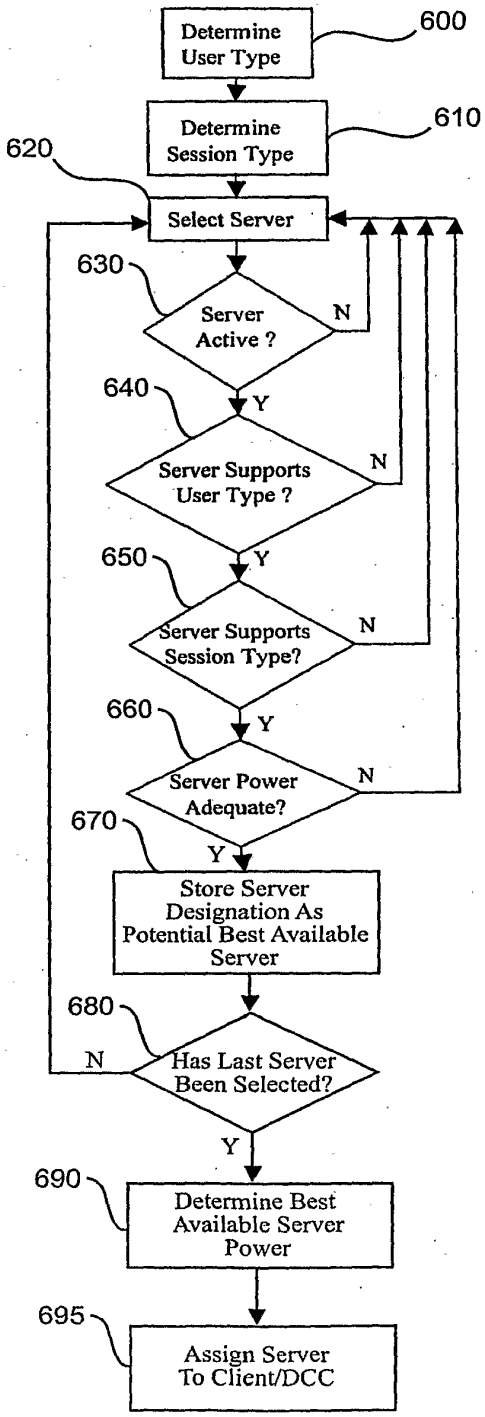


FIG. 5

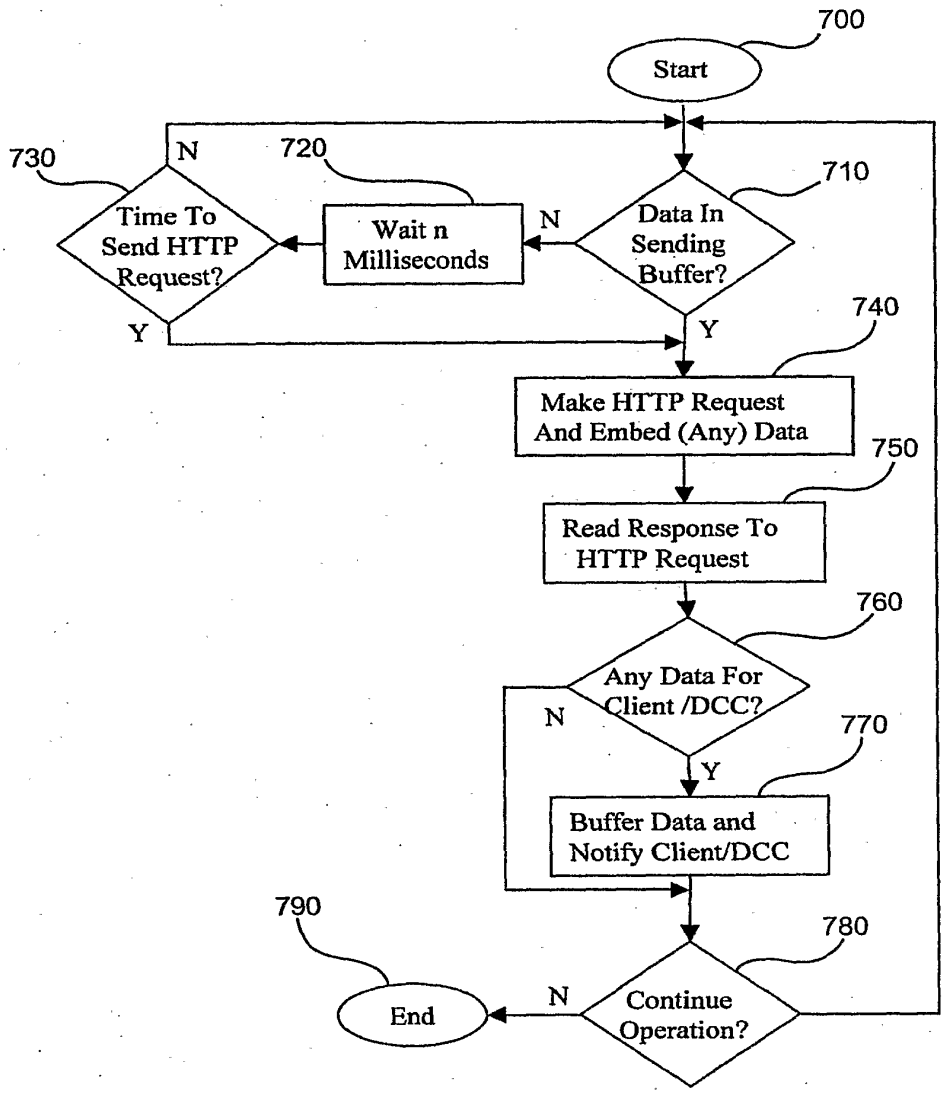
Dropbox Exhibit 1002 - Page 237
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

FIG. 6



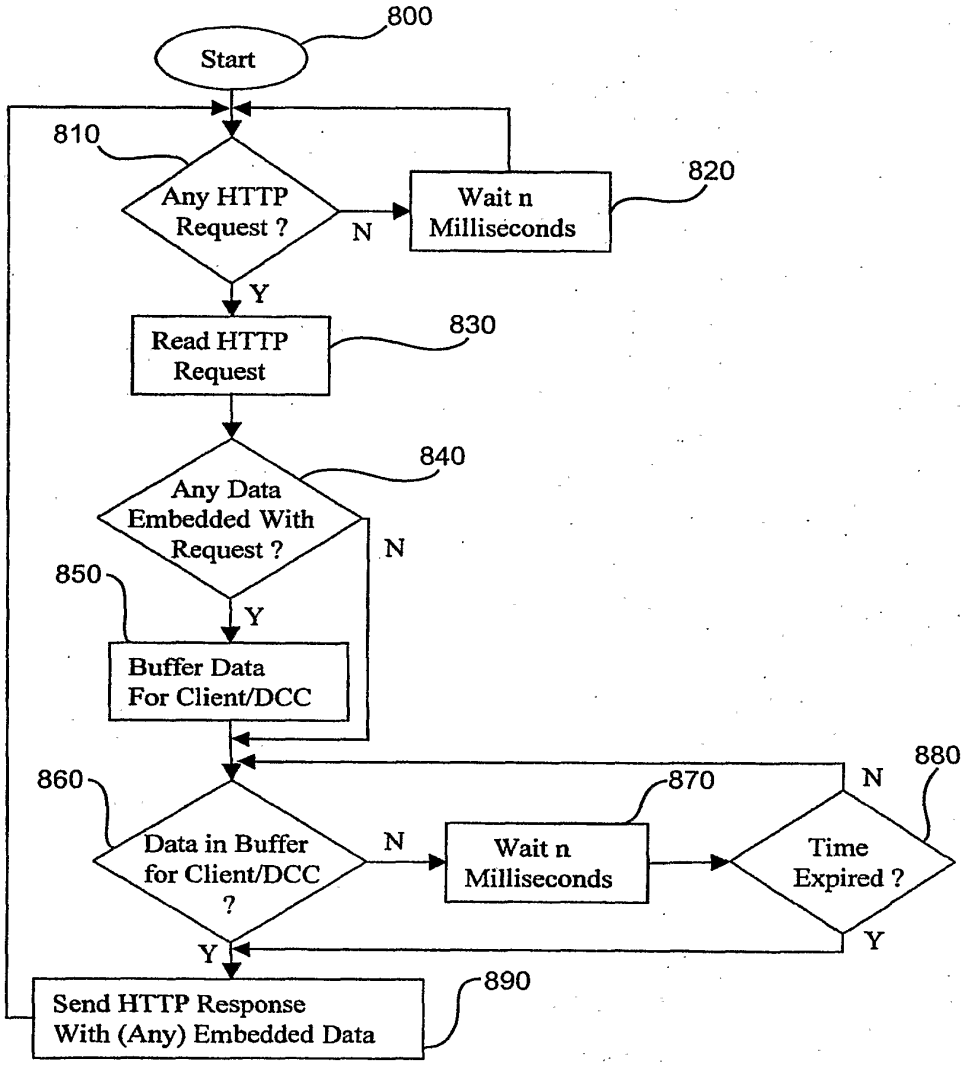
Dropbox Exhibit 1002 - Page 238
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

FIG. 7



Dropbox Exhibit 1002 - Page 239
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

FIG. 8



Dropbox Exhibit 1002 - Page 240
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2002 (10.01.2002)

PCT

(10) International Publication Number
WO 02/03046 A2

(51) International Patent Classification[7]: G01N

(21) International Application Number: PCT/US01/20253

(22) International Filing Date: 26 June 2001 (26.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/608,865 30 June 2000 (30.06.2000) US

(71) Applicant: **BROWN UNIVERSITY RESEARCH FOUNDATION** [US/US]; 42 Charlesfield Street, Providence, RI 02912 (US).

(72) Inventor: **MARIS, Humphrey, J.**; 9 Echo Drive, Barrington, RI 02806 (US).

(74) Agent: **SMITH, Harry, F.**; Ohlandt, Greeley, Ruggiero & Perle, LLP, One Landmark Square, 10th Floor, Stamford, CT 06901-2682 (US).

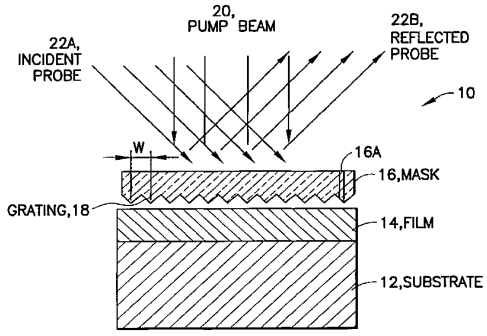
(81) Designated States *(national)*: CA, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ULTRASONIC GENERATOR AND DETECTOR USING AN OPTICAL MASK HAVING A GRATING FOR LAUNCHING A PLURALITY OF SPATIALLY DISTRIBUTED, TIME VARYING STRAIN PULSES IN A SAMPLE



(57) Abstract: A method and a system are disclosed for determining at least one characteristic of a sample that contains a substrate and at least one film disposed on or over a surface of the substrate. The method includes a first step of placing a mask over a free surface of the at least one film, where the mask has a top surface and a bottom surface that is place adjacent to the free surface of the film. The bottom surface of the mask has formed therein or thereon a plurality of features for forming at least one grating. A next step directs optical pump pulses through the mask to the free surface of the film, where individual ones of the pump pulses are followed by at least one optical probe pulse. The pump pulses are spatially distributed by the grating for launching a plurality of spatially distributed, time varying strain pulses within the film, which cause a detectable change in optical constants of the film. A next step detects a reflected or a transmitted portion of the probe pulses, which are also spatially distributed by the grating. A next step measures a change in at least one characteristic of a least one of reflected or transmitted probe pulse due to the change in optical constants, and a further step determines the at least one characteristic of the sample from the measured change in the at least one characteristic of the probe pulses. An optical mask is also disclosed herein, and forms a part of these teachings.

WO 02/03046 A2

Dropbox Exhibit 1002 - Page 241
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

ULTRASONIC GENERATOR AND DETECTOR USING AN OPTICAL MASK HAVING A GRATING FOR LAUNCHING A PLURALITY OF SPATIALLY DISTRIBUTED, TIME VARYING STRAIN PULSES IN A SAMPLE

FIELD OF THE INVENTION:

This invention relates generally to non-destructive material analysis and characterization systems and methods and, more particularly, relates to optically based materials analysis and characterization systems that employ light pulses of picosecond and sub-picosecond duration to generate a localized stress in a sample that results in propagating strain waves, and that detect changes in optical constants of the sample material due to the propagating strain waves.

BACKGROUND OF THE INVENTION:

A number of U.S. Patents exist in the general area of picosecond ultrasonics. In most of these U.S. Patents a pump light pulse is directed at the surface of a sample. The pump light pulse raises the temperature of a layer near the surface of the sample and sets up a stress in this region. A time-varying strain is then generated in the sample. The strain is detected by means of a probe light pulse applied to the sample at a later time. Hereinafter this approach will be referred to as the "standard method". From the arrival time, amplitude, and shape of the detected signals, a data processor is enabled to determine a number of characteristics of the sample. These characteristics include, but are not limited to, the film thickness, the adhesion between a film and the substrate, the adhesion between one film and another film, the orientation of crystalline grains making up a film, the size of grains, the crystal phase of a film, the electrical resistivity of a film, the rate of electromigration within a film, and the yield stress of a film.

In some of these U.S. Patents measurements can be made by means of a second method, referred to herein for convenience as a "grating method". In this approach, the pump light is divided into two beams that are directed onto the sample surface at oblique angles. Because of the constructive and destructive interference between the two beams, the intensity of the pump light varies periodically across the sample surface. Thus, the temperature rise of the sample surface and the induced stress will also vary periodically across the sample surface. This stress launches a strain disturbance into the sample that varies periodically across the sample surface. This strain field causes the optical constants of the sample, and the displacement of the sample surface, to vary across the sample

Dropbox Exhibit 1002 - Page 242
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

surface and, as a consequence, when a probe pulse is incident onto the surface a fraction of the probe pulse will be diffracted, rather than undergoing specular reflection. Thus, the strain field acts as a diffraction grating. By a measurement of the intensity of the diffracted probe light as a function of the time after the application of the pump light pulse, the propagation of strain in the sample can be investigated, and physical properties of the sample determined. The grating method can also be used to determine the various sample properties that were listed above.

These two methods each have some limitations. For example, in the standard method, in order to determine the thickness of a film the sound velocity in the film must be known. This value can be taken from measurements made on a bulk sample of the same material composition as the film. In some cases, it is also possible to estimate the sound velocity from a measurement of the reflection coefficient of the strain pulse at the interface between one film and another. This measurement enables a comparison of the acoustic impedances of the two films to be made.

The grating method also exhibits a number of limitations. For example, it is necessary to build the apparatus in a way that ensures that the phase relation between the two pump beams remains constant. In addition, the diffracted component of the probe light may have a low intensity and thus may be difficult to measure accurately in the presence of light diffusely scattered from the surface of the sample.

Based on the foregoing, it can be appreciated that a need exists to provide an improved approach to ultrasonic sample characterization that overcomes the foregoing and other problems.

OBJECTS AND ADVANTAGES:

It is a first object and advantage of these teachings to provide an improved sample characterization system and method that overcomes the foregoing an other problems.

It is another object and advantage of these teachings to provide an improved sample characterization system and method that employs an optical mask.

SUMMARY OF THE INVENTION

The foregoing and other problems are overcome and the objects of the invention are realized by methods and apparatus in accordance with embodiments of this invention.

An improved method and apparatus in accordance with these teachings generates and detects strain pulses in a sample, while retaining many of the advantages of the standard method, while at the same time making it possible to determine the sound velocity in the sample. A transparent plate, referred to herein for convenience as a mask, is placed over the sample. The bottom of the plate has a periodic grating etched into its surface. A pump light pulse is directed through the transparent mask onto the sample. The periodic grating of the mask distorts the wavefront of the light pulse and, as a result, the intensity of the light incident onto the film varies periodically with position across the sample surface. This results in a heating of the film surface that varies periodically with position. The regions of the film that are heated expand and, as a result, spatially distributed strain pulses (disturbances) are launched into the sample. The strain pulses result in a change in the optical constants of the sample, and this change is detected by means of a time-delayed probe pulse also directed onto the sample through the transparent mask. As in the standard method and the grating method, the improved method in accordance with the teachings herein can be used to determine various characteristics of the sample. These characteristics include, but need not be limited to, the film thickness, the adhesion between a film and the substrate, the adhesion between one film and another film, the orientation of crystalline grains making up a film, the size of grains, the crystal phase of a film, the electrical resistivity of a film, the rate of electromigration within a film, and the yield stress of a film.

In one preferred embodiment, the pump and probe beams are directed through the mask at normal incidence. The probe is delayed relative to the pump by means of a variable optical path provided by a movable stage. The change in the intensity of the reflected probe beam is measured as a function of the time delay between the application of the pump and probe pulses. To improve the signal to noise ratio the intensity of the pulses composing the pump beam is modulated at frequency **f** by means of an acousto-optic modulator. The output of the detector of the reflected probe beam is fed into a lock-in amplifier for which the reference signal is at the same frequency **f**. The measured change $\Delta R(t)$ in reflectivity of the sample is compared with the results of a simulated reflectivity change $\Delta R_{sim}(t)$. The change $\Delta R_{sim}(t)$ can be determined as follows: A) An initial estimate is made for the parameters of the sample. These parameters include, but are not

Dropbox Exhibit 1002 - Page 244
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

necessarily limited to, the thickness, density, sound velocity, thermal expansion, specific heat, and optical constants of the different films, the adhesion between the films, the orientation of crystalline grains making up a film, the size of grains, the crystal phase and electrical resistivity of each film. B) Based on these assumed values, the stress in the structure that is induced by the pump light pulse is calculated. C) The time-dependent strain in the sample is then calculated. D) From this strain, the expected change in reflectivity $\Delta R_{sim}(t)$ is found. E) This change is compared with the measured reflectivity $\Delta R(t)$. The parameters of the sample are then adjusted and the procedure repeated in order to achieve the best possible agreement between $\Delta R(t)$ and $\Delta R_{sim}(t)$.

A method and a system are thus disclosed for determining at least one characteristic of a sample containing a substrate and at least one film disposed on or over a surface of the substrate. The method includes a first step of placing a mask over a free surface of the at least one film, where the mask has a top surface and a bottom surface that is placed adjacent to the free surface of the film. The bottom surface of the mask has formed therein or thereon a plurality of features for forming at least one grating. A next step directs optical pump pulses through the mask to the free surface of the film, where individual ones of the pump pulses are followed by at least one optical probe pulse.

In accordance with an aspect of these teachings the pump pulses are spatially distributed by the grating for launching a plurality of spatially distributed, time varying strain pulses within the film. The strain pulses cause a detectable change in optical constants of the film.

A next step detects a reflected or a transmitted portion of the probe pulses, which are also spatially distributed by the grating.

A next step of the method measures a change in at least one characteristic of at least one of reflected or transmitted probe pulses due to the change in optical constants, and a further step determines the at least one characteristic of the sample from the measured change in the at least one characteristic of the probe pulses.

In addition to changes in reflectivity arising from the strain pulses that are launched in the sample, there may be components that arise from a spatial variation in temperature, and/or from a spatial variation in a density of electrons and holes in the sample.

For example, the sample may include at least one region that is implanted during an ion implant process and, using the spatially varying density of electrons and holes in the film,

Dropbox Exhibit 1002 - Page 245
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

a determined characteristic of the sample can be related to at least one of (A) a number of ions implanted per unit area of the surface of the sample; (B) a kinetic energy of the ions that are directed at the surface of the sample; (C) a direction at which the ion beam is incident onto the surface of the sample; (D) an ion current per unit area during the ion implant process; (E) the species of the implanted ion; (F) the charge on the implanted ion; (G) a duration of time that the ion-implanted sample is annealed; and (H) a temperature at which the ion-implanted sample is annealed.

An optical mask is also disclosed herein, and forms a part of these teachings.

Also disclosed is a method for determining the electrical resistivity of a film that comprises part of a sample having an underlying substrate. The method includes steps of: (A) placing a mask over a free surface of the film, the mask having a top surface and a bottom surface that is placed adjacent to the free surface of the film, the bottom surface of the mask comprising a plurality of features having a known feature repeat distance w; (B) directing optical pump pulses through the mask to the free surface of the film, individual ones of the pump pulses being followed by at least one optical probe pulse, said pump pulses being spatially distributed by said at least one grating for generating a spatially distributed temperature variation within the film that causes a change in optical constants of the film; (C) detecting a reflected or transmitted portion of said probe pulses, said probe pulses also being spatially distributed by said at least one grating; (D) measuring $\Delta R(t)$ as a function of the time t after the application of the pump pulses using the mask of known repeat distance w; (E) assuming values for the thermal conductivity κ_{film} of the film, the thermal conductivity κ_{sub} of the substrate, and the Kapitza conductance σ_K between the film and the substrate; (F) calculating an initial temperature distribution within the film; (G) calculating the temperature distribution within the film at later times based on the assumed values for the thermal conductivity of the film, the thermal conductivity of the substrate, and the Kapitza conductance between the film and the substrate; (H) calculating an expected change in reflectivity $\Delta R(t)$ based on the calculated temperature distribution; (I) adjusting the parameters κ_{film}, κ_{sub}, and σ_K, and repeating Steps (F)-(H) so as to obtain a best fit to the measured $\Delta R(t)$; and calculating the electrical resistivity from the thermal conductivity.

Dropbox Exhibit 1002 - Page 246
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

BRIEF DESCRIPTION OF THE DRAWINGS

The above set forth and other features of the invention are made more apparent in the ensuing Detailed Description of the Invention when read in conjunction with the attached Drawings, wherein:

Fig. 1 is an enlarged, cross-sectional view, not to scale, of a sample having a substrate, at least one film, and a mask disposed over a surface thereof in accordance with these teachings;

Fig. 2 is a simplified block diagram of a material characterization system in accordance with these teachings;

Fig. 3 is a logic flow diagram of a method for operating the data processor shown in Fig. 2 for generating a simulation of a change in sample reflectivity, and for comparing the simulation to a measured change in sample reflectivity;

Fig. 4 is an enlarged, cross-sectional view, not to scale, of a sample having a substrate, at least one film, and a mask disposed over a surface thereof in accordance with a further embodiment of these teachings, wherein the grating region of the mask is at a different height than all or a portion of the surrounding area of the lower surface of the mask;

Fig. 5 is a logic flow diagram of a method for the determination of the electrical resistivity of a metal film using the optical mask in accordance with the teachings herein; and

Fig. 6 depicts in an enlarged cross-sectional view a sample having laterally patterned features.

DETAILED DESCRIPTION OF THE INVENTION

Referring first to Fig. 1, a sample 10 includes a substrate 12, such as semiconductor material (e.g., silicon, a Group III-V material, or a Group II-VI material) having at least one film 14, such as a metal film or semiconductor or a dielectric film, disposed on or over a top surface thereof. A transparent plate, referred to herein as a mask 16, is placed on top of the sample 10. The mask 16 has a periodic grating 18 formed on or within a lower surface thereof. A pump light pulse 20 from a pump light source 30 (Fig. 2) is

Dropbox Exhibit 1002 - Page 247
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

directed through the mask 16 onto the sample 10, specifically onto the free (upper) surface of the film 14. The mask 16 distorts the wavefront of the pump light pulse and, as a result, the intensity of the light incident onto the free surface of the film 14 varies periodically with position across the sample's surface. This causes a heating of the surface of the film 14 that varies in a spatially periodic manner as a function of position. The regions of the film 14 that are heated expand. As a result, strain pulses are launched into the sample 10 from each of the expanding regions. These strain disturbances result in a change in the optical constants of the sample 10, and this change is detected by means of a time-delayed probe pulse 22A that is also directed onto the sample 10 through the mask 16, specifically by detecting (in this embodiment) a reflected portion 22B of the probe pulse. The probe pulse 22A originates from a probe source 32, which could be the pump source 30 as well. Preferably, the pump and probe pulses are laser pulses of picosecond or sub-picosecond duration, and originate from one laser or from two lasers. As in the standard method and the grating method, one or more characteristics of the sample 10 may be determined, such as those listed above.

In one preferred embodiment, and referring as well to Fig. 2, the pump and probe beams 20, 22A are directed through the mask 16 at normal incidence. The probe beam 22A is delayed relative to the pump beam 20, preferably by means of a variable optical path 34 provided by a movable stage or by some other technique. The sample 10 is assumed to be supported by some suitable type of fixed or movable sample stage 36. The change in the intensity of the reflected probe beam 22B is sensed by a detector 38 and measured as a function of a time delay **t** between the application of the pump and probe pulses 20, 22A. To improve the signal to noise ratio the intensity of the pulses composing the pump beam 20 can be modulated at some frequency **f** by means of an acousto-optic modulator (AOM) 30A. The output of the detector 38, which is an electrical signal indicative of the intensity of the reflected probe beam 22B, is fed into a lock-in amplifier 40 for which the reference signal is at the same frequency **f** as the modulation frequency of the AOM 30A. A data processor 42 has an input coupled to an output of the lock-in amplifier 40, and is further coupled to a memory 44, such as a hard disk, RAM, ROM, etc., wherein is stored an operating program, simulation results and other required data, constants and the like. The measured change $\Delta \mathbf{R(t)}$ in reflectivity is compared by the data processor 42 with the results of a simulated reflectivity change $\Delta \mathbf{R}_{sim}\mathbf{(t)}$ stored in the memory 44.

The change $\Delta \mathbf{R}_{sim}\mathbf{(t)}$ is preferably determined in accordance with the following method. Reference can also be made to the logic flow diagram of Fig. 3.

Dropbox Exhibit 1002 - Page 248
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

At Step A an initial estimate is made for the parameters of the sample 10. These parameters include, but are not necessarily limited to, the thickness, density, sound velocity, thermal expansion, specific heat, optical constants of the different films, the adhesion between the films, the orientation of crystalline grains making up a film, the size of grains, the crystal phase and electrical resistivity of each film.

Based on the assumed values, at Step B the stress in the sample 10 that is induced by the pump light pulse 20 is calculated.

At Step C, the time-dependent strain in the sample 10 is calculated.

From the calculated strain, at Step D the expected change in reflectivity $\Delta R_{sim}(t)$ is found.

At Step E, the expected change in reflectivity $\Delta R_{sim}(t)$ is compared with the measured change in reflectivity $\Delta R(t)$.

At Step F, the parameters of the sample are adjusted and the procedure iterated one or more times in order to achieve the best possible agreement between $\Delta R(t)$ and $\Delta R_{sim}(t)$.

For certain samples, it may be possible to simplify the procedure just described. Consider first a sample 10 that includes a single film 14 deposited onto the substrate 12 (as in Fig. 1), where the thickness **d** of the film 14 is significantly greater than the spacing **w** of the grating lines 18 on the mask 16. For a time **t** less than the time required for a strain pulse to propagate through the thickness of the film 14 to the substrate 12 and return to the top surface of the film 14, the reflectivity change $\Delta R(t)$ is unaffected by the existence of the substrate 12, i.e., the response $\Delta R(t)$ is the same as would be obtained on a bulk material of the same composition and material properties as the film 14. The stress set up by the pump pulse 20 excites a Rayleigh surface wave that is confined to the region near to the upper surface of the film 14. This wave may be considered to be a standing wave of wavelength $\lambda = w$. The frequency of this standing wave is given by $f_R = c_R/w$, where c_R is the Rayleigh wave velocity. The presence of this standing wave causes a periodic modulation of the elastic strain in the surface layer of the film 14, which in turn causes a contribution to $\Delta R(t)$ that varies in time with the frequency f_R. An analysis of the measured $\Delta R(t)$ can be used to obtain the frequency f_R, and from this frequency, and from the known value of **w**, the Raleigh wave velocity of the material of the film 14 can be found. This velocity can be expressed in terms of the elastic constants of the film

Dropbox Exhibit 1002 - Page 249
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

material using a well-known formula.

One reference for the velocity of a Rayleigh surface wave is L.D. Landau and E.M. Lifshitz, "Theory of Elasticity", second edition, Pergamon Press, 1970, section 24. The theory of Rayleigh velocity in elastically anisotropic crystals is complicated but, in general, for an elastically isotropic solid, $\mathbf{c_R}$ is given as follows. First define the quantity $\varsigma \equiv \mathbf{c_R}/\mathbf{c_T}$. It can then be shown (see Landau et al.) that ς is the solution for the following equation:

$$\xi^6 - 8\xi^4 + 8\xi^2\left(3 - 2\frac{c_T^2}{c_L^2}\right) - 16\left(1 - \frac{c_T^2}{c_L^2}\right) = 0$$

where $\mathbf{c_T}$ and $\mathbf{c_L}$ are the velocities of longitudinal and transverse sound, respectively.

If the material of the film 14 is elastically isotropic, a knowledge of the Rayleigh velocity, together with an assumed value for Poisson's ratio, can be used to estimate the longitudinal and transverse sound velocities in the material of the film 14.

$$\xi^6 - 8\xi^4 + 8\xi^2\left(3 - 2\frac{c_T^2}{c_L^2}\right) - 16\left(1 - \frac{c_T^2}{c_L^2}\right) = 0$$

More specifically, the ratio of the velocity of the transverse and longitudinal sound is given by

$$\frac{c_T}{c_L} = \sqrt{\frac{1-2\sigma}{2(1-\sigma)}}.$$

Therefore,

$$\xi^6 - 8\xi^4 + 8\xi^2\frac{2-\sigma}{1-\sigma} - 16\frac{1}{2(1-\sigma)} = 0$$

Hence, if σ is known, the value of ξ can be calculated from the preceding equation. A measurement of $\mathbf{c_R}$ can then be used to give $\mathbf{c_T}$ via the relation

$$c_T = \frac{c_R}{\xi},$$

and $\mathbf{c}_L$ can be found from

$$c_L = c_T\sqrt{\frac{2(1-\sigma)}{1-2\sigma}} = \frac{c_R}{\xi}\sqrt{\frac{2(1-\sigma)}{1-2\sigma}}.$$

For this type of sample, a strain pulse will also propagate away from the surface of the film 14 and into the volume of the film 14. The strain pulse is partially reflected at the interface between the film 14 and the substrate 12, and returns to the free (upper) surface of the film 14. The return of the reflected strain pulse results in a sharp feature in $\Delta\mathbf{R(t)}$ at a time τ_L equal to $\mathbf{2w/c}_L$, where $\mathbf{c}_L$ is the longitudinal sound velocity. Hence, this time can be used to determine the thickness of the film 14. The value of $\mathbf{c}_L$ can be estimated from the results of the measurements of the Rayleigh velocity as described above. Alternatively, for films of known composition and elastic properties, the value of $\mathbf{c}_L$ can be taken from the scientific literature.

A simplified analysis can also be made for those samples 10 in which the thickness of the film 14 is much less than the grating period **w**. In this case the penetration depth of the Rayleigh wave is greater than the thickness of the film 14. Thus, the Rayleigh wave will not be confined within the film thickness and will penetrate into the substrate 12. The velocity of the Rayleigh wave is now dependent on the elastic properties and densities of both the film 14 and the substrate 12, and is also affected by the thickness of the film 14. Measurement of the frequency of the oscillations in $\Delta\mathbf{R(t)}$ gives the Rayleigh wave velocity. There is also a component of the strain that propagates through the thickness of the film 14 and that is reflected back at the interface with the substrate 12, thereby giving the sharp feature in $\Delta\mathbf{R(t)}$ at a time $\mathbf{2w/c}_L$. Again, from the measured Rayleigh wave velocity $\mathbf{c}_R$ and the time τ_L, the longitudinal and transverse sound velocity, and the thickness of the film 14, can be determined.

It is within the scope of these teachings to make a number of variations in these measurement techniques.

For example, the pump light pulse 20 and the measuring probe light pulse 22A can be directed at the surface of the sample 10 at normal or oblique incidence. Furthermore, the angle of incidence of the probe pulse 22A can be the same as the angle of incidence of

the pump pulse 20, or the angle of incidence of the probe pulse 22A may be different than the angle of incidence of the pump pulse 20. Also, the wavelength of the pump and probe beams 20, 22A can be the same, or they can be different. If the wavelengths are different, and for the case where it is desired to detect a diffracted probe beam, the wavelength of the probe beam 22A is set to be less than the line spacing of the mask 16.

In the description given above, the detection of the time varying strain in the sample 10 is made through a measurement of the change in the intensity of the reflected probe light 22B. However, it is also within the scope of these teachings for measurements to be made of the change in the intensity of transmitted (as opposed to reflected) probe light. Also, measurements can be made of a change in the polarization of the reflected or transmitted probe light, a change in the optical phase of the reflected or transmitted probe light, or a change in propagation direction of the reflected or transmitted probe light. Measurements may be made of more than one of these characteristics, such as a measurement of intensity of the reflected or transmitted probe light and a measurement of optical phase of the reflected or transmitted probe light. Further by example, a measurement could be made of the intensity of the transmitted probe light in conjunction with a measurement of optical phase of the reflected probe light.

The pump and/or the probe light can be brought to the mask 16 through free space or through optical fiber(s). Measurements can be made of the component of the probe light that is specularly reflected from the sample (angle of reflection equal to angle of incidence), or diffracted at an angle as a result of the presence of the grating in the mask 16, or from that part of the probe light that is scattered diffusely from the surface of the sample 10.

The mask 16 can be made of a number of transparent materials, such as silica, other glasses, or polymers. It is straightforward to obtain gratings that have a line spacing as small as 2000 Å, and this distance can be made even smaller through the use of electron beam lithography.

The mask 16 can also be constructed using a slab of a transparent material with opposing flat surfaces, and the grating 18 formed with a patterned thin film of a dielectric material, or with a metal deposited onto its lower surface. The thickness of the mask 16 need not be uniform, as a wedged or tapered thickness mask could be used as well.

Furthermore, a single mask 16 could have two or more gratings 18 on the lower surface, where each grating has different line spacings. In this case the pump and probe beams 20, 22A could be directed to different regions of the mask 16 where the spacing of the grating 18 has a chosen value, and in this way a measurement of $\Delta R(t)$ can be made for two or more different values of the spacing **w** of the lines on the grating 18. Alternatively, the pump and probe beams 20, 22A can be directed to a fixed location on the surface of the sample 10, and the mask 16 moved, using a mask positioning system 46 (Fig. 4), so that regions of the mask 16 with different grating line spacing are positioned in the region where the pump and probe beams are located.

In some applications it may advantageous to use a mask 16 having a two dimensional array of grating features (e.g., a square array), rather than a sequence of lines (one-dimensional array).

The mask 16 can be positioned by the mask positioning system 46 by being placed in direct contact with the sample surface, i.e., with the free (upper) surface of the film 14. It is also possible through the use of nanomachining techniques to construct a mask 16 that is prevented from coming into direct contact with the free surface of the film 14 by means of an air cushion produced by passing air through small holes 16A in the mask 16, as is done, for example, in an air track used in physics teaching laboratories. In this case the spacing of the mask 16 from the surface of the film 14 is preferably no larger than the spacing between the lines of the grating 18. It is also within the scope of these teachings to construct a mask 16 that has the grating 18 in a center section that is lower than most or all of a surrounding area of the mask 16, as shown in Fig. 4. That is, the grating portion of the lower surface of the mask 16 is not coplanar with the surrounding surface area. This approach is useful for those samples 10 that have surfaces that are not flat, as it ensures that the grating 18 can be placed in close proximity to the surface of the film 14.

The mask 16 can be lowered onto the sample 10 and raised from the surface of the sample 10 by the mask positioning system 46 using a number of different techniques. For example, electrical or magnetic forces can be applied to the mask 16, or the mask 16 can be raised or lowered by means of air currents.

Measurements can be made on a single film 14 on a substrate 12, on a stack of thin films of different thickness and material composition, or on samples 10 that are laterally patterned. For example, Fig. 6 shows a sample 10 having laterally patterned features

Dropbox Exhibit 1002 - Page 253
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

10A, such as embedded metalization lines, and the mask 16 positioned over a surface of the sample 10 in accordance with the teachings herein. The metalization lines need not be embedded, and could as well be located on a top surface of the film 14. In this embodiment it may be advantageous to make the period of the mask 16 match the period of the features 10A, or to mismatch the period of the mask 16 with the period of the features 10A. It may also be advantageous to provide a predetermined relationship between the size(s) of features 10A and the period(s) of the mask 16 (where the mask 16 can be provided with two or more characteristic periods for the grating 18, or where more than one mask is used).

Based on the foregoing it can be appreciated that these teachings overcome the problems discussed above with relation to the prior art. For example, the sound velocity in the sample can be measured directly, and need not be known a priori. Furthermore, the use of the mask relaxes the requirement that the sample characterization apparatus be constructed so as ensure that the phase relation between a plurality of pump beams remains constant, as a single pump beam is sufficient to provide the spatially distributed heating effect at the surface of the sample.

In addition to the changes in reflectivity arising from the strain pulses that are launched in the sample 10, there can be changes in reflectivity that arise from the change in the temperature, and in the density of electrons and holes. The change in reflectivity arising from these effects can be distinguished from the change in reflectivity that arises from the propagation of strain pulses.

More particularly, strain pulses give rise to either sharp pulses (from sound echoing back and forth in a film) or to an oscillatory contribution (from the Rayleigh surface waves), while the contribution to the change in reflectivity that arises from the change in temperature or from the change in the electron and hole concentration varies more smoothly with time.

The teachings of this invention also make it possible to measure the electrical resistivity of a metal film, provided that the film has a thickness lying within a certain range. In this embodiment, a determination is first made of the thermal conductivity κ_{film} of the metal film. From κ_{film} the electrical resistivity ρ_{film} can be calculated using the Wiedemann-Franz law:

Dropbox Exhibit 1002 - Page 254
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

$$\rho_{film} = \frac{LT}{\kappa_{film}},$$

where **L** is the Lorenz number and **T** is the absolute temperature (see, for example, C. Kittel, Introduction to Solid State Physics, 7th edition, Wiley, p. 168).

The following is a method for the determination of the thermal conductivity. Consider a metal film of thickness d deposited onto a substrate. Let the mask have a line spacing **w** with lines running parallel to the y axis, and let the normal to the substrate be in the z direction. Assume that the intensity $\mathbf{I_{pump}(x)}$ of the pump light varies with position on the sample surface according to

$$I_{pump}(x) = I^{o}_{pump}[1+\cos(kx)],$$

where $\mathbf{I^o_{pump}}$ is a constant, $\mathbf{k = 2\pi/w}$, and x is an axis running across the surface in a direction perpendicular to the direction of the lines. The form of the intensity variation across the surface of the sample is dependent on the geometry of the mask 16 and on its optical properties. The particular form given above is for illustration and is not intended to imply that this variation will occur for all masks 16. The pump light pulse induces a temperature rise $\mathbf{\Delta T}$ that varies across the sample surface. Again, for illustration, we take this to have the same form:

$$\Delta T(x, z=0) = \Delta T_0[1+\cos(kx)],$$

where $\mathbf{\Delta T_0}$ is a constant. This is the temperature at the surface located on the plane z=0; the temperature rise at a distance below the surface will be less. The variation of the temperature rise with distance z into the film is determined by: 1) the distance ζ that the light penetrates into the metal, 2) by the distance ξ that the conduction electrons that are excited by the light diffuse before they lose their energy to the thermal phonons and come into thermal equilibrium with the lattice (see G. Tas and H.J. Maris, Electron Diffusion in Metals Studied by Picosecond Ultrasonics, Physical Review B 49, 15046 (1994)), and 3) by the film thickness. Note that since the lines on the mask 16 run parallel to the y-axis there is no dependence of the temperature on the coordinate y.

Dropbox Exhibit 1002 - Page 255
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

The change in temperature of the sample surface results in a change in the optical reflectivity that is different at each point on the surface. In the absence of the mask 16 it is reasonable, as a first approximation, to consider that the change in reflectivity of the probe beam due to the temperature change would be proportional to the average of the change in temperature taken over the area of the surface onto which the probe light is incident. However, it is important to recognize that the mask 16 distorts the probe beam so that, just like the pump beam, it has a greater intensity at some points on the surface of the sample 10 than at others. If one take the intensity of the probe light at the surface of the sample 10 to vary with position as:

$$I_{probe}(x) = I^{o}_{probe}[1+\cos(kx)],$$

where $\mathbf{I^{o}_{probe}}$ is a constant, then the change $\mathbf{\Delta R}$ in reflectivity is proportional to the average over the surface of the product of the probe intensity with the temperature change at the surface, i.e.,

$$\Delta R \propto \int dx I_{probe}(x)\Delta T(x, z=0)$$
$$\propto I_{probe}[A+B],$$

where

$$A \equiv \int dx \Delta T(x, z=0)$$
$$B \equiv \int dx \cos(kx)\Delta T(x, z=0).$$

At a time **t** after the application of the pump pulse, the temperature distribution in the film will have changed because of heat flow. A measurement of $\mathbf{\Delta R(t)}$ as a function of time can provide information about this heat flow. It should be noted that the reflectivity change $\mathbf{\Delta R}$ contains the term **A** which is proportional to the temperature change of the film averaged across its surface, and also contains the term **B** that vanishes when the temperature distribution across the film surface is uniform. Thus, $\mathbf{\Delta R(t)}$ is affected both by heat flow out of the film into the substrate (this primarily affects the term **A**), as well as by heat flow within the film which tends to make the temperature distribution across the surface of the film uniform, and hence reduces the magnitude of the term **B**.

The heat flow within the metal film may have components both parallel and perpendicular to the plane of the film. The heat flux $\overline{q}$ at any point is equal to $\kappa_{film}\nabla\mathbf{T}$, where κ_{film} is the thermal conductivity of the metal film. The heat flow across the interface into the substrate per unit area is equal to $\sigma_K\Delta\mathbf{T}_{int}$, where $\Delta\mathbf{T}_{int}$ is the temperature jump across the interface and σ_K is the Kapitza conductance at the interface. Note that since $\Delta\mathbf{T}_{int}$ is the difference between the temperature of the film and the temperature of the substrate, this heat flow is also affected by the thermal conductivity κ_{sub} of the substrate.

Referring now to Fig. 5, one procedure for the determination of the electrical resistivity of the metal film is as follows:

Step (A): $\Delta\mathbf{R(t)}$ is measured as a function of the time **t** after the application of the pump pulse using a mask of known repeat distance **w**.

Step (B): Values are assumed for the thermal conductivity κ_{film} of the film, the thermal conductivity κ_{sub} of the substrate, and the Kapitza conductance σ_K between the film and the substrate.

Step (C): The initial temperature distribution within the film is calculated. This calculation is preferably based on the known geometry, line spacing or repeat distance **w** and on the optical characteristics of the mask 16. The temperature distribution is affected by the diffusion coefficient of the hot electrons excited by the pump pulse. This diffusion coefficient can be estimated from the assumed value of the thermal conductivity of the film, as described by Tas and Maris in the publication referenced above.

Step (D): The temperature distribution within the film is then calculated at later times based on the assumed values for the thermal conductivity of the film, the thermal conductivity of the substrate, and the Kapitza conductance between the film and the substrate.

Step (E): The expected change in reflectivity $\Delta\mathbf{R(t)}$ based on the temperature distribution determined in Step (D) is then calculated.

Step (F) The parameters κ_{film}, κ_{sub}, and σ_K, are then adjusted, and Steps (C)-(E) are repeated so as to obtain a best fit to the measured $\Delta\mathbf{R(t)}$.

The electrical resistivity of the film is then calculated using the thermal conductivity, as described above.

It is important to note that the optimum choice of the repeat distance **w** of the mask 16 depends on the thickness **d** of the film and on the values of κ_{film}, κ_{sub}, and σ_K. For

Dropbox Exhibit 1002 - Page 257
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

example, if **w** is chosen to be too small, the hot electrons will diffuse so far that the initial temperature distribution will be almost uniform across the surface of the film, i.e., the temperature distribution in the film will be independent of x. The term B will then be absent. Suppose now that it is also true that the thickness of the film **d** is less than the diffusion length ξ. In this case the initial temperature distribution throughout the film will be uniform. As a result, the temperature at later times, and hence also the reflectivity change $\Delta R(t)$, will only be affected by the Kapitza conductance σ_K. Under these conditions, the measurement of $\Delta R(t)$ generally cannot be readily analyzed to determine the thermal conductivity of the film.

It is noted that if the mask 16 is not used, the initial temperature distribution would be uniform across the sample surface. For films whose parameters **d**, κ_{film}, κ_{sub}, and σ_K lie in a suitable range it would be possible to perform an analysis of the measured $\Delta R(t)$ to determine κ_{film}. However, the range of film parameters for which the accurate determination of κ_{film} is possible is greatly increased through the use of a mask 16 of suitably chosen repeat distance **w**.

It is within the scope of the teachings of this invention to make measurements on a single sample using a series of masks 16 of different repeat distances **w**, and to fit the totality of results so obtained by adjustment of the parameters κ_{film}, κ_{sub}, and σ_K.

As an alternate method, one may compare the measured $\Delta R(t)$ on a sample of unknown resistance with the results of measurements of $\Delta R(t)$.

The mask 16 can also be used to advantage for the characterization of samples 10 into which ions have been implanted (or, more generally, the mask 16 may be used with altered materials). Reference with regard to such altered materials may be made to U.S. Patent No.: 5,706,094, "Ultrafast Technique for the Characterization of Altered Materials", by H.J. Maris, as well as to U.S. Patent No.: 6,008,906, "Optical Method for the Characterization of the Electrical Properties of Semiconductors and Insulating Films", by H.J. Maris.

In general, the characteristics of a sample 10 that has been ion implanted are affected by the following parameters:

(A) the number of ions implanted per unit area of the surface of the sample 10, referred to as the dose;

(B) the kinetic energy of the ions that are directed at the sample surface, referred to as

the energy;
(C) the direction at which the ion beam is incident onto the sample 10;
(D) the ion current per unit area during the implant process;
(E) the species of the implanted ion;
(F) the charge on the ion, e.g., singly or double ionized;
(G) the duration of time that the ion-implanted sample 10 is annealed; and
(H) the temperature at which the ion-implanted sample 10 is annealed.

In the above-referenced U.S. Patent No.: 5,706,094 it was disclosed to investigate as many as possible of these characteristics through measurements of the change in reflectivity $\Delta R(t)$ of the probe pulse applied directly to the surface at a time **t** after the application of the pump pulse. Experimental parameters that were varied included the wavelength of the pump and/or the probe light, where a change in wavelength changes the distance over which the pump and probe light is absorbed; and the intensity of the pump and/or the probe light, which changes the density of electrons and holes excited in the sample.

While a variation in the wavelength and/or the intensity can be helpful in providing a more extended characterization of a sample, it may be difficult to obtain a complete characterization of a sample 10 by these means alone, given the large number of sample parameters that can affect the measurement. In addition, while it is possible to build an instrument in which the wavelength of the pump and/or the probe light can be selected to have two different values (for example, by the use of a frequency doubling crystal), it can be difficult to build an instrument in which the pump and probe wavelengths are continuously adjustable.

The use of present invention has the advantage that the repeat distance **w** of the mask 16 can be selected so as to optimize the amount of information that can be obtained for a particular type of sample. The mask repeat distance can also be selected so as to make the measured $\Delta R(t)$ particularly sensitive to one or more of the sample characteristics (A)-(H) listed above. Furthermore, measurements can be made for a number of different mask 16 repeat distances **w** in order to achieve a more complete characterization. Also, measurements can be made for line masks or for masks 16 with two dimensional arrays of features.

For the analysis of the data, the most practical method in many applications may be by comparison with data taken on reference samples of known characteristics. However, the

data analysis may also be performed by comparison of the data to simulations, together with adjustment of parameters and iteration to achieve a best fit.

While the invention has been particularly shown and described with respect to preferred embodiments thereof, it will be understood by those skilled in the art that changes in form and details may be made therein without departing from the scope and spirit of the invention.

Dropbox Exhibit 1002 - Page 260
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

CLAIMS

What is claimed is:

1. A method for determining at least one characteristic of a sample comprising a substrate and at least one film disposed on or over a surface of the substrate, comprising steps of:

placing a mask over a free surface of the at least one film, the mask having a top surface and a bottom surface that is placed adjacent to the free surface of the film, the bottom surface of the mask comprising a plurality of features forming at least one grating;

directing optical pump pulses through the mask to the free surface of the film, individual ones of the pump pulses being followed by at least one optical probe pulse, said pump pulses being spatially distributed by said at least one grating for launching a plurality of spatially distributed strain pulses within the film, said strain pulses causing a change in optical constants of the film;

detecting a reflected or transmitted portion of said probe pulses, said probe pulses also being spatially distributed by said at least one grating;

measuring a change in at least one characteristic of at least one of reflected or transmitted probe pulses due to the change in optical constants; and

determining the at least one characteristic of the sample from the measured change in the at least one characteristic of the probe pulses.

2. A method as in claim 1, wherein the determined at least one characteristic of the sample is film thickness.

3. A method as in claim 1, wherein the determined at least one characteristic of the sample is an adhesion between the film and the substrate.

4. A method as in claim 1, wherein the determined at least one characteristic of the sample is an adhesion between the film and another film.

5. A method as in claim 1, wherein the determined at least one characteristic of the sample is an orientation of crystalline grains that comprise the film.

6. A method as in claim 1, wherein the determined at least one characteristic of the sample is a size of crystalline grains that comprise the film.

7. A method as in claim 1, wherein the determined at least one characteristic of the sample is a crystal phase of a film.

8. A method as in claim 1, wherein said pump pulses being spatially distributed by said at least one grating induce a spatial variation in temperature of the film, wherein the variation in temperature causes a change in optical constants of the film, and where the determined at least one characteristic of the sample is an electrical resistivity of the film.

9. A method as in claim 1, wherein the determined at least one characteristic of the sample is a rate of electromigration within the film.

10. A method as in claim 1, wherein the determined at least one characteristic of the sample is a yield stress of the film.

11. A method as in claim 1, wherein the step of determining the at least one characteristic of the sample comprises steps of:

simulating a response of the sample to the application of the pump pulses through said mask using assumed sample properties;

comparing the measured change in the least one characteristic of the probe pulses to the simulated response; and

changing the assumed sample properties, and repeating the steps of simulating and comparing until the measured change agrees with a result of the simulation.

12. A method as in claim 1, wherein the step of measuring measures at least one of an intensity of reflected or transmitted probe pulses; a polarization of reflected or transmitted probe pulses, a change in an optical phase of reflected or transmitted probe pulses, and a change in a propagation direction of reflected or transmitted probe pulses.

13. A method as in claim 1, wherein said mask has a period that is a function of a thickness of said at least one film.

14. A method as in claim 1, wherein said mask has a period that is greater than a thickness of said at least one film.

15. A method as in claim 1, wherein said mask has a period that is less than a thickness of said at least one film.

16. A method as in claim 1, wherein said pump pulses excite a Rayleigh standing surface wave in the film of wavelength $\lambda = \mathbf{w}$, where **w** is the grating period, the Rayleigh standing surface wave having a frequency given by $\mathbf{f_R} = \mathbf{c_R}/\mathbf{w}$, where $\mathbf{c_R}$ is the Rayleigh wave velocity, the standing wave causing a periodic modulation of elastic strain in the film which in turn causes a contribution to $\mathbf{\Delta R(t)}$ that varies in time with the frequency $\mathbf{f_R}$, further comprising steps of:

analyzing a measured $\mathbf{\Delta R(t)}$ to obtain the frequency $\mathbf{f_R}$, and from this frequency, and from a known value of **w**, determining the Raleigh wave velocity of material that comprises the film; and

using the determined Rayleigh wave velocity, together with a value for Poisson's ratio, estimating longitudinal and transverse sound velocities in the material that comprises the film.

17. A method as in claim 16, wherein for a case where **w** is less than a thickness of the film, strain pulses are partially reflected at an interface between the film and the substrate and return to the upper surface of the film resulting in a sharp feature in $\mathbf{\Delta R(t)}$ at a time τ_L equal to $\mathbf{2w/c_L}$, where $\mathbf{c_L}$ is the longitudinal sound velocity, and further comprising a step of determining the thickness of the film using the time τ_L.

18. A method as in claim 16, wherein for a case where **w** is greater than a thickness of the film, wherein the velocity of the Rayleigh wave is dependent on elastic properties and densities of both the film and the substrate, and is also dependent on the thickness of the film, further comprising steps of:

measuring frequency of oscillations in $\mathbf{\Delta R(t)}$ to obtain the Rayleigh wave velocity $\mathbf{c_R}$;

Dropbox Exhibit 1002 - Page 263
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

detecting a component of the strain pulse that propagates through the thickness of the film and that is reflected back at the interface with the substrate, thereby giving a sharp feature in $\Delta R(t)$ at a time $2w/c_L$; and

using the determined Rayleigh wave velocity c_R and a time τ_L equal to $2w/c_L$, where c_L is the longitudinal sound velocity, determining the longitudinal and transverse sound velocity and the thickness of the film.

19. A method as in claim 1, wherein at least one of the pump pulses and the probe pulses are directed through the mask at normal incidence to the free surface of the film.

20. A method as in claim 1, wherein at least one of the pump pulses and the probe pulses are directed through the mask at oblique incidence to the free surface of the film.

21. A method as in claim 1, wherein the sample comprises features that are laterally patterned.

22. A system for determining at least one characteristic of a sample comprising a substrate and at least one film disposed on or over a surface of the substrate, comprising:

a mask adapted for being placed over a free surface of the at least one film, the mask having a top surface and a bottom surface that is placed adjacent to the free surface of the film, the bottom surface of the mask comprising a plurality of features forming at least one grating;

an optical system for directing optical pump pulses through the mask to the free surface of the film, individual ones of the pump pulses being followed by at least one optical probe pulse, said pump pulses being spatially distributed by said at least one grating for launching a plurality of spatially distributed strain pulses within the film, said strain pulses causing a change in optical constants of the film;

an optical detector for detecting a reflected or transmitted portion of said probe pulses, said probe pulses also being spatially distributed by said at least one grating; and

a data processor for measuring a change in at least one characteristic of at least one of reflected or transmitted probe pulses due to the change in optical constants and for determining the at least one characteristic of the sample from the measured change in the at least one characteristic of the probe pulses.

23. A system as in claim 22, wherein the determined at least one characteristic of the sample is selected from one of film thickness, an adhesion between the film and the substrate, an adhesion between the film and another film, an orientation of crystalline grains that comprise the film, a size of crystalline grains that comprise the film, a crystal phase of a film, a rate of electromigration within the film, and a yield stress of the film, further wherein said pump pulses being spatially distributed by said at least one grating induce a spatial variation in temperature of the film, wherein the variation in temperature causes a change in optical constants of the film, and where the determined at least one characteristic of the sample is an electrical resistivity of the film..

24. A system as in claim 22, wherein said data processor operates to simulate a response of the sample to the application of the pump pulses through said mask using assumed sample properties, to compare the measured change in the least one characteristic of the probe pulses to the simulated response, and to change the assumed sample properties and iteratively simulate and compare until the measured change agrees with a result of the simulation.

25. A system as in claim 22, wherein said data processor measures at least one of an intensity of reflected or transmitted probe pulses; a polarization of reflected or transmitted probe pulses, a change in an optical phase of reflected or transmitted probe pulses, and a change in a propagation direction of reflected or transmitted probe pulses.

26. A system as in claim 22, wherein said mask has a period that is a function of a thickness of said at least one film.

27. A system as in claim 22, wherein said pump pulses excite a Rayleigh standing surface wave in the film of wavelength $\lambda = \mathbf{w}$, where $\mathbf{w}$ is the grating period, the Rayleigh standing surface wave having a frequency given by $\mathbf{f_R} = \mathbf{c_R}/\mathbf{w}$, where $\mathbf{c_R}$ is the Rayleigh wave velocity, the standing wave causing a periodic modulation of elastic strain in the film which in turn causes a contribution to $\Delta\mathbf{R(t)}$ that varies in time with the frequency $\mathbf{f_R}$, and where said data processor operates to analyze a measured $\Delta\mathbf{R(t)}$ to obtain the frequency $\mathbf{f_R}$, and from this frequency, and from a known value of $\mathbf{w}$, to

Dropbox Exhibit 1002 - Page 265
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

determine the Raleigh wave velocity of material that comprises the film; and further operates, using the determined Rayleigh wave velocity, together with a value for Poisson's ratio, to estimate longitudinal and transverse sound velocities in the material that comprises the film.

28. A system as in claim 27, where for a case where **w** is less than a thickness of the film, strain pulses are partially reflected at an interface between the film and the substrate and return to the upper surface of the film resulting in a sharp feature in $\Delta R(t)$ at a time τ_L equal to $2w/c_L$, where c_L is the longitudinal sound velocity, and where said data processor determines the thickness of the film using the time τ_L.

29. A system as in claim 27, where for a case where **w** is greater than a thickness of the film, where the velocity of the Rayleigh wave is dependent on elastic properties and densities of both the film and the substrate, and is also dependent on the thickness of the film, said data processor further operates to measure frequency of oscillations in $\Delta R(t)$ to obtain the Rayleigh wave velocity c_R; to detect a component of the strain pulses that propagates through the thickness of the film and that is reflected back at the interface with the substrate, thereby giving a sharp feature in $\Delta R(t)$ at a time $2w/c_L$; and, using the determined Rayleigh wave velocity c_R and a time τ_L equal to $2w/c_L$, where c_L is the longitudinal sound velocity, to determine the longitudinal and transverse sound velocity and the thickness of the film.

30. A system as in claim 22, wherein at least one of the pump pulses and the probe pulses are directed through said mask by said optical system at normal incidence to the free surface of the film.

31. A system as in claim 22, wherein at least one of the pump pulses and the probe pulses are directed through said mask by said optical system at oblique incidence to the free surface of the film.

32. A system as in claim 22, wherein the sample comprises features that are laterally patterned.

32. A system as in claim 22, wherein the sample includes at least one region that is implanted during an ion implant process, wherein said pump pulses being spatially distributed by said at least one grating generate a spatially distributed density of electrons and holes within the sample, said spatially distributed density of electrons and holes

Dropbox Exhibit 1002 - Page 266
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

causing a change in optical constants of the sample, and wherein the determined at least one characteristic of the sample is related to at least one of (A) a number of ions implanted per unit area of the surface of the sample; (B) a kinetic energy of the ions that are directed at the surface of the sample; (C) a direction at which the ion beam is incident onto the surface of the sample; (D) an ion current per unit area during the ion implant process; (E) the species of the implanted ion; (F) the charge on the implanted ion; (G) a duration of time that the ion-implanted sample is annealed; and (H) a temperature at which the ion-implanted sample is annealed.

33. A mask adapted to be placed over a free surface of a film to be characterized, said mask being transparent and having a top surface and a bottom surface that is placed adjacent to the free surface of the film, the bottom surface of said mask comprising a plurality of features forming at least one grating for spatially distributing optical pump pulses so as to launch a plurality of spatially distributed strain pulses within the film, the strain pulses causing a change in optical constants of the film, said at least one grating further for spatially distributing optical probe pulses individual ones of which are applied after an individual one of the optical pump pulses.

34. A mask as in claim 33, wherein features of said grating are spaced apart by an amount that is a function of a thickness of the film.

35. A mask as in claim 33, wherein features of said grating form a one dimensional or a two dimensional array of features.

36. A mask as in claim 33, wherein features of said grating are etched into said bottom surface.

37. A mask as in claim 33, wherein features of said grating are formed upon said bottom surface.

38. A mask as in claim 33, wherein said mask has a non-uniform thickness such that features of said grating are at least partially surrounded by an area of said bottom surface that is not coplanar with said features.

39. A method for determining the electrical resistivity of a film that comprises part of a sample having an underlying substrate, comprising steps of:

Dropbox Exhibit 1002 - Page 267
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

(A) placing a mask over a free surface of the film, the mask having a top surface and a bottom surface that is placed adjacent to the free surface of the film, the bottom surface of the mask comprising a plurality of features having a known feature repeat distance **w**;

(B) directing optical pump pulses through the mask to the free surface of the film, individual ones of the pump pulses being followed by at least one optical probe pulse, said pump pulses being spatially distributed by said at least one grating for spatially varying the temperature within the film and causing a causing a change in optical constants of the film;

(C) detecting a reflected or transmitted portion of said probe pulses, said probe pulses also being spatially distributed by said at least one grating;

(D) measuring $\Delta R(t)$ as a function of a time **t** after the application of the pump pulses using the mask of known repeat distance **w**;

(E) assuming values for the thermal conductivity κ_{film} of the film, the thermal conductivity κ_{sub} of the substrate, and the Kapitza conductance σ_K between the film and the substrate;

(F) calculating an initial temperature distribution within the film;

(G) calculating the temperature distribution within the film at later times based on the assumed values for the thermal conductivity of the film, the thermal conductivity of the substrate, and the Kapitza conductance between the film and the substrate;

(H) calculating an expected change in reflectivity $\Delta R(t)$ based on the calculated temperature distribution;

(I) adjusting the parameters κ_{film}, κ_{sub}, and σ_K, and repeating Steps (F)-(H) so as to obtain a best fit to the measured $\Delta R(t)$; and

(J) calculating the electrical resistivity from the thermal conductivity.

40. A method for determining at least one characteristic of a sample comprising

a substrate and at least one film disposed on or over a surface of the substrate, the sample further comprising at least one region that is implanted during an ion implant process, comprising steps of:

placing a mask over a free surface of the at least one film, the mask having a top surface and a bottom surface that is placed adjacent to the free surface of the film, the bottom surface of the mask comprising a plurality of features forming at least one grating;

directing optical pump pulses through the mask to the free surface of the film, individual ones of the pump pulses being followed by at least one optical probe pulse, said pump pulses being spatially distributed by said at least one grating for generating a spatially distributed density of electrons and holes within the sample, said spatially distributed density of electrons and holes causing a change in optical constants of the sample;

detecting a reflected or transmitted portion of said probe pulses, said probe pulses also being spatially distributed by said at least one grating;

measuring a change in at least one characteristic of at least one of reflected or transmitted probe pulses due to the change in optical constants; and

determining at least one characteristic of the ion implanted region from the measured change in the at least one characteristic of the probe pulses.

41. A method as in claim 40, wherein the determined at least one characteristic is related to a number of ions implanted per unit area of the surface of the sample.

42. A method as in claim 40, wherein the determined at least one characteristic is related to a kinetic energy of the ions that are directed at the surface of the sample.

43. A method as in claim 40, wherein the determined at least one characteristic is related to a direction at which an ion beam is incident onto the surface of the sample.

44. A method as in claim 40, wherein the determined at least one characteristic is related to an ion current per unit area during the ion implant process.

Dropbox Exhibit 1002 - Page 269
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

45. A method as in claim 40, wherein the determined at least one characteristic is related to the species of the implanted ion.

46. A method as in claim 40, wherein the determined at least one characteristic is related to the charge on the implanted ion.

47. A method as in claim 40, wherein the determined at least one characteristic is related to a duration of time that the ion-implanted sample is annealed.

48. A method as in claim 40, wherein the determined at least one characteristic is related to a temperature at which the ion-implanted sample is annealed.

49. A system for determining at least one characteristic of a sample comprising a substrate and at least one film disposed on or over a surface of the substrate, the sample comprising at least one region that is implanted during an ion implant process, comprising:

a mask adapted for being placed over a free surface of the at least one film, the mask having a top surface and a bottom surface that is placed adjacent to the free surface of the film, the bottom surface of the mask comprising a plurality of features forming at least one grating;

an optical system for directing optical pump pulses through the mask to the free surface of the film, individual ones of the pump pulses being followed by at least one optical probe pulse, said pump pulses being spatially distributed by said at least one grating for generating a spatially distributed density of electrons and holes within the sample, said spatially distributed density of electrons and holes causing a change in optical constants of the sample;

an optical detector for detecting a reflected or transmitted portion of said probe pulses, said probe pulses also being spatially distributed by said at least one grating; and

a data processor for measuring a change in at least one characteristic of at least one of reflected or transmitted probe pulses due to the change in optical constants and for determining at least one characteristic of the ion implanted region from the measured change in the at least one characteristic of the probe

Dropbox Exhibit 1002 - Page 270
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

pulses.

50. A system as in claim 49, wherein the determined at least one characteristic is related to at least one of (A) a number of ions implanted per unit area of the surface of the sample; (B) a kinetic energy of the ions that are directed at the surface of the sample; (C) a direction at which the ion beam is incident onto the surface of the sample; (D) an ion current per unit area during the ion implant process; (E) the species of the implanted ion; (F) the charge on the implanted ion; (G) a duration of time that the ion-implanted sample is annealed; and (H) a temperature at which the ion-implanted sample is annealed.

51. A method for determining at least one characteristic of a sample comprising a substrate and at least one film disposed on or over a surface of the substrate, comprising steps of:

placing a mask over a free surface of the at least one film, the mask having a top surface and a bottom surface that is placed adjacent to the free surface of the film, the bottom surface of the mask comprising a plurality of features forming at least one grating;

directing optical pump pulses through the mask to the free surface of the film, individual ones of the pump pulses being followed by at least one optical probe pulse, said pump pulses being spatially distributed by said at least one grating for generating a spatially distributed variation in temperature in the film, said spatially distributed variation in temperature causing a change in optical constants of the film;

detecting a reflected or transmitted portion of said probe pulses, said probe pulses also being spatially distributed by said at least one grating;

measuring a change in at least one characteristic of at least one of reflected or transmitted probe pulses due to the change in optical constants; and

determining the at least one characteristic of the sample from the measured change in the at least one characteristic of the probe pulses.

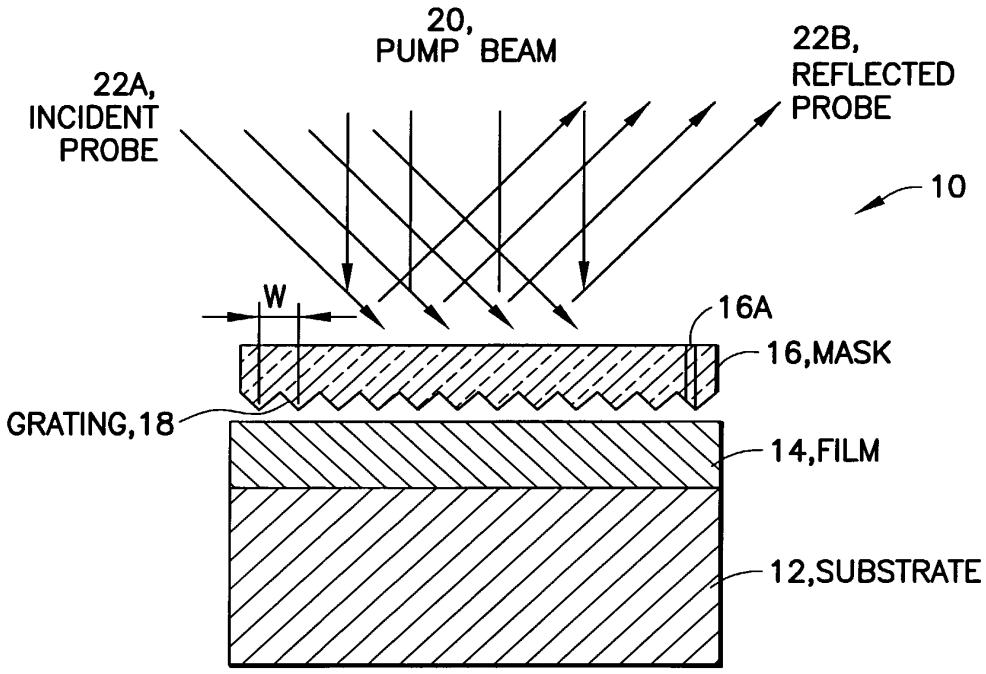

20,
PUMP BEAM
22A,
INCIDENT
PROBE
22B,
REFLECTED
PROBE
10
W
16A
16,MASK
GRATING,18
14,FILM
12,SUBSTRATE

FIG. 1

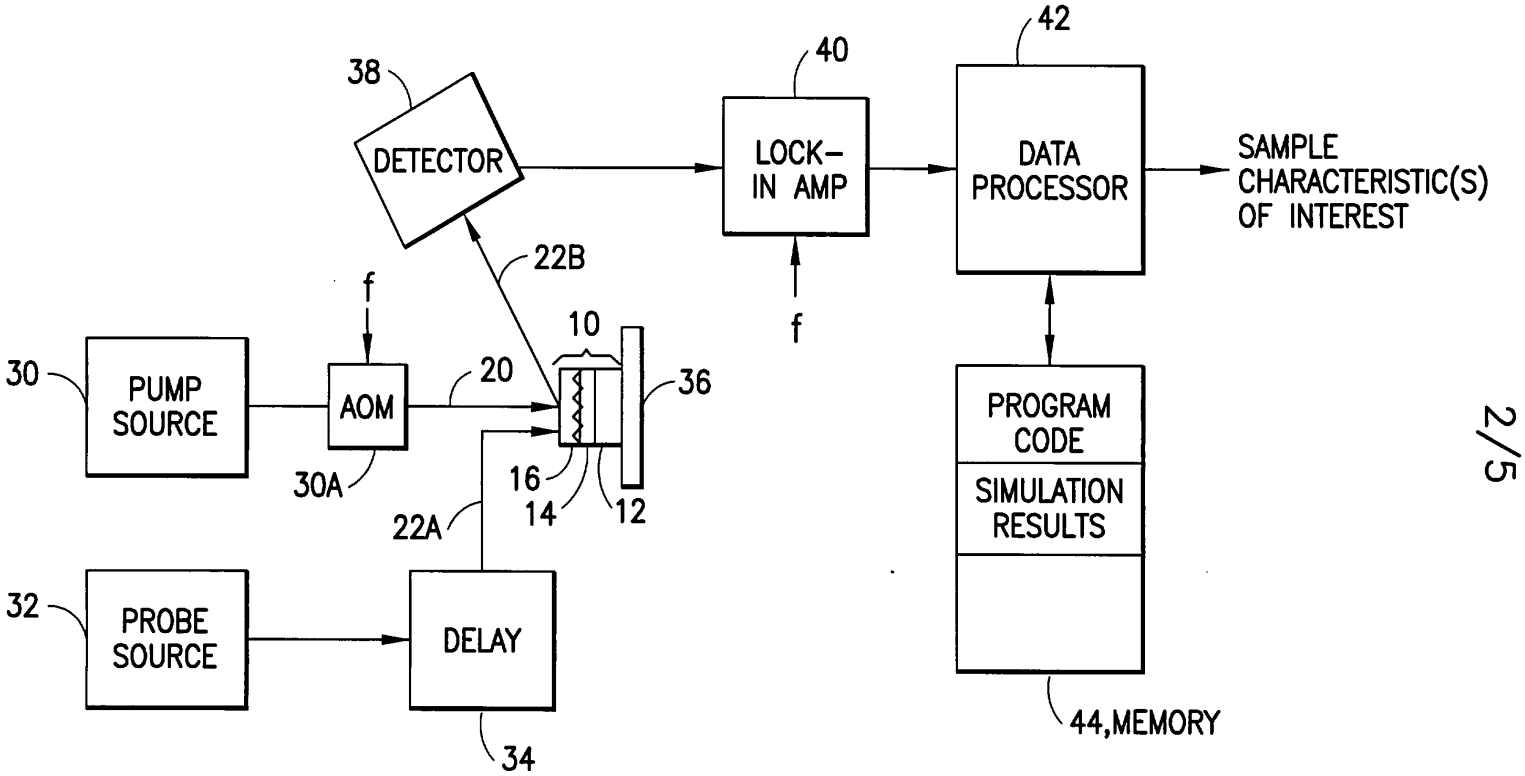


FIG.2

Dropbox Exhibit 1002 - Page 273
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

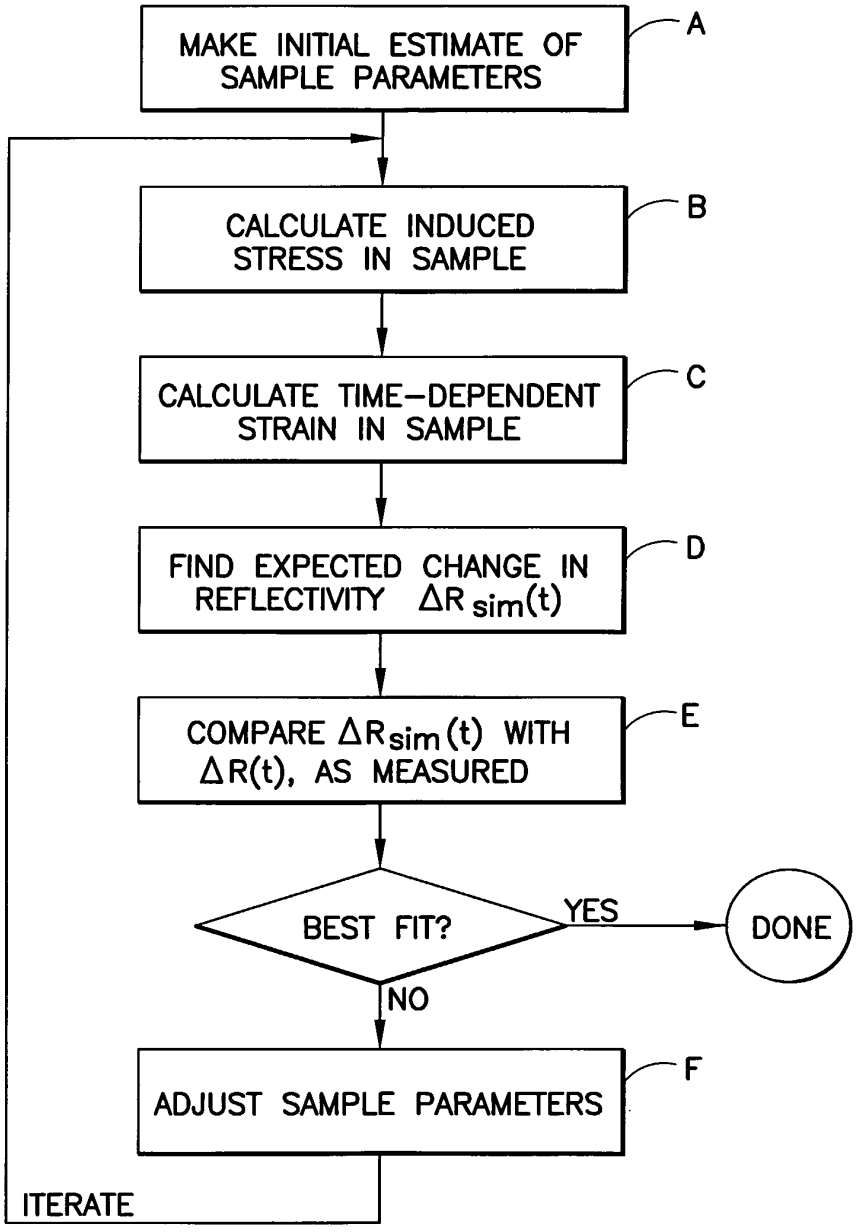

MAKE INITIAL ESTIMATE OF SAMPLE PARAMETERS
A
CALCULATE INDUCED STRESS IN SAMPLE
B
CALCULATE TIME-DEPENDENT STRAIN IN SAMPLE
C
FIND EXPECTED CHANGE IN REFLECTIVITY $\Delta R_{sim}(t)$
D
COMPARE $\Delta R_{sim}(t)$ WITH $\Delta R(t)$, AS MEASURED
E
BEST FIT?
YES
DONE
NO
ADJUST SAMPLE PARAMETERS
F
ITERATE

FIG.3

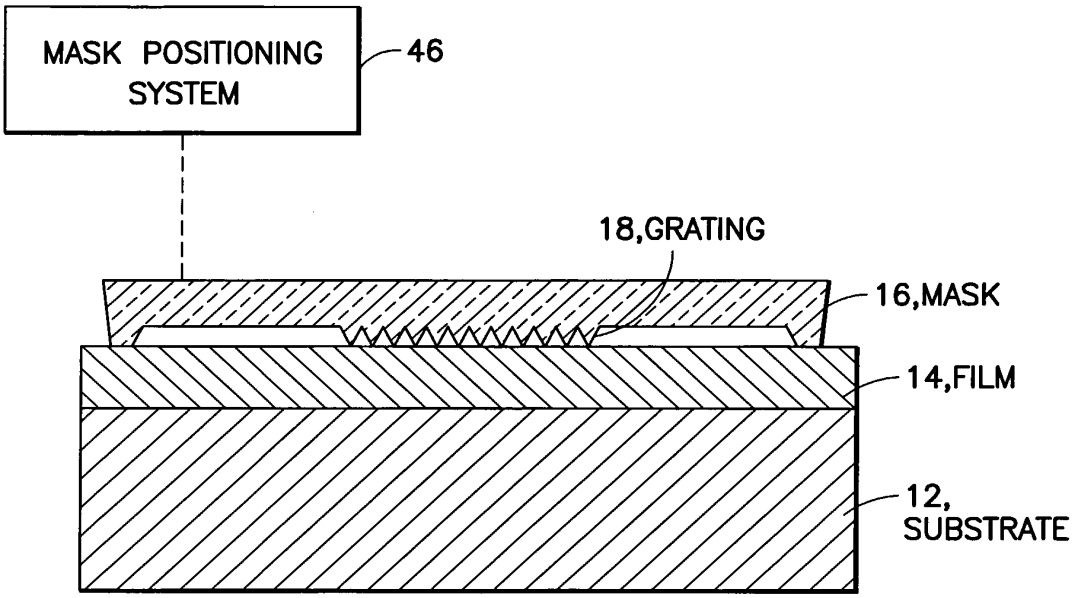

MASK POSITIONING SYSTEM
46
18,GRATING
16,MASK
14,FILM
12, SUBSTRATE

FIG.4

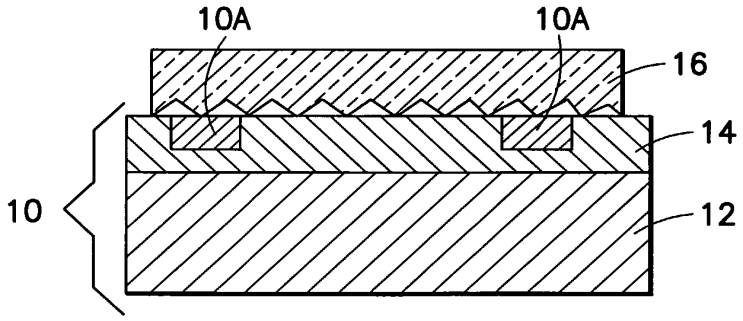

10A
10A
16
14
12
10

FIG.6

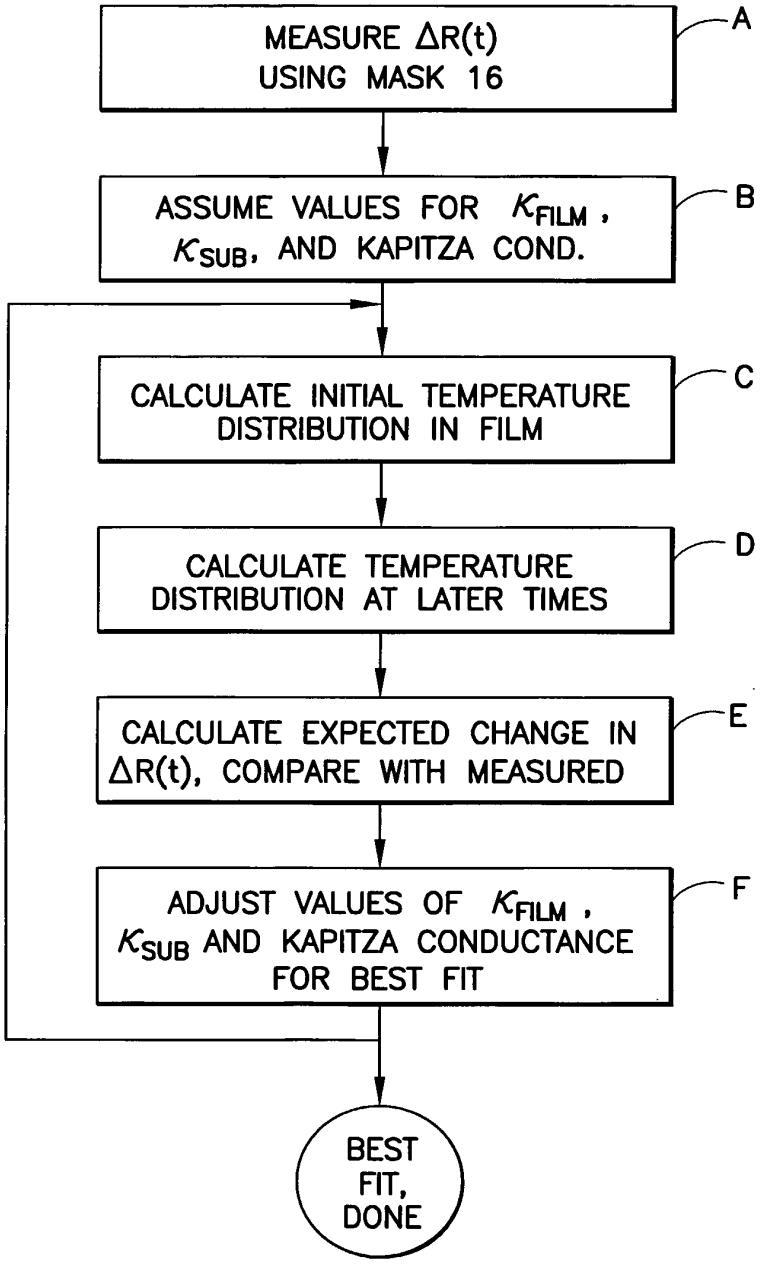

MEASURE ΔR(t) USING MASK 16
A
ASSUME VALUES FOR K_{FILM}, K_{SUB}, AND KAPITZA COND.
B
CALCULATE INITIAL TEMPERATURE DISTRIBUTION IN FILM
C
CALCULATE TEMPERATURE DISTRIBUTION AT LATER TIMES
D
CALCULATE EXPECTED CHANGE IN ΔR(t), COMPARE WITH MEASURED
E
ADJUST VALUES OF K_{FILM}, K_{SUB} AND KAPITZA CONDUCTANCE FOR BEST FIT
F
BEST FIT, DONE

FIG.5

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 June 2001 (07.06.2001)

PCT

(10) International Publication Number
WO 01/40887 A1

(51) International Patent Classification[7]: G05B 23/02, G06F 15/16

(21) International Application Number: PCT/US00/32734

(22) International Filing Date: 1 December 2000 (01.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/454,178 2 December 1999 (02.12.1999) US
09/608,685 29 June 2000 (29.06.2000) US

(71) Applicant: **SENVID, INC.** [US/US]; 2995 Woodside Road, #400-438, Woodside, CA 94062 (US).

(72) Inventors: **HESSELINK, Lambertus**; 101 Greenoaks Drive, Atherton, CA 94027 (US). **RIZAL, Dharmarus**; 353 Everett Avenue, #106, Palo Alto, CA 94301 (US). **VAN BEURDEN, Joep**; 10395 Melissa Court, Cupertino, CA 95014 (US).

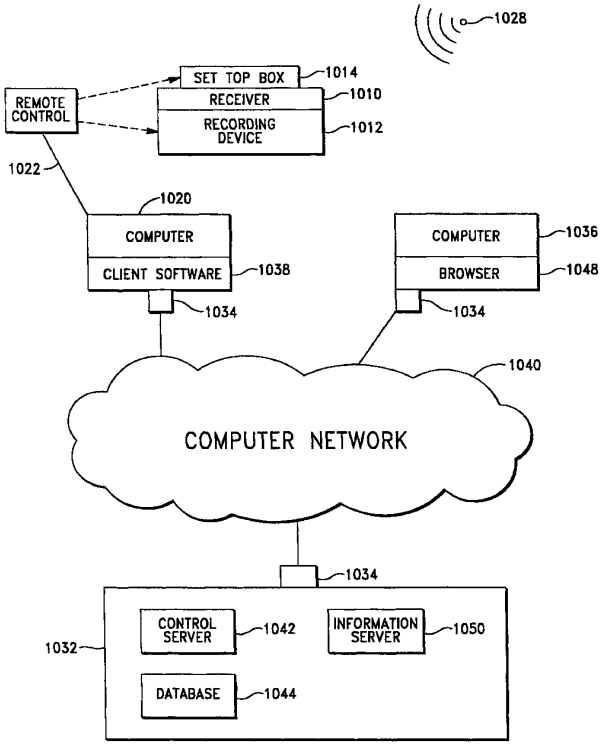
(74) Agents: **TEST, Aldo, J.** et al.; Flehr Hohbach Test Albritton & Herbert LLP, 4 Embarcadero Center, Suite 3400, San Francisco, CA 94111-4187 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD, SYSTEM AND SERVICE MODEL FOR REMOTE RECORDING OF TELEVISION PROGRAMS



(57) Abstract: Entities (1020, 1036) connected to computer networks such as the Internet (1040) and web-browser software (1048) can schedule recordings of television programs and/or operate the recording equipment (1012). In an example scenario, a user who maintains recording equipment (1012) at home may utilize the present invention from his or her workplace or vacation place, accesses a service provider website (1050) with her/his user name and password, views the schedule of television programs provided by a broadcaster or other distributor of programming and selects the television programs to be recorded. The application service provider (1042) in turn transmits the selected television program information to a computer (1020) connected to a later described remote control unit (1018) to execute and operate the recording of selected programs. In this manner, the present invention enables anyone with Internet access to remotely operate recording equipment to record television programs.

WO 01/40887 A1

Dropbox Exhibit 1002 - Page 277
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Dropbox Exhibit 1002 - Page 278
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

METHOD, SYSTEM AND SERVICE MODEL FOR REMOTE RECORDING OF TELEVISION PROGRAMS

This application is a continuation in part of U.S. patent application serial no. 09/454,178, "Control and Observation of Physical Devices, Equipment and Processes by Multiple Users Over Computer Networks," filed December 2, 1999, which is co-pending.

FIELD OF THE INVENTION

The present invention relates broadly to the remote control of signal recording equipment. Specifically, the present invention relates to the control of remotely located recording equipment via a computer network.

BACKGROUND OF THE INVENTION

Most consumer video/audio recording equipment today such as the video cassette recorder (VCR) is equipped with scheduling features. Scheduling features allow users to schedule recording of television programs based on user-specified time and channels. Most equipment can be controlled by remote control. However, for average users the process of scheduling television program recordings can be cumbersome. The user must be present at the location of recording equipment where a remote control unit is situated within an effective operating distance of the recording device. In the case where the remote control unit transmits commands in the form of infrared signals, the remote control unit must also establish line of sight to the recording equipment. Before operating a timer mechanism in conjunction with the recording equipment, the internal clock of video/audio recording equipment must be set to conform to local time. A user reviews schedule information of television programs to be recorded, such as program date, time and channel. A user typically

Dropbox Exhibit 1002 - Page 279
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

selects a desired program to be recorded and enters schedule information using the remote control unit into the recording equipment. This step may consist of several key entries on the remote control units, since for every intended consecutive scheduled recording, the user specifies the time to begin recording as well as the time to terminate recording.

U.S. Patents 5,692,2101014 and 5,988,078 to Levine teach implementations of an electronic schedule stored in memory to allow cursor based programming on a conventional video recorder through use of an associated personal computer. The computer communicates with the video recorder via infrared signals of the type used for remote control of the video recorder. Programming schedule information may be provided to the personal computer from a remote database by telephonic communication, broadcast, or use of disposable memories. A remote transmitter connected to the personal computer is used at the time of the recording to send signals to the video recorder to initiate recording of a preselected program, allowing unattended programming memory of the video recorder to initiate recording of a specific channel at a proper time. The method taught by Levine includes the steps of providing at the viewing location a computerized unit having an operator input and a modem; establishing a connection to a wide area network through the modem; transmitting information to a service provider regarding the geographical location of the particular viewing location; and receiving from the service provider information specific to the type of programming available to the particular viewing location. However, neither of the Levine patents address the problem of trying to operate a video recorder from a remote location.

SUMMARY OF THE INVENTION

The present invention addresses the problems identified above and provides an apparatus, method and service model which simplify conventional methods for schedule

Dropbox Exhibit 1002 - Page 280
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

recordings of television programs and enable users to control recording equipment from any location via the Internet. Entities connected to computer networks such as the Internet and web-browser software can schedule recordings of television programs and/or operate the recording equipment. In an example scenario, a user who maintains recording equipment at home may utilize the present invention from his or her workplace or vacation place, accesses a service provider website using her/his user name and password, views the a schedule of television programs provided by a broadcaster or other distributor of programming and selects the television programs to be recorded. The application service provider in turn transmits the selected television program information to a computer connected to a later described remote control unit to execute and operate the recording of selected programs. In this manner, the present invention enables anyone with internet access to remotely operate recording equipment to record television programs.

Another attendant advantage of the present invention is an inexpensive solution to provide global connectivity of the Internet to existing recording equipment. The present invention can be utilized to operate recording equipment such as video cassette recorders, that typically have infrared sensors to receive control commands. Other recording equipment such as DVD recorders, hard drive based video recorders, etc. can also be controlled using the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The forgoing aspects and many of the attendant advantages of the present invention will become more readily apparent in the following detailed description and accompanying drawings, wherein:

FIG. 1A is a diagrammatic representation of the computer network utilized by the present

Dropbox Exhibit 1002 - Page 281
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

invention;

FIG. 1B is a diagrammatic representation in block form of the system architecture of the present invention;

FIG. 2 illustrates the DNP packet format utilized in the present invention;

FIG. 3 shows a packet sent from a client process to a lab server;

FIG. 4 shows a response packet sent from the lab server 112 to a client process;

FIG. 5 is a flow chart illustrating the logical sequence of steps for the lab server to transmit raw data from physical processes for calculating results based on computational analysis of the raw data;

FIG. 6 is a flow chart illustrating the logical sequence of steps for the lab server to interpret client instructions, execute the commands and generate responses;

FIG. 7 is a flowchart illustrating the basic operation of the connection monitor;

FIG. 8 displays several routing modes that may be performed by the connections server;

FIG. 9 is a flowchart illustrating the basic operation of the connection handler;

FIG. 10 is a flowchart illustrating client DNP packet processing;

FIG. 11 is a diagrammatic representation of a two-dimensional set of DCT components;

FIG. 12 is a flowchart illustrating the logical sequence of steps executed by the server for performing the encoding process;

FIG. 13 is a flowchart illustrating the logical sequence of steps executed by the client process for performing the decoding process;

FIG. 14 illustrates in block diagram form the major components utilized in an alternative embodiment of the present invention;

FIG. 15 illustrates in block diagram form the remote control device of an alternative embodiment present invention;

Dropbox Exhibit 1002 - Page 282
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

FIG. 16 illustrates another alternative embodiment of the present invention; and

FIG. 17 illustrates an alternative embodiment of the service model of the present invention.

DETAILED DESCRIPTION

FIG. 1A shows a computer 10 connected via a computer network such as Internet 50 to computer 60 that manipulates devices in a laboratory. Computers 10, 60 may have a conventional design, incorporating a processor chassis utilizing a central processing unit (CPU), various memory and supporting integrated circuitry. Connected to the processor is a keyboard 12 and monitor 16. A user may control the computer 10 using the keyboard 12 or mouse 18 to manipulate a cursor moved about on the screen of the monitor 14 to make selections in programs executed on the computer 10. Floppy drive 20 and hard disk 22 may also be incorporated in the computers 10, 60.

Although a desktop type of computer is illustrated, it is to be understood that other forms of computers, such as workstations, laptops, palm tops, dumb terminals, or any computer capable of communicating with other computers may be used in connection with embodiments of the present invention.

Computers 10, 60 may communicate over the computer network 50 via modem and telephone line. An operating system and browser program may also be included in computers 10, 60 so that a user may access the laboratory. However, other media may also be used, such as a direct connection or high speed data line. The computer network 50, as described above, may be a large and complex system, incorporating a vast number of nodes and components.

Computer 60 is located at a laboratory where physical processes are to be conducted. For illustrative purposes, the operation of a laser and optical equipment is described herein,

Dropbox Exhibit 1002 - Page 283
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

but it is to be understood that other types of physical processes may be used in connection with the present invention. An interface 62 is connected to the processor in computer 60 that allows a user to control laser 64. The beam from laser 64 may be directed through various optical equipment 66, which may be adjusted on table 68 by interface 62. In an embodiment of the present invention, interface 62 may use a PCI-GPIB board to control and monitor laser 64. To acquire images of the laser beam that have been processed by optical equipment 66, a CCD detector that transmits digitized images to a IMAQ PCI-1424 board may be used. The optical equipment 66 may be mechanically adjusted and aligned by motorized stages on which the equipment is mounted. To display live pictures of the processes and equipment, an IMAQ PCI-1408 board may be used to digitize the analog video signal from camera 70. Motion of camera 70 may be controlled by a motion control system available through a software application such as LabView, which may be stored and executed on computer 60. Camera 70 is provided with frame grabber 72 to provide video feedback of the physical process, and are controlled by the video server 72, which may be executed on the processor of computer 60. System software on computer 60 may also include IMAQ Vision for G that provides image processing libraries such as a Fast Fourier Transform (FFT) routine to speed up development of live data analysis software.

Directing attention to FIG. 1B, the system architecture 100 integrates hardware and software that facilitate two-way communication between physical processes 110 to on-line users across computer networks. The system can be divided into several processes based on functionality: physical processes 110, lab server 112, connection server 114, clients 118, database server 120. These processes can be implemented as software programs that are executed in computing devices such as computers. As used herein, physical processes 110 are defined as physical, biological and/or chemical processes or phenomena that can be

Dropbox Exhibit 1002 - Page 284
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

detected, measured, quantified and/or controlled by electronic devices such as detectors, sensors, motors, power source, etc. to various interfaces such as GPIB, RS-232, PCI, USB, ethernet, etc., the electronic devices that monitor and control the physical processes 110 and communicate with computer 60 that runs the lab server process 112.

Data from the physical processes 110 are collected by the lab server 112 for purposes of storing into the database via the database server 120 and/or distributing to the clients 118 via the connection server 114. Prior to sending data, the lab server 112 can also perform analysis and transformation of the data such as statistics and FFT computation. The lab server 112 also receives data from the clients 118 such as control commands through the connection server 114. After analyzing these commands, the lab server 112 then passes the commands to the electronic devices or equipment (i.e. laser, motors, detectors, etc.). As shown in FIG. 1B, there are multiple physical processes 110, namely physical process 110-1 and physical process 110-12, as well as multiple lab servers 112-1, 112-2.

The connection server 114 serves as the distributor of data that accepts, verifies and routes information from data sources to appropriate destinations. The connection server 114 supports full duplex point-to-point and point-to-multipoints data transmissions between the clients 118, lab server 112, and database server 120. Several transmission modes will be discussed below. Additionally, the connection server 114 also monitors the status of network connections throughout the entire process.

The clients' processes 118 provide user interfaces (UI) for users' input and output functions. The clients' processes 118 are implemented as software programs that can be run on clients' computing devices such as desktop computers. The client also establishes two-way communications with the connection server 114. Data from the connection server 114 are decoded and displayed according to associated formats such as the video, graph, LED

Dropbox Exhibit 1002 - Page 285
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

displays, etc.

In a preferred embodiment, communications between the processes above are carried out using a common language, such as Data Network Protocol (DNP). Besides transporting various data types, DNP also carries network and communications related messages between different processes. DNP packet format is also discussed in the later sections.

The lab server 112 may reside at the location of the physical process 110 to have direct local control of the physical process. The lab server 112 is the process that broadcasts data from the physical process 110 and well as control the physical process 110 based on requests from clients 118. The lab server 112 can be implemented as a multi-threaded software that implements communication functions across computer networks such as the internet 116. To provide universal and reliable communications, all data can be transported using standard connection based network protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP). Each connection (in this case between the lab server process 112, connection server process 114, and clients 118) is commonly called socket that consists of a network or IP address and a port number. However, the data itself and other communication messages are encoded in a format called Data Network Protocol (DNP). In the OSI network model, DNP can be considered as an application layer protocol like HTTP and FTP. The unique design of DNP provides a common language between different processes that enables collaborative environments between multiple users across the internet.

DNP is designed to carry various types of digital data such as float, integer, Boolean, video and arrays of data. Data is encoded using DNP into one information entity called a packet that has two main sections: the overhead section 205 and instruction section 225. Directing attention to FIG. 2, the DNP packet format is illustrated. The overhead section 205 may contain the following fixed-size fields:

Dropbox Exhibit 1002 - Page 286
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Packet size 210: the length of the entire packet normally in byte words (8 bits unit).

Destination ID 212: may contain client ID, lab server ID, connection server ID, all-clients-group ID, all-clients-and-lab-server-group ID, or connection server group ID where the packet is sent.

Source ID 214: may contain client ID, lab server ID or connection server ID where the packet is originated.

Instruction number 216: contains the number of instructions following the overhead section 205. For example in FIG. 2, there are N instructions.

The instruction section 225 may contain a number of instructions. Each instruction can be a specific command or request that contains the following fields.

Component ID 230: identification number of specific device/equipment for user interface component.

Command ID 232: identification number of specific command/request to be performed.

Command Value 234: parameter values used to perform the commands or requests. Based on the associated command/request, the data type of common values can vary (i.e. float data, integer data, video data, array of data). Consequently this field has variable size. Both sender and receiver of the request may have a look-up list of data types associated with the component ID's and command ID's. Hence, the data type information need not be carried in the packet itself. The instruction section may be extended to include component ID's, command ID's and command values 252-262. FIG. 3 shows an example packet sent from a client 118 to a lab server 112 that is a request to change the current value of laser equipment to 45.4 mA. In overhead section 305 there is a packet size section 302, a lab server ID section 304 and a client ID section 306. In instruction section 315 there is a laser ID section 320, a change current value section 322 and the target milliamps 45.4 in section 324.

Dropbox Exhibit 1002 - Page 287
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

FIG. 4 shows a typical response packet from the lab server 112 to all clients 118 to update two of their user interface components: a graph and message board display with a value of 45.4 and a message in message section 456 which reads, "your command has been successfully performed."

Two main functions may be performed by the lab server: broadcast data from the physical processes 110; and perform clients' requests and general associated responses. To keep clients 118 up to date with the current states of the physical processes 110, the lab server 112 can broadcast information that is directly collected from the physical processes 110. Data from the physical processes 110 that are encoded in the DNP packet are transmitted to connections server 114 for distribution. The connections server can then look at the overhead section of the transmitted DNP packet and forward the packet to appropriate destinations. Details on the routing algorithm in the connections server are discussed below.

Sensors, detectors and other measurement instruments detect and/or measure various physical phenomena (i.e. electric fields, electromagnetic radiation, temperature, pressure, etc.), and send this information to the lab server 112. The lab server 112 that has established network connection to the connections server 114 can then put the received information or its computed analysis into the instruction section of the DNP packet. This process can be repeated if more than one instruction is needed to be sent. Once all the instructions have been written in the instruction section of the DNP packet, the corresponding overhead sections can also be constructed. Once the DNP packet is complete, it can then be sent to the connections server 114.

Directing attention to FIG. 5, the lab server 112 can broadcast the raw data from physical processes 110 for calculating results based on computational analysis of the raw data. In some cases, data from the physical process 110 are analyzed for the purposes of

Dropbox Exhibit 1002 - Page 288
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

scientific visualization, statistical analysis or data compression. For example, raw video data from the physical process are analyzed for both spatial and temporal redundancy. After performing a compression algorithm, the compressed format of the video data is written to the instruction section of the DNP packet. Video compression that is suitable for this application is described below. For the clients to receive a continuous update of information the entire process in FIG. 5 can be repeated on a periodic basis. The repetition period of this process can be adjusted according to a particular application. At step 502 the lab server 112 gets data from the physical process 110. Control may proceed to optional step 504, where the lab server 112 performs computational analysis. Control proceeds to step 506 where a look-up data type table is constructed. Control proceeds to step 508 where data is written in the instruction sections of the DNP packet. This may be part of an iterative loop where control returns to step 502. Control may also proceed from step 508 to step 510 where the DNP packet is written to the overhead section. Control continues to step 512 where the DNP packet is sent to the connections server 114.

Another function of the lab server 112 is to process clients' requests and generate associated responses. The lab server 112 can receive a DNP packet from the connections server 114 that contains the clients' requests for instructions. It is the responsibility of the lab server 112 to interpret these instructions, execute the commands and generate responses. This process is described in FIG. 6. Control begins at step 520 where the lab server 112 waits for the DNP packet to be received from the connections server 114. Proceeding to step 522, the overhead section of the DNP packet is read. Control continues to step 524, where one instruction in the instructions section of the DNP packet is read. Control proceeds to step 526, where the lab server 112 executes the request/instruction by calling equipment/instruction drivers. Control proceeds to step 528, where the lab server 112 writes

Dropbox Exhibit 1002 - Page 289
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

response data in the instruction section of the DNP packet. From step 528, control may return to step 524 in an iterative loop according to the number of instructions; control may also proceed to step 530, where the DNP packet is written to the overhead section. Control proceeds to step 532, where a response DNP packet is sent to the connections server 114.

Execution of a client's requests may involve calling particular software drivers that send the commands to instruments via the associated computer interface such as GPIB, RS-232, USB, ethernet, etc. The request may also contain instructions for information management such as recording the client's request, storing collected values from instruments, and querying previously collected information. In the case of information management, the lab server 112 can interact directly with local or remote database servers through standard database drivers such as ODBC or JDCB.

Unlike the broadcasting functions that may continuously send DNP packets to clients, this function of the lab server 112 only generates responses when client requests are received. When the lab server 112 is implemented in a software program, this function may be run in a separate thread for parallel processing with other functions.

The connections server 114 can be run in the same computer where the lab server 112 resides. For additional reliability, in the preferred embodiment the connections server 114 may be executed in a separate computer. The connections server 114 may be implemented using object oriented, network-enable and multi-threaded software development environments such as JAVA or C++. Two of the main functions performed by the connections server 114 include: monitoring and maintaining reliable network connections with all active clients and lab servers; and routing DNP packets to appropriate destinations.

The connections server 114 maintains network connections with all the processes, namely: lab server 112, database server 120, and clients 118. A connection handler, which

Dropbox Exhibit 1002 - Page 290
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

may be a class or object in object-oriented programming terminology, can perform readings from and writing to each of the connections. Each connection handler should be run in a separate thread for parallel processing. Once the connections server 114 accepts or establishes a connection, it can then pass the connection information (i.e. the socket information that contains remote post address and remote port number) to the connection handler for further processing. The connections server 114 maintains an array or table of connection handlers, namely the connection table, to perform and monitor network related processes. A connection monitor is another important process included in the connections server 114 that runs on a periodic basis. The connection monitor may be implemented as a subclass of the connections server 114 and may be executed in a separate thread. A function of the connection monitor is to monitor and control the network communications of the processes (i.e. clients 118 and lab server 112) connected to the connections server.

FIG. 7 illustrates the basic operation of the connection monitor. Beginning at step 550, the connection monitor searches for clients in the connection table. Proceeding to decision step 552, if a client is found in the connection table, control proceeds to step 554 where the connection monitor checks the validity of the current session. This operation is normally done by consulting the database server 120 to check whether the current clients have access to the physical process 110. If a client is not found, control proceeds from decision step 552 to 556, where the connection monitor instructs all connection handlers to close their connections. Returning to step 554, control proceeds to decision step 558. If the session is valid, control proceeds to step 560; otherwise control returns to step 556. At step 560, the connection monitor searches for a lab server 112 in the connection table. Control proceeds to decision step 562, where, if a lab server is found, the program terminates. Otherwise, control proceeds to step 564, where the connection monitor establishes a

Dropbox Exhibit 1002 - Page 291
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

connection with a lab server 112. As shown in FIG. 7, the operation of checking whether a lab server 112 is connected is performed in a loop, since there may be more than one lab server 112 contacted for backup purposes. If a failure in the system or device at the physical process 110 occurs, the lab server 112 that is physically connected to the physical process 110 would refuse any connection requests from the connection server. Thus, the connection monitor attempts to establish connection with another lab server 112. The entire operation in FIG. 7 should be performed periodically to continuously monitor the communication process.

The connections server serves as the distributor of data that accepts, verifies and routs DNP packets to appropriate destinations. The connections server supports full duplex point-to-point and point-to-multipoints data transmissions based on the destination ID field of the DNP packet. As a result, both clients 118 and lab server 112 processes may synchronously receive events that are generated by any processes. FIG. 8 displays several routing modes that may be performed by the connections server. FIG. 8 is an example case of three clients and a lab server connected to the connections server. The maximum number of clients that may be served varies according to the available network bandwidth.

As discussed above, the connection handler is part of the connections server and may perform reading from and writing to each connection. The connections server 114 listens to any connection request, and passes the network information to the connection handler once a valid connection is established. FIG. 9 shows the flow diagram of the connection handler. Beginning at step 600, the connection handler receives network information from an accepted connection from the connections server. Control proceeds to step 602, where the connection handler checks to see if the connection is valid. If the connection is not valid (decision step 604), control proceeds to step 606, where the connection handler closes the connection and control terminates. However, if the connection is valid, control proceeds to step 608, where

Dropbox Exhibit 1002 - Page 292
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

the connection handler waits and listens for incoming DNP packets for a certain time-out period. From step 608, control proceeds to decision step 610. At decision step 610, if a DNP packet is received before the time-out, control proceeds to step 612, where the overhead section of the DNP packet is read. However, if a DNP packet is not received before the time-out, control returns to step 602. From step 612, control proceeds to step 614, where again the connection handler attempts to validate the connection. If the connection is not valid (decision step 616), control returns to step 606. However, if the connection is valid, control proceeds to step 618, where the rest of the DNP packet is read according to its packet length. Control then proceeds to step 620, where connection handlers in the connection table are found based on the destination ID in the DNP overhead section. Control then proceeds to step 622, where all DNP packets are sent to all destinations via the connection handlers found in the connection table. From step 622 control returns to step 602. The operations described above are repeated until the connection is no longer valid.

Client processes provide a graphical user interface for the end users of the physical process 110. The clients may be implemented in any object-oriented and network-enabled software development environment such as C++ or JAVA. The client should contain graphical components that may be used for getting user inputs and/or display information. Some of the components may include dials, graphs, switches, LED displays, buttons, etc.

The client process 118 may be executed from any computer that is connected to a TCP/IP network such as the internet. When the client process is run, it will first attempt to establish network connections to the connections server 114. User requests/commands that are received from the UI components are encoded into DNP packets to be sent to the connections server 114. The client 118 may also process DNP packets from other remote clients and lab servers 112 that are received via the connections server 114. This operation

Dropbox Exhibit 1002 - Page 293
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

may also be executed in a separate thread for parallel processing.

FIG. 10 is a flow diagram of a client DNP packet processing. The client process 118 normally executes the instructions in a DNP packet by calling functions or methods of its UI components. The instructions may involve updating the graph display, turning a dial, decoding and displaying video data, etc. By receiving live events from physical processes 110 and other client processes, the user may experience an interactive and collaborative environment in controlling remote physical processes. Beginning at step 624, the client waits for DNP packets from the connections server 114. Control then proceeds to step 626, where the DNP packet's overhead section is read. Control then proceeds to step 628, where one instruction in the instruction section of the DNP packet is read. Control then proceeds to step 629, where the request/instruction is executed by calling the functions of the user interface components. From step 629, control may return to step 628 in a loop that repeats according to the number of instructions.

The database server 120 manages a database containing information that is essential to the operation of other processes. The remote operation of the database server 120 can be facilitated using database application programming interface standards such as ODDC or JDDC. The database server 120 manages the following list of information: user information, user physical process data, scheduling information, and event data.

The database server 120 manages user profiles. A user profile contains user accessed information such as log-in name and password that enables the connections server 114 to verify connection requests from the clients 118. In addition, the user profile also includes the client's progress information by tracking the status of accomplished actions/requests. Data from the physical processes 118 (i.e. sensor readings, states of equipment, etc.) may also be recorded on behalf of a client's request. This data be time stamped and may be made

Dropbox Exhibit 1002 - Page 294
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

available to the user via an interactive "laboratory notebook" user interface. Using a common gateway interface (CGI) or JAVA servlet program that may interact with the database server 120, clients may search and retrieve previously recorded physical process data. The search may be based on chronological order, keyword, or other characteristics of the recorded data. Scheduling information ensures that only the appropriate clients are given access to the physical processes 110 in a certain time period. Every event received by the lab server may also be automatically recorded. This data may be used to analyze clients' behavior and usage patterns in controlling the physical process 110. The interactive laboratory notebook may also contain lab parameters, "to do" lists, and personal notes.

The interactive laboratory notebook is part of a user interface that may be constructed using Interface Builder or similar software application, and may be accessed by users during the course of an experiment. The interactive laboratory notebook may be implemented to include a database stored on a hard disk or other nonvolatile memory of computer 60, as well as a user interface to access the database. Where the present invention is utilized for distance learning, the interactive laboratory notebook provides a central repository for information and is an essential tool for instructors to evaluate the progress and performance of students using the online laboratory.

The user interface may include animated switches, dials, buttons, and LED displays rather than traditional browser forms. Online graphing of the real time data along with other customized user interface components allows users to experience a hands-on look and feel. The user interface may closely resemble the front panels of the actual instruments in functionality, layout, and appearance. The live video stream may also be included in the user interface.

Dropbox Exhibit 1002 - Page 295
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Real Time Video Observation

Observing physical processes in real time via the internet is a key feature of the present invention. Returning to FIG. 1B, video camera 70 is used to acquire live images from a system that the user interacts with and whose actions affect the observed video. Video capture (or frame grabber) hardware 72 is used on a computer to capture images desired to be sent to the user with minimum latency. A video server computer 74 compresses new image data and forms packets to be transmitted to the user (client) through the computer network 50. The client, using a standard browser, is able to view the live video and interact with the system. In order to transmit video via the internet in real time, spatial and temporal compression is performed. In spatial compression, the acquired image from frame grabber 72 is represented as gray-scale or as a color image in terms of hue, saturation, and value (HSV). In both cases values are represented as integers. The image data is divided into square blocks (8x8 pixels or 16x16 pixels, for example). A two-dimensional discrete cosine transform (a standard mathematical operation often abbreviated as DCT) is performed on each block.

To perform temporal compression, the server 74 subtracts the ideal DCT data from the DCT data that the client currently holds. This difference in DCT data is the information that the client must receive in order to allow its video to be updated to the desired image. This compression uses a single new frame to calculate data to be sent. This sacrifices compression efficiency (i.e. that obtained using the MPEG4 standard) in order to minimize latency. An approximation to this difference is calculated which meets the requirements of the specified fixed packet size (specified in bits). By basing compression on a specified packet size, compressed video matches transmission limitations of the client 110. The data rate (PACKET_SIZE * PACKETS_PER_SECOND) that is used for a particular client is dynamically determined and updated as video is sent. This allows the quality of video that is

Dropbox Exhibit 1002 - Page 296
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

sent to a client to vary according to the abilities of each client's internet connection. This also allows the data rate to vary in response to changes in a client's allowable data rate. By having the client intermittently inform the server of the times that it received transmitted packets, the latency and allowable data rate of the client may be calculated.

FIG. 11 shows the two-dimensional set of DCT components. Component 0 is in the upper left corner, and the path of the arrow shows the order that each component is enumerated. DCT components are transmitted in groups of components (i.e. eight groups of eight components). Not all groups of DCT components are transmitted in a single packet. Groups of "difference in DCT data" are chosen to be sent based on the magnitude of the components in the group. In eight SV images, the eye is more sensitive to differences in value than to differences in hue or saturation. Thus a relative weight is used in comparing the magnitudes of groups or of a different type. Data is transmitted with rounding in order to use fewer bits to transmit an approximation of the data. The video compression system has been optimized to minimize response time (latency). This priority is unique for a system that depends on the user promptly receiving video feedback in response to his actions.

FIG. 12 illustrates the encoding process performed by the server 74. Beginning at step 630, the current DCT data for the client is initialized to zero. Control proceeds to step 632, where, if this is the first packet being transmitted, then initialization information is placed at the beginning of the packet. This initialization information includes: width of display, height of display and type of display (gray-scale or HSV). Control proceeds to step 634, where an image is acquired using video camera 70 and frame grabber 72. At step 636, image data is divided into square blocks (8x8 pixels or 16x16 pixels). At step 638 a two-dimensional discrete cosine transform is performed on each block. This produces the ideal DCT data which corresponds to an image with minimal error. At step 640, the difference

Dropbox Exhibit 1002 - Page 297
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

between ideal DCT data and the DCT data that the client is currently using is calculated. This produces "difference in DCT data". At step 642 groups of "difference in DCT data" are chosen to be sent based on the magnitude of the components in the group. In HSV images, the eye is more sensitive to differences in value than to differences in hue or saturation. Thus a relative weight is used in comparing the magnitudes of groups that are of a different type. At step 644 an approximation to the data in these groups is stored in a packet which is then transmitted over the network through a socket connection with the client. Control proceeds to step 648, where the "approximated difference in DCT data" that the client will decode is then calculated by the server 74. At step 650, this difference is then added to the client's DCT data that the server 74 keeps a record of. By keeping track of the client's current data, the error caused by approximation does not propagate as multiple transmissions are sent. Control may then return to step 632 in order to produce another packet to be sent to the client.

FIG. 13 illustrates the structure of the decoding process performed by the client. Beginning at step 652, the current DCT data is initialized to zero. At step 654 a socket connection is used to receive a packet from the server 74. At step 656, if this is the first packet received, initialization information is processed. This initialization information includes: width of display, height of display and type of display (gray-scale or HSV). At step 658, the packet is decoded to produce the approximated difference in DCT data. At step 660, by adding this difference back to the current DCT data, the updated value for the current DCT data is determined. Control proceeds to step 662, where the inverse discrete cosine transform is then used to convert DCT data into image data. This transformation is only performed on blocks that have been modified by the approximated difference in DCT data. This allows the image data to be updated with no buffering, and thus the delay in updating the image is minimized. Control proceeds to step 664, where the image date is displayed to the

Dropbox Exhibit 1002 - Page 298
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

user through a standard browser. Control may then return to step 654 in order to process an additional updated image sent from the server 74.

The instructions described above as well as the user interface and interactive laboratory notebook may be implemented in software and stored in the computer 60 and executed in accordance with the preferred embodiment of the present invention.

While the description above explains the operation of a laser and optical equipment, it is to be understood that a wide variety of physical processes may be performed using the present invention, and other forms of data may be recorded such as time, temperature, voltage, current, magnetic field, electromagnetic radiation, and the like. Additional applications of the present invention may extend to entertainment, for example the remote control of toys in an interactive setting, where multiple users may access computer 60 via the computer network 50 and play games involving multiple users. The real time video taught by the present invention is an integral part of such an application.

In other applications of the present invention, computer 60 and camera 70 may be utilized as a sales or development tool to demonstrate equipment or processes to prospective clients, customers, or developers by providing a demonstration of the equipment or processes in real time and eliminating the expenditure of resources required to travel to a location where the equipment or processes are located.

In embodiments of the present invention where video recording is to be performed in accordance with the present invention, two types of equipment are needed to record audio and video signals transmitted from a programming source: a tuning device capable of tuning/separating television channel among designated frequency bands, and a recording device capable of storing analog video/audio signal on recording media such as magnetic tapes, magnetic disks or optical disks. Many recording devices such as VCRs are equipped

Dropbox Exhibit 1002 - Page 299
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

with built-in television tuners. In this case, the process of recording television programs can be accomplished by manipulating a single piece of equipment. For recording devices that do not have built-in television tuners, broadcast television signal must be processed by tuning a particular television channel and converting such channel into video and audio signal prior to recording. In this case, the process of recording television programs can be accomplished by manipulating both television receiver 1010 and recording device 1012. Most television receivers are equipped with a built-in tuner, however in some cases a set-top box 1014 such as cable box or satellite receiver is used instead of a conventional tuner not only to tune television channels but also to decode paid programs such as premium channels, pay-per-view channels, etc. Programming is broadcast by a programming provider 1028.

TV receiver 1010, recording device 1012 and set-top box 1014 are often equipped with infrared sensors that allow remote control from infrared transmitting devices operated within effective distance. Most remote control units emit infrared signal with a certain modulation method and carrier frequency to transmit digital commands for operating such devices. The methods used to demodulate such infrared signals vary by manufacturer. Many equipment manufacturers use conventional digital modulation methods such as on-off shift keying, pulse length modulation, etc. with carrier frequencies ranging from 20-60 kHz. By using a diode detector, such signals can be learned and stored in a conventional memory. Video/audio recording equipment is controlled by transmitting a sequence of stored commands using infrared emitting diode 1016 in the remote control unit 1018. FIG. 15 shows the preferred embodiment of remote control unit used in the present invention. The remote control unit 18 is connected to a computer 1020 via standard I/O connection 1022 such as RS-232, USB, etc. Computer 1020 is a conventional computer such as a workstation, desktop or laptop personal computer, or personal digital assistant (PDA), which includes a

Dropbox Exhibit 1002 - Page 300
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

microprocessor and supporting circuitry, memory, and communications circuitry. Remote control unit 1018 includes a microprocessor 1024 and circuitry to control infrared diode 1016 to emit infrared commands that are stored in memory 1026. The microprocessor can control the transmission of such commands to emulate a particular sequence of commands to record TV programs that is conventionally performed by users operating the recording equipment 1012. Using the computer connection 1022, the microprocessor 1024 also executes the process of downloading information pertaining to user selections to be recorded. Such information may include start time, end time and channel number of selected television programs can be stored in memory 1026. Furthermore, the remote control unit may contain an internal clock 1030. Microprocessor 1024 can monitor and check the selected television programs stored in memory 1026 with the clock 1030 to start and stop the recording process.

In an alternative embodiment of the remote control unit 1018, the clock 1030 and/or memory 1026 can be excluded. In this case, the transmission of infrared signal from remote control unit 1018 is controlled using microprocessor, memory and clock of computer 1020. In this alternative embodiment the remote control unit 1018 and computer 1020 stay connected during the process of recording television programs.

In another alternative embodiment of the present invention, means for controlling the recording device 1012 and accessing an online-based application service provider 1032 can be built internal to the recording device 1012. In this case, recording device 1012 incorporates microprocessor 1024, memory 1026, clock 1030, modem 1034 and client software 1038 can be controlled through electronics means without any external device such as the remote control unit and computer.

Computer 1020 can include an application program such as Client Software 1038 executed by computer 1020 to receive user-selected TV scheduling information from the

Dropbox Exhibit 1002 - Page 301
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Application Service Provider 1032 and transmit such information to remote control unit 1018. As shown in Fig. 1, Computer 1020 is connected to a computer network 1040 such as a wide area network or public, global network such as the Internet. Computer 1020 also includes a modem or network interface unit to facilitate communication via network 1040. During start-up, Client Software 1038 establishes an IP (Internet Protocol) based network connection to the Control Server 1042 located at the Application Service Provider 1032 site. It is recommended that Transmission Control Protocol (TCP) is used to implement such a network connection due to its reliability and connection-based properties. During initialization of the network connection, the Client Software also transmits authentication information such as user id and/or password to allow the Control Server 1042 to identify and verify the designated user account stored in the database 1044. Once the Control Server 1042 has authenticated and verified the connection request, it checks the user account in the database 1044 for the selected TV programs to be transmitted to the Client Software 1038. Control Server 1042 may indicate the state of network connection to the Client Software 1038 or record the status in the database 1044. The Information Server 1050 can receive new television information updates over the Internet. The Information Server 1050 searches the database 44 to find an appropriate Control Server 1042 that maintains a valid connection with a Client Software 38, and instructs the Control Server 1042 to transmit such information to the Client Software 38. After the initialization of the network connection, the Client Software 38 waits for information updates of user selections transmitted by the Control Server 1042. Whenever the information updates are received from the Control Server 1042, the Client Software 38 transmits such information to the remote control unit 18 to be stored in the memory 26. Once the selected television programs are stored in the memory 26 of the remote control unit 18, the microprocessor 24 then compares the selected television programs

Dropbox Exhibit 1002 - Page 302
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

with the clock 30 to start and stop the recording process. A certain time delay may also be added before the start of the recording to skip preliminary section of the program. By connecting remote control unit 18 with a computer 20 that executes the Client Software 38, audio/video recording equipment can be operated from a wide area network such as the Internet.

In the case where there is no line of sight between the remote control unit and the recording equipment, such as the case where computer 20 and remote control device 18 are located in different rooms, communication between the remote control unit and a computer can be performed using radio frequency (RF) transmitter 21 and receiver 23, as shown in Fig. 3.

Commands in the form of digital information can be encoded and modulated using RF frequency, which in turn is received and decoded by an RF receiver to be passed to the remote control unit 18 for controlling the audio/video recording equipment. A physical connection between the controlling computer (Computer 2) to either remote control unit 18 (Fig. 1) or RF transmitter (Fig. 3) may be facilitated using standard computer I/O connection such as RS-232, USB, and the like.

INTERNET-BASED SERVICE MODEL

The goals of the service model of the present invention proposed system are to simplify the process of recording TV programs using existing audio/video recording equipment through an Internet-based user interface. Using standard web browser programs such as. Netscape Navigator or Microsoft Internet Explorer, users can browse, search and select television programs to be recorded. In turn, the system will automatically obtain information about the selected television programs (such as start times, end times and channel

Dropbox Exhibit 1002 - Page 303
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

numbers), and send such information to the remote control unit 18 that operates the audio/video recording equipment.

Another goal of the service model of the present invention is to provide global access to audio/video equipment. Users can operate audio/video equipment from virtually anywhere through the Internet.

Yet another goal of the service model is to guide users in selecting TV programs by providing suggestions based on analysis of user preferences and viewing history.

In the preferred embodiment of the invention as shown in Fig. 1, a user operates computer 36 to access the Internet-based Application service provider 32. Computer 36 is a device that has a central processing unit, memory and communication means to access a wide area network such as the Internet. Computer 36 can be in the form of desktop, lap top or palm top devices that have the appropriate web browser software 48 installed in their memories. For widest access and compatibility, it is recommended that both Computer 36 and Information Server 1050 use a standard and widely adopted network protocol such as TCP/IP. In the preferred embodiment, the HTTP protocol is chosen to facilitate network communication between Computer 36 and Information Server 1050. In the preferred embodiment, Information Server 1050 is an HTTP compliant server and Computer 36 is a conventional computer with a standard web-browser software such as Netscape Navigator or Microsoft Internet Explorer. Although Computer 36 and Computer 20 are two separate computers 20, 36 as shown in FIG. 1, it is important to realize that the two functions served by Computers 20,36 can be accomplished by a single computer having same components as both Computer 20, 36. The embodiment in FIG. 14 highlights the feature in which the recording equipment can be globally accessed and controlled over the Internet.

Database 44 is connected to the Information Server 1050, facilitated by workstation or

Dropbox Exhibit 1002 - Page 304
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Local Area Network at the Application Service Provider 32 site. The database 44 may serve as a data center to manage information regarding user accounts, television schedule information, and operation of the system. New users are required to register with the Application Service Provider 32. Using HTML forms, a user from Computer 36 can submit registration data to be processed by the Information Server 1050. Information provided by the user for proper operation of recording equipments includes the authentication information, equipment and connectivity identification, and programming source. Other information about the user such as email, telephone and/or fax may also be stored in the user account, hence the user may receive information such as selected television programs, reminders and other information regarding television program recordings via email, telephone and/or fax.

Upon receiving the above registration information from a user, the Information Server 1050 stores the registration information in the database 44 on behalf of the user in her/his individual user account. Once the registration process is complete, the user then selects television programs to be recorded. The Information Server 1050 serves HTML pages containing textual and graphical information regarding TV programming schedules stored in the database 44. To serve the HTML-pages, the Information Server 1050 executes computer programs in the forms of Java Servlet or Common Gateway Interface (CGI) to search the database and display television programming schedules. A user can view and select television programming schedules that are displayed based on her/his preferences such as: viewing dates, topics, actors, show genres, reviews, etc. The Information Server 1050 formats the retrieved television information into HTML pages that allow users to select TV programs to be recorded. The television schedule information may be displayed in spreadsheet forms having the axes time versus channels. For devices that only have a single

Dropbox Exhibit 1002 - Page 305
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

television tuner, a spreadsheet user interface may be used in the following applications.

Whenever a user select a valid or non-conflicting television program, the interface disables the selection options for all conflicting television programs that are broadcast during the same time period. This method forces the user to deselect the current selection in order to select another program in the same scheduled time period. Whenever a user select a television program, the interface deselects all selected television programs that have conflicting viewing schedules.

Once the user submits his/her television program selections to the Information Server 1050, the information is stored in her/his account in the database 44. Also stored in his/her account is information regarding the status of network connection between the Client Software 38 and Control Server 1042. Whenever a Client Software 38 establishes or terminates network connection with the Control Server 1042, the events are noted in the user account to track the status of the network connection. Upon receiving the user selections, Information Server 1050 accesses the user-account to check whether a valid network connection has been established between the Client Software 38 and Control Server 1042. If a valid connection is found, the Information Server 1050 notifies the appropriate Control Server 1042 via Local Area Network that new user selections have been received and stored in the database 44 on behalf of the user. Upon receiving the notification from the Information Server 1050, the Control Server 1042 may also access the database 44 via Local Area Network to retrieve user-selected television information that has not been transmitted to Client Software 38. The Control Server 1042 then formats the retrieved information and transmits it to Client Software 38. Upon receiving the user selections, the Client Software 38 sends them to the remote control unit 18 and updates the television recording schedule information in the memory 26. Once the user selections are stored in the memory 26 of the

Dropbox Exhibit 1002 - Page 306
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

remote control unit 18, the microprocessor 24 can then compare the selected television programs with the clock 30 to start and stop the recording process.

In the preferred embodiment, Control Server 1042 is an application program executed in a conventional computer that is capable of establishing network communication with other computers using standard network protocol such as the Internet Protocol (IP). Client Software 38 executed in Computer 20 as shown in FIG. 14 can establish a persistent network connection with the Control Server 1042 through TCP-IP protocol. The Control Server 1042 is connected to the database 44 to retrieve user-selected TV program scheduling information. In the proposed system, there are at least two ways for the Control Server 1042 to initiate the process of retrieving from the database 44 the user-selected television program information and sending the information to Client Software 38.

Initiation may be based on notification from the Information Server 1050. When Information Server 1050 obtains user-specified television scheduling information to be recorded, it notifies the Control Server 1042. In turn, if network communication has been established between the Control Server 1042 and Client Software 1038, the Control Server 1042 retrieves the user selections and sends them to the Client Software 1038.

Alternatively, initiation may be based on notification from Client Software 1038. The Client Software 1038 notifies the Control Server 1042 to transmit user selections for recording. This notification would normally be sent when the Client Software 1038 initially establishes network connection with the Control Server 1042. The Control Server 1042 then retrieves user selections and sends them to Client Software 1038.

Information indicating user selections is stored in the database 1044. Such information can convey user preferences, useful in providing targeted advertising, rating of television programs, providing television program guides, suggestions, etc.

Dropbox Exhibit 1002 - Page 307
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Directing attention to Fig. 4, in an alternative embodiment, service provider 1060 can maintain recording equipment at various physical locations 1062-1, 1062-2, ...1062-n, where n can be any number. Users can contact the service provider 1060's website and select programs for recording at the various physical locations 1062. Operating the recording equipment at the locations 1062 as explained above, the service provider can provide localized recordings to its users, either by transmitting audio and video over the computer network 1040 to computers 1036, 1020, or sending the user a copy of the recording on a portable storage medium such as optical or magnetic storage.

While an apparatus, method, and service model for the remote control of recording devices via a computer network have been described in preferred embodiments, those of ordinary skill in the art will understand that many modifications maybe made thereto without changing the scope of the claims that follow. Accordingly, it is not intended that the scope of the invention in any way be limited by the above description, but instead be determined by reference to the claims that follow.

Dropbox Exhibit 1002 - Page 308
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

CLAIMS

What is claimed is:

1. An apparatus to remotely operate recording equipment to record television programs using a public wide area network such as the Internet comprising:

(a) recording equipment, said recording equipment including a controlling means for directing the recording of television programs;

(b) means for storing data associated with control signals;

(c) means for receiving information associated with programs selected by a user; for recording, said information transmitted over a computer network; and

(d) means for transmitting said data associated with control signals over said computer network to control said recording equipment.

Dropbox Exhibit 1002 - Page 309
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

SUBSTITUTE SHEET (RULE 26)

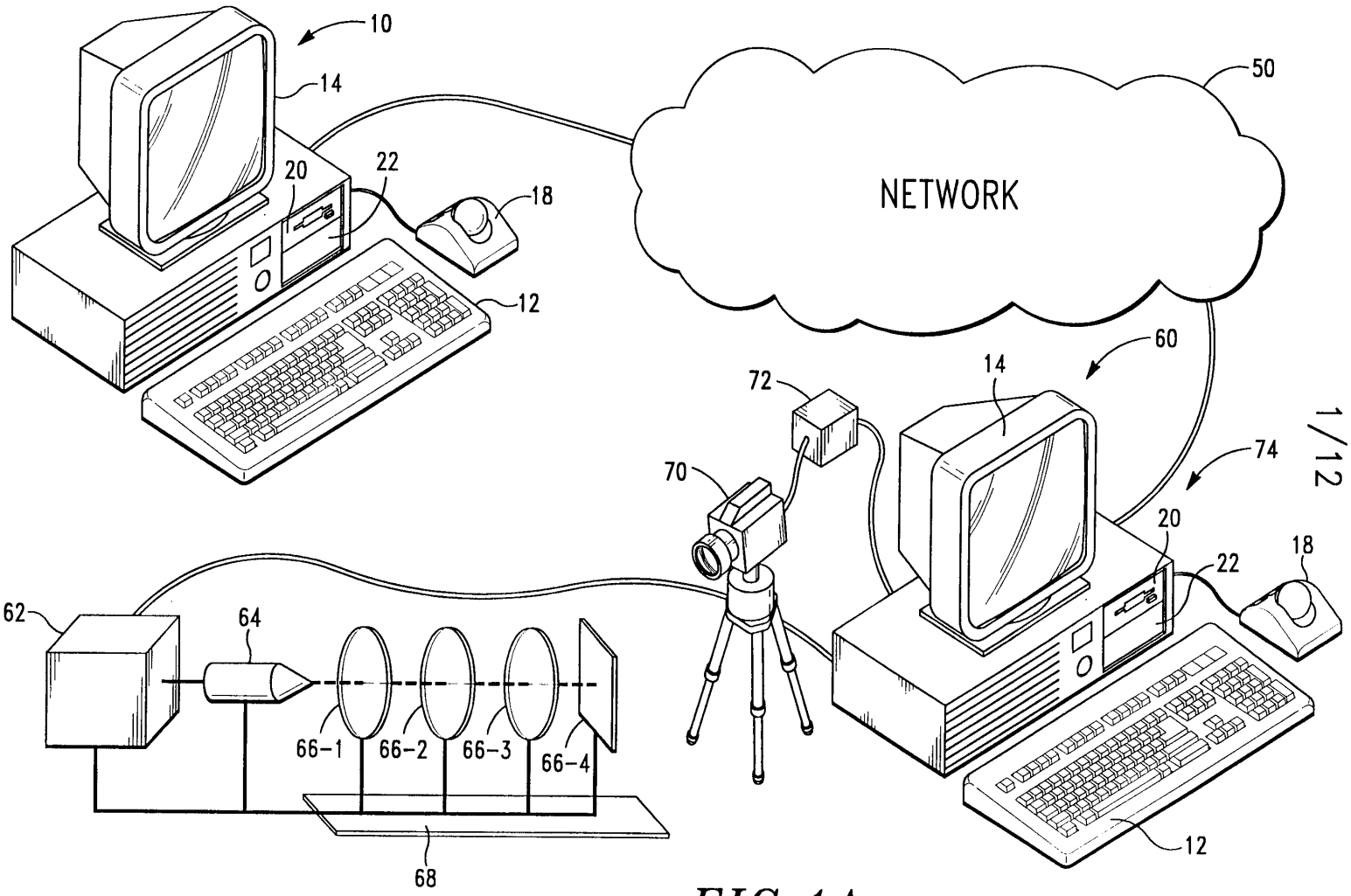


FIG. 1A

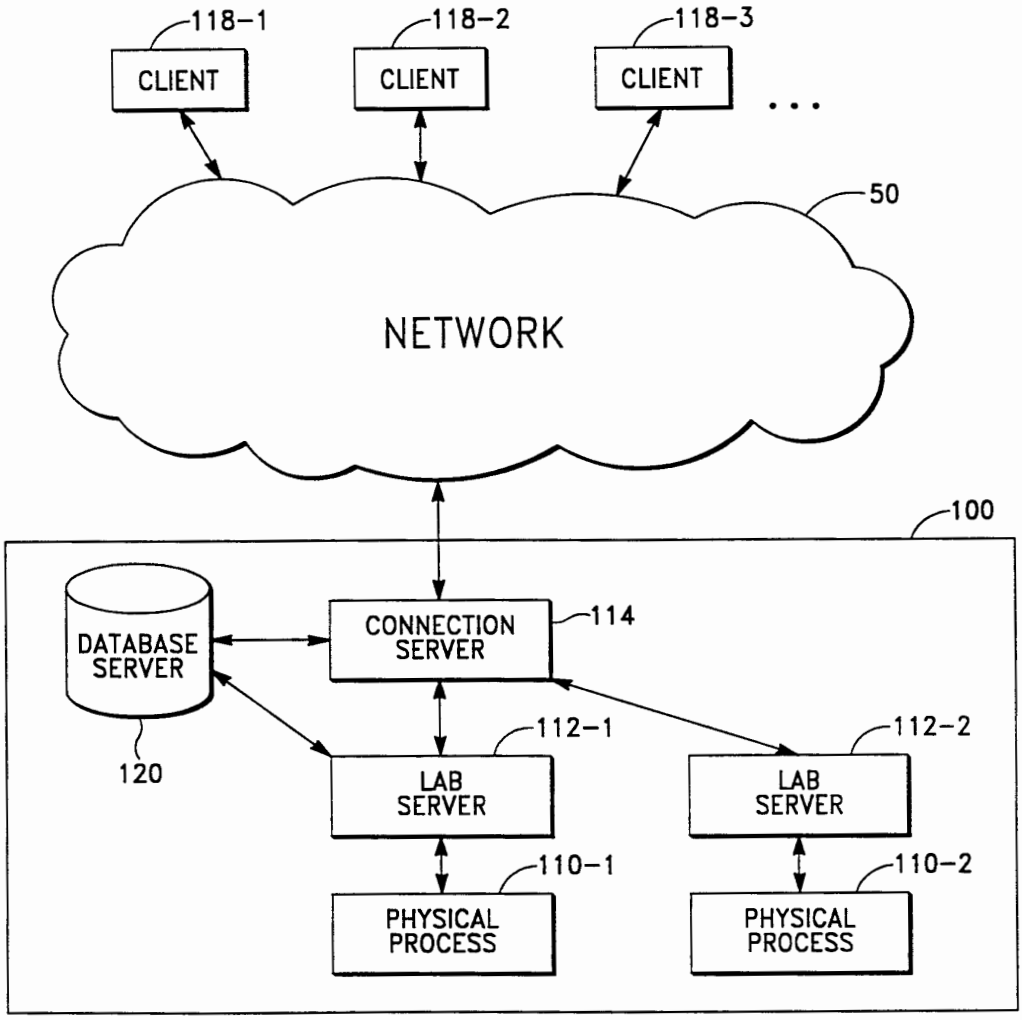


FIG. 1B

Dropbox Exhibit 1002 - Page 311
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

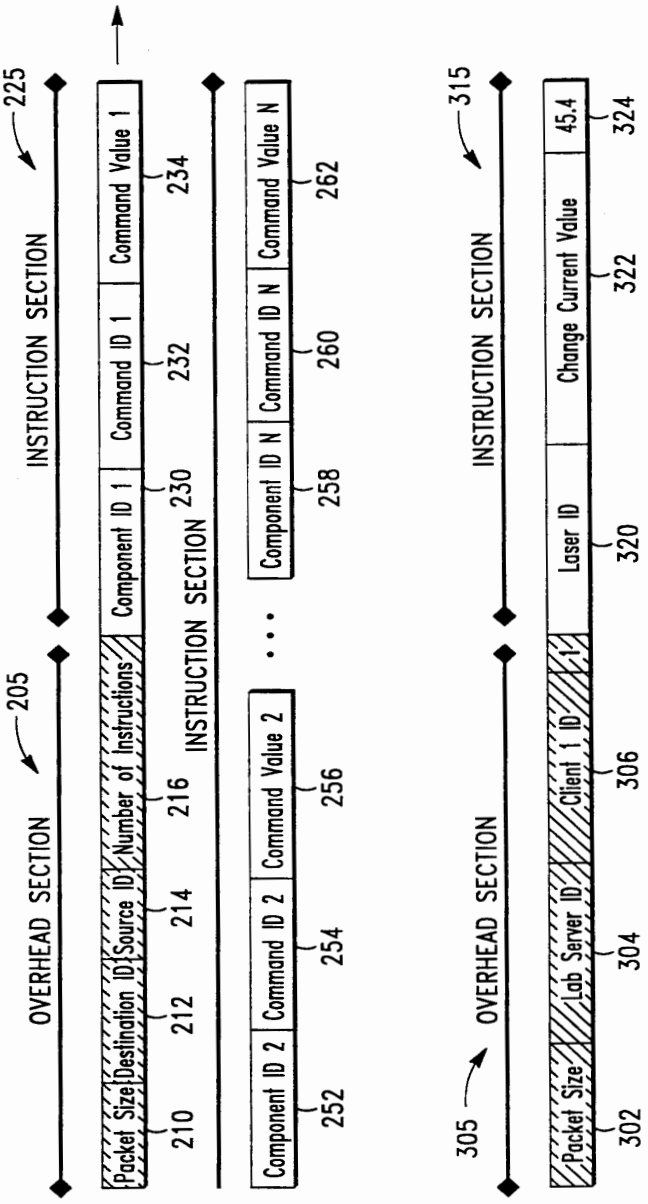


FIG.2

FIG.3

Dropbox Exhibit 1002 - Page 312
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

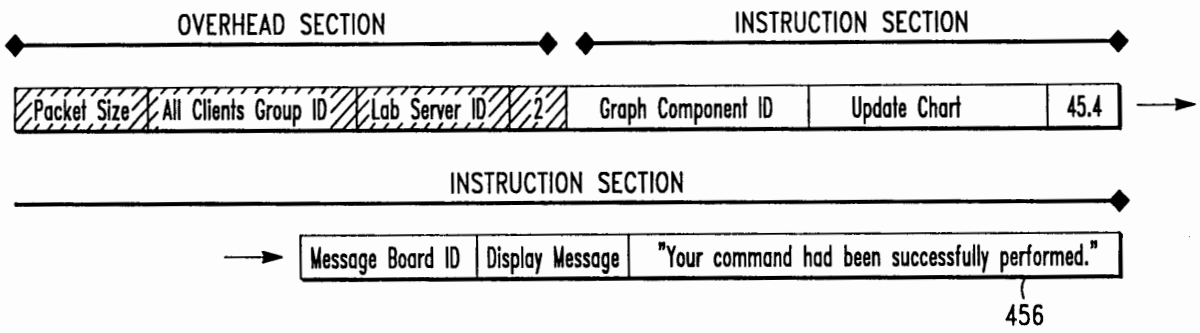


FIG.4

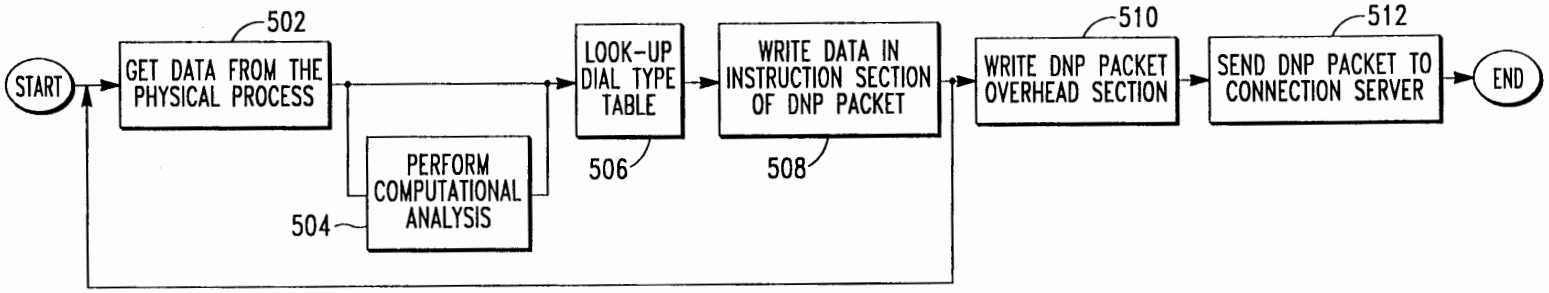


FIG.5

SUBSTITUTE SHEET (RULE 26)

Dropbox Exhibit 1002 - Page 313
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

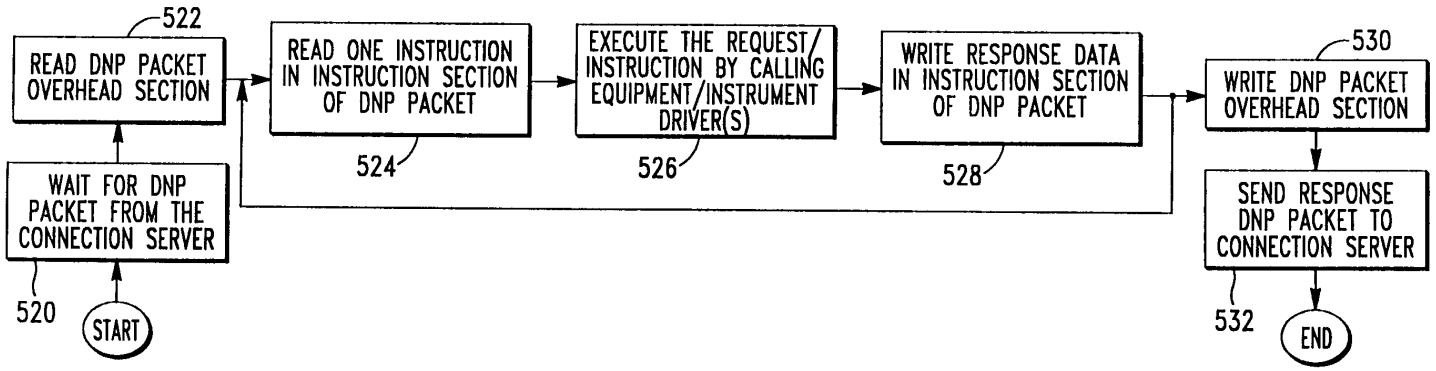


FIG.6

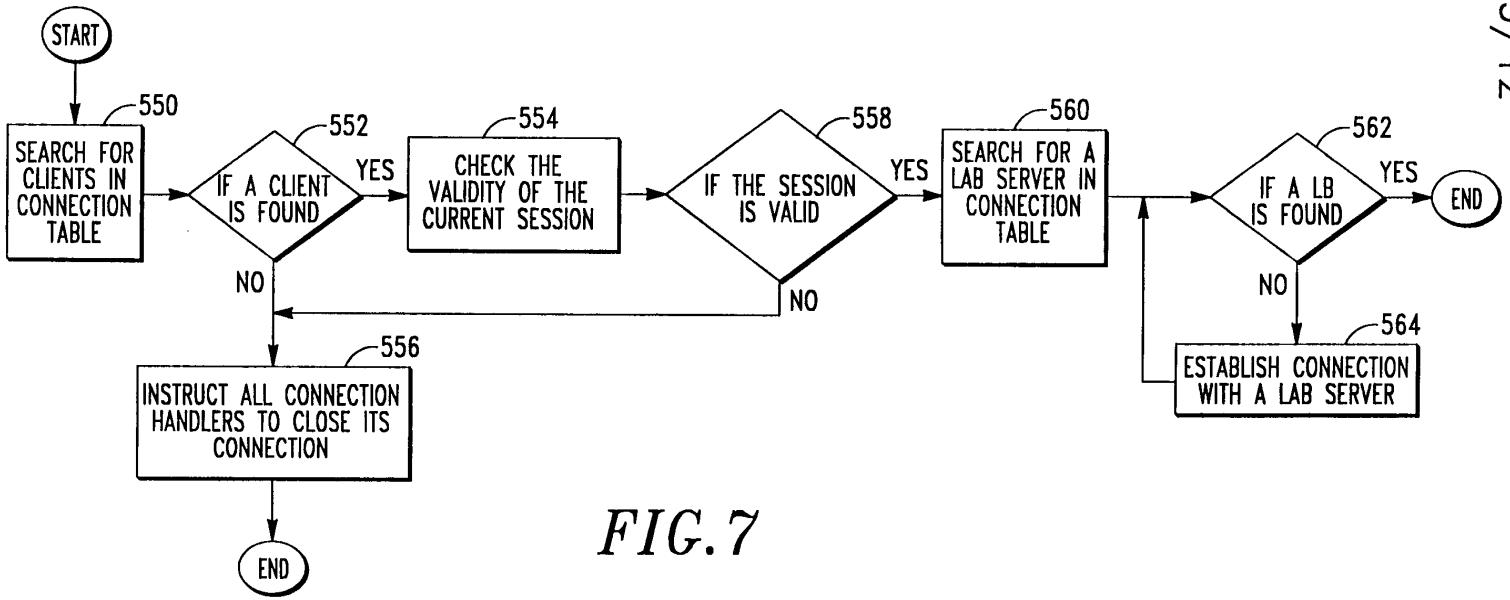


FIG.7

SUBSTITUTE SHEET (RULE 26)

Dropbox Exhibit 1002 - Page 314
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

SUBSTITUTE SHEET (RULE 26)

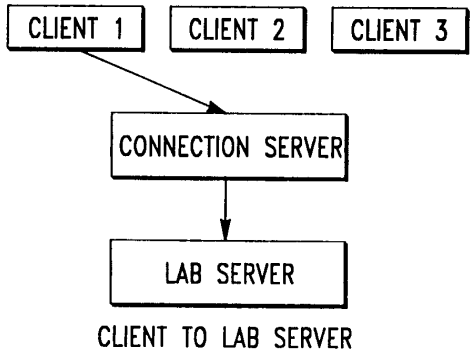


FIG.8A

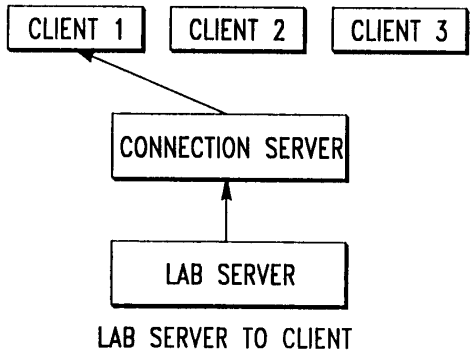


FIG.8B

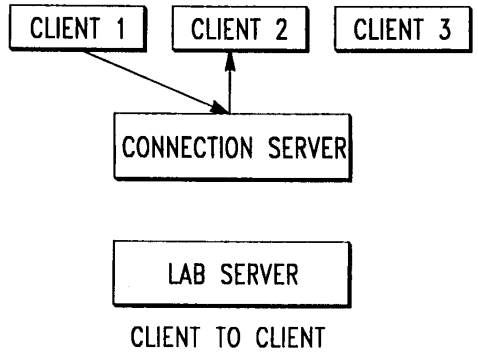


FIG.8C

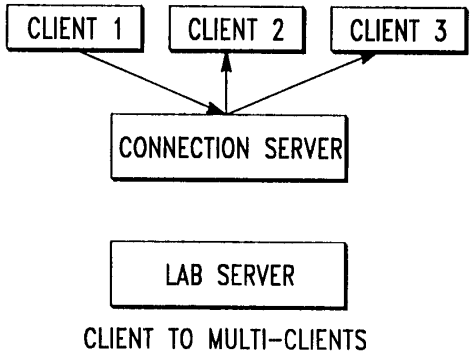


FIG.8D

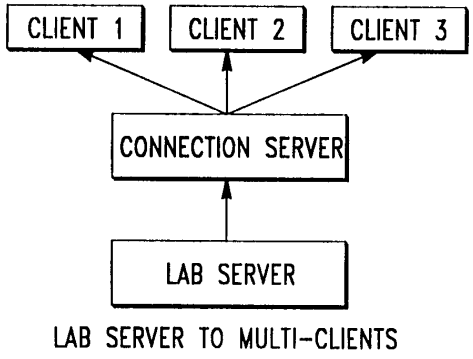


FIG.8E

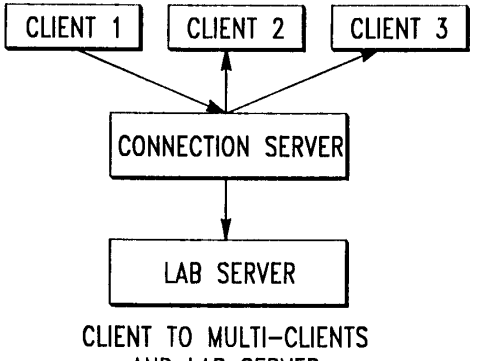


FIG.8F

Dropbox Exhibit 1002 - Page 315
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

SUBSTITUTE SHEET (RULE 26)

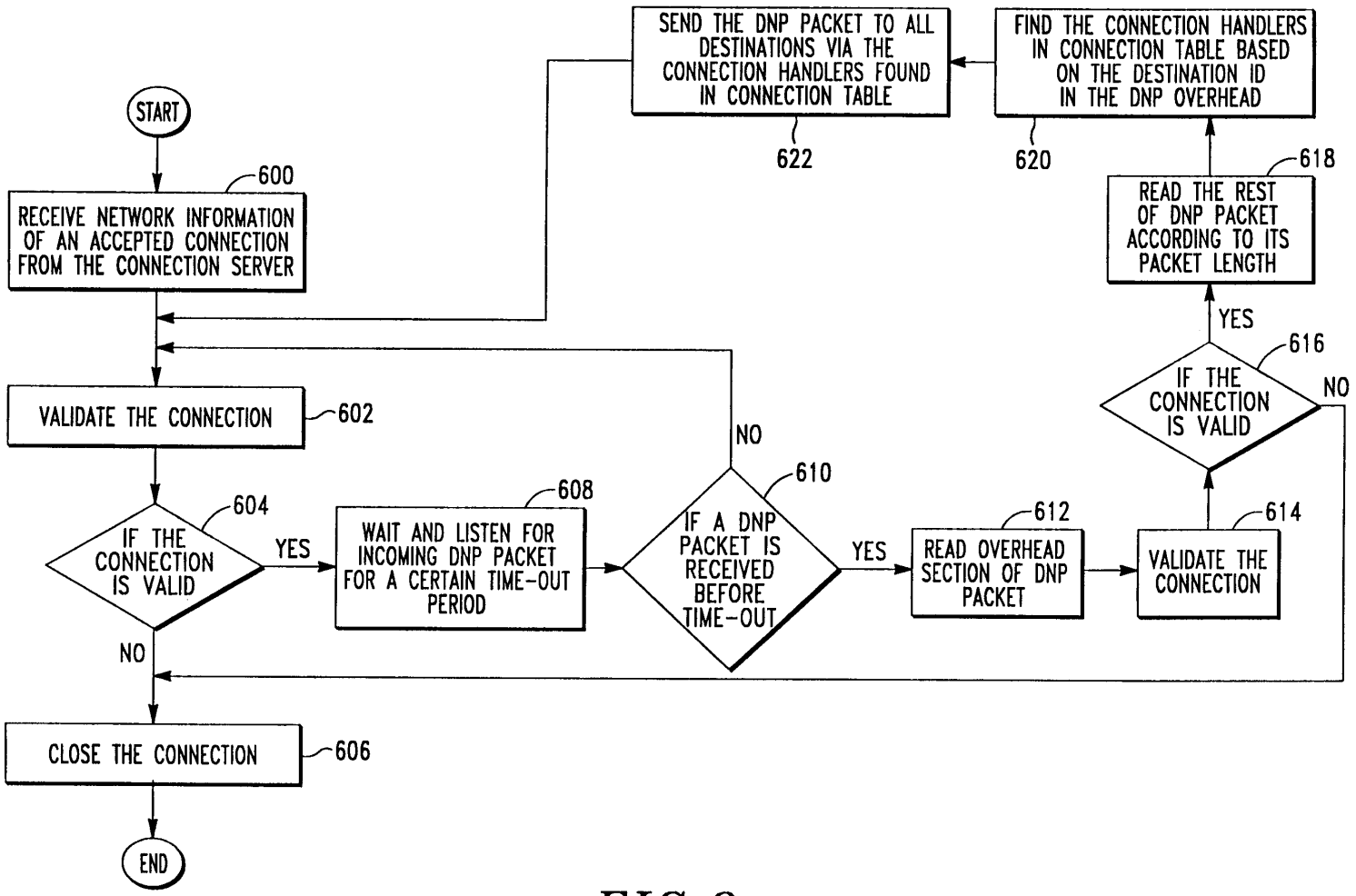


FIG. 9

Dropbox Exhibit 1002 - Page 316
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

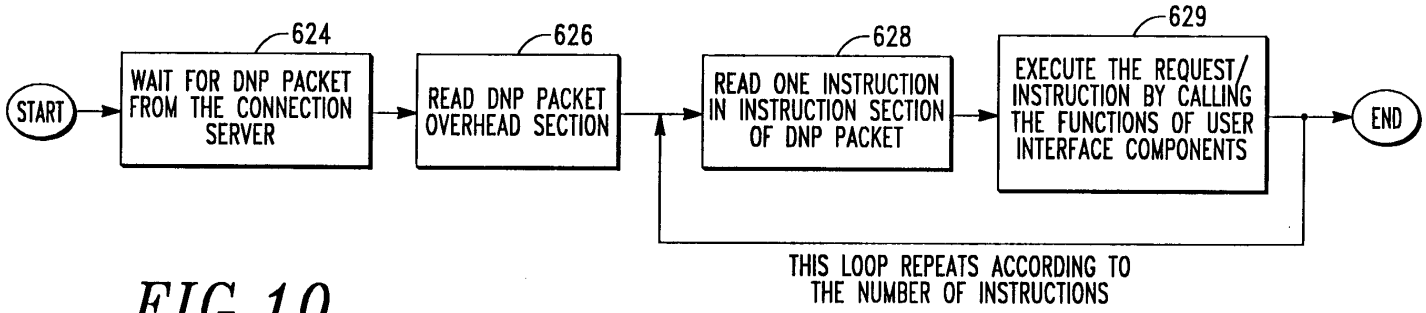


FIG. 10

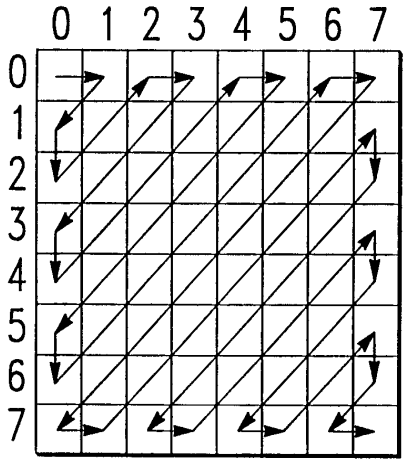


FIG. 11

Dropbox Exhibit 1002 - Page 317
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

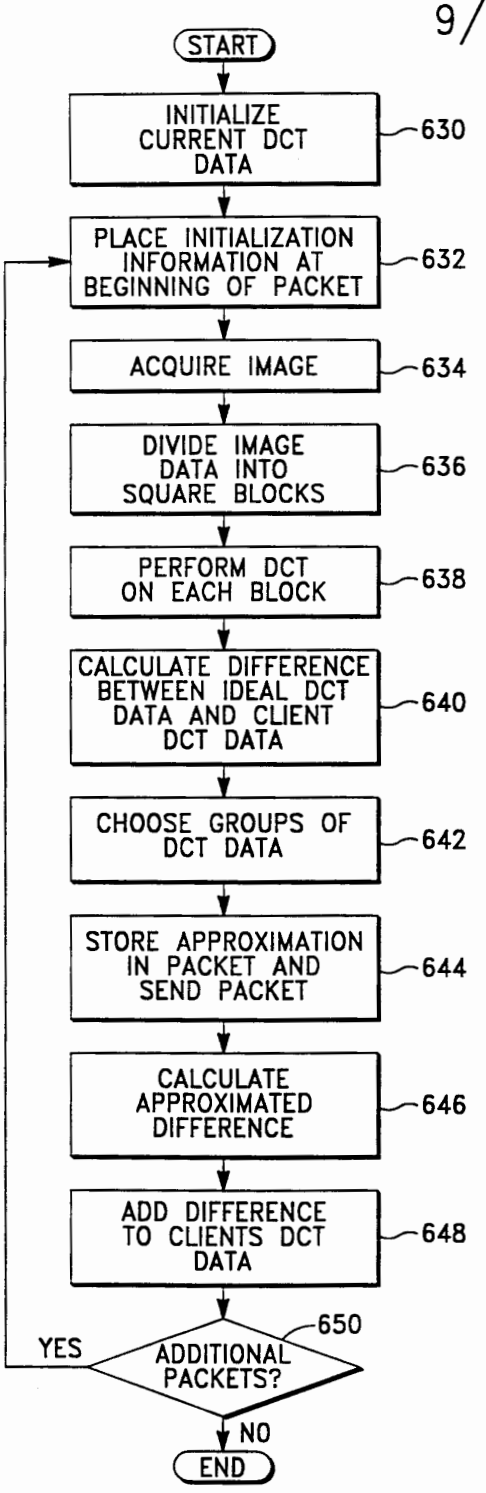


FIG. 12

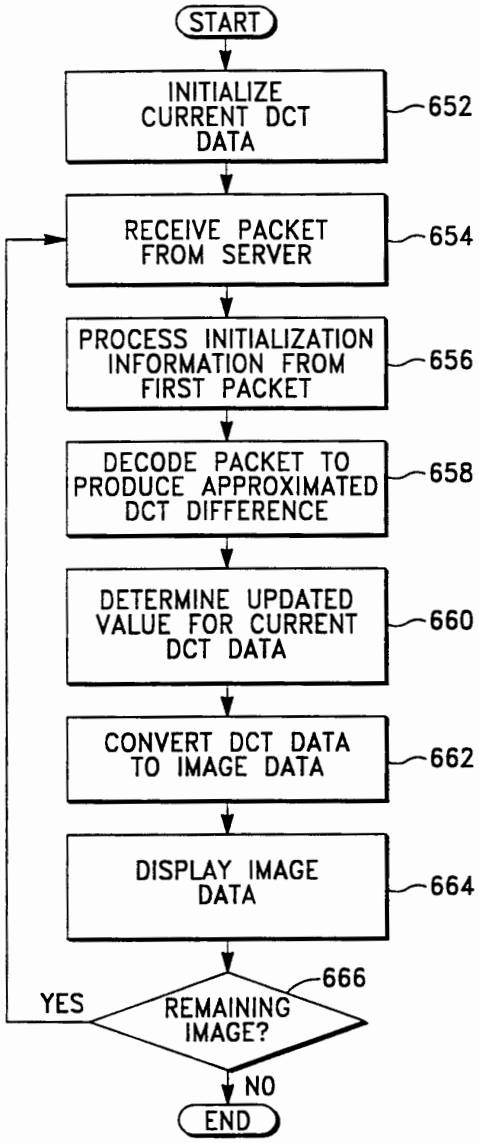


FIG. 13

Dropbox Exhibit 1002 - Page 318
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

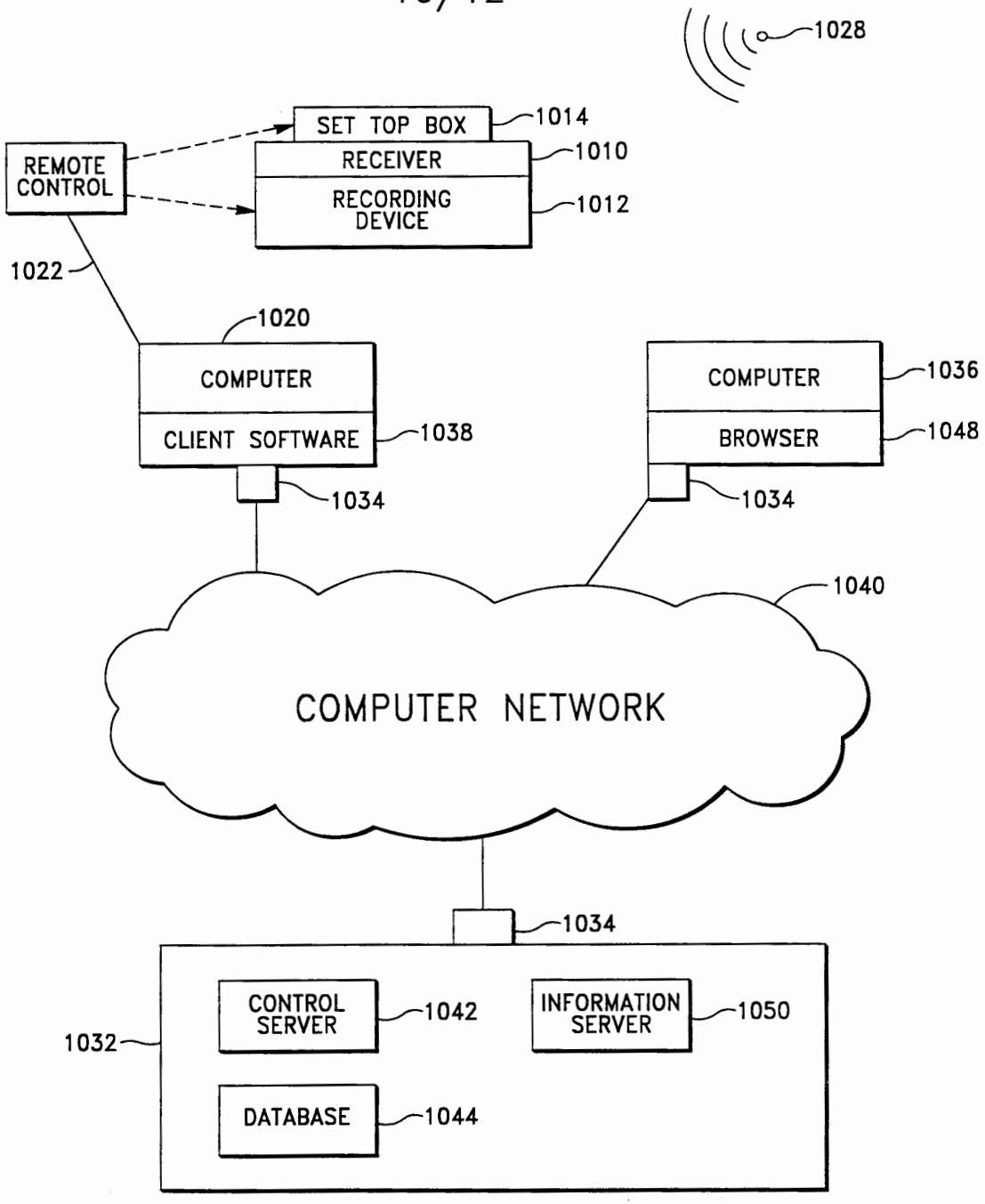


FIG. 14

Dropbox Exhibit 1002 - Page 319
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

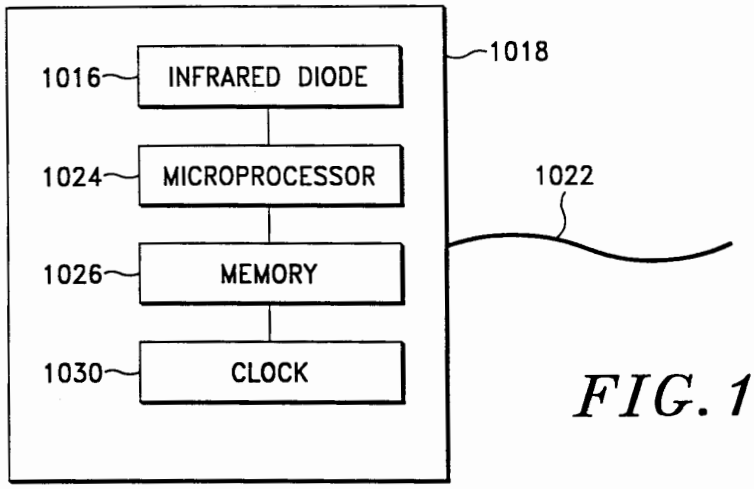


FIG. 15

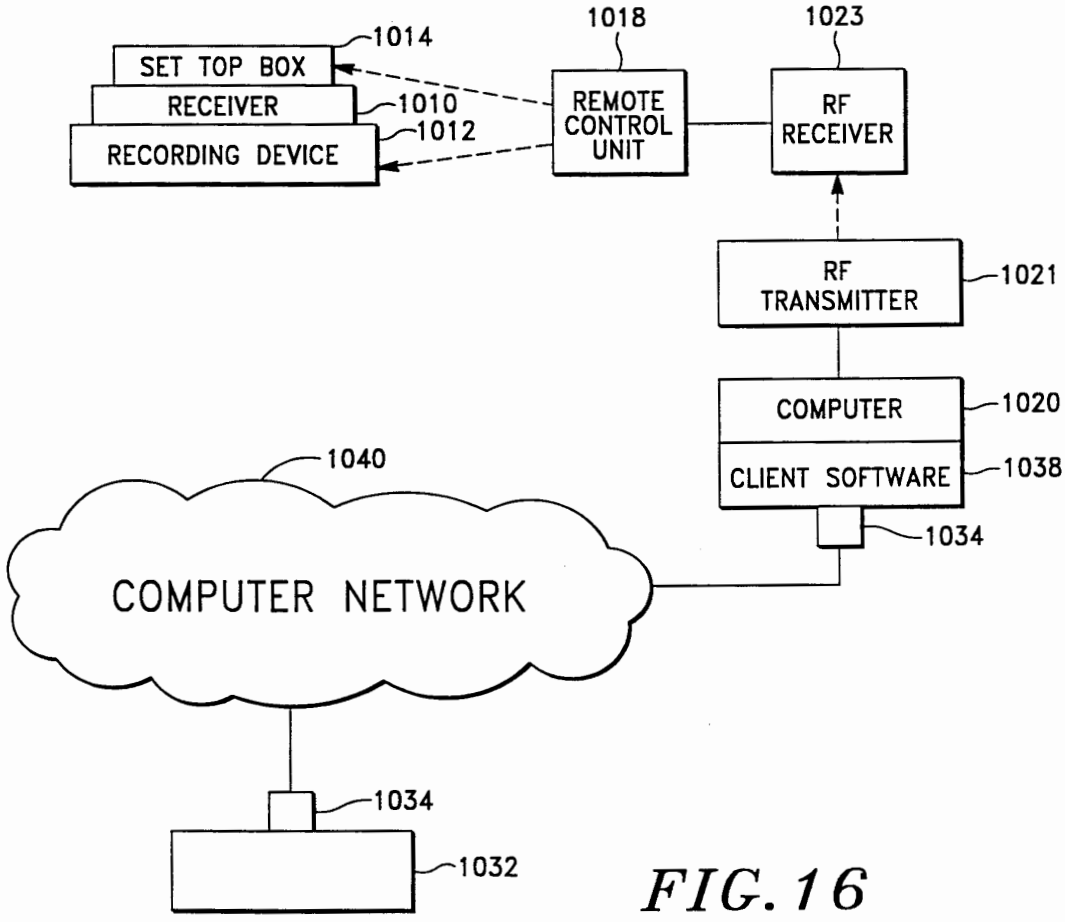


FIG. 16

Dropbox Exhibit 1002 - Page 320
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

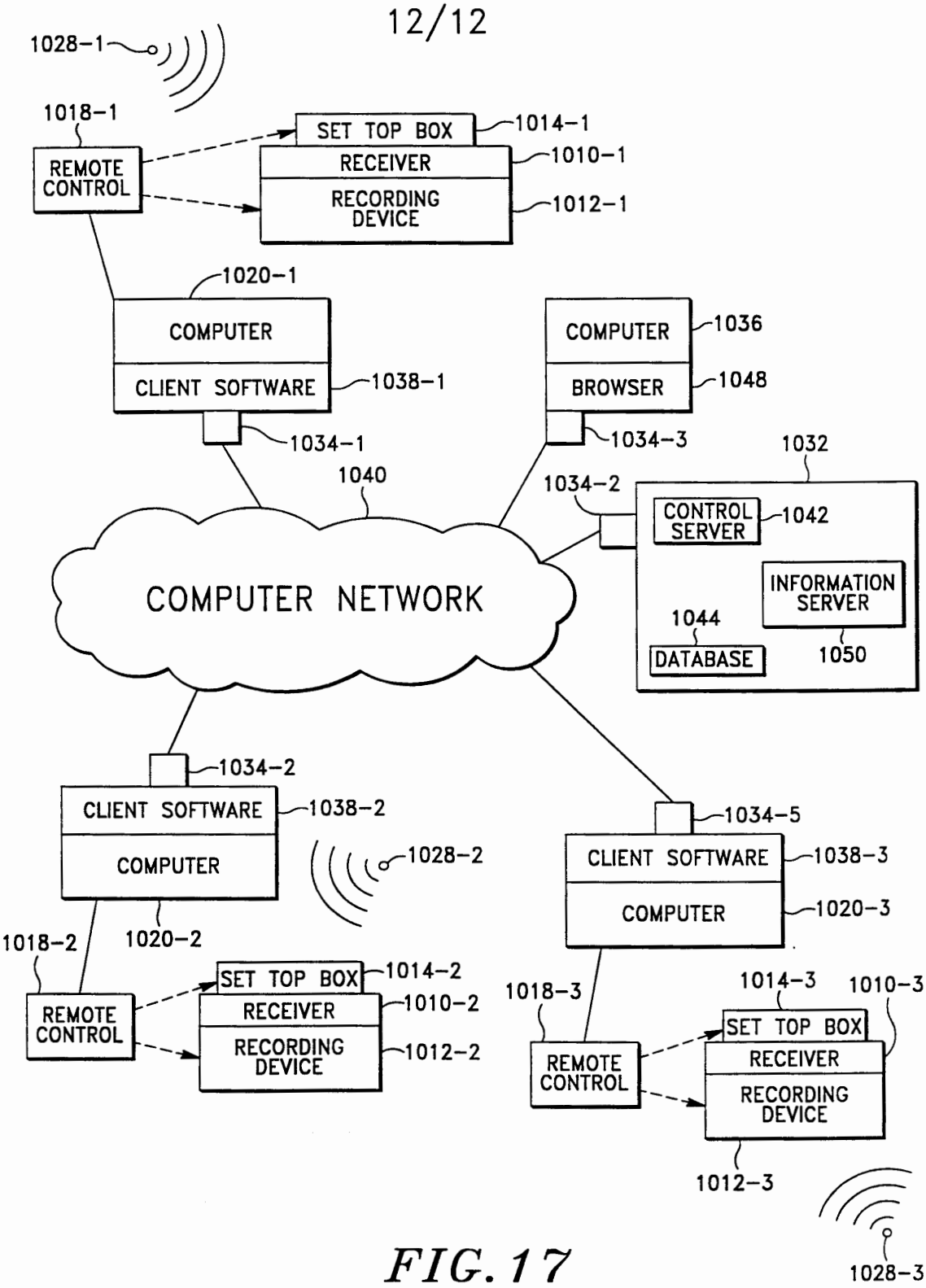


FIG. 17

Dropbox Exhibit 1002 - Page 321
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/32734

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :G05B 23/02; G06F 15/16
US CL :340/825.06; 709/218

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)

U.S. : 340/825.06; 345/327; 348/12; 709/209, 218

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

Microsoft Press COMPUTER DICTIONARY

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

East US Patents, WEST DERWENT API
search terms: remote, control, internet or brower-interface, vcr or recording

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,907,322 A (KELLY et al.) 25 May 1999, col. 6, line 43 - col. 7, line 10	1
X	US 5,956,487 A (VENKATRAMAN et al.) 21 September 1999, col. 4, lines 29-46	1
A	US 5,990,884 A (DOUMA et al.) 23 November 1999, abstract	1
A,P	US 6,052,750 A (LEA) 18 April 2000, abstract	1
A,E	US 6,182,094 B1, (HUMPLEMAN et al.) 30 January 2001, abstract	1

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier document published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search 20 FEBRUARY 2001	Date of mailing of the international search report 19 MAR 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer PATRICE WINDER James R. Matthews Telephone No. (703) 305-3938

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

Dropbox Exhibit 1002 - Page 322
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 October 2003 (16.10.2003)

PCT

(10) International Publication Number
WO 03/085559 A1

(51) International Patent Classification[7]: G06F 17/30

(21) International Application Number: PCT/US03/10227

(22) International Filing Date: 3 April 2003 (03.04.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/115,448 3 April 2002 (03.04.2002) US
10/268,043 8 October 2002 (08.10.2002) US

(71) Applicant: **SYNERDRIVE, INC.** [US/US]; Suite 1850, 10900 NE 4th Street, Bellevue, WA 98004 (US).

(72) Inventors: **ABOULHOSN, Amir L.**; 1500-701 West Georgia Street, Vancouver, British Columbia V7Y 1C6 (CA). **CHEN, Rui**; 1725 Crestlawn Crt, Burnaby, British Columbia V5B 3K2 (CA). **KOO, David M.**; Suite 808, 1060 Alberni Street, Vancouver, British Columbia V6E 4K2 (CA). **VINEBERG, David J.**; 230 SE Bush, Issaquah, WA 98027 (US). **WALD, James F.**; 3211 Perkins Lane W, Seattle, WA 98199 (US). **MURPHY, Stephen**; Apt. 404, 2161 W 12th Avenue, Vancouver, British Columbia V6K 4S7 (CA).

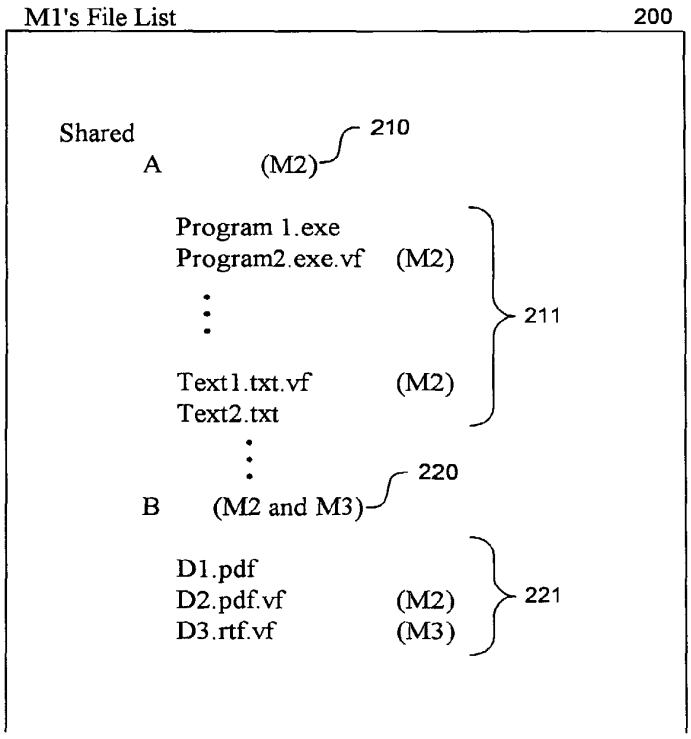
(74) Agents: **PIRIO, Maurice, J.** et al.; Patent-Sea, P.O. Box 1247, Seattle, WA 98111-1247 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: PEER-TO-PEER FILE SHARING



(57) Abstract: A method for sharing files (101-103) between a group of computer systems (510, 520). The file sharing system (100, 200, 300, 400) allows a group of computer systems (510, 520) to be defined. The files shared (101-103) by a group (514) are associated with a group folder (310-311, 320-321). A group folder (310-311, 320-321) is represented by a folder created by the file system (512) of each member (510) of the group (514). The files (1001, 1003) in thefolder of a member (510) may be actual files stored at that member, which contains the content of the shared file (101-103). When a member (510) accesses a virtual file (631-632), the file sharing system detects the access (631-632) and requests that the file owner (1001, 1003) provide a copy of the file (1001, 1003) to the accessing member (631-632) on a peer-to-peer basis (511). Whenever a shared file (101-103) is modified, the file owner (1001, 1003) sends updated metadata (1004).

WO 03/085559 A1

Dropbox Exhibit 1002 - Page 323
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Dropbox Exhibit 1002 - Page 324
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

PEER-TO-PEER FILE SHARING

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority of U.S. Patent Application No. 10/115,448, filed April 03, 2002, which is hereby incorporated by reference in its entirety.

TECHNICAL FIELD

The described technology relates generally to methods of and systems for peer-to-peer file sharing between computers.

BACKGROUND

There are a variety of known methods and systems of differing complexity for sharing files between two or more computers, both centralized and distributed. Conventional centralized client-server file sharing systems often require a massive server storage infrastructure. More basic file sharing systems that merely allow files to be uploaded to and then to be downloaded from a centralized site (e.g., an FTP site on the Internet) likewise may need to provide a substantial amount of centralized storage space. Distributed systems reduce the need for centralized file storage, but they may suffer from one or more disadvantages such as an unfamiliar user interface, a need for a substantial amount of user training, lack of up-to-date information on files currently available for retrieval, and so forth.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a display page illustrating a file system folder structure with a shared folder in one embodiment.

Figures 2-4 are display pages illustrating the file system folder structure for members of various groups.

Figure 5 is a block diagram illustrating components of the file sharing system in one embodiment.

Figures 6A-6E are diagrams illustrating the message flows between members of a group in one embodiment.

Figure 7 is a flow diagram illustrating the processing of an invite component or peer component in one embodiment.

Figure 8 is a flow diagram illustrating the processing of the peer component when it receives an invitation request message in one embodiment.

Figure 9 is a flow diagram illustrating the processing of the peer component when it receives an invitation response message in one embodiment.

Figure 10 is a flow diagram illustrating the processing of the peer component when it receives a synchronization response message in one embodiment.

Figure 11 is a flow diagram illustrating the processing of discovering a computer system.

DETAILED DESCRIPTION

A method and system for sharing files between a group of computer systems is provided. In one embodiment, the file sharing system allows a group of computer systems to be defined. One computer system of the group may be designated as the "group owner." The group owner may have the sole authority to invite other computer systems to join the group. Alternatively, other computer systems of the group ("members of the group") may have the authority to also invite other computer systems to join the group. In one embodiment, the files shared by a group are associated with a group folder. A group folder is represented by a folder created by the file system of each member. The folder at each member contains a file for each file that is shared by the group. The files in the folder of a member may be actual files stored at that member, which contains the content of the shared file, or virtual files identifying the actual file that is stored at another member. A shared file is identified by metadata stored in association with the virtual file (e.g., as properties of the virtual file). A member who shares a file that is stored at that member is referred to as the "file owner." When a file is shared, the folder of the file owner contains the actual file and the folders of the other members of the group contain a virtual file corresponding to the shared file. When a member accesses a virtual file, the file sharing system detects the access and requests that the file owner provide a copy

Dropbox Exhibit 1002 - Page 326
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

of the file to the accessing member on a peer-to-peer basis. Whenever a shared file is modified, the file owner sends updated metadata for that file to the other members of the group. In this way, the members use their local file systems to represent each shared file of the group and defer downloading a shared file until it is accessed by a member who is not the file owner.

In one embodiment of the file sharing system, the members receive from another member a notification that a file is to be shared with the members of the group. The notification includes metadata describing the file to be shared. For example, the metadata may identify the file name, the file owner, the create date of the file, the last modified date of the file, the size of the file, and so on. Upon receiving the notification, the member creates a virtual file in their folder for the group using the file system of that member. A virtual file may be a file that has the same name as the file being shared except for an identifying extension, may have no actual content (e.g., a file size of 0), and may have the metadata represented as attributes of the virtual file. Whenever the actual file is changed at the file owner, the file owner sends the updated metadata for the file to the other members, who update the metadata associated with their corresponding virtual file as appropriate. The members, who are not the file owner, use the metadata when accessing the shared file.

In one embodiment, the group owner maintains a list of the group members. All messages related to metadata updates are routed through the group owner. For example, when a shared file is updated, the file owner sends a message to the group owner containing new metadata for the shared file. The group owner identifies the other members of the group and sends the updated metadata to each member. A member may be either online or offline. (More generally, a computer system, regardless of whether it is currently a member of a group, can be online or offline.) If a member is online, then the member can receive messages from other members, can access the files whose file owners are also online, and can notify other members of changes that it makes to the shared files that it owns. If a member is offline, the member can neither receive nor send any messages. In one embodiment, the file sharing system may have a server (e.g., an authorization server) that controls whether a member is currently online or offline. A member goes online by providing authentication information to the authentication server.

When the information can be authenticated, the member is online. The authentication server, when requested by a member, provides access information for another online member. When a member goes online, it contacts the group owner (assuming that the group owner is currently online) to synchronize its copy of the group folder with the group owner. For example, files of the group folder may have been added, deleted, or updated while the member was offline. Also, the member while offline may have added, deleted, or updated files of the group folder. When a member goes online, its access information (e.g., IP address) is provided to the authentication server so that other members of the group can send messages (e.g., metadata updates) to that member. When a computer system goes online the authentication server notifies the group owners who can forward the notification to the group members as appropriate. In an alternate embodiment, a group owner can delegate to another member its responsibility to route metadata updates, member status updates, and so on. The delegation will allow the group to function even while the group owner is offline.

A group owner may invite other computer systems to join the group as members. In one embodiment, a computer system is eligible to be a member of a group after the computer system has registered with the authentication server. The registration process ensures that the computer system is authorized to be a member and provides authentication information for use in subsequently authenticating the computer system when it comes online. Also, a group owner and file owner may, before interacting with a member, verify with the authentication server that the member is still registered. This verification will help to prevent access to the shared files by a member whose registration has lapsed. The group owner requests the address of the computer system to be invited from the authentication server. If the computer system to be invited is currently online, the authentication server provides the address. The group owner then sends an invitation message. When the computer system receives an invitation request message, it can either accept or decline the invitation via an invitation response message sent to the group owner. If the invitation is accepted, the group owner adds the new member to its list of members for that group. The new member then synchronizes its folder with the group owner. If the computer system that is being invited to join the group is not currently online, then the group owner may queue the message until the computer

system goes online. Similarly, the computer system may queue its response to the invitation if the group owner is not currently online.

In one embodiment, a file owner may decide that ownership of a file should be transferred to the group owner. In such case, the group owner is considered the proxy file owner and is provided with a copy of that file. When other members access that shared file, they direct their requests to the proxy file owner. The group owner is also responsible for distributing updates to the metadata of the shared file. The use of a proxy file owner allows other members of the group to have access to a shared file even though the actual file owner of the shared file may be offline at that time. Such proxying of file ownership is particularly useful when the group owner is generally online and the file owner is generally offline (e.g., the file owner is a laptop computer).

In one embodiment, a group owner may delete a group. To delete a group, the group owner sends a message to each group member. When a group member receives the message, it typically deletes its local shared folder for the group. The group owner also deletes its local shared folder for the group and then suspends sending of synchronization messages (e.g., new shared file metadata) for the group. Alternatively, a group member can elect not to delete its local shared folder. In such a case, the folder becomes inactive that is a folder with no synchronization. The virtual files within an inactive folder can still be accessed assuming that the file owner also did not delete its local shared folder.

Figure 1 is a display page illustrating a file system folder structure with a shared folder in one embodiment. Display page 100 displays a folder 101, named "Shared," that contains a member's folders corresponding to shared folders. In this example, a shared folder "A" contains the shared files of group "A". The display page also contains a menu 103 that is displayed when the shared folder "A" is selected by a user. The file sharing system may receive event notifications from the file system relating to access to the shared folders such as when a user right clicks on a shared folder. The menu lists various menu items that are available. The "share" menu item allows the user to access functions of the file sharing system related to the sharing of the files within the shared folder, such as sending invitations.

Figures 2-4 are display pages illustrating the file system folder structure for members of various groups. In the example illustrated, three computers system are identified as M1, M2, and M3. M1 and M2 are members of a group "A," and M1, M2, and M3 are members of group "B." Display pages illustrating the file system folder structure for the shared folders of M1, M2, and M3 are illustrated in Figures 2, 3, and 4, respectively. Although these display pages do not illustrate shared subfolders, one skilled in the art will appreciate that a shared folder may contain shared subfolders.

Display page 200 of Figure 2 illustrates that M1 has a shared folder named "A" for group "A" 210 and a shared folder named "B" for group "B" 220. The parentheticals next to the folder names identify the other members of the group and would typically not be displayed by a file system. Shared folder "A" contains four shared files 211 named "Program1.exe," "Program2.exe.vf," "Text1.txt.vf," and "Text2.txt." The file name extension of "vf" identifies a shared file as a virtual file. The second-to-the-last file name extension of a virtual file corresponds to the last file name extension of the actual file. For example, the second-to-the-last file name extension of "Program2.exe.vf" is "exe," which identifies that the actual file is an executable file. In one embodiment, the name of a virtual file is the same as the corresponding actual file, except with the "vf" extension appended. Alternatively, the name of a virtual file could be completely different from the name of the corresponding actual file. In such a case, the metadata can include the name of the actual file. The shared files, "Program2.exe.vf" and "Text1.txt.vf," are virtual files and, as indicated by the parentheticals, are stored at M2. The shared files, "Program1.exe" and "Text2.txt," are stored at M1 and are thus not virtual files for M1. The shared folder "B" contains three shared files 221 named "D1.pdf," "D2.pdf.vf," and "D3.pdf.vf."

Display page 300 of Figure 3 illustrates that M2 has a shared folder "A" for group "A" 310 and a shared folder "B" for group "B" 320. Shared folder "A" contains a file 311 for each of the four shared files for group "A." In this example, since the files "Program1.exe" and "Text2.txt" are stored at M1, they are represented at M2 as virtual files as indicated by the "vf" extensions. Similarly, since the shared files "D1.pdf" and "D3.rtf" 321 of shared folder "B" are stored at M1 and M3, respectively, they are represented as virtual files at M2.

Display page 400 of Figure 4 illustrates that M3 has a shared folder "B" for group "B" 410. Shared folder "B" contains a file for each of the three shared files for group "B." In this example, since the shared files "D1.pdf" and "D2.pdf" 411 of shared folder "B" are stored at M1 and M2, respectively, they are represented at M3 as virtual files.

Figure 5 is a block diagram illustrating components of the file sharing system in one embodiment. The computer systems 510 communicate with each other and with authentication server 520 via communications link 530. Computer systems 510 include a peer component 511, a file system 512, shared folders 513, a group members table 514, a pending transfer table 516, and other components not illustrated in this figure. The peer component, which may be downloaded from the authentication server when the computer system is registered, controls the sharing of files with other computer systems. The functions of the peer component, which are described in detail below, include registering a computer system, placing a computer system online, creating groups, inviting computer systems to become members of a group, sending updates to metadata, and so on. The file system may be a conventional file system provided by an operating system. The shared folders represent the folders within the file system folder structure that have been created by the file sharing system. The shared folders include a folder for each group for which this computer system is a member. The group member table is maintained by the group owners and contains the identification of each member of the group. The pending transfer table contains information related to the state of the transfers that that were interrupted for some reason (e.g., failure of the communications link). The pending transfer information allows a file transfer to be resumed at the point it was interrupted.

The authentication server includes a receive message component 521, an online table 522, a registered table 523, a process online message component 524, a process discover message component 525, and other components not illustrated in this figure. The receive message component receives messages from the computer systems and forwards them to the appropriate components for processing. The registered table contains an entry for each computer system that is currently registered with the file sharing system. Each entry may contain authentication information that is used to authenticate a computer system that attempts to come

online. The online table contains an entry for each computer system that is currently online. Each entry contains the address (e.g., internet protocol address) of the online computer system. The process online message component coordinates the requests of computer systems to come online. The process discover message component retrieves the address of an identified computer system (if it is online) from the online table and provides it to the requesting computer system. The functions of the authentication server may be divided among multiple servers. For example, there may be separate servers for handling registration requests, online requests, and discovery requests.

The computer systems and servers may include a central processing unit, memory, input devices (e.g., keyboard and pointing devices), output devices (e.g., display devices), and storage devices (e.g., disk drives). The memory and storage devices are computer-readable media that may contain instructions that implement the file sharing system. In addition, the data structures and message structures may be stored or transmitted via a data transmission medium, such as a signal on a communications link. Various communications links may be used, such as the Internet, a local area network, a wide area network, or a point-to-point dial-up connection. In some cases, one computer system may not be able to communicate direct with or initiate communications with another computer system. For example, one computer system may be behind a firewall that does not allow communications to be initiated by a computer system on the other side of the firewall. Also, a computer system may connect to the network via a Network Address Translator. In such cases, various well-known mechanisms may be used to allow the computer systems to communicate, such as an intermediate or tunneling server mechanism.

Figures 6A-6E are diagrams illustrating the message flows between members of a group in one embodiment. Figure 6A is a diagram illustrating the message flows when a group owner invites a computer system to become a new member. The group owner initially receives an indication from its user that a registered computer system is to be invited to join the group. The file sharing system may provide to the user a list of the registered computer systems (e.g., stored in the registered table) so that the user can identify the computer system to be invited. The group owner then sends an invitation request message 611 to the invited computer system. The group owner accesses the authentication server to retrieve

the address for the invited computer system (i.e., to discover the invited computer system). If the invited computer system is currently online, then the authentication server provides the address and the group owner sends the invitation request message to that address. If, however, the invited computer system is not currently online, then the group owner queues the invitation request message until the group owner is notified by the authentication server that the invited computer system comes online. (In general, a registered computer system sends a message to another registered computer system by first retrieving the address of the recipient computer system from the authentication server. If the computer system is not currently registered or is offline, then the authentication server returns an error message. The sending computer system then sends the message directly to the address. If the authentication server does not return an address for the recipient computer system, then the sending computer system may queue certain types of messages until the recipient computer system comes online. Other types of messages might not be queued because the information of the message can be obtained, for example, during a synchronization process.) When the invited computer system receives the invitation request message, it notifies its user of the invitation request. The user may be notified by the creation of a shared folder for the group, by a flashing icon, or by some other means. When the user eventually decides to accept or reject the invitation request, the invited computer system sends an invitation response message 612 to the group owner. When the group owner receives the invitation response message, it updates its member list for that group accordingly. Assuming that the invited computer system accepted the invitation, the group owner sends an out-of-synchronization message 613 to the new member. The out-of-synchronization message notifies the new member that it needs to synchronize its copy of the shared folder with the group owner's copy. The new member then sends a synchronization request message 614 to the group owner. Upon receiving the synchronization request message, the group owner collects the metadata for the shared files of the group and sends that metadata to the new member via a synchronization response message 615. When the new member receives the synchronization response message, it creates the appropriate virtual files in the shared folder.

Figure 6B is a diagram illustrating the message flows when a member of the group updates the group folder. A member updates a folder by adding, deleting, or modifying a file of the shared folder. The member that updates the folder sends an out-of-synchronization message 621 to the group owner, unless it is the group owner itself that updates the folder. In response, the group owner sends a synchronization request message 622 to the updating member. The updating member responds with a synchronization response message 623 that contains the metadata describing the update. The group owner upon receiving the metadata updates to the metadata associated with the shared folder. The group owner then notifies each other group member of the update. The group owner notifies a member by first sending an out-of-synchronization message 624 to the member. The member then responds by sending to the group owner a synchronization request message 625. In response, the group owner sends the metadata to the members via a synchronization response message 626. Upon receiving the metadata, the member updates its folder. In one embodiment, certain messages relating to updating a folder are not queued if a member is offline. When that member comes online, the online synchronization process will result in synchronization of the folders.

Figure 6C is a diagram illustrating the message flows when a member accesses a virtual file. When a member detects access of a virtual file, the member sends an access request message 631 to the file owner. The metadata stored at the member for the accessed virtual file contains the identification of the file owner. Upon receiving the access request message, the file owner retrieves the data of the file and sends the data to the accessing member via an access response message 632. In one embodiment, the access response message may be a series of messages each containing a portion of the access file. In such a case, the accessing member may persistently maintain an indication of the portion of the access file that has been received so far. In the event that the transfer of the file is interrupted, the accessing member may request the file owner to resume the transfer of the file where it left off.

Figure 6D is a diagram illustrating the message flows when a member comes online. A member comes online by providing authentication information to the authentication server. Once authenticated, the member is online and sends its

queued messages into the recipient computer systems that are currently online. The member then sends a synchronization request message 642 to the group owner. The group owner collects the metadata for the shared folder and sends a synchronization response message 643 to the new online member. When the new online member receives the metadata, it updates its folder accordingly. The new online member may also identify whether it made updates to the folder while it was offline. If so, the member notifies the group owner that it is out of synchronization, and the updating of the metadata is performed in a manner similar to that illustrated in Figure 6B. Alternatively, the updates that have been made while the member was offline may be reflected in queued messages.

Figure 6E is a diagram illustrating the message flows when a group owner comes online. When a group owner becomes online, it sends a synchronization request message 651 to each member. Each member responds with a synchronization response message 652 containing the metadata for that shared folder. The group owner then updates its shared folder to correspond to all the updates by any of the members that occurred while the group owner was offline. The group owner then sends an out-of-synchronization message 653 to each member. In response, each member sends a synchronization request message 654 to the group owner. The group owner then sends the current metadata for the shared folder in a synchronization response message 655 to each member. The members then update their folders accordingly.

Figure 7 is a flow diagram illustrating the processing of an invite component of a peer component in one embodiment. The invite component controls the sending of an invitation request message to each computer system that is invited to be a member of a group. In block 701, the component receives the identification of each computer system that is to be invited to join the group. In block 702-704, the component loops selecting each invited computer system and sending it an invitation request message. In block 702, the component selects the next invited computer system. In decision block 703, if all the invited computer systems have already been selected, then the component completes, else the component continues at block 704. In block 704, the component sends an invitation request message to the selected computer system. The component then loops to block 702 to select the next invited computer system. As described above, a message is sent

to a computer system by providing the identification of that computer system to the authentication server. The authentication server then returns the address of that identified computer system if it is currently online. If not online, then the sending computer system queues the invitation request message.

Figure 8 is a flow diagram illustrating the processing of the peer component when it receives an invitation request message in one embodiment. In block 801, the component notifies its user that an invitation request message has been received. The component may notify the user in various ways such as creating the shared folder with an indication that the computer system has been invited to join the group associated with that folder, by highlighting an icon for the file sharing system that may be displayed on a program tray, and so on. In decision block 802, if the user accepts the invitation, then the component continues at block 804, else the component continues at block 803. In block 803, the component sends an invitation response message to the group owner indicating that it has declined the invitation and then completes. In block 804, the component sends an invitation response message to the group owner indicating that it has accepted the invitation. In block 805, the component notes that the computer system is now a member of that group and then completes.

Figure 9 is a flow diagram illustrating the processing of the peer component when it receives an invitation response message in one embodiment. In block 901, the component updates the membership list for the group as appropriate. In decision block 902, if the computer system accepted the invitation, then the component continues at block 903, else the component completes. In block 903, the component sends an out-of-synchronization message to the new member and then completes.

Figure 10 is a flow diagram illustrating the processing of the peer component when it receives a synchronization response message in one embodiment. The synchronization response message contains metadata for each file currently in the group. The component updates the metadata for each file in the group, creating new files as necessary. In addition, the component deletes any virtual files that it has locally that are not represented by metadata. In block 1001, the component selects the next file. In decision block 1002, if all the files have already been selected, then the component continues at block 1006, else the component

continues at block 1003. In decision block 1003, if the selected file already exists in the shared folder, then the component continues at block 1004, else the component continues at block 1005. In block 1004, the component updates the metadata for the existing file and then loops to block 1001 to select the next file. In block 1005, the component creates a new virtual file based on the metadata for that file and then loops to block 1001 to select the next file. In block 1006, the component deletes any virtual files of the shared folder that is not represented by the metadata and then completes.

Figure 11 is a flow diagram illustrating the processing of discovering a computer system. This component is invoked when a computer system wants to send a message to another computer system. The component is passed the identification of the computer system to be discovered. The authentication server maps the identification of online computer systems to their corresponding addresses. In block 1101, the component sends a discover request message to the authentication server. In block 1102, the component receives a discover response message from the authentication server. In decision block 1103, if the computer system is online, then the component continues at block 1104, else the component returns an indication that the computer system is not online. In block 1104, the component sends a validate message to the computer system at the received address. In block 1105, the component receives a validate response message from the computer system or an error message. In decision block 1106, if the computer system has been validated, then the component returns an indication that the computer system is online, else the component returns an indication that computer system is not online.

From the foregoing it will be appreciated that although specific embodiments of the file sharing system have been described herein for purposes of illustration, various modifications may be made without deviating from the spirit and scope of the invention. Accordingly, the invention is not limited except by the appended claims.

CLAIMS

I/We claim:

1. A method in a computer system for sharing a file stored at another computer system, the method comprising:

receiving from the other computer system a notification that the file is to be shared with the computer system, the notification including metadata of the file;

creating a virtual file using a file system of the computer system;

storing the metadata of the file in association with the virtual file; and

after the file is changed at the other computer system, receiving from the other computer system metadata for the file and updating the metadata stored in association with the virtual file based on the received metadata.

2. The method of claim 1 including when the virtual file is accessed, retrieving the file stored at the other computer system using the metadata associated with the virtual file.

3. The method of claim 2 wherein when the virtual file is accessed, a virtual file component receives a notification from the file system, retrieves metadata associated with the virtual file, and controls the retrieving of the file stored at the other computer system.

4. The method of claim 2 including before retrieving the file stored at the other computer system, retrieving from a server an address for the other computer system.

5. The method of claim 4 wherein the address is an IP address.

6. The method of claim 4 including before retrieving the file stored at the other computer system, retrieving from the server a public key for the other computer system.

7. The method of claim 6 wherein the public key is used to validate authenticity of the other computer system.

8. The method of claim 2 wherein including before retrieving the file stored at the other computer system, logging on to a server.

9. The method of claim 8 wherein the logging on includes providing an address to the server and a private key.

10. The method of claim 2 wherein the file is transferred on a peer-to-peer basis.

11. The method of claim 1 wherein metadata for the created virtual file is stored as attributes of the created virtual file.

12. The method of claim 1 wherein the virtual file has a file type indicating that it is a virtual file.

13. The method of claim 12 wherein a virtual file program is associated with the file type so that when the virtual file is accessed the virtual file program executes to coordinate the access.

14. The method of claim 1 wherein the created virtual file is stored in a file system folder associated with the other computer system.

15. The method of claim 1 wherein the metadata includes an identifier of the other computer system.

16. The method of claim 1 including requesting the other computer system to provide current metadata for the virtual file.

17. The method of claim 16 wherein the requesting is performed when the computer system logs on to a server.

18. The method of claim 1 wherein the computer system and the other computer system are members of a group of computer systems that share files.

19. The method of claim 18 wherein one computer system of the group is designated as a group owner, the computer system that stores the shared file is designated as the file owner, and changes to the metadata of the shared file are sent from the file owner to the group owner for distribution to other member of the group.

20. The method of claim 18 wherein one computer system of the group is designated as a group owner, the computer system that stores the shared file is designated as the file owner, and the file owner transfers the shared file to the group owner to act as a proxy file owner.

21. A method in a computer system for sharing a file stored at another computer system, the method comprising:

receiving from the other computer system a notification that the file is to be shared with the computer system, the notification including metadata of the file;

creating a virtual file using a file system of the computer system;

storing the metadata of the file in association with the virtual file; and

when the virtual file is accessed, retrieving the file stored at the other computer system using the metadata associated with the virtual file.

22. The method of claim 21 wherein when the virtual file is accessed, a virtual file component receives a notification from the file system, retrieves metadata

associated with the virtual file, and controls the retrieving of the file stored at the other computer system.

23. The method of claim 21 including before retrieving the file stored at the other computer system, retrieving from a server an address for the other computer system.

24. The method of claim 21 wherein including before retrieving the file stored at the other computer system, logging on to a server.

25. The method of claim 21 wherein the file is transferred on a peer-to-peer basis.

26. The method of claim 21 wherein metadata for the created virtual file is stored as attributes of the created virtual file.

27. The method of claim 1 wherein the computer system and the other computer system are members of a group of computer systems that share files.

28. A computer system for sharing a file stored at another computer system, comprising:

means for receiving from the other computer system a notification that the file is to be shared with the computer system, the notification including metadata of the file;

means for creating a virtual file using a file system of the computer system;

means for storing the metadata of the file in association with the virtual file; and

means for retrieving the file stored at the other computer system using the metadata associated with the virtual file.

29. The computer system of claim 28 including means for retrieving from a server an address for the other computer system.

30. The computer system of claim 28 wherein the file is transferred on a peer-to-peer basis.

31. The computer system of claim 28 including means for storing metadata for the created virtual file as attributes of the created virtual file.

32. A computer-readable medium accessible by a computer system containing a data structure comprising a list of files that are stored by the file system of the computer system, the files being stored within a folder of the file system, the files including a virtual file corresponding to an actual file stored on another computer system wherein when the virtual file is accessed the actual file is retrieved from the other computer system.

33. The computer-readable medium of claim 32 wherein the data structure includes metadata associated with the virtual file.

34. The computer-readable medium of claim 33 wherein the metadata includes an identification of the other computer system.

35. The computer-readable medium of claim 33 wherein the metadata is updated when the actual file is modified.

36. A system for sharing files among a group of computer systems, comprising:

a group owner component that creates a group, that invites computer systems to join the group as members, and that distributes status messages to the members; and

a member component that includes

a file owner component that controls the sharing of an actual file with other members; and

a virtual file component that creates a virtual file for the shared filed and that retrieves the actual file when the virtual file is accessed.

37. The system of claim 36 including an authentication server component for authenticating computer systems.

38. The system of claim 36 including an authentication client component for authenticating a computer system with an authentication server.

39. A system for sharing files among a group of computer systems comprising:

a file owner component that notifies a group owner computer system when a file of a computer system is to be shared with other computer systems, wherein a shared file is represented as a virtual file at the other computer systems; and

a file access component that receives from another computer system a request to access the shared file and that provides the shared file to the other computer system on a peer-to-peer basis.

40. The system of claim 39 wherein the group owner computer system notifies the other computer systems that the file is being shared.

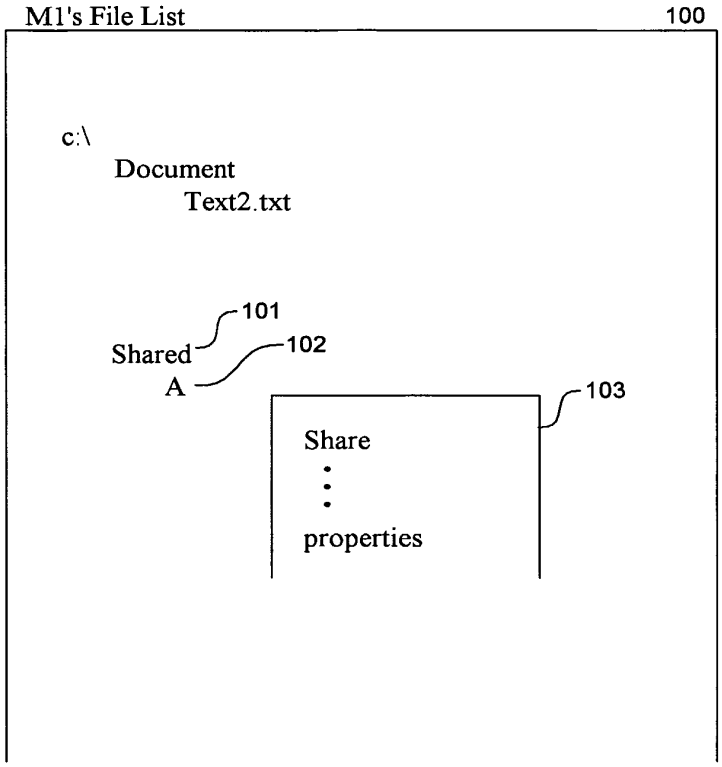

M1's File List
100
c:\
Document
Text2.txt
101
Shared
102
A
103
Share
properties

Fig. 1

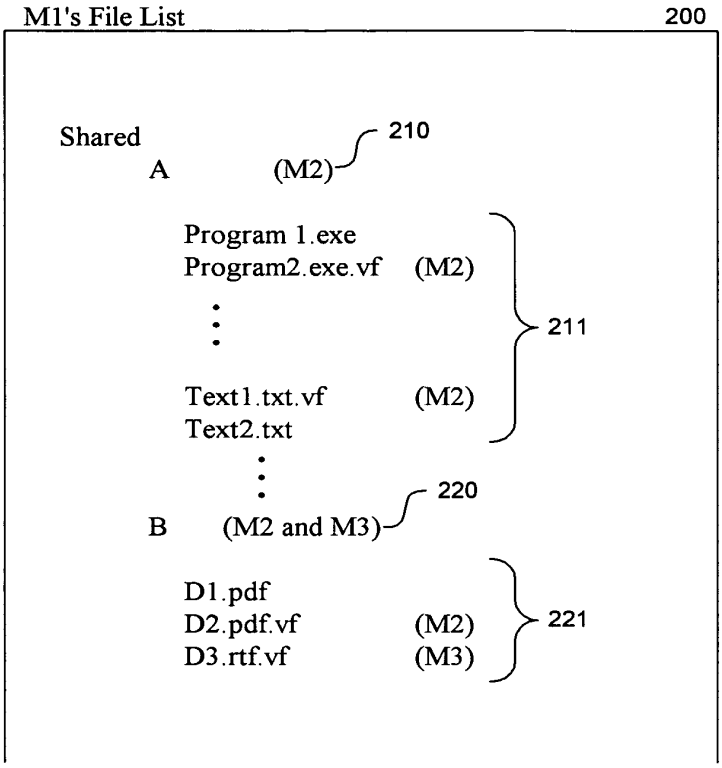

M1's File List
200
Shared
A
(M2)
210
Program 1.exe
Program2.exe.vf (M2)
211
Text1.txt.vf (M2)
Text2.txt
B
(M2 and M3)
220
D1.pdf
D2.pdf.vf (M2)
D3.rtf.vf (M3)
221

Fig. 2

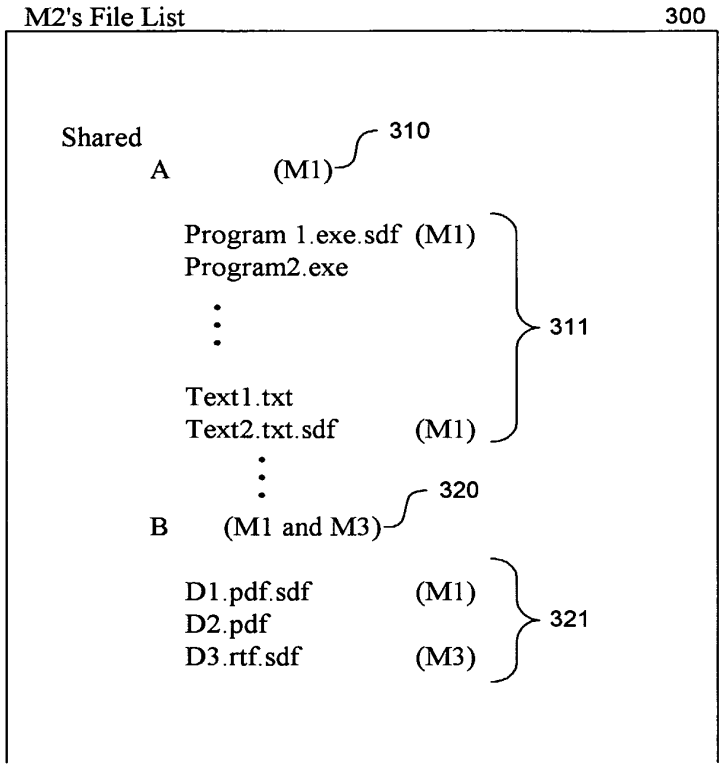

M2's File List
300
Shared
A
(M1)
310
Program 1.exe.sdf (M1)
Program2.exe
311
Text1.txt
Text2.txt.sdf (M1)
320
B
(M1 and M3)
D1.pdf.sdf (M1)
D2.pdf
D3.rtf.sdf (M3)
321

Fig. 3

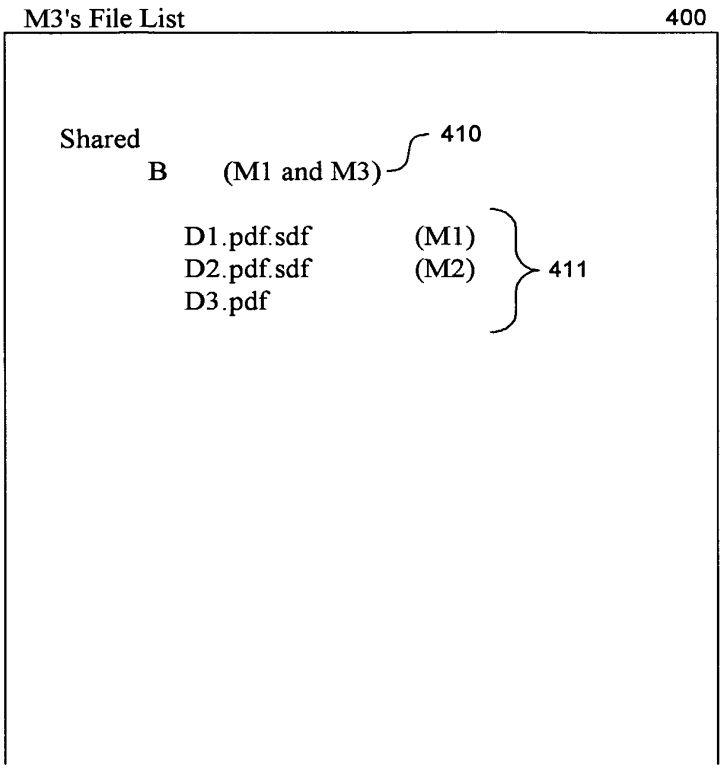

M3's File List
400
Shared
B
(M1 and M3)
410
D1.pdf.sdf
(M1)
D2.pdf.sdf
(M2)
D3.pdf
411

Fig. 4

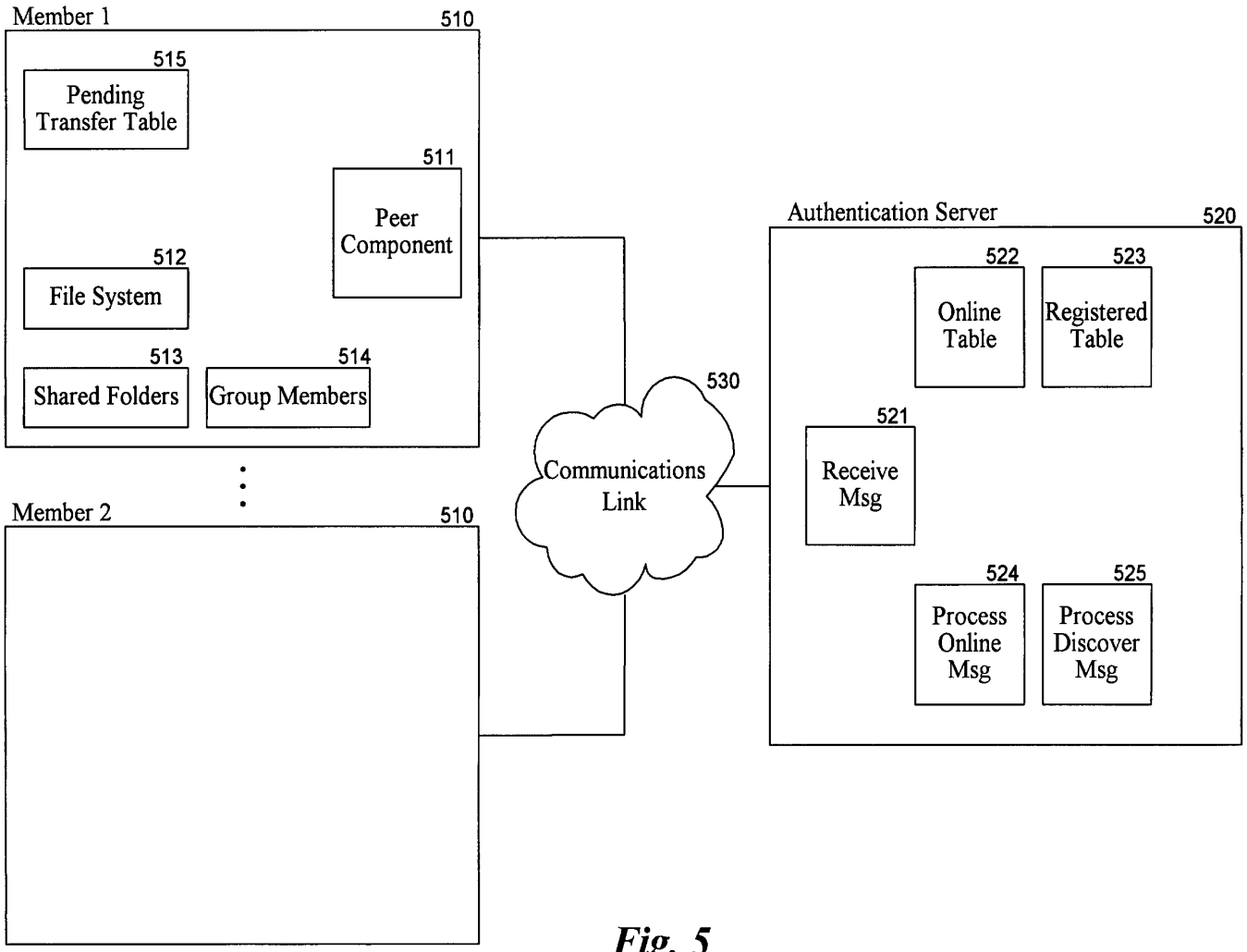
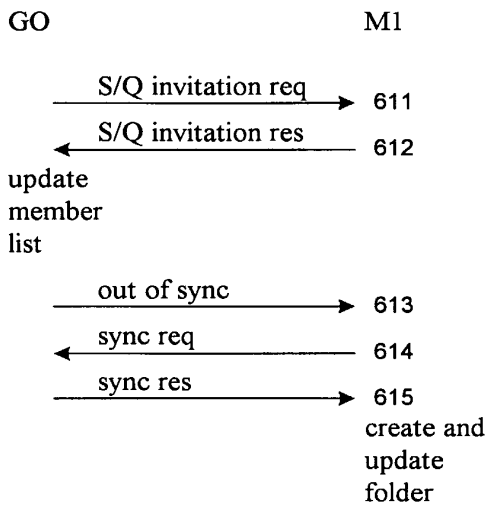

Member 1
510
515
Pending Transfer Table
511
Peer Component
512
File System
513
Shared Folders
514
Group Members
Member 2
510
530
Communications Link
Authentication Server
520
522
Online Table
523
Registered Table
521
Receive Msg
524
Process Online Msg
525
Process Discover Msg

Fig. 5



Invite New Member

Fig. 6A

Dropbox Exhibit 1002 - Page 349
Dropbox, Inc. v. Entangled Media, LLC
IPR2024-00284 - U.S. Patent No. 8,296,338

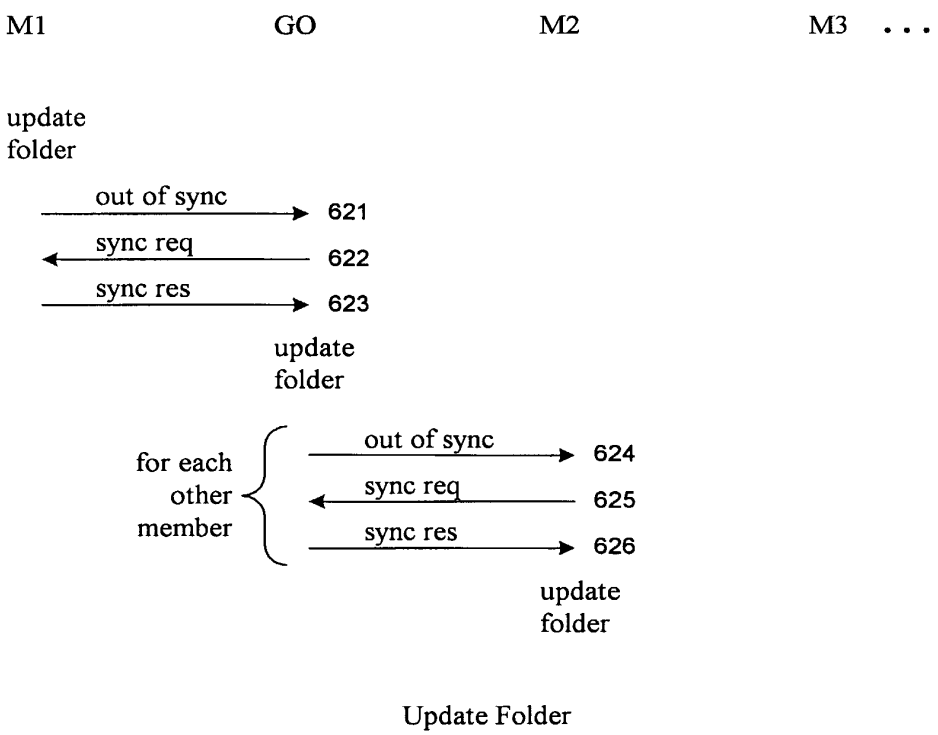
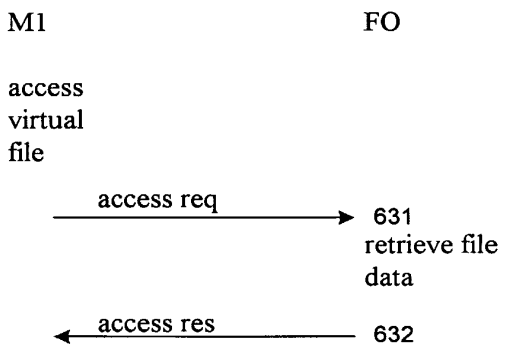

M1
GO
M2
M3 . . .
update folder
out of sync
621
sync req
622
sync res
623
update folder
for each other member
out of sync
624
sync req
625
sync res
626
update folder
Update Folder

Fig. 6B



Access Virtual File

Fig. 6C

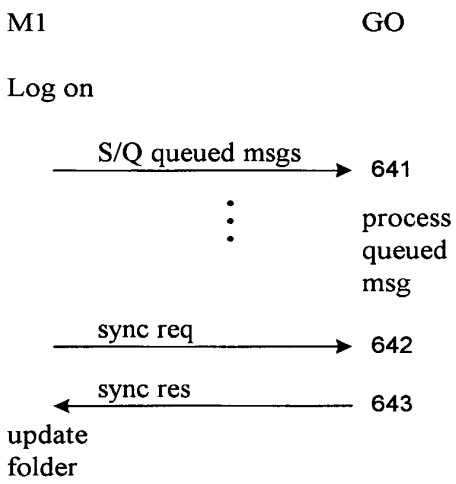

M1
GO
Log on
S/Q queued msgs
641
process
queued
msg
sync req
642
sync res
643
update
folder
Log on

Fig. 6D

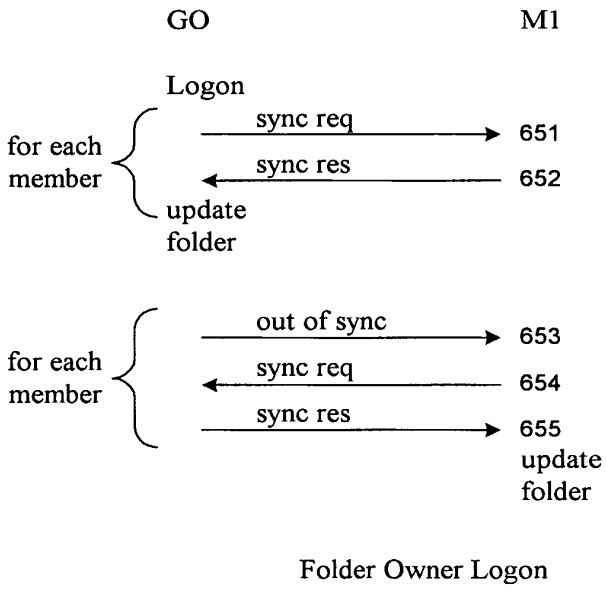

GO
M1
Logon
for each member
sync req
651
sync res
652
update folder
for each member
out of sync
653
sync req
654
sync res
655
update folder
Folder Owner Logon

Fig. 6E

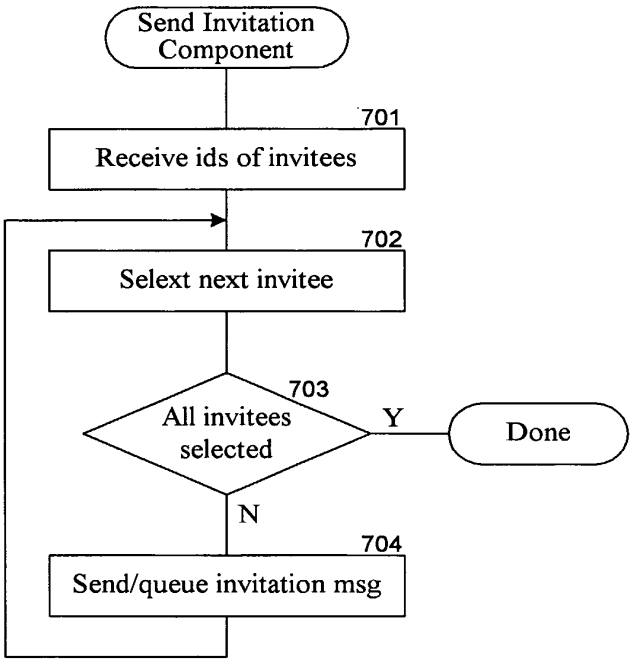

Send Invitation Component
701
Receive ids of invitees
702
Selext next invitee
703
All invitees selected
Y
Done
N
704
Send/queue invitation msg

Fig. 7

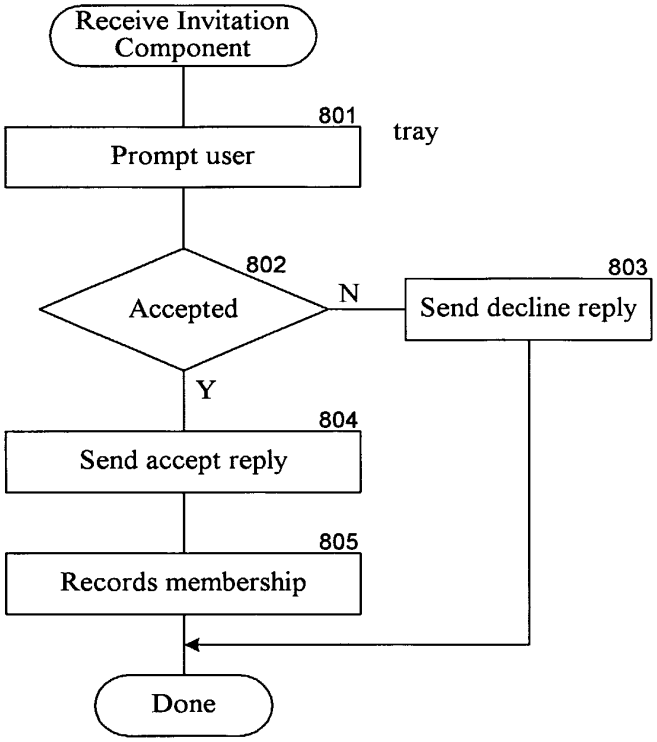

Receive Invitation Component
801
Prompt user
tray
802
Accepted
N
803
Send decline reply
Y
804
Send accept reply
805
Records membership
Done

Fig. 8

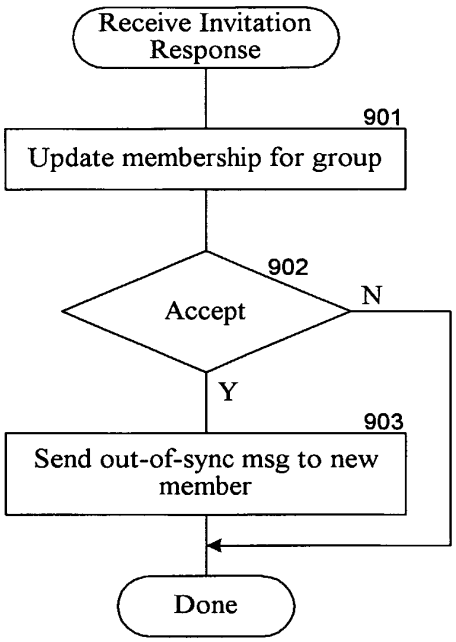

Receive Invitation Response
901
Update membership for group
902
Accept
N
Y
903
Send out-of-sync msg to new member
Done

Fig. 9

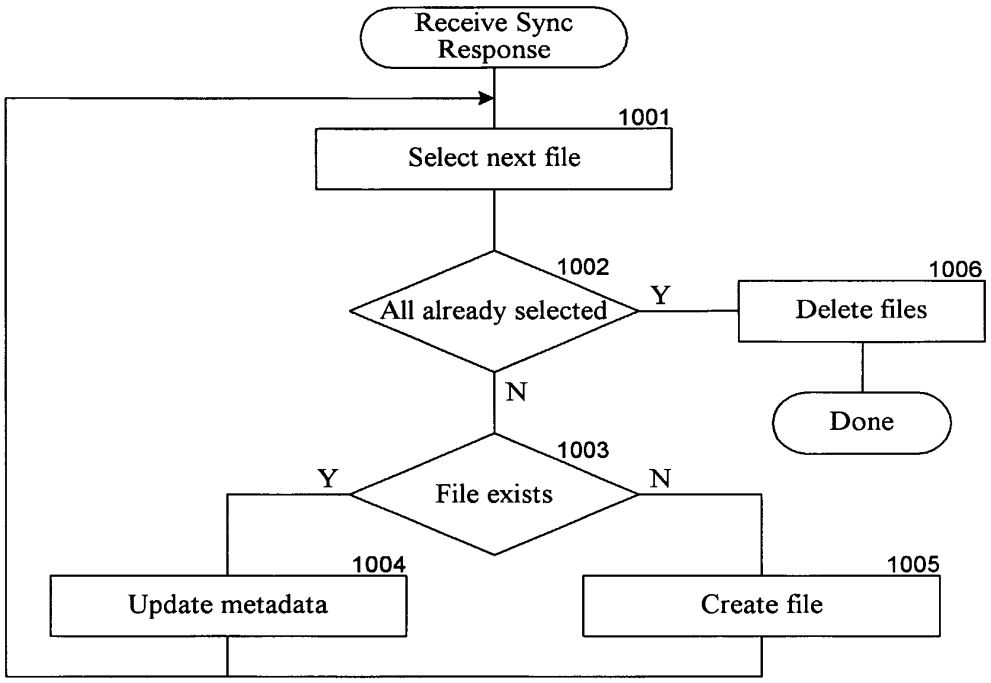

Receive Sync Response
1001
Select next file
1002
All already selected
Y
1006
Delete files
Done
N
1003
File exists
Y
N
1004
Update metadata
1005
Create file

Fig. 10

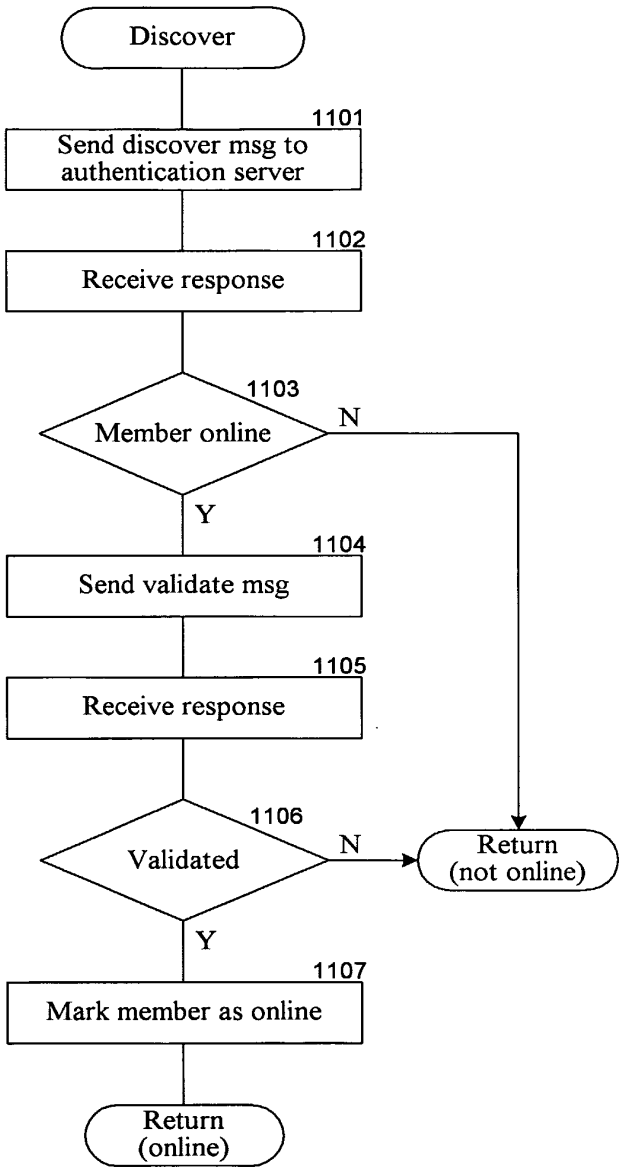

Discover
1101
Send discover msg to authentication server
1102
Receive response
1103
Member online
N
Y
1104
Send validate msg
1105
Receive response
1106
Validated
N
Return (not online)
Y
1107
Mark member as online
Return (online)

Fig. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/10227

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/30
US CL : 707/200-204, 1, 3

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)
U.S. : 707/200-204, 1, 3

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,881,229 A (SINGH et al) 09 March 1999 (09.03.1999), column 5, lines 30-67.	1-40
Y	US 6,256,636 B1 (CHOY) 03 July 2001 (03.07.2001), column 5, lines 1-35.	1-40

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
01 August 2003 (01.08.2003)	26 AUG 2003
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Cam-Y Truong for James R. Matthews Telephone No. (703) 605-1169

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

1. PATENT ABSTRACTS OF JAPAN

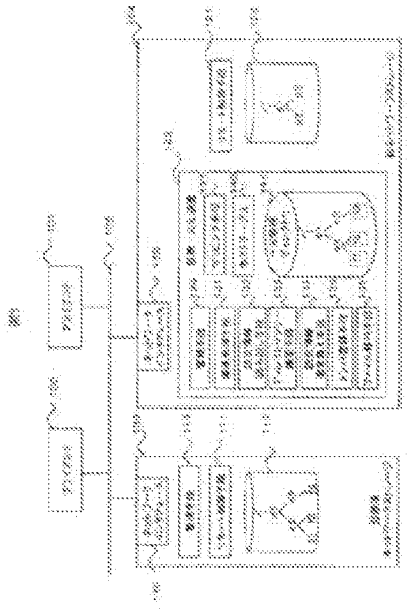
(11)Publication number : **2004-046661**
(43)Date of publication of application : **12.02.2004**

(51)Int.Cl. G06F 12/00
G06F 3/06

(21)Application number : **2002-205002**
(22)Date of filing : **15.07.2002**

(71)Applicant : **HITACHI LTD**
(72)Inventor : **YASUDA YOSHIKO**
HIGUCHI TATSUO
KAWAMOTO SHINICHI
EBATA ATSUSHI
OKITSU JUN

(54) **METHOD AND DEVICE FOR VIRTUAL UNIFICATION OF PLURALITY OF NETWORK STORAGES**



(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method for virtual unification capable of easily increasing the capacity of an installed network storage by adding a new network storage even if the installed network storage does not have the function of virtual unification.
SOLUTION: A virtual unification device on the new network storage is provided with a means for reading information on the settings of the installed network storage according to a manager's request to add storage; a means for registering the installed network storage as a member of the virtual unification device; a means for copying the directory tree structure of the installed network storage; and a means for replacing information on the settings of the installed network storage with information on the settings of the new network storage.

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems
First Named Inventor/Applicant Name:	Erik Caso
Filer:	Dawn-Marie Bey./Jeanne Paolella-Bald
Attorney Docket Number:	ENT0001-US

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	82	82
Utility Search Fee	2111	1	270	270
Utility Examination Fee	2311	1	110	110
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
	Total in USD ($)			**462**

Electronic Acknowledgement Receipt

EFS ID:	7555795
Application Number:	12774231
International Application Number:	
Confirmation Number:	7527
Title of Invention:	Method For a Cloud-Based Meta-File System to Virtually Unify Remote and Local Files Across a Range of Devices' Local File Systems
First Named Inventor/Applicant Name:	Erik Caso
Customer Number:	74877
Filer:	Dawn-Marie Bey./Jeanne Paolella-Bald
Filer Authorized By:	Dawn-Marie Bey.
Attorney Docket Number:	ENT0001-US
Receipt Date:	05-MAY-2010
Filing Date:	
Time Stamp:	14:45:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$462
RAM confirmation Number	957
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	Transmittal of New Application	ent0001_utiltrans.pdf	62944 374aa0eeef76cb45fa9204e1c93557c962b954b6	no	1
Warnings:					
Information:					
2	Specification	ent0001_spec.pdf	140053 bd4e12ea12b92897a008a31e870c2da41fabd9d8	no	20
Warnings:					
Information:					
3	Drawings-only black and white line drawings	ent0001_figs.pdf	325633 f11d6821e62e57de1894006f139761ff7ed158c7	no	6
Warnings:					
Information:					
4	Oath or Declaration filed	ent0001_dec.pdf	2177813 a364e93035f4de676c28edf33edbb2b8c869406e	no	3
Warnings:					
Information:					
5	Transmittal Letter	ent0001_idstrans.pdf	101666 587a2d6af5e64ffd2b0f9e0b4c0cce102de65efc	no	2
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Filed (SB/08)	ent0001_1449frm.pdf	100371 cfe51df3db2c866cddf4aa108770d994a778f5cf	no	2
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
7	Foreign Reference	ent0001_ref1.pdf	850153 60406d3645d19b3468cf67d451ce60cf59bed696	no	29
Warnings:					
Information:					
8	Foreign Reference	ent0001_ref2.pdf	3897510 eb3a621c295f83df8c90956d987ae8e2a2a95fc5	no	77
Warnings:					
Information:					
9	Foreign Reference	ent0001_ref3.pdf	1596354 81834151776ce7d230f71f2b27902e780cbb1c3d	no	36

Warnings:					
Information:					
10	Foreign Reference	ent0001_ref4.pdf	1813835 48ac8649a0587ece47623c685fbc9fdc8d9c94c0	no	46
Warnings:					
Information:					
11	Foreign Reference	ent0001_ref5.pdf	1154846 061b61c773e35c758cbaf1b561bcfa6371dcf25e	no	37
Warnings:					
Information:					
12	Foreign Reference	ent0001_ref6.pdf	102572 7c0c7667ac7f0f6bd8e072470dd1430464327d7b	no	1
Warnings:					
Information:					
13	Fee Worksheet (PTO-875)	fee-info.pdf	33089 0275e8f413e6df3de4752f018c9b42fd527e30dc	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	12356839	

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.

DocCode - SCORE

SCORE Placeholder Sheet for IFW Content

Application Number: 12774231 Document Date: 5/5/2010

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://es/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: February 8, 2006

PTO/SB/06 (12-04)

Approved for use through 7/31/2006. OMB 0651-0032

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 displays a valid OMB control number.

Date: 05/05/10

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 12/774,231

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	82		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	270		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	110		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	15 minus 20 =		X$26=		OR	X$52	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	X$110=			X$220=	
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			N/A			N/A	
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	462		TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A		OR	N/A	
						TOTAL ADD'T FEE		OR	TOTAL ADD'T FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					N/A		OR	N/A	
						TOTAL ADD'T FEE		OR	TOTAL ADD'T FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** 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.